

**National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme**



Validation Report

for the

**Cisco Aggregation Services Router 9000 (ASR9K) running
IOS-XR 7.11**

Report Number: CCEVS-VR-VID11484-2025

Dated: January 23, 2025

Version: 1.2

**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 Meade, MD 20755-6982**

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers

Meredith Martinez

The Aerospace Corporation

Common Criteria Testing Laboratory

Greg McLearn

Brandon Solberg

Kevin Steiner

Lightship Security, USA

Table of Contents

1.	Executive Summary	1
2.	Identification	2
3.	Architectural Information	4
3.1.	TOE Evaluated Configuration	4
3.2.	Physical Boundary	6
3.3.	Supported non-TOE Hardware/ Software/ Firmware.....	9
4.	Security Policy	9
4.1.1.	Security Audit	9
4.1.2.	Cryptographic Support.....	10
4.1.3.	Identification and authentication.....	12
4.1.4.	Security Management	12
4.1.5.	Protection of the TSF	13
4.1.6.	TOE Access	13
4.1.7.	Trusted path/Channels	13
5.	Assumptions.....	13
6.	Clarification of Scope	13
7.	Documentation	15
8.	IT Product Testing	16
8.1.	Developer Testing.....	16
8.2.	Evaluation Team Independent Testing	16
8.3.	Evaluated Configuration.....	16
9.	Results of the Evaluation	19
9.1.	Evaluation of Security Target (ASE).....	19
9.2.	Evaluation of Development Documentation (ADV)	19
9.3.	Evaluation of Guidance Documents (AGD).....	19
9.4.	Evaluation of Life Cycle Support Activities (ALC).....	20
9.5.	Evaluation of Test Documentation and the Test Activity (ATE).....	20
9.6.	Vulnerability Assessment Activity (VAN).....	20
9.7.	Summary of Evaluation Results	21
10.	Validator Comments	22
11.	Annexes.....	23

12. Security Target.....	24
13. Glossary	25
14. Acronym List	26
15. Bibliography	27

List of Tables

Table 1: Evaluation Identifiers.....	2
Table 2: Devices in the Testing Environment.....	16
Table 3: Tools Used for Testing	Error! Bookmark not defined.

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 solution provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in January 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). 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 and PP-Module for MACsec Ethernet Encryption, Version 1.0.

The TOE is the Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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). 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 (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, 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.

The technical information included in this report was obtained from the *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Security Target, Version 1.1, January 17, 2025* and analysis performed by the Validation Team.

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) using the Common Evaluation Methodology (CEM) 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. Developers of information technology 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 Validated Products 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 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
Evaluated Product	Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11
Sponsor and Developer	Cisco Systems, Inc.
CCTL	Lightship Security USA 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e PP-Module for MACsec Ethernet Encryption, Version 1.0, 2023-03-02
ST	Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Security Target, Version 1.1, January 17, 2025
Evaluation Technical Report	Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Evaluation Technical Report, v1.3, January 20, 2025
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Lightship USA: Greg McLearn, Brandon Solberg, Kevin Steiner
CCEVS Validators	The Aerospace Corporation: Jerome Myers, Meredith Martinez

3. Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Cisco Aggregation Services Router 9000 (ASR9K) is a purpose-built, routing platform that also supports MACsec encryption.

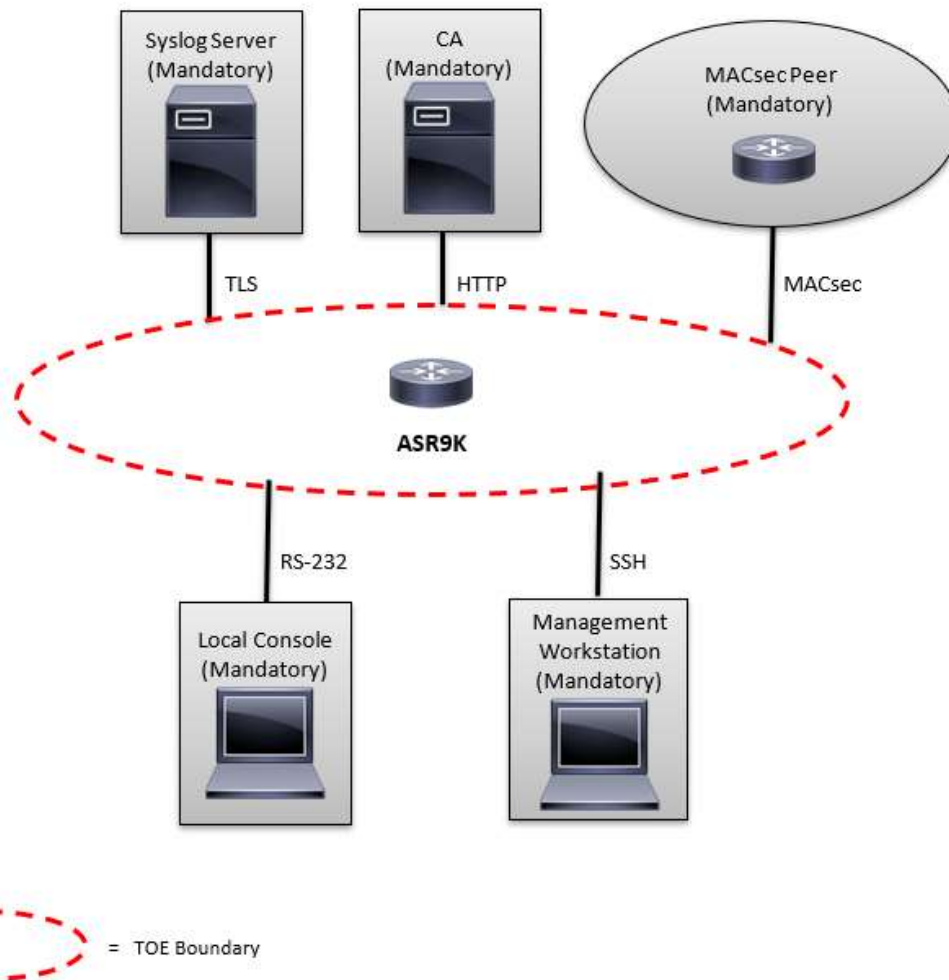
3.1. TOE Evaluated Configuration

The TOE consists of one or more physical devices as specified in section 1.7 of the *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Security Target* along with MACsec-supporting hardware A99-4HG-FLEX, A9K-4HG-FLEX, A9K-8HG-FLEX, A9K-20HG-FLEX, A99-10X400GE-X, A99-4T, ASR9902, ASR9903, A9903-8HG-PEC, A9903-20HG-PEC, non-MACsec line cards A99-32X100GE-X (Non-MACsec), A99-32HG (Non-MACsec), and includes the Cisco IOS-XR software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XR configuration determines how packets are handled to and from the TOE's network interfaces. The router configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination.

An external syslog server must be used to store audit records. The TOE authenticates those devices with X.509v3 certificates and protects communication channels with the TLS protocol. Secure remote administration is protected with SSH which is implemented with authentication failure handling.

For remote administration, a secure session using SSHv2 must be established.

The following figure provides a visual depiction of an example TOE deployment:



The previous figure includes the following:

- Examples of TOE Models
- The following are considered to be in the IT Environment:
 - MACsec Peer
 - Management Workstation
 - Audit (Syslog) Server
 - Local Console
 - Certificate Authority

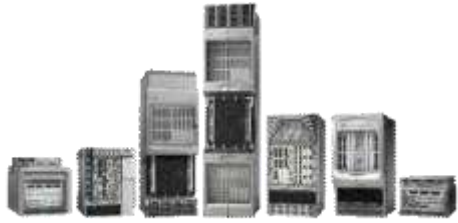
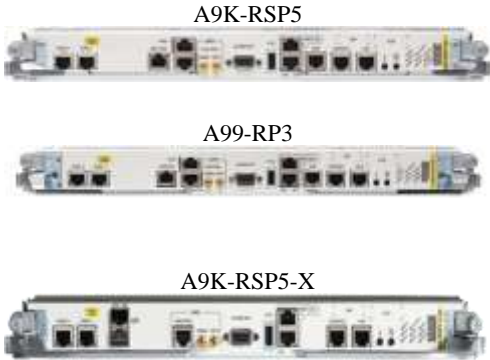
NOTE: While the previous figure includes several non-TOE IT environment devices, the TOE is only the ASR9K device. Only one TOE device is required for deployment in an evaluated configuration.



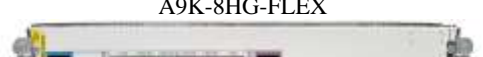



3.2. Physical Boundary






The TOE is a hardware and software solution that makes up the router models as follows:

- Chassis: ASR-9006-SYS, ASR-9010-SYS, ASR-9902, ASR-9903, ASR-9904, ASR-9906, ASR-9910, ASR-9912, ASR-9922
- Route Processors: A99-RP3, A9K-RSP5, A99-RP3-X, A9K-RSP5-X, A99-RP-F
- Line Cards: A99-4HG-FLEX, A9K-4HG-FLEX, A9K-8HG-FLEX, A9K-20HG-FLEX, A99-10X400GE-X, A99-4T, A9903-8HG-PEC, A9903-20HG-PEC, A99-32X100GE-X (Non-MACsec), A99-32HG (Non-MACsec)

The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XR software image Release 7.11. In addition, the software image is also downloadable from the Cisco web site. A login id and password is required to download the software image. The TOE guidance documentation, Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Common Criteria Operational User Guidance, that is considered to be part of the TOE is also available for download in PDF format. The TOE is comprised of the following physical specifications as described in the below:

Hardware	Picture	Specifications
Modular Chassis		<p>Physical dimensions (H x W x D in.)</p> <ul style="list-style-type: none"> • 9006: 17.50 x 17.38 x 29.05 - 10 RU • 9010: 36.75 x 17.38 x 28.24 - 21 RU • 9904: 10.38 x 17.57 x 25.02 - 6RU • 9906: 24.39 x 17.60 x 31.45 - 14RU • 9910: 36.69 x 17.60 x 30.41 - 21RU • 9912: 52.5 x 17.60 x 29.25 - 30RU • 9922: 77 x 17.60 x 30.1 - 44RU
Route Processors		<p>RSP5</p> <ul style="list-style-type: none"> • CPU - Intel Xeon Silver 4109T (Skylake) • 16, 24 or 40 GB DRAM • 1 RS-232 console • 2 GE management ports • 1 auxiliary port • 1 USB 2.0 port <p>RP3</p> <ul style="list-style-type: none"> • CPU - Intel Xeon Silver 4109T (Skylake) • 16, 24 or 40 GB DRAM

Hardware	Picture	Specifications
	<p style="text-align: center;">A99-RP3-X</p> 	<ul style="list-style-type: none"> • 1 RS-232 console • 2 GE management ports • 1 auxiliary port • 1 USB 2.0 port <p>RSP5-X</p> <ul style="list-style-type: none"> • CPU - Intel Xeon D-1573N (Broadwell) • 24 or 48 GB DRAM • 1 RS-232 console • 2 GE management ports • 1 auxiliary port • 1 USB 2.0 port <p>RP3-X</p> <ul style="list-style-type: none"> • CPU - Intel Xeon D-1573N (Broadwell) • 24 or 48 GB DRAM • 1 RS-232 console • 2 GE management ports • 1 auxiliary port • 1 USB 2.0 port
Line Cards	<p style="text-align: center;">A9K-4HG-FLEX, A99-4HG-FLEX</p>  <p style="text-align: center;">A9K-8HG-FLEX</p>  <p style="text-align: center;">A9K-20HG-FLEX</p>  <p style="text-align: center;">A99-10X400GE-X , A99-4T</p>  <p style="text-align: center;">A99-32X100GE-X, A99-32HG</p> 	<p>A9K-4HG-FLEX, A99-4HG-FLEX</p> <ul style="list-style-type: none"> • MACsec MPU - Microchip META-DX1 PM6110 • 4x40/100GE QSFP ports • 16x10/15GE SFP ports • 24x10GE SFP+ ports <p>A9K-8HG-FLEX</p> <ul style="list-style-type: none"> • MACsec MPU - Microchip META-DX1 PM6110 • 6x10/40/100GE QSFP ports • 2x10/40/100/200/400GB QSFP ports <p>A9K-20HG-FLEX</p> <ul style="list-style-type: none"> • MACsec MPU - Microchip META-DX1 PM6110 • 2x10/40/100GE QSFP ports • 5x10/40/100/200/400GE QSFP ports <p>A99-10X400GE-X , A99-4T</p> <ul style="list-style-type: none"> • MACsec MPU – Microchip META-DX1 PM6110

Hardware	Picture	Specifications
		<ul style="list-style-type: none"> 10x10/25/40/100/400GE QSFP ports <p>A99-32X100GE-X, A99-32HG (Non-MACsec)</p> <ul style="list-style-type: none"> 32x100GE QSFP ports
Standalone Chassis	<p style="text-align: center;">A99-RP-F</p>  <p style="text-align: center;">ASR-9902</p>  <p style="text-align: center;">ASR-9903</p>  <p style="text-align: center;">A9903-8HG-PEC</p>  <p style="text-align: center;">A9903-20HG-PEC</p> 	<p>A99-RP-F - 9902 / 9903 Route Processor</p> <ul style="list-style-type: none"> CPU - Intel Xeon D-1533N (Broadwell) 32GB SDRAM 1 RS-232 console 2 GE management ports 1 auxiliary port 1 USB 2.0 port <p>Dimensions (in.)</p> <ul style="list-style-type: none"> 9902: 3.46 x 17.32 x 19 – 2RU 9903: 5.18 x 17.475 x 30 – 3RU <p>9902 Integrated Interfaces</p> <ul style="list-style-type: none"> MACsec MPU – Microchip META-DX1 PM6108 2x10/40/100GE QSFP ports 6x10/40/100GE QSFP ports 16x25/10GE SFP, 24x10GE SFP+ ports <p>9903 Integrated Interfaces</p> <ul style="list-style-type: none"> MACsec MPU – Microchip META-DX1 PM6110 16x10/40/100GE QSFP ports 20x10GE SFP+ ports <p>A9903-8HG-PEC Line card</p> <ul style="list-style-type: none"> MACsec MPU – Microchip META-DX1 PM6110 32x25GE/10GE SFP+ ports 16x10GE SFP+ ports <p>A9903-20HG-PEC Line card</p> <ul style="list-style-type: none"> MACsec MPU – Microchip META-DX1 PM6108 5x20 400GE/200GE/100GE QSFP ports 15x100GE QSFP ports

Note: All Cisco HW devices are shipped via courier.

3.3. Supported non-TOE Hardware/ Software/ Firmware

The TOE supports the following hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
MACsec Peer	Yes	This includes any MACsec peer with which the TOE participates in MACsec communications. MACsec Peer may be any device that supports MACsec communications.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Also referred to as audit server in the ST
Certificate Authority	Yes	This includes any Operational Environment Certificate Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1.1. Security Audit

The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations and manages audit data storage. The TOE provides the administrator with a circular audit trail. The TOE is configured to transmit its audit messages to an external syslog server over an encrypted channel using TLS.

4.1.2. Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates (Operational Environment – Intel Xeon D-1533N (Broadwell Intel Xeon D-1573N (Broadwell), Intel Xeon Silver 4109T (Skylake). In addition, the TOE supports MACsec using the Microchip META-DX1 PM6110 processor (see the Table below for certificate references).

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
AES	Used for symmetric encryption/decryption	CBC (128 and 256)	FOM 7.3a	A4446	FCS_COP.1/DataEncryption
		GCM (128 and 256)	FOM 7.3a	A4446	FCS_COP.1/DataEncryption
		CMAC (128 and 256)	FOM 7.3a	A4446	FCS_COP.1/CMAC
		AES Key Wrap (128 and 256)	FOM 7.3a	A4446	FCS_COP.1/MACSEC
		GCM (128 and 256)	MACsec	A1104	FCS_COP.1/MACSEC
SHS (SHA1, SHA-256, SHA-384, SHA-512)	Cryptographic hashing services	Byte Oriented	FOM 7.3a	A4446	FCS_COP.1/Hash
HMAC (SHA1, SHA-256, SHA-384, SHA-512)	Keyed hashing services and software integrity test	Byte Oriented	FOM 7.3a	A4446	FCS_COP.1/KeyedHash
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	HMAC_DRBG	FOM 7.3a	A4446	FCS_RBG_EXT.1
RSA	Signature Verification and Key Transport	PKCS#1 v.1.5, 2048 and 3072 bit key	FOM 7.3a	A4446	FCS_COP.1/SigGen
	Key Generation	FIPS 186-4 Key Gen	FOM 7.3a	A4446	FCS_CKM.1
ECDSA	Key Generation	FIPS 186-4 Key Gen	FOM 7.3a	A4446	FCS_CKM.1

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
KAS-ECC	Key Agreement	NIST Special Publication 800-56A	FOM 7.3a	A4446	FCS_CKM.2

The TOE provides cryptography in support of remote administrative management via SSHv2 and secures the session between the ASR9K and remote syslog server using TLS.

The TOE authenticates and encrypts packets between itself and a MACsec peer. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys to protect data exchanged by the peers.

The cryptographic services provided by the TOE are described in the table below:

Cryptographic Method	Use within the TOE
Secure Shell Establishment	Used to establish initial SSH session.
RSA Signature Services	Used in SSH session establishment. Used in TLS session establishment. X.509 certificate signing.
SHS	Used to provide SSH traffic integrity verification Used for keyed-hash message authentication
AES	Used to encrypt SSH session traffic. Used to encrypt TLS session traffic. Used to encrypt MACsec traffic.
HMAC	Used for keyed hash, integrity services in SSH session establishment.
TLS	Used to secure traffic to the syslog server.
AES-CMAC	Used to encrypt MACsec keys.

Cryptographic Method	Use within the TOE
ISO/IEC 18031:2011 HMAC_DRBG	Used for random number generation, key generation and seeds to asymmetric key generation Used in TLS session establishment Used in SSH session establishment Used in MACsec session establishment

4.1.3. Identification and authentication

The TOE provides authentication services for administrative users wishing to connect to the TOEs secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules.

After a configurable number of incorrect login attempts, ASR9K will lockout the account until a configured amount of time for lockout expires.

The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys.

The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections.

4.1.4. Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection. The TOE provides the ability to securely manage all TOE administrative users, all identification and authentication, all audit functionality of the TOE, all TOE cryptographic functionality, the timestamps maintained by the TOE, and updates to the TOE. The TOE supports a privileged administrator role. Only the privileged administrator can perform the above security relevant management functions.

Administrators can create configurable login banners to be displayed at time of login and can also define an inactivity timeout for each admin interface to terminate sessions after a set period of inactivity.

4.1.5. Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally, Cisco IOS-XR is not a general-purpose operating system and access to Cisco IOS-XR memory space is restricted to only Cisco IOS-XR functions.

The TOE is also able to detect replay of information received via secure channels (MACsec). The detection applied to network packets that terminate at the TOE, such as trusted communications between the TOE and an IT entity (e.g., MACsec peer). If replay is detected, the packets are discarded.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually. Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

4.1.6. TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. 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 Security Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

4.1.7. Trusted path/Channels

The TOE establishes a trusted path between the appliance and the CLI using SSHv2 and the syslog server using TLS. MACsec is used to secure communication channels between MACsec peers at Layer 2.

5. Assumptions

The Security Problem Definition, including the assumptions, can be found in the following documents:

- *collaborative Protection Profile for Network Devices, Version 2.2e*
- *PP-Module for MACsec Ethernet Encryption, Version 1.0*

That information has not been reproduced here and CPP_ND_V2.2E and MOD_MACSEC_V1.0 should be consulted if there is interest in that material.

6. Clarification of Scope

The scope of this evaluation was limited to the security functional requirements and assurances covered in CPP_ND_V2.2E and MOD_MACSEC_V1.0 as described for this

TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices in the operational environment needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

No other versions of the TOE and software, either earlier or later, were evaluated.

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 in accordance with the assurance activities specified in the CPP_ND_V2.2E and MOD_MACSEC_V1.0 and performed by the Evaluation team.
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- Apart from the documentation listed in Section 7, additional customer documentation was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the CPP_ND_V2.2E and MOD_MACSEC_V1.0 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation. In particular, the security functionality listed in Section 1.9 of the ST is explicitly excluded from the scope of this evaluation.

7. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11, Common Criteria Operational User Guidance, 0.4, November 26, 2024*
- *Cisco System Security Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x, 2023-11-30*

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

8. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Detailed Test Report, Version 1.2, December 19, 2024 (DTR)*, which is not publicly available. The *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Assurance Activity Report, v1.3, January 20, 2025*, 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 conducted independent testing at Lightship Security USA lab in Baltimore, MD from May 2024 through December 2024. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

8.3. Evaluated Configuration

The evaluated configuration is the Cisco Aggregation Services Router 9000 (ASR9K) network device running IOS-XR 7.11.

The TOE testing environment components are identified in the following tables. Other details regarding the test environment, test tools, and configuration, including a diagram, is found in Section 2 of the AAR.

Table 2: Devices in the Testing Environment

Name / HW / SW	Description / Functions	Test Tools
RSP5 HW: A9K-RSP5-SE and A9K-4HG-FLEX- SE SW: IOS-XR 7.11.1	Fully tested TOE route processor and MACsec-capable linecard. TLS SSH MACsec	N/A
RSP5-X	Fully tested TOE route processor and MACsec-capable linecard.	N/A

Name / HW / SW	Description / Functions	Test Tools
HW: A9K-RSP5-X-TR and A9K-4HG-FLEX-SE SW: IOS-XR 7.11.1	TLS SSH MACsec	
Services VM HW: Test Hypervisor SW: Debian 10	Logging Server (TLS) DNS Server CRL server (part of the role of "Certificate Authority") TFTP server (during system rescue) Packet captures	Logging: syslog-ng 3.19.1 DNS: dnsmasq 2.80 CRL server: python 3.7.3 http module Packet captures: tcpdump 4.9.3
MACsec Node A HW: MACsec Hypervisor SW: Debian 12 with Linux kernel 6.1	MACsec Manual packet construction using Python3 and Scapy Packet captures Ethernet packet flooding	Custom MACsec MKPDU controller: v2.10-lightship-1.0 Custom Linux kernel modules for MPDU manipulation for FCS_MACSEC_EXT.1 Test 5 (v1.0), FCS_MACSEC_EXT.2 Test 8 (v1.0), and FCS_MKA_EXT.1 Test 12 (v1.0). Linux tc utility: iproute2-6.1.0, libbbf 1.1.0 Python 3.11.2 Scapy 2.5.0 Packet captures: tcpdump 4.99.3 Ethernet packet flooding: Lightship eth-flood v1.0
MACsec Node B HW: MACsec Hypervisor SW: Debian 12 with Linux kernel 6.1	MACsec (third peer only) Packet captures	Custom MACsec MKPDU controller: v2.10-lightship-1.0 Packet captures: tcpdump 4.99.3
Management Workstation HW: Test Hypervisor SW: Kali 2023-2 with kernel 6.1.0-kali9-amd64	SSH client (SSH) SSH server (for copying to/from TOE) Protocol test host (TLS/SSH) X.509 certificate management (part of the role of "Certificate Authority") Packet captures	Lightship Greenlight v3.0.35 with GL tools 3.0.53 including OpenSSL 3.0.1 SSH client: OpenSSH_9.7p1 Debian-5 SSH-server: OpenSSH_9.7p1 Debian-5

Name / HW / SW	Description / Functions	Test Tools
	Entropy analysis	TLS server: OpenSSL 3.2.2-dev Packet capture: tcpdump 4.99.3 NIST 800-90B Entropy Analyzer: GitHub Commit 0a2372810ad535158795177381f61ea4821bf2ce
Test Hypervisor HW: Dell PowerEdge R440 SW: ESXi, 7.0.3	Hypervisor for the Services VM and Management Workstation	None
MACsec Hypervisor HW: Dell PowerEdge R540 SW: ESXi 6.7.0	Hypervisor for the MACsec nodes	BCM57412 10G capable network card
Netgear Switch HW: ProSafe Plus GS105E	Physical disconnect packet captures for FTP_ITC.1.	N/A
Packet Capture Laptop HW: Lenovo ThinkPad T14 SW: Windows 11 Pro	Physical disconnect packet captures for FTP_ITC.1.	Wireshark 3.4.16

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 Evaluation Technical Report (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 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined the Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in CPP_ND_V2.2E and MOD_MACSEC_V1.0.

9.1. Evaluation of Security Target (ASE)

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 Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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 (ADV)

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 and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the CPP_ND_V2.2E and MOD_MACSEC_V1.0 related to the examination of the information contained in the TSS.

The Validation 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.

9.3. Evaluation of Guidance Documents (AGD)

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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

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.

9.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

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 (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the CPP_ND_V2.2E and MOD_MACSEC_V1.0 and recorded the results in a Test Report, summarized in the AAR.

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.

9.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 NDcPP 2.2E Vulnerability Assessment, v1.3, January 17, 2025*, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on January 17, 2025, did not uncover any residual vulnerability.

The Evaluation team searched:

- [Cisco Security Advisories:](https://sec.cloudapps.cisco.com/security/center/publicationListing.x#~FilterByProduct)
<https://sec.cloudapps.cisco.com/security/center/publicationListing.x#~FilterByProduct>
- NIST National Vulnerabilities Database (NVD) (can be used to access CVE and US-CERT databases identified below): <https://web.nvd.nist.gov/view/vuln/search>
- CISA - Known Exploited Vulnerabilities Catalog: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- OpenSSL Vulnerabilities: <https://www.openssl.org/news/vulnerabilities.html>

The Evaluation team performed a search using the following keywords:

- Cisco IOS-XR 7.11.1
- Cisco ASR 9010
- Cisco ASR 9903
- Cisco ASR 9922
- Cisco ASR 9912
- Cisco A99-RP3-TR
- Cisco ASR 9910
- Cisco A99-32X100GE-TR
- Cisco A9K-RSP5-SE
- Cisco A99-32X100GE-GM
- Cisco ASR 9906
- Cisco ASR 9904
- Cisco A99-RP3-SE
- Cisco ASR 9902
- Cisco A9K-RSP5-TR
- Cisco ASR 9006
- ASR9K
- IOS XR 64-bit
- Cisco ASR 9000 Series Aggregation Services Routers
- OpenSSL
- OpenSSH
- Intel Xeon Silver 4109T
- Intel Xeon D-1573N
- Intel Xeon D-1533N
- MACsec

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.

9.7. 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 followed the procedures defined in the CEM and performed the Assurance Activities in the CPP_ND_V2.2E and MOD_MACSEC_V1.0 and correctly verified that the product meets the claims in the ST.

10. Validator Comments

All validator comments have been addressed elsewhere in this Validation Report.

11. Annexes

Not applicable.

12. Security Target

*Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Security Target,
1.1, January 17, 2025.*

13. Glossary

- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

15. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model*, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements*, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements*, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
5. *collaborative Protection Profile for Network Devices, Version 2.2e*, 23-March-2020
6. *Evaluation Activities for Network Device cPP*, December-2019, Version 2.2
7. *PP-Module for MACsec Ethernet Encryption, Version 1.0*, 2023-03-02
8. *Supporting Document Mandatory Technical Document PP-Module for MACsec Ethernet Encryption, Version 1.0*, 2023-03-02
9. *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Security Target*, 1.1, January 17, 2025
10. *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11, Common Criteria Operational User Guidance*, 0.4, November 26, 2024
11. *Cisco System Security Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x*, 2023-11-30
12. *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Assurance Activity Report*, v1.3, January 20, 2025
13. *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 NDcPP 2.2E Vulnerability Assessment*, v1.3, January 17, 2025
14. *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Evaluation Technical Report*, v1.3, January 20, 2025
15. *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Detailed Test Report*, v1.2, December 19, 2024
16. *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Detailed Test Report Evidence*, v1.1, December 19, 2024