National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

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

Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, 4500X)

Report Number: CCEVS-VR-10489-0001
Dated: 13 December 2012
Version: 0.2

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 Donndelinger
Aerospace Corporation
Columbia, MD

Kenneth Stutterheim
Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Gary Grainger
Eve Pierre
Science Applications International Corporation
Columbia, Maryland

Table of Contents

Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) 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 June 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 Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X running IOS XE 3.3.1SG (IOS 15.1(1)SG1.) 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 Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) Security Target and analysis performed by the Validation Team.

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 Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) running IOS XE 3.3.1SG (IOS 15.1(1)SG1.) (Specific models identified in the Validated Products List Entry)
Protection Profile	None
ST:	Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X)Security Target, Version 0.98, November 27, 2012
Evaluation Technical Report	Evaluation Technical Report For Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) (Proprietary), Version 2.0, October 29, 2012
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 3

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

Architectural Information

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

The Catalyst Switches that comprise the TOE have common hardware characteristics. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware:

- Central processor that supports all system operations
- Dynamic memory, used by the central processor for all system operations
- Flash memory (EEPROM), used to store the Cisco IOS image (binary program)
- USB slot, used to connect USB devices to the TOE (not relevant as none of the USB devices are included in the TOE)
- Non-volatile read-only memory (ROM) is used to store the bootstrap program and power-on diagnostic programs
- Non-volatile random-access memory (NVRAM) is used to store switch configuration parameters used to initialize the system at start-up
- Physical network interfaces (minimally two) (e.g. RJ45 serial and standard 10/100 Ethernet ports). Some models have a fixed number and/or type of interfaces; some models have slots that accept additional network interfaces
- 10 Gigabit Ethernet (GE) uplinks and supports Power over Ethernet Plus (PoE+) and Universal POEP (UPOE). (Universal POEP is an enhancement to the PoEP (802.3at) standard to allow powered devices up to 60W to connect over a single Cat 5e cable. Standard PoEP uses only 2 twisted pairs (out of 4) in the Ethernet cable. UPOE uses all 4 twisted pairs to deliver 60W to the port.)
- Redundant power supplies and fans

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 as described in Section 1.7 Logical Scope of the TOE below.

TOE Evaluated Configuration

The TOE consists of one or more physical devices; the Catalyst Switch with Cisco IOS XE software. The Catalyst Switch has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS configuration determines how packets are handled to and from the switches' network interfaces. The switch 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. BGPv4, EIGRP, EIGRPv6 for IPv6, RIPv2, and OSPFv2 Routing protocols are used on all of the Catalyst Switch models.

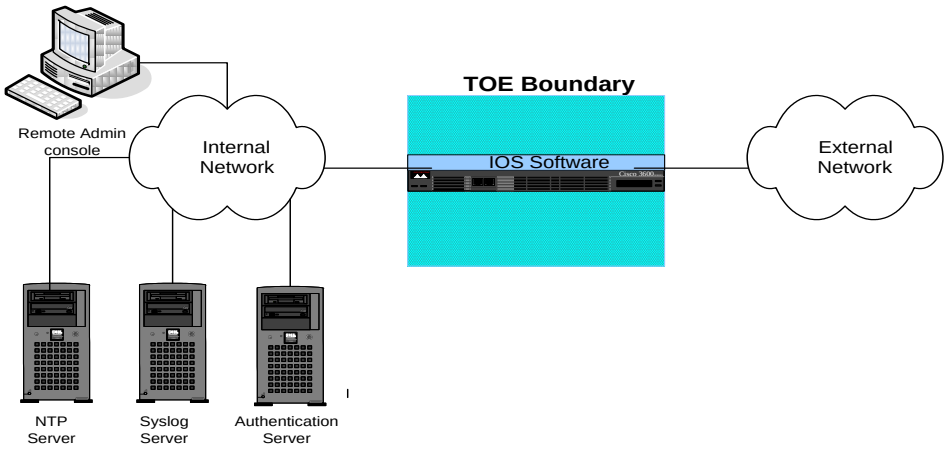
The Catalyst Switch E-Series chassis come in four different form factors: 3-slot (4503-E), 6-slot (4506-E), 7-slot (4507R+E/4507R-E), and 10-slot (4510R+E/4510R-E). 4503-E, 4506-E, 4507R+E, and 4510R+E chassis are extremely flexible and support 6 Gbps, 24 Gbps, or 48Gbps per line-card slot. 4507R-E and 4510R-E chassis are limited to 6 Gbps and 24 Gbps per line-card slot. Integrated resiliency in the Cisco Catalyst 4500E Series includes 1+1 supervisor engine redundancy (10-slot and 7-slot only), redundant fans, software-based fault tolerance, and 1+1 power supply redundancy. This integrated resiliency in both hardware and software minimizes network downtime[1].

The Catalyst Switch 4500-X series is a fixed aggregation switch that provides services for space-constrained environments.

The TOE can optionally connect to an NTP server on its internal network for time services. In addition, if the Catalyst Switch 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 following figure provides a visual depiction of an example TOE deployment.

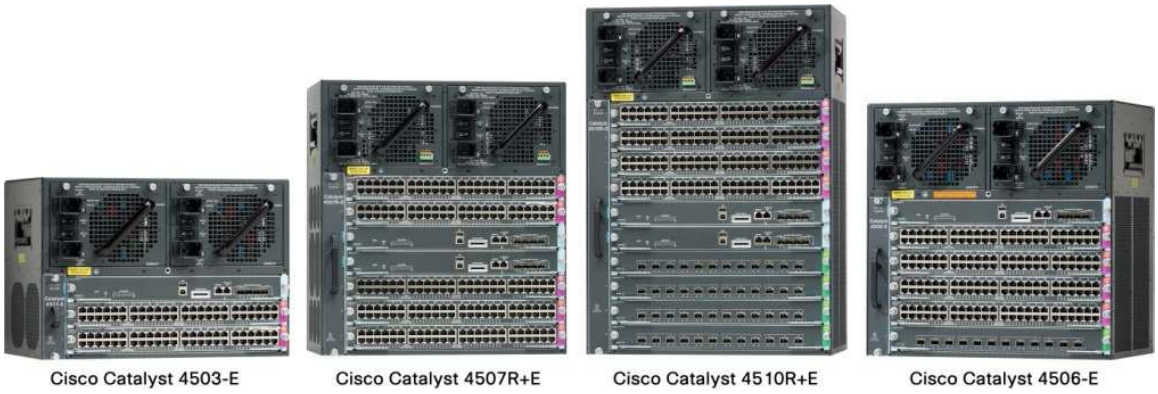
[1] Fault tolerance is not being claimed, as all features are not supported on all models.



Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the following switch models; Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) running IOS XE 3.3.1SG (IOS 15.1(1)SG1). The following tables further identify the supported configurations. The network, on which they reside, is part of the environment.

The Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, and 4510R-E) offers four chassis options and four supervisor engine options, however only the Supervisor 7-E and Supervisor 7L-E are included in the evaluated configuration.



Feature	Cisco Catalyst WS-C4503-E Chassis	Cisco Catalyst WS-C4506-E Chassis	Cisco Catalyst WS-C4507R+E Chassis	Cisco Catalyst WS-C4510R+E Chassis
Total number of	3	6	7	10

Feature	Cisco Catalyst WS-C4503-E Chassis	Cisco Catalyst WS-C4506-E Chassis	Cisco Catalyst WS-C4507R+E Chassis	Cisco Catalyst WS-C4510R+E Chassis
slots				
Line-card slots	2	5	5	8
Supervisor engine slots	1[2]	1	2[3]	2[4]
Dedicated supervisor engine slot numbers	1	1	3 and 4	5 and 6
Supervisor engine redundancy	No	No	Yes	Yes (Supervisor V-10GE, 6-E and 7-E)
Supervisor engines supported	Supervisor 7-E Supervisor 7L-E	Supervisor 7-E Supervisor 7L-E	Supervisor 7-E Supervisor 7L-E	Supervisor 7-E
Maximum PoE per slot	1,500W	1,500W	1,500W	1,500W slots 1 and 2, 750W slots 3,4,7-10
Bandwidth scalability per line-card slot	Up to 48 Gbps on all slots	Up to 48 Gbps on all slots	Up to 48 Gbps on all slots	Up to 48 Gbps on all slots[5]
Number of power supply bays	2	2	2	2
AC input power	Yes	Yes	Yes	Yes
DC Input power	Yes	Yes	Yes	Yes
Integrated Power over Ethernet	Yes	Yes	Yes	Yes
Minimum number of	1	1	1	1

[2] Slot 1 is reserved for supervisor engine only; slots 2 and higher are reserved for line cards.
[3] Slots 3 and 4 are reserved for supervisor engines only in Cisco Catalyst 4507R-E and 4507R+E; slots 1-2 and 5-7 are reserved for line cards
[4] Slots 5 and 6 are reserved for supervisor engines only in Cisco Catalyst 4510R-E and 4510R+E; slots 1-4 and 7-10 are reserved for line cards

Feature	Cisco Catalyst WS-C4503-E Chassis	Cisco Catalyst WS-C4506-E Chassis	Cisco Catalyst WS-C4507R+E Chassis	Cisco Catalyst WS-C4510R+E Chassis
power supplies				
Power supplies supported	● 1000W AC ● 1400W AC ● 1300W ACV ● 2800W ACV ● 4200W ACV ● 6000W ACV ● 1400W DC (triple input) ● 1400W-DC-P	● 1000W AC ● 1400W AC ● 1300W ACV ● 2800W ACV ● 4200W ACV ● 6000W ACV ● 1400W DC (triple input) ● 1400W-DC-P	● 1000W AC ● 1400W AC ● 1300W ACV ● 2800W ACV ● 4200W ACV ● 6000W ACV ● 1400W DC (triple input) ● 1400W-DC-P	● 1400W AC ● 2800W ACV ● 4200W ACV ● 6000W ACV ● 1400W DC (triple input) ● 1400W-DC-P
Number of fan-tray bays	1	1	1	1
Location of 19-inch rack mount	Front	Front	Front	Front
Location of 23-inch rack mount	Front (option)	Front (option)	Front (option)	Front (option)

Cisco Catalyst 4500 Series line cards can be mixed and matched to suit numerous LAN access, server connectivity, or branch-office deployments. The Cisco Catalyst 4500 Series supports the following line cards, by product number:

Product Number /Description
Cisco Catalyst 4500E Series Line Cards
WS-X4748-UPOE+E Cisco Catalyst 4500E Series 48-Port UPOE 10/100/1000 (RJ-45) **WS-X4748-RJ45V+E** Cisco Catalyst 4500E Series 48-Port 802.3at PoEP 10/100/1000 (RJ-45) **WS-X4748-RJ45-E** Cisco Catalyst 4500E Series 48-Port 10/100/1000 (RJ-45) **WS-X4712-SFP+E** Cisco Catalyst 4500E Series 12-port 10 Gigabit Ethernet (SFP+) **WS-X4624-SFP-E** Cisco Catalyst 4500E Series 24-port GE (SFP) **WS-X4612-SFP-E** Cisco Catalyst 4500E Series 12-port GE (SFP) **WS-X4648-RJ45V-E** Cisco Catalyst 4500E Series 48-Port PoE 10/100/1000(RJ45) **WS-X4648-RJ45V+E** Cisco Catalyst 4500E Series 48-Port Premium PoE 10/100/1000(RJ45) **WS-X4606-X2-E** Cisco Catalyst 4500E Series 6-Port 10GE (X2) **WS-X4648-RJ45-E** Cisco Catalyst 4500E Series 48-Port Data 10/100/1000(RJ45)
Cisco Catalyst 4500 Classic 10/100 Line Cards
WS-X4148-RJ Cisco Catalyst 4500 10/100 Auto Module, 48-Port (RJ-45)

WS-X4248-RJ45V Cisco Catalyst 4500 PoE 802.3af 10/100, 48-Port (RJ-45)
Cisco Catalyst 4500 Classic 10/100/1000 Line Cards
WS-X4548-GB-RJ45 Cisco Catalyst 4500 Enhanced 48-Port 10/100/1000 Module (RJ-45) **WS-X4548-RJ45V+** Cisco Catalyst 4500 48-Port 802.3af PoE and 802.3at PoEP 10/100/1000 (RJ-45) **WS-X4548-GB-RJ45V** Cisco Catalyst 4500 PoE IEEE 802.3af 10/100/1000, 48 Ports (RJ-45)
Cisco Catalyst 4500 Classic 100 BASE-X FE Line Cards
WS-X4248-FE-SFP Cisco Catalyst 4500 Fast Ethernet Switching Module, 48-Port 100BASE-X (SFP)
Cisco Catalyst 4500 Classic 1000 BASE-X GE Line Cards
WS-X4306-GB Cisco Catalyst 4500 Gigabit Ethernet Module, 6 Ports (GBIC) **WS-X4506-GB-T** Cisco Catalyst 4500 6-Port 10/100/1000 RJ-45 PoE IEEE 802.3af and 1000BASE-X (SFP) **WS-X4418-GB** Cisco Catalyst 4500 Gigabit Ethernet Module, Server Switching 18 Ports (GBIC) **WS-X4448-GB-SFP** Cisco Catalyst 4500 Gigabit Ethernet Module, 48 Ports 1000X (SFP)

The Cisco Catalyst 4500 Series has flexible interface types and port densities that allow network configurations to be mixed and matched to meet the specific needs of the organizations network.

Cisco Catalyst 4500 Series Switching Modules Number of	Number of Interfaces Supported per Line Card	Cisco Catalyst 4503-E	Cisco Catalyst 4506-E	Cisco Catalyst 4507R+E	Cisco Catalyst 4510R+E
Switched 10/100 Fast Ethernet (RJ-45)	48	96	240	240	384
Switched 10/100 Fast Ethernet (RJ-45) with IEEE 802.3af at Power over Ethernet (PoE/PoEP)	48	96	240	240	384
Switched 100 FX Fast Ethernet (MT-RJ)	48	96	240	240	384
Switched 1000BASE-X (Fiber)	6, 18, or 48	104	244	244	388
Switched	48	96	240	240	384

Cisco Catalyst 4500 Series Switching Modules Number of	Number of Interfaces Supported per Line Card	Cisco Catalyst 4503-E	Cisco Catalyst 4506-E	Cisco Catalyst 4507R+E	Cisco Catalyst 4510R+E
10/100/1000BASE-T Gigabit Ethernet					
Switched 10/100/1000BASE-T Gigabit Ethernet with IEEE 802.3af at PoE/PoEP	48	96	240	240	384
Switched 10/100/1000BASE-T Gigabit Ethernet with UPOE	48	96	240	240	384
Switched 10 Gigabit Ethernet	6 or 12	24	60	60[6]	96[7]

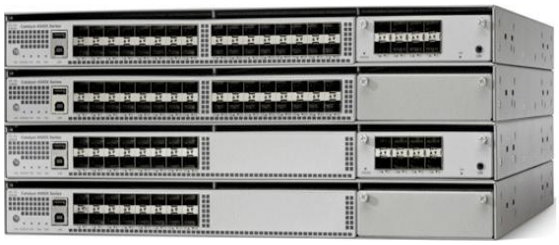
The Cisco Catalyst 4500-X Series Switch is a fixed 10 Gigabit Ethernet aggregation platform that provides flexibility through two versions of base switches along with optional uplink module. Both the 32- and 16-port versions can be configured with optional network modules and offer similar features. The Small Form-Factor Pluggable Plus (SFP+) interface supports both 10 Gigabit Ethernet and 1 Gigabit Ethernet ports, allowing upgrades to 10 Gigabit Ethernet when organizational demands change. The uplink module is hot swappable.

Deployment Options include:

- 16- and 32-port 10 Gigabit Ethernet Small Form-Factor Pluggable Plus (SFP+) models
- 8-port 10 Gigabit Ethernet SFP+ removable uplink module
- Dual-redundant AC/DC power supply and five field-replaceable unit (FRU) fans

The figure below shows the Cisco Catalyst 4500-X Series Switch with and without the optional 8-port uplink module and back of the switch.

[6] WS-C4507R-E and WS-C4510R-E chassis support up to 34 switched 10 Gigabit Ethernet ports
[7] WS-C4507R-E and WS-C4510R-E chassis support up to 34 switched 10 Gigabit Ethernet ports



Supported non-TOE Hardware/ Software/ Firmware

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

Table 1 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Authentication Server	No	The authentication server (RADIUS and TACACS+) provides central authentication for user authorized to use the TOE. The TOE correctly leverages the services provided by the authentication server.
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.
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.
NTP Server	No	The TOE supports communications with an NTP server to synchronize time.

Security Policy

This section summaries 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

Security Audit

The TOE generates a comprehensive set of audit logs 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.

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. The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; digital signature using RSA; cryptographic hashing using SHA1; keyed-hash message authentication using HMAC-SHA1. The TOE also implements SSHv2 secure protocol for secure remote administration. In the evaluated configuration, the TOE must be operated in FIPS mode of operation per the FIPS Security Policy.

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 the routing tables. The routing tables can also 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 the routing protocol that is security relevant in this TOE is the ability to authenticate neighbor routers using shared passwords. Other security features and configuration options of routing protocols are 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.

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. For RADIUS, only the password is encrypted, while TACACS+ encrypts the entire packet body except the header. Note the remote authentication server is not included within the scope of the TOE evaluated configuration, it is considered to be provided by the operational environment.

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.

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, 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.

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)). A separate VLAN should be used to ensure the routing protocol communications between the TOE and neighbor routers (including routing table updates and neighbor router authentication) is logically isolated from the traffic on other VLANs.

The TOE also supports replay detection, though it is only applicable to the encrypted sessions for remote administration via SSHv2. 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.

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.

Evaluation

The purpose of this section is to describe the evaluation processes followed by the SAIC CCTL when performing the evaluation of Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X). The SAIC CCTL considers this information proprietary. The details of the evaluation processes are presented in the proprietary ETR submitted as a separate document.

Assumptions

The following assumptions were made during the evaluation of Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X):

- 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.

Documentation

The following documentation was used as evidence for the evaluation of the Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X):

Design Documentation

1. Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) Security Architecture Document Draft, Revision 0.1, February 7, 2012
2. Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) Functional Specification, Revision 0.5, October 3, 2012
3. Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) TOE Design Specification, Revision 0.4, September 28, 2012
4. Annex A: Security Relevant CLI Commands, February 7, 2012
5. Annex B: RFC Security Parameter Relevancy, October 2, 2012

Guidance Documentation

1. Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) Common Criteria Operational User Guidance and Preparative Procedures, version .7, October 26, 2012
2. Catalyst 4500 E Series Installation Guide
3. Cisco IOS Configuration Fundamentals Configuration Guide, Release 15.0
4. Cisco IOS Security Configuration Guide: Securing User Services, Release 15.0
5. Cisco Configuration Fundamentals Configuration Guide Cisco IOS XE, Release 3S
6. Cisco Catalyst 4500 Series Switches Cisco IOS Command Reference, Release IOS XE 3.3 OSG and IOS 15.1(1)SG
7. Cisco IOS Security Command Reference, April 2010

Life Cycle

1. Configuration Management, Delivery Procedures, Development Security, and Flaw Remediation for Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X), version 6.5, October 18, 2012

Testing

1. Cisco Project Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) EAL2 non-NDPP Common Criteria Detailed Test Plan, October 17, 2012
2. Test Case Mapping (Cat4K-EAL2-non-NDPP-TestCaseMapping-20120817.xlsx)
3. CommonCriteriaTestBed.ppt

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 Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X), Version 1.0, October 29, 2012

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

Evaluation Team Independent Testing

The evaluation team verified the product according the *Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) 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.

Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) running

- IOS XE 3.3 ISG (IOS 15.1(1)SG1.

To use the product in the evaluated configuration, the product must be configured as specified in the **Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) Common Criteria Operational User Guidance and Preparative Procedures** document.

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 Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) 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.

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 Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) 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.

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.

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.

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 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.

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.

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.

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.

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.

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 noted that the conformance testing was performed against an earlier revision of the software; the vendor has provided assurance that the claimed security functionality was not affected with the minor revision.

The validation activities are complete pending the products obtaining the necessary FIPS 140-2 certificates. The validation team encourages the purchaser to review the documentation thoroughly prior to use; paying special note to the excluded functionality as described in section 1.8 of the Security Target as the use of those excluded components would remove the product from the evaluated configuration.

Annexes

Not applicable.

Security Target

The Security Target is identified as *Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) Security Target, Version 0.98, November 27, 2012*.

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.

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 3, dated: July 2009.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 3, dated: July 2009.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 3, dated: July 2009

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 3, dated: July 2009.

[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 Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) Part 2 (Proprietary)*, Version 2.0, October 29, 2012.

[7] Science Applications International Corporation. *Evaluation Team Test Report for the Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X), ETR Part 2 Supplement (SAIC and Cisco Proprietary)*, Version 1.0, October 29, 2012.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] Cisco Catalyst Switches (4503-E, 4506-E, 4507R+E, 4507R-E, 4510R+E, 4510R-E, and 4500X) Security Target, Version 0.97, October 29, 2012.