

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

**Cisco Systems, Inc., 170 West Tasman Dr., San Jose, CA
95134**

Cisco Catalyst 6500 Series Switches

Report Number: CCEVS-VR-10490-2012
Dated: July 27, 2012
Version: 0.1

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

**National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940**

ACKNOWLEDGEMENTS

Validation Team

James Dondelinger
Aerospace Corporation
Columbia, MD

Kenneth Stutterheim
Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Tammy Compton
Julie Cowan
Gary Grainger
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1	Executive Summary	1
2	Identification	2
3	Architectural Information	3
3.1	TOE Evaluated Configuration	3
3.2	Physical Scope of the TOE	4
3.3	Supported non-TOE Hardware/ Software/ Firmware	4
4	Security Policy	5
4.1	Security Audit	5
4.2	Cryptographic Support.....	5
4.3	Traffic Filtering and Switching (VLAN Processing and ACLs)	5
4.4	Identification and Authentication	6
4.5	Security Management	7
4.6	Protection of the TSF	8
4.7	TOE access.....	9
5	Assumptions.....	9
6	Documentation	9
6.1	Design Documentation.....	9
6.2	Guidance Documentation.....	10
6.3	Life Cycle.....	10
6.4	Testing.....	10
7	IT Product Testing	10
7.1	Developer Testing.....	11
7.2	Evaluation Team Independent Testing	11
8	Evaluated Configuration	11
9	Results of the Evaluation	11
9.1	Evaluation of the Security Target (ASE)	12
9.2	Evaluation of the Development (ADV)	12
9.3	Evaluation of the Guidance Documents (AGD)	12
9.4	Evaluation of the Life Cycle Support Activities (ALC)	13
9.5	Evaluation of the Test Documentation and the Test Activity (ATE)	13
9.6	Vulnerability Assessment Activity (VAN).....	13
9.7	Summary of Evaluation Results.....	14
10	Validator Comments/Recommendations	14
11	Annexes.....	14
12	Security Target.....	14
13	Glossary	15
14	Bibliography	15

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Catalyst 6500 Series Switches solution provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in August 2012. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 2 augmented with ALC_FLR.2 and ALC_DVS.1.

The TOE is the Cisco Catalyst 6500 Series Switches running IOS 15.0(1)SY1. The TOE is a purpose-built, switching and routing platform with OSI Layer2 and Layer3 traffic filtering capabilities.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 3) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 3). This Validation Report 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 evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, 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 of 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 evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 2 augmented with ALC_FLR.2 and ALC_DVS.1) have been met.

The technical information included in this report was obtained from the Cisco Catalyst 6500 Series Switches Security Target and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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) for Evaluation Assurance Level (EAL) 1 through 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. 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 Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (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
TOE:	Cisco Catalyst 6500 Series Switches 6506-E, 6509-E, and 6513-E with Supervisor Engine 2T (VS-S2T-10G or VS-S2T-10G-XL) running IOS 15.0(1)SY1 (Specific models identified in the Validated Products List Entry)
Protection Profile	None
ST:	Cisco Catalyst 6500 Series Switches Security Target, Version 1.0, July 26, 2012
Evaluation Technical Report	Evaluation Technical Report For Cisco Catalyst 6500 Series Switches (Proprietary), Version 2.0, July 27, 2012
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 3
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD

Item	Identifier
CCEVS Validators	Kenneth Stutterheim, Aerospace Corporation, Columbia, MD James Donndelinger, Aerospace Corporation, Columbia, MD

3 Architectural Information

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

Cisco IOS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself.

3.1 TOE Evaluated Configuration

The TOE consists of any one of a number of hardware configurations, each running the same version of IOS software. The 6500 chassis provides power, cooling, and backplane for the Supervisor Engine, line cards, and service modules. The Supervisor Engines run the IOS software. The evaluated configurations consist of the following:

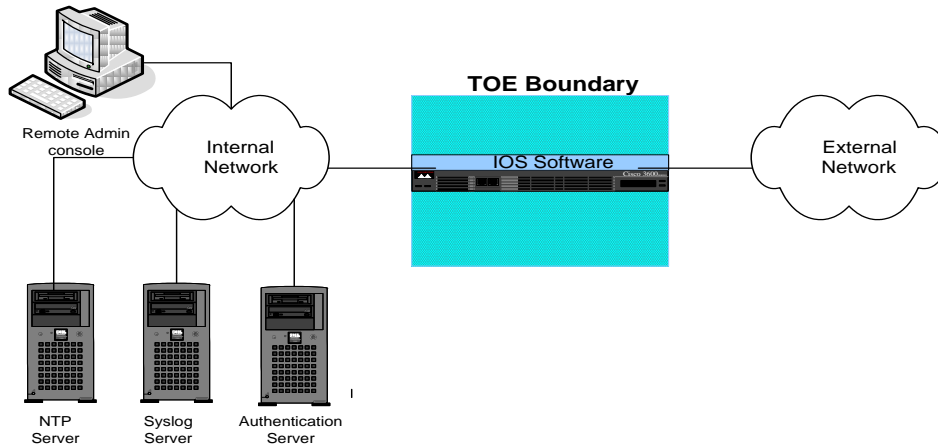
- One or two Supervisor 2T Cards (VS-S2T-10G or VS-S2T-10G-XL) per chassis (Two Sup cards in one chassis provide Supervisor failover within the chassis.)
- Each Sup2T running IOS 15.0(1)SY1 (FIPS validated)
- Sup2T cards installed into one or more 6506-E, 6509-E, or 6513-E Switch Chassis (Two chassis can be configured together to support HA with VSS.)
- With one or more WS-X6908-10G or WS-X6908-10G-2TXL Line Cards

The TOE can optionally connect to an NTP server on its internal network for time services. If an NTP server is used, it must only be accessible via the internal network (an internal network isolated from user traffic and intended for use by TOE administrators only).

In addition, if the TOE is to be remotely administered, then the management station must be connected to an internal network, SSHv2 must be used to connect to the switch. A syslog server can also be used to store audit records. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.

The TOE can optionally support any other line card or service module that is compatible with the supervisors and chassis models included in the TOE. These line cards and SMs are not security-relevant to the CC-evaluated security functional requirements.

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



3.2 Physical Scope of the TOE

The TOE is a hardware and software solution that uses a combination of chassis, supervisor engine, and line cards: the Cisco Catalyst 6500 Series Switches 6506-E, 6509-E, and 6513-E with Supervisor Engine 2T (VS-S2T-10G or VS-S2T-10G-XL), with Cisco IOS 15.0(1)SY1 running on the Supervisor Engine.

3.3 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment:

IT Environment Components

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.
NTP Server	No	The TOE supports communications with an NTP server to receive clock updates.
Syslog server	No	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE.
Authentication Server	No	The authentication server (RADIUS and TACACS+) is used to provide centralized authentication and related auditing for one or more distributed instances of the TOE.

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. User data protection
4. Identification and authentication
5. Secure Management
6. Protection of the TSF
7. TOE access

4.1 Security Audit

The TOE generates audit messages that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include: modifications to the group of users that are part of the authorized administrator roles (assigned the appropriate privilege level), all use of the user identification mechanism; any use of the authentication mechanism; any change in the configuration of the TOE; any matching of packets to access control entries in ACLs when traversing the TOE; and any failure of a packet to match an access control list (ACL) rule allowing traversal of the TOE. The TOE will write audit records to the local logging buffer by default and can be configured to send audit data via syslog to a remote audit server, or display to the local console. The TOE does not have an interface to modify audit records, though there is an interface available for the authorized administrator to delete audit data stored locally on the TOE.

4.2 Cryptographic Support

The TOE provides cryptography support for secure communications and protection of information when operated in FIPS mode. The crypto module is FIPS 140-2 SL2 validated (certificate number 1717). The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; digital signature using RSA; cryptographic hashing using SHA1; and keyed-hash message authentication using HMAC-SHA1. The TOE also implements SSHv2 for secure remote administration. In the evaluated configuration, the TOE must be operated in FIPS mode of operation per the FIPS Security Policy (certificate 1717).

4.3 Traffic Filtering and Switching (VLAN Processing and ACLs)

VLANs control whether Ethernet frames are passed through the switch interfaces based on the VLAN tag information in the frame header. IP ACLs or ICMP ACLs control whether routed IP packets are forwarded or blocked at Layer 3 TOE interfaces (interfaces that have been configured with IP addresses). VACLs (using access

mapping) control whether non-routed frames (by inspection of MAC addresses in the frame header) and packets (by inspection of IP addresses in the packet header) are forwarded or blocked at Layer 2 ports assigned to VLANs. The TOE examines each frame and packet to determine whether to forward or drop it, on the basis of criteria specified within the VLANs access lists and access maps applied to the interfaces through which the traffic would enter and leave the TOE. For those interfaces configured with Layer-3 addressing the ACLs can be configured to filter IP traffic using: the source address of the traffic; the destination address of the traffic; and the upper-layer protocol identifier. Layer-2 interfaces can be made part of Private VLANs (PVLANS), to allow traffic to pass in a pre-defined manner among a primary, and secondary ('isolated' or 'community') VLANs within the same PVLAN.

VACL access mapping is used to match IP ACLs or MAC ACLs to the action to be taken by the TOE as the traffic crosses the interface, causing the packet to be forwarded or dropped. The traffic is matched only against access lists of the same protocol type; IP packets can be matched against IP access lists, and any Ethernet frame can be matched against MAC access lists. Both IP and MAC addresses can be specified within the VLAN access map.

Use of Access Control Lists (ACLs) also allows restriction of remote administration connectivity to specific interfaces of the TOE so that sessions will only be accepted from approved management station addresses identified as specified by the administrator.

The TOE supports routing protocols including BGPv4, EIGRP, EIGRPv6 for IPv6, RIPv2, and OSPFv2 to maintain routing tables, or routing tables can be configured and maintained manually. Since routing tables are used to determine which egress ACL is applied, the authority to modify the routing tables is restricted to authenticated administrators, and authenticated neighbor routers. The only aspects of routing protocols that are security relevant in this TOE is the TOE's ability to authenticate neighbor routers using shared passwords. Other security features and configuration options of routing protocols are beyond the scope of this Security Target and described in administrative guidance.

The TOE supports VACLs (VLAN ACLs), which can filter traffic traversing VLANs on the TOE based on IP addressing and MAC addressing.

The TOE also ensures that packets transmitted from the TOE do not contain residual information from previous packets. Packets that are not the required length use zeros for padding so that residual data from previous traffic is never transmitted from the TOE.

4.4 Identification and Authentication

The TOE performs authentication, using Cisco IOS platform authentication mechanisms, to authenticate access to user EXEC and privileged EXEC command

modes. All users wanting to use TOE services are identified and authenticated prior to being allowed access to any of the services. Once a user attempts to access the management functionality of the TOE (via EXEC mode), the TOE prompts the user for a user name and password. Only after the administrative user presents the correct identification and authentication credentials will access to the TOE functionality be granted.

The TOE supports use of a remote AAA server (RADIUS and TACACS+) as the enforcement point for identifying and authenticating users, including login and password dialog, challenge and response, and messaging support. Encryption of the packet body is provided through the use of RADIUS (note RADIUS only encrypts the password within the packet body, while TACACS+ encrypts the entire packet body except the header).

The TOE can be configured to display an advisory banner when administrators log in and also to terminate administrator sessions after a configured period of inactivity.

The TOE also supports authentication of other routers using router authentication supported by BGPv4, EIGRP, EIGRPv6 for IPv6, RIPv2, and OSPFv2. Each of these protocols supports authentication by transmission of MD5-hashed password strings, which each neighbor router uses to authenticate others. It is noted that per the FIPS Security Policy, that MD5 is not a validated algorithm during FIPS mode of operation. For additional security, it is recommended router protocol traffic also be isolated to separate VLANs.

4.5 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 through either a secure session via SSHv2, a terminal server directly connected to the Catalysis Switch (RJ45), or a local console connection (serial port). The TOE provides the ability to perform the following actions:

- allows authorized administrators to add new administrators,
- start-up and shutdown the device,
- create, modify, or delete configuration items,
- create, modify, or delete information flow policies,
- create, modify, or delete routing tables,
- modify and set session inactivity thresholds,
- modify and set the time and date,
- and create, delete, empty, and review the audit trail

All of these management functions are restricted to the authorized administrator of the TOE.

The TOE switch platform maintains administrative privilege level and non-administrative access. Non-administrative access is granted to authenticated neighbor routers for the ability to receive updated routing tables per the information flow rules. There is no other access or functions associated with non-administrative access. The administrative privilege levels include:

- Administrators are assigned to privilege levels 0 and 1. Privilege levels 0 and 1 are defined by default and are customizable. These levels have a very limited scope and access to CLI commands that include basic functions such as login, show running system information, turn on/off privileged commands, logout.
- Semi-privileged administrators equate to any privilege level that has a subset of the privileges assigned to level 15; levels 2-14. These levels are undefined by default and are customizable. The custom level privileges are explained in the example below.
- Privileged administrators are equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15.

The term “authorized administrator” is used to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions.

4.6 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. Additionally Cisco IOS is not a general-purpose operating system and access to Cisco IOS memory space is restricted to only Cisco IOS functions.

The TOE provides secure transmission when TSF data is transmitted between separate parts of the TOE (encrypted sessions for remote administration (via SSHv2)). Use of separate VLANs are used to ensure routing protocol communications between the TOE and neighbor routers including routing table updates and neighbor router authentication will be logically isolated from traffic on other VLANs.

The TOE is also able to detect replay of information and/or operations. The detection applied to network packets that terminate at the TOE, such as trusted communications between the administrators and the TOE, or between an IT entity (e.g., authentication server) and the TOE. If replay is detected, the packets are discarded.

In addition, the TOE internally maintains the date and time. This date and time is used as the time stamp that is applied to TOE generated audit records. Alternatively, an NTP server can be used to synchronize the date-timestamp. Finally, the TOE performs testing to verify correct operation of the switch itself and that of the cryptographic module.

4.7 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.

5 Assumptions

The following assumptions were made during the evaluation of Cisco Catalyst 6500 Series Switches:

- All authorized administrators are assumed not evil and will not disrupt the operation of the TOE intentionally.
- Administrators will be trained to periodically review audit logs to identify sources of concern.
- Personnel will be trained in the appropriate use of the TOE to ensure security.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- Copies of TOE configuration data including representations of authentication data maintained off the TOE in hard-copy or soft-copy will be kept confidential and access will be limited to authorized administrators. Audit data transmitted by the TOE and routing table updates exchanged with neighbor routers, and associated neighbor router authentication data will be protected from unauthorized disclosure through isolation of associated network traffic.
- The TOE will be able to function with the software and hardware of other switch vendors on the network.
- The threat of malicious attacks aimed at exploiting the TOE is considered low.

6 Documentation

The following documentation was used as evidence for the evaluation of the Cisco Catalyst 6500 Series Switches:

6.1 Design Documentation

1. Cisco Catalyst 6500 Series Switches Security Architecture Document Draft, Revision 0.1, February 22, 2012
2. Cisco Catalyst 6500 Series Switches Functional Specification, Revision 0.1, February 22, 2012
3. Cisco Catalyst 6500 Series Switches TOE Design Specification, Revision 0.2, March 9, 2012

4. Annex A: Security Relevant CLI Commands, February 2012
5. Annex B: RFC Security Parameter Relevancy, February 22, 2012

6.2 Guidance Documentation

1. Cisco Catalyst 6500 Series Switches Common Criteria Operational User Guidance and Preparative Procedures, version 0.5, July 26, 2012
2. Release Notes for Catalyst 6500 Series Switch, Cisco IOS Release 15.0SY – Feb. 24, 2012
3. Catalyst 6500 Series Switches Installation Guide
4. Cisco IOS Configuration Fundamentals Configuration Guide, Release 15.0
5. Cisco IOS Security Configuration Guide: Securing User Services, Release 15.0
6. Cisco IOS Network Management Configuration Guide, Release 15.0
7. Catalyst 6500 Series Software Configuration Guide, 8.7
8. Cisco IOS Security Command Reference, April 2011
9. Cisco Catalyst 6500 Series Switch FIPS 140-2 Level 2 Non-Proprietary Security Policy
10. Cisco IOS IP Routing Protocols Configuration Guide

6.3 Life Cycle

1. Configuration Management, Delivery Procedures, Development Security, and Flaw Remediation for Cisco Catalyst Switches 6500 Series, Reference: CAT6K_ALC-CM-DVS-DEL-FLR-20120528, July 26, 2012, Version 4.0

6.4 Testing

1. Cisco Project Catalyst 6500 Series Switches EAL2 non-NDPP Common Criteria Detailed Test Plan, Revision 7, 07/26/2012
2. Cat6K-EAL2-TestCaseMapping-20120626.xls

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the Cisco Catalyst 6500 Series Switches, Version 1.0, July 26, 2012.

7.1 Developer Testing

At EAL2, testing must demonstrate correspondence between the tests and the functional specification. The vendor testing addressed each of the security functions identified in the ST and interfaces in the design. These security functions include:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Secure Management
- Protection of the TSF
- TOE access

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the *Cisco Catalyst 6500 Series Switches Common Criteria Operational User Guidance and Preparative Procedures*, ran a subset of vendor test suite and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

The evaluation team testing focused on testing boundary conditions not tested by Cisco. For vulnerability testing the evaluation team performed port and vulnerability scanning as well as other team developed tests.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Cisco Catalyst 6500 Series Switches including:

- One or two Supervisor 2T Cards (VS-S2T-10G or VS-S2T-10G-XL) per chassis (Two Sup cards in one chassis provide Supervisor failover within the chassis.)
- Each Sup2T running IOS 15.0(1)SY1 (FIPS validated)
- Sup2T cards installed into one or more 6506-E, 6509-E, or 6513-E Switch Chassis (Two chassis can be configured together to support HA with VSS.)
- With one or more WS-X6908-10G or WS-X6908-10G-2TXL Line Cards

To use the product in the evaluated configuration, the product must be configured as specified in the **Cisco Catalyst 6500 Series Switches Common Criteria Operational User Guidance and Preparative Procedures** document.

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 ETR. The reader of this document can assume that all

EAL2 augmented with ALC_FLR.2 and ALC_DVS.1 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 3 and CEM version 3.1 rev 3. The evaluation determined the Cisco Catalyst 6500 Series Switches TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 2) augmented with ALC_FLR.2 and ALC_DVS.1 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the 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 Catalyst 6500 Series Switches product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 the Development (ADV)

The evaluation team applied each EAL 2 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 and a high-level design document.

The validator 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 the Guidance Documents (AGD)

The evaluation team applied each EAL 2 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. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator 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 the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 2 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The ALC evaluation also ensured the TOE is identified such that the consumer is able to identify the evaluated TOE.

In addition to the EAL 2 ALC CEM work units, the evaluation team applied the ALC_FLR.2 and ALC_DVS.1 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE, while the security procedures (for physical, procedural and personnel security) for the development sites were evaluated to ensure that controls exist to ensure the secure development of the TOE.

The validator 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 the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The validator 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 EAL 2 VAN CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

The validator 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 performance of the entire vendor tests suite, the independent tests, and the penetration test 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 correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team considers the evaluated subset of product functions to be consistent with the product's intended purpose and mode of operation. The rationale for excluded features is plausible and introduces no unreasonable constraints.

The evaluation team observed that the vendor's security tests are predominantly manual and apparently not closely integrated with the extensive automated testing performed as a routine part of product development. While these evaluated tests are sufficient to satisfy Common Criteria requirements, the validation team recommends a closer integration in future efforts, in order to improve test integration and provide greater test coverage.

The validation team emphasizes the need for administrators to closely follow the Common Criteria Operational User Guidance and Preparative Procedures Version 0.4 when configuring the switches for use and not to use Cisco's Smart Install for the initial configuration. Administrators should pay particular attention to the evaluated configurations excluded functionality; features such as HTTP/HTTPS, telnet, and SNMP are not to be enabled in the Common Criteria compliant operational environment configuration as those functions may introduce vulnerabilities.

While the product has a FIPS certification, not all algorithms are validated by the FIPS program. For customers requiring FIPS validated algorithm protection, the MD5 algorithm used in various routing protocols is not a validated algorithm. For additional security, it is recommended router protocol traffic also be isolated to separate VLANs.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Cisco Catalyst 6500 Series Switches Security Target, Version 1.0, July 26, 2012*.

13 Glossary

The following definitions are used throughout this document:

- **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:

- [1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.
- [2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.
- [3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007

- [4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology*, Version 3.1, Revision 2, dated: September 2007.
- [5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.
- [6] Science Applications International Corporation. *Evaluation Technical Report for the Cisco Catalyst 6500 Series Switches Part 2 (Proprietary)*, Version 2.0, July 27, 2012.
- [7] Science Applications International Corporation. *Evaluation Team Test Report for the Cisco Catalyst 6500 Series Switches, ETR Part 2 Supplement (SAIC and Cisco Proprietary)*, Version 2.0, July 27, 2012.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.
- [10] Cisco Catalyst 6500 Series Switches Security Target, Version 1.0, July 26, 2012.