National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Cisco Systems Catalyst Switches (2900 running 12.1(22)EA10 or 12.2(25)SEE4; 3500 and 3750 running 12.2(25)SEE4; 4500 and 4948 running 12.2(31)SG2; 6500 running 12.2(18)SXF11) and Cisco Secure ACS for Windows Server version 4.1.4.13

Report Number:	**CCEVS-VR-VID6012-2008**
Dated:	**May 27, 2008**
Version:	**0.9 FINAL**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, Maryland 20878

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

Acknowledgements:

The TOE evaluation was sponsored by:

Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95124-1706
USA

Evaluation Personnel:
Arca Common Criteria Testing Laboratory

Ken Dill
Maria Tadeo
.

Validation Personnel:

Robin Medlock, The MITRE Corporation
Jandria Alexander, The Aerospace Corporation

Table of Contents

1 Executive Summary

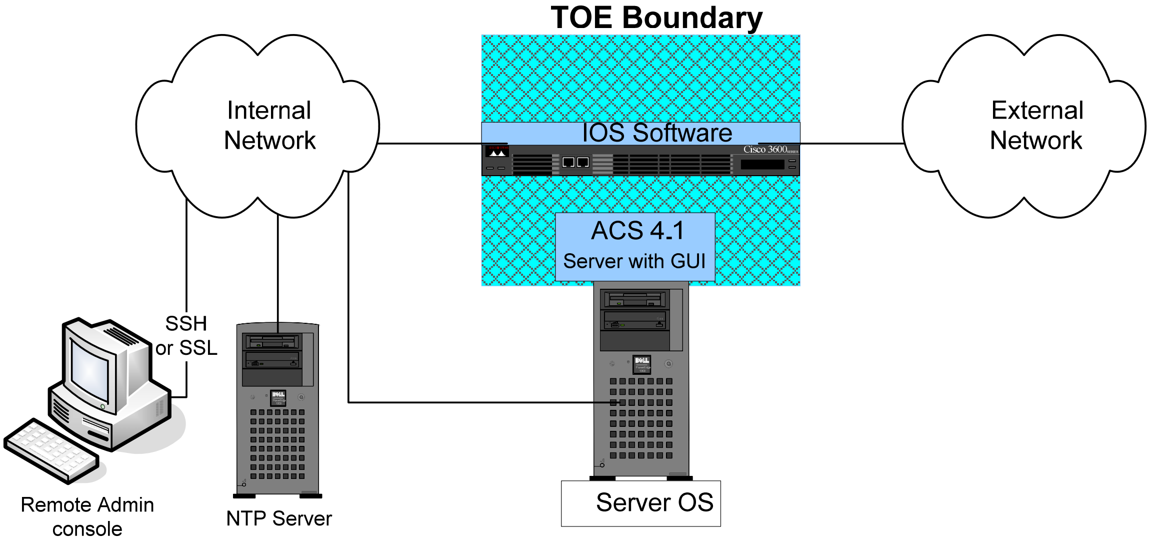
This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Systems Catalyst Switches (2900 running 12.1(22)EA10 or 12.2(25)SEE4; 3500 and 3750 running 12.2(25)SEE4; 4500 and 4948 running 12.2(31)SG2; 6500 running 12.2(18)SXF11) and Cisco Secure ACS for Windows Server version 4.1.4.13. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the Cisco Switches and Cisco ACS was performed by the Arca Common Criteria Testing Laboratory (CCTL) in the United States and was completed during November 2007. The information in this report is largely derived from the Security Target (ST), written by Cisco Systems, Inc. and the Evaluation Technical Report (ETR) and associated Evaluation Team Test Report, both written by Arca CCTL. The evaluation team determined the product to be CC version 2.2 Part 2 and Part 3 conformant, including all Information Technology Security Evaluation Final Interpretations from January 2004 through March 25, 2004, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 3 augmented with Flaw Remediation (ALC_FLR.1) have been met.

The TOE is the Cisco Systems Catalyst Switches (2900 running 12.1(22)EA10 or 12.2(25)SEE4; 3500 and 3750 running 12.2(25)SEE4; 4500 and 4948 running 12.2(31)SG2; 6500 running 12.2(18)SXF11) running IOS and a Cisco Secure Access Control Server. Catalyst switches are hardware devices used to construct IP networks by interconnecting multiple smaller networks or network segments. The TOE also includes ACS, a software application that provides authentication, authorization, and accounting (AAA) services to network devices that function as AAA clients, including switches.

Figure 1 illustrates the TOE and its environment. The TOE includes the Cisco Switch, the IOS version running on the switch (shown by the switch in the diagram), and the Cisco Secure ACS version 4.1.4.13 (ACS 4.1 server in the diagram).

Figure 1: Typical TOE Configuration



The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the Common Evaluation Methodology (CEM) work unit verdicts), and reviewed successive versions of the ETR and test report.

The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 3 augmented with ALC_FLR.1 evaluation. Therefore the validation team concludes that the Arca CCTL findings are accurate, and the conclusions justified.

2 Identification

The CCEVS is a National Security Agency (NSA) 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) or candidate CCTLs using the CEM for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs and candidate 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 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 organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Cisco Systems Catalyst Switches (2900 running 12.1(22)EA10 or 12.2(25)SEE4; 3500 and 3750 running 12.2(25)SEE4; 4500 and 4948 running 12.2(31)SG2; 6500 running 12.2(18)SXF11) and Cisco Secure ACS for Windows Server version 4.1.4.13
Security Target	Cisco Systems Catalyst Switches EAL3 Security Target Version 1.7 dated, February 27, 2008

Item	Identifier
Evaluation Technical Report	• ASE (Security Target Evaluation): ASE Evaluation Technical Report for Cisco Systems Catalyst Switches EAL3, document Version 0.8, released February 27, 2008. • ACM (Configuration Management Evaluation): ACM_CAP.3; ACM_SCP.1 Evaluation Technical Report for Cisco Systems Catalyst Switches EAL3, document Version 0.8, released February 27, 2008. • ALC (Life Cycle Evaluation): ALC_DVS.1; ALC_FLR.1; Evaluation Technical Report for Cisco Systems Catalyst Switches EAL3, document version 0.6, released January 31, 2008. • ADO (Delivery and Installation Evaluation): ADO_DEL.1; ADO_IGS.1 Evaluation Technical Report for Cisco Systems Catalyst Switches EAL3, document Version 0.8, released February 27, 2008. • ADV (Development Evaluation): ADV_FSP.1; ADV_HLD.2; ADV_RCR.1; Evaluation Technical Report for Cisco Systems Catalyst Switches EAL3, document Version 0.8, released February 27, 2008. • AGD (Administrative and User Guidance Evaluation): AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for Cisco Systems Catalyst Switches EAL3, document Version 0.8, released February 27, 2008. • ATE (Functional Testing, Testing Coverage, Testing Depth and Independent Testing Evaluation): ATE_COV.2; ATE_DPT.1, ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for Cisco Systems Catalyst Switches EAL3, document Version 0.7, released February 27, 2008. • AVA Vulnerability Assessment Evaluation): AVA_MSU.1; AVA_VLA.1; AVA_SOF.1 Evaluation Technical Report for Cisco Systems Catalyst Switches EAL3, document Version 0.8, released February 27, 2008.
Protection Profile	None
Conformance Result	CC Part 2 and CC Part 3 conformant, EAL 3 augmented ALC_FLR.1
Applicable interpretations and precedents	▪ Compliant with all international interpretations with effective dates on or before February 25, 2004.
Sponsor	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95124-1706
Common Criteria Testing Lab (CCTL)	SAVVIS Communications Arca Common Criteria Testing Laboratory NVLAP Lab Code 200429 45901 Nokes Boulevard Sterling, VA 20166

Item	Identifier
CCEVS Validator(s)	Robin Medlock The MITRE Corporation 7515 Colshire Drive McLean, VA 22102 Jandria Alexander The Aerospace Corporation 6940 Columbia Gateway Drive Columbia, Maryland 21046

3 Security Functions

3.1 Audit (Accounting)

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. Audited events include; Modifications to the group of users that are part of the authorized administrator roles, all use of the user identification mechanism, any use of the authentication mechanism, any change in the configuration of the TOE or any failure of a packet to match an ACL rule allowing traversal of the switch.

3.2 Identification & Authentication (Authentication)

The switch performs authentication, using IOS platform authentication mechanisms, to authenticate access to user exec and privileged exec command modes.

Identification and Authentication provides the method of 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 TACACS+ or RADIUS. TACACS+. Terminal Access Controller Access Control System (TACACS+) is part of AAA. TACACS+ provides ACS centralized user password authentication for all switches that the ACS manages and is an option that can be installed with ACS. Whenever a user requests some action, the switch sends the user name and password to a central server located on the same server as the ACS. The server consults its access control database and either permits or denies the requested action.

3.3 Traffic Filtering and Switching (VLAN Processing)

VLANs enable efficient traffic separation, provide better bandwidth utilization, and alleviate scaling issues by logically segmenting the physical local-area network (LAN) infrastructure into different subnets so that VLAN packets are presented to interfaces within the same VLAN. The most important requirement of VLANs is the ability to identify which packets belong to which VLANs to ensure packets can only travel to interfaces for which they are authorized.

Restricts remote terminal connectivity, using TOE platform access-control list functionality, to specific interfaces of the TOE so that sessions will only be accepted from the management station(s) identified in the management session TOE security policy.

Access lists filter network traffic by controlling whether VLAN tagged packets are passed on and whether routed packets are forwarded or blocked at the switches' IP interfaces. The switch examines each packet to determine whether to forward or drop the packet, on the basis of the criteria specified within the access lists. Access list criteria include the source and destination

VLAN tags, and for those switches that include Layer-3 capabilities could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

3.4 Security Management/Access Control (Authorization)

The ACS and switch allow authorized administrators to add new administrators, start-up and shutdown the device, create, modify, or delete configuration items, modify and set the time and date, and create, delete, empty, and review the audit trail. The ACS, when using TACACS+ or RADIUS, allows authentication administrators to modify and set the threshold for the number of permitted consecutive authentication attempt failures, and to restore authentication capabilities for users that have met or exceeded the threshold for permitted consecutive authentication attempt failures.

The TOE switch platform maintains privileged and semi-privileged administrator roles. The switch performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged modes.

3.5 Protection of the TSF

The switch protects against interference and tampering by untrusted subjects by implementing identification, authentication and access controls to limit configuration to privileged administrators. Additionally IOS is not a general purpose operating system and access to IOS memory space is restricted to only IOS functions.

The ACS component protects against interference and tampering by untrusted subjects through its own interfaces by implementing identification, authentication, and roles.

Both the switch and ACS component ensure that when data is transmitted between them that security functions to protect the data from packet sniffing are invoked successfully before that data is transmitted.

The Cisco IOS contains a collection of features that build on the core components of the system. Those features that are not to be used include the HTTP Server, the IEEE 802.11 Wireless Standards, MAC address filtering, SNMP, Telnet, and VPN.

Apart from these exceptions all types of network traffic through and to the TOE are within the scope of the evaluation.

4 Assumptions

The assumptions are ordered into three groups: Personnel Assumptions, Physical Environment Assumptions, and Operational Assumptions.

4.1.1 Personnel Assumptions

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error.

A.TRAIN_AUDIT Administrators will be trained to periodically review audit logs to identify sources of concern

A.TRAIN_GUIDAN Personnel will be trained in the appropriate use of the TOE to ensure security.

4.1.2 Physical Environment Assumptions

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

4.1.3 Operational Assumptions

A.CONFIDENTIALITY The hard copy documents that describe the configuration of the TOE, I&A information and Audit storage will be kept confidential and access will be limited to Authorized administrators.

A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.INTEROPERABILITY The TOE will be able to function with the software and hardware of other switch vendors on the network.

A.LOWEXP The threat of malicious attacks aimed at exploiting the TOE is considered low.

5 Architectural Information

The TOE is the Cisco Switch running IOS. The network, on which they reside, is part of the environment.

The following table lists the software, hardware and switch operating system, and declares whether or not each is part of the TOE.

Table 2: TOE Boundary

HARDWARE	**TOE?**
Switch	Yes
ACS Server hardware	No
OS	
Windows 2000 Server (ACS Server OS)	No
SOFTWARE	
Cisco ACS for Windows Server Version 4.1.4.13	Yes
TACACS+ or RADIUS[1]	Yes
IOS (version listed above in table 2)	Yes

[1] Software installed with ACS: Includes TACACS+ protocol as defined by Cisco Systems in draft 1.78 and RADIUS as specified in RFC 2865. The versions of TACACS+ and RADIUS are dependent upon ACS, so they are the same for all of the IOS versions included in the TOE.

Table 3: Evaluated Configurations

.

IOS Version	Models in TOE
• 12.1(22)EA10	• 2940 • 2950 • 2950RLE • 2955
• 12.2(25)SEE4	• 2960 • 2970 • 3550 • 3560 • 3750 • 3750-METRO
• 12.2(31)SG2	• 4500-SUP2-PLUS • 4500-SUP2-PLUS-10GE • 4500-SUP2-PLUS-TS • 4500-SUP4 • 4500-SUP5 • 4500-SUP5-10GE • 4948 • 4948-10GE
• 12.2(18)SXF11	• 6500-SUP2/MSFC2 • 6500-SUP32/MSFC2A • 6500-SUP720/MSFC3

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor):

Table 5: Evaluation Evidence

Component	Description
Installation and Configuration for Common Criteria EAL3 Evaluated Cisco IOS/AAA Switches (ADM/IGS)	Version 0-11, November 2007
Cisco Systems IOS/AAA Functional Specification EAL3 (FSP)	Version 0-13 November 21, 2007.
Cisco Systems IOS/AAA High Level Design EAL3 (HLD)	Version 0-11, October 26, 2007
Cisco's Configuration Management ,Plan and Delivery Procedures (CMP) Cisco AAA Configuration Items (CI)	Version 0.9, April 2007 Version 0-9 November 2007

Cisco Systems Vulnerability, Misuse and Strength of Function EAL3 (MSU_VLA_SOF)	Version 0-9, November 21, 2007
Cisco IOS Catalyst Switches EAL3 Detailed Test Plan (ATE)	Version 1.12 November 2007
Cisco Systems Catalyst Switches EAL3 Security Target (ST)	Version 1.7 February 27, 2008

6.1 Guidance Documentation

The following is the list of other evaluation evidence provided by the sponsor:

- *Security Target for Cisco IOS/AAA Switches, version 1.5*
- *Cisco IOS Security Configuration Guide, Release 12.1 (http://www.cisco.com/en/US/docs/ios/12_1/security/configuration/guide/secur_c.html)*
- *Cisco IOS Security Configuration Guide, Release 12.2 (http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080087df1.html)*
- *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2 (http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080080ff9.html)*
- *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.1 (http://www.cisco.com/en/US/docs/ios/12_1/configfun/configuration/guide/fun_c.html)*
- *Specific to IOS 12.2(18)SXF11:*
    - *Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2* (http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a00801c8339.html)
    - *Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 Series MSFC (http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a008019e1e9.html)*
    - *Catalyst 6500 Series MSFC Cisco IOS Command Reference, 12.2SX (http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/hybrid/command/reference/msfc_cr.html)*
    - *Catalyst 6500 Release 12.2SX Software Configuration Guide (http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/book.html)*
    - *Catalyst 6500 Series Switch Supervisor Engine Guide (http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_book09186a00803648c1.html)*
    - *Catalyst 6500 Series Switch Module Guide (http://www.cisco.com/en/US/products/hw/switches/ps708/products_module_configuration_guide_book09186a008036fa45.html)*

- *Specific to IOS 12.1(22)EA10:*
    - *Release Notes for the Catalyst 2955, Catalyst 2950, and Catalyst 2940 Switches, Cisco IOS Release 12.1(22)EA10 and Later* (http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_22_ea10/release/notes/OL12607.html)
    - *Catalyst 2950 and Catalyst 2955 Switch Command Reference, 12.1(22)EA7* (http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_22ea/CR/cr.html)
    - *Catalyst 2940 Switch Command Reference, 12.1(22)EA7* (http://www.cisco.com/en/US/docs/switches/lan/catalyst2940/software/release/12.1_22_ea7/command/reference/cr.html)
    - *Catalyst 2940 Switch Software Configuration Guide, 12.1(22)EA7* (http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst2940/software/release/12.1_22_ea7/configuration/guide/scg1.html)
    - *Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide, 12.1(19)EA1* (http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst2950/software/release/12.1_19_ea1/configuration/guide/2950scg.html)
- *Specific to IOS 12.2(25)SEE4:*
    - *Release Notes for the Catalyst 3750, 3560, 2970, and 2960 Switches* (http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_see1_2/release/notes/OL9586.html)
    - *Catalyst 2960 Switch Command Reference, 12.2(25)SEE* (http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_25_see/command/reference/cr.html)
    - *Release Notes for the Catalyst 3550 Multilayer Switch, Cisco IOS Release 12.2(25)SEE* (http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.2_25_see/release/notes/OL8567.html)
    - *Catalyst 3550 Multilayer Switch Command Reference, Rel. 12.2(25)SEE* (http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.2_25_see/command/reference/cr.html)
    - *Catalyst 3560 Switch Command Reference, Rel. 12.2(25)SEE* (http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_25_see/command/reference/cr.html)
    - *Catalyst 3750 Switch Command Reference, 12.2(25)SEE* (http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_see/command/reference/cr.html)
    - *Release Notes for the Catalyst 3750 Metro Switch, Cisco IOS Release 12.2(25)SEE and Later* (http://www.cisco.com/en/US/docs/switches/metro/catalyst3750m/software/release/12.2_25_see/release/notes/OL8650.html)

    - *Catalyst 3750 Metro Switch Software Command Reference* (http://www.cisco.com/en/US/docs/switches/metro/catalyst3750m/software/release/12.2_25_seg_seg1/command/reference/3750mcr.html)

    - *Catalyst 2960 Switch Software Configuration Guide, 12.2(25)SEE* (http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_25_see/configuration/guide/scg_1.html

- *Specific to IOS 12.2(31)SG2:*

    - *Release Note for the Catalyst 4500 Series Switch, Cisco IOS, 12.2EW and 12.2SG* (http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_5184.html)

    - *Release Note for Catalyst 4948 Series Switch, Cisco IOS 12.2EW and 12.2SG* (http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_9592.html)

    - *Catalyst 4500 Series Switch Cisco IOS Command Reference, 12.2(31)SG (4948 references these as well)* (http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/command/reference/cmdref.html)

    - *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(31)SG (4948 references these as well)* (http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/configuration/guide/conf.html)

- *Installation Guide for Cisco Secure ACS for Windows, Release 4.1, Text Part Number: OL-9970-02* (http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/installation/guide/windows/IGwn41P.pdf)
- *User Guide for Cisco Secure Access Control Server Release 4.1 , Text Part Number: OL-9971-01* (http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/ACSugP.pdf)

- *Catalyst 2940 and 2950 Series*:

    - *Catalyst 2940 Switch Getting Started Guide* *http://www.cisco.com/en/US/docs/switches/lan/catalyst2940/hardware/quick/guide/2940GSG.html*

    - *Catalyst 2950 Switch Getting Started Guide* *http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/hardware/quick/guide/2950gsg.html*

    - *Cisco Catalyst 2955 Switch Hardware Installation Guide* *http://www.cisco.com/en/US/docs/switches/lan/catalyst2955/hardware/installation/guide/2955hg.html*

- *Catalyst 2960 and 2970 Series:*

    - *Catalyst 2960 Switch Getting Started Guide* *http://www.cisco.com/en/US/products/ps6406/products_getting_started_guide_book09186a0080693b06.html*

    - *Catalyst 2970 Switch Getting Started Guide*
      http://www.cisco.com/en/US/docs/switches/lan/catalyst2970/hardware/quick/guide/2970GSG2.html

- *Catalyst 3550 and 3560 Series:*

    - *Catalyst 3550 Multilayer Switch Getting Started Guide*
      http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/hardware/quick/guide/3550GSG.html

    - *Catalyst 3560 Switch Getting Started Guide*
      http://www.cisco.com/en/US/products/hw/switches/ps5528/products_getting_started_guide09186a008078058e.html

- *Catalyst 3750 Series:*

    - *Catalyst 3750 Switch Getting Started Guide*
      http://www.cisco.com/en/US/products/hw/switches/ps5023/products_getting_started_guide09186a0080438fb6.html

    - *Catalyst 3750 Metro Switch Getting Started Guide*
      http://www.cisco.com/en/US/docs/switches/metro/catalyst3750m/hardware/quick/guide/3750MGSG.html

- *Catalyst 4500 Series:*

    - Catalyst 4500 Series Installation Guide
      http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/installation/guide/78-14409-08/4500inst.html

    - *Installation and Configuration Note for the Catalyst 4500 Series Supervisor Engine II-Plus*
      http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/configuration/notes/78_15783.html

    - *Installation and Configuration Note for the Catalyst 4500 Series Supervisor Engine II-Plus 10GE*
      http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/configuration/notes/78_17176.html

    - *Installation and Configuration Note for the Catalyst 4500 Series Supervisor Engine II-Plus TS*
      http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/configuration/notes/78_16551.html

    - *Installation and Configuration Note for the Catalyst 4500 Series Supervisor Engine IV*
      http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/configuration/notes/78_14496.html

    - *Installation and Configuration Note for the Catalyst 4500 Series Supervisor Engine V* *http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/configuration/notes/78_15590.html*

- o *Installation and Configuration Note for the Catalyst 4500 Series Supervisor Engine V-10GE*
  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/configuration/notes/78_16727.html

- *Catalyst 4900 Series:*

  - o *Catalyst 4948 Install Guide*
    http://www.cisco.com/en/US/docs/switches/lan/catalyst4900/4948/4948_in.html

  - o *Catalyst 4948-10GE Installation Guide*
    http://www.cisco.com/en/US/docs/switches/lan/catalyst4900/4948-10ge/4948_10.html

- *Catalyst 6500 Series:*

  - o *Catalyst 6500 Series Switch Installation Guide*
    http://www.cisco.com/en/US/products/hw/switches/ps708/prod_installation_guides_list.hmtl

  - o *Catalyst 6500 Series Switch Module Installation Note*
    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Module_Installation/Mod_Install_Note/78_15767.html

- *ACS Software (Cisco Secure ACS for Windows Server) v 4.1.4.13:*

  - o *Installation Guide for Cisco Secure ACS for Windows 4.1*
    http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/installation/guide/windows/IGwn41P.pdf

  - o *User Guide for Cisco Secure ACS for Windows 4.1*
    http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/ACSugP.pdf

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

7.1 Developer Testing

The developer performed a testing and coverage analysis, which examined each SFR and developed one or more Cisco test cases that verify the function or command requirement. These tests were documented in the Cisco IOS Catalyst Switches EAL3 Detailed Test Plan. The scope of the developer tests included all TOE Security Functions.

The developer testing addresses the following security functionality claimed by the TOE: ssh communications, acl, demonstrates user lockout collaboration between the TOE device and ACS server, logging messages to the ACS server using Radius or TACACS+, syslog connections and also capabilities of the TOE to maintain audit records in the local buffer, ability of the AAA subsystem to authenticate users for console login using username/password configured locally on the switch, attributes of a user and proving that a user cannot do any TSF mediated actions prior to identification and authentication, ability of administrators to carry out management functions, and traffic-filtering requirements.

See Appendices, Switch modules, which identify the individual modules that can compose the evaluated product.

The evaluation team determined that the developer's test methodology met the coverage and depth requirements and that the actual test results matched the expected results.

7.2 Evaluation Team Independent Testing

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 developer test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team also ensured that all subsystem interfaces were tested by the developer by creating a mapping of test cases to subsystem and SFR's.

The evaluation team performed a sample of the developer's test suite and devised an independent set of team tests and penetration tests. The evaluation team reran a subset of the developer's test suite that tested all TSF, and 24 SFRs.

The evaluation team also performed a penetration flaw hypothesis analysis of the product to prepare for a penetration testing effort. The analysis examined each SFR to determine whether it was possible that the evaluated configuration could be susceptible to a vulnerability. The specific penetration tests executed include the following:

- Use a port scanner against the target network device to determine whether the target device may have different services listening on multiple TCP/IP-enabled interfaces and scanned each type of interface Checked for open ports on the target host/device.
- Test the different privilege levels and granting command access to the different levels.
- Test potential abuse privilege levels using the "autocommand" command.
- Checked for known vulnerabilities on the target host/device using nessus.
- Test potential misuse of the "kron" command to run commands as another user.

The evaluation team constructed and ran each of the identified tests. The results of the penetration test execution verified that none of the hypothesized flaws was exploitable.

8 Evaluated Configuration

The evaluated configuration was tested in the configuration identified in Figure 2, below. The evaluation results are valid for all configurations of the TOE identified in section 4 of this report.

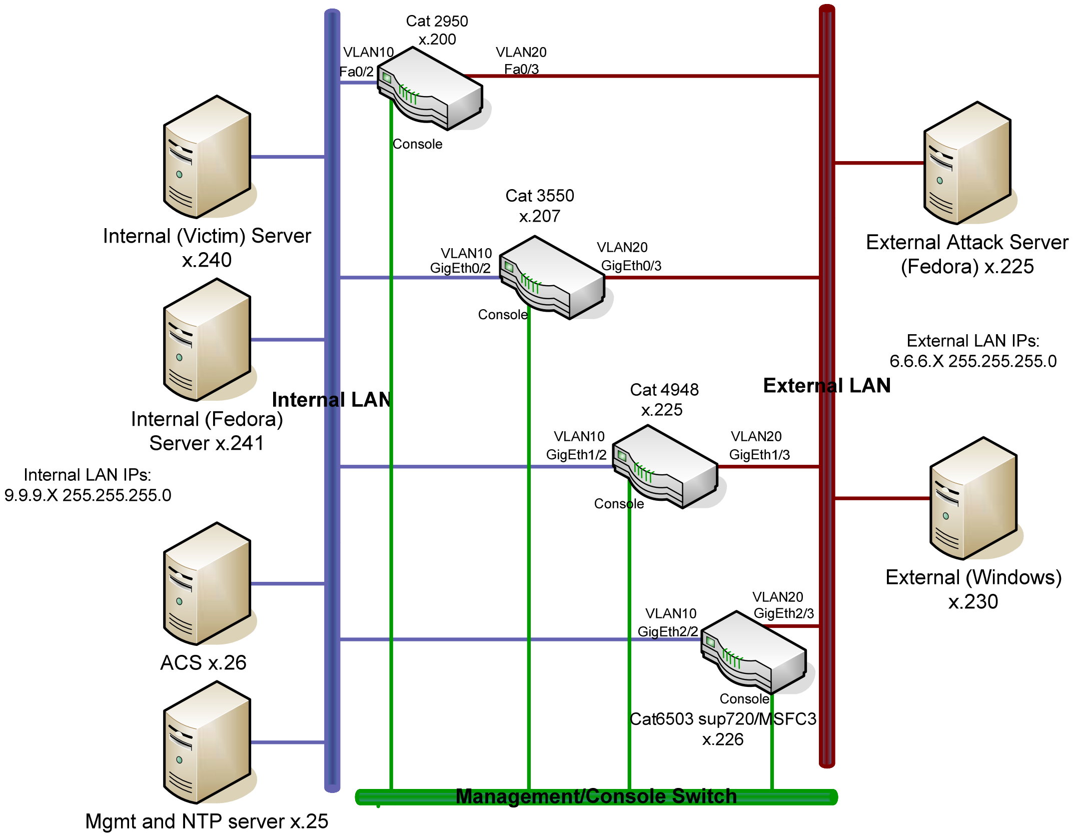


Figure 2: Testing Environment

Table 6: Hardware and Software Components Tested

IOS Version	Models in TOE	Tested by CCTL	Switch Type
• 12.1(22)EA10	• 2940 • 2950 • 2950RLE • 2955	2950	Layer 2

IOS Version	Models in TOE	Tested by CCTL	Switch Type
• 12.2(25)SEE4	• 2960 • 2970 • 3550 • 3560 • 3750 • 3750-METRO	3550	Layer 2
• 12.2(31)SG2	• 4500-SUP2-PLUS • 4500-SUP2-PLUS-10GE • 4500-SUP2-PLUS-TS • 4500-SUP4 • 4500-SUP5 • 4500-SUP5-10GE • 4948 • 4948-10GE	4948	Layer 2 & 3
• 12.2(18)SXF11	• 6500-SUP2/MSFC2 • 6500-SUP32/MSFC2A • 6500-SUP720/MSFC3	6503-SUP720/MSFC3	Layer 2 & 3

9 Validator Comments

The validator has reviewed the evaluation technical report and agrees with the conclusion of this evaluation. The customer is reminded that the following were not included within the scope of the evaluation.

- There are no Protection Profile compliance claims.
- The TOE does not address encryption (IPSec), VPNs, or Quality of Service (QoS).
- The ACS Server hardware and Windows 2000 Server (ACS Server OS) are not part of the TOE.
- The TOE can optionally connect to an NTP server on its internal network for time services. Also, if the Catalyst Switch or ACS Server are to be remotely administered, then the management station must be connected to an internal network. SSH must be used to connect to the switch, and SSL must be used to connect to the ACS. The ACS, remote management, and NTP boxes (if used) must all be attached to the internal (trusted) network.
- The Cisco IOS contains a collection of features that build on the core components of the system. Those features that are not to be used include the HTTP Server, the IEEE 802.11 Wireless Standards, MAC address filtering, SNMP, Telnet, and VPN.

10 Security Target

Cisco Systems Catalyst Switches EAL3 Security Target, Version 1.7, February 27, 2008.

11 List of Acronyms

ACL	Access Control List
API	Application Programming Interface
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme (US CC Validation Scheme)
CCIMB	Common Criteria Implementation Board
CCTL	Common Criteria Testing laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CMS	Certificate Management System
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ID	Identifier
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
RFC	Request for Comment
SAR	Security Functional Requirement
SFR	Security Assurance Requirement
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target Of Evaluation
TSF	TOE Security Function
URL	Uniform Resource Locator
VR	Validation Report

12 Bibliography

The following documents referenced during preparation of the validation report.

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

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

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

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

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

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated January 2004, Version 2.2.

[7] Security Target for Cisco Systems Catalyst Switches EAL3, Version 1-5, November 21, 2007.

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

[9] Cisco IOS Catalyst Switches EAL3 Detailed Test Plan Version 1.11, November 21, 2007

[10] Installation and Configuration for Common Criteria EAL3 Evaluated Cisco IOS/AAA Switches, version 0-11, November 2007 .

13 Interpretations

13.1 International Interpretations

Official start date of the evaluation was February 25, 2004. The evaluation team performed an analysis of the international interpretations and applied those that were applicable and had impact to the TOE evaluation as the CEM work units were applied.

The following international interpretations were applied for this evaluation:

- The TOE is also compliant with all International interpretations with effective dates on or before Feb 25, 2004

13.2 Interpretations Validation

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

- The TOE is also compliant with all International interpretations with effective dates on or before Feb 25, 2004

Appendix A.1: Catalyst 4500 Modules

- WS-F4531-Cisco Catalyst 4500 NetFlow Services Daughter Card
- WS-X4148-FE-LX-MT-Cisco Catalyst 4500 Fast Ethernet Switching Module, 48-port 100BASE-LX10 single-mode fiber (SMF) (MT-RJ)
- WS-X4148-FE-BD-LC-Cisco Catalyst 4500 Fast Ethernet Switching Module, 48-port 100BASE-BX-D SMF (LC)
- WS-X4124-FX-MT-Cisco Catalyst 4000 Fast Ethernet Switching Module, 24-port 100BASE-FX (MT-RJ)
- WS-X4148-FX-MT-Cisco Catalyst 4500 Fast Ethernet Switching Module, 48-port 100BASE-FX multimode fiber (MMF) (MT-RJ)
- WS-X4124-RJ45-Cisco Catalyst 4500 10/100 Module, 24-port (RJ-45)
- WS-X4148-RJ-Cisco Catalyst 4500 10/100 Module, 48-port (RJ-45)
- WS-X4148-RJ21-Cisco Catalyst 4500 10/100 Module, 48-port telco (4 x RJ-21)
- WS-X4248-RJ21V-Cisco Catalyst 4500 PoE 802.3af 10/100, 48-port (RJ-21)
- WS-X4148-RJ45V-Cisco Catalyst 4500 Cisco prestandard PoE 10/100, 48-port (RJ-45)
- WS-X4224-RJ45V-Cisco Catalyst 4500 PoE 803.3af 10/100, 24-port (RJ-45)
- WS-X4248-RJ45V-Cisco Catalyst 4500 PoE 802.3af 10/100, 48-port (RJ-45)
- WS-X4232-GB-RJ-Cisco Catalyst 4500 32-port 10/100 (RJ-45), 2-Gigabit Ethernet (GBIC) Module
- WS-X4232-RJ-XX-Cisco Catalyst 4500 32-port 10/100 (RJ-45), plus modular uplink slot
- WS-U4504-FX-MT-Cisco Catalyst 4500 Fast Ethernet Uplink Daughter Card for WS-X4232-RJ-XX, 4-port 100BASE-FX (MT-RJ)
- WS-X4302-GB-Cisco Catalyst 4500 Gigabit Ethernet Module, 2-port (GBIC)
- WS-X4306-GB-Cisco Catalyst 4500 Gigabit Ethernet Module, 6-port (GBIC)
- WS-X4506-GB-T-Cisco Catalyst 4500 Gigabit Ethernet Module, 6-port 10/100/1000 802.3af PoE or 1000BASE-X (SFP)
- WS-X4418-GB-Cisco Catalyst 4500 Gigabit Ethernet Module, server switching 18-port (GBIC)
- WS-X4448-GB-LX-Cisco Catalyst 4500 48-Port 1000BASE-LX (SFP optics included)
- WS-X4448-GB-SFP-Catalyst 4500 Gigabit Ethernet Module, 48-Port 1000BASE-X (optional SFP optics)
- WS-X4424-GB-RJ45-Cisco Catalyst 4500 24-Port 10/100/1000 Module (RJ-45)
- WS-X4448-GB-RJ45-Cisco Catalyst 4500 48-Port 10/100/1000 Module (RJ-45)
- WS-X4548-GB-RJ45-Cisco Catalyst 4500 Enhanced 48-Port 10/100/1000 Module (RJ-45)
- WS-X4524-GB-RJ45V-Cisco Catalyst 4500 PoE 802.3af 10/100/1000, 24-port (RJ-45)
- WS-X4548-GB-RJ45V-Cisco Catalyst 4500 PoE 802.3af 10/100/1000, 48-port (RJ-45)
- WS-G5483-Cisco 1000BASE-T GBIC
- WS-G5484-Cisco 1000BASE-SX Short-Wavelength GBIC (multimode only)
- WS-G5486-Cisco 1000BASE-LX/LH Long-Haul GBIC (single-mode or multimode)
- WS-G5487-Cisco 1000BASE-ZX Extended-Reach GBIC (single-mode)

- GLC-T-1000BASE-T SFP
- GLC-SC-MM-GE SFP, LC connector SX transceiver
- GLC-LH-SM-GE SFP, LC connector LX/LH transceiver
- GLC-ZX-SM-1000BASE-ZX SFP
- Cisco CWDM GBIC solution
- Cisco CWDM SFP solution
- X2 Optic Support

Appendix A.2: Catalyst 6500 Modules

Supervisor Modules

Product Number	Description
WS-X6K-S1A-MSFC2	Cisco Catalyst 6500 Supervisor Engine1A, 2GE, plus MSFC-2 and PFC
WS-X6K-S2-PFC2	Cisco Catalyst 6500 Supervisor Engine 2, 2GE, plus PFC-2
WS-X6K-S2-MSFC2	Cisco Catalyst 6500 Supervisor Engine 2, 2GE, plus MSFC-2/PFC-2
WS-X6K-S1A-MSFC2	Supervisor Engine 1A with PFC+MSFC2
WS-X6K-S1A-MSFC2=	Supervisor Engine 1A with PFC+MSFC2=
WS-X6K-S1A-MSFC2/2	Supervisor Engine 1A with PFC+MSFC2/2
WS-SUP720-3BXL	Catalyst 6500/Cisco 7600 Supervisor 720 Fabric MSFC3 PFC3BXL
WS-SUP720-3B	Catalyst 6500/Cisco 7600 Supervisor 720 Fabric MSFC3 PFC3B
WS-SUP720	Catalyst 6500/Cisco 7600 Supervisor 720 Fabric MSFC3 PFC3A

Optical Services Modules

Optical services modules (OSMs) are line cards that provide high-speed WAN connectivity with onboard network processors for distributed-line-rate IP services applications. For more information about OSMs, see the following data sheets:

Product Number	Description
WS-X6148-FE-SFP	Cisco Catalyst 6500 48-port 100BASE-X Classic Interface Module (requires SFPs)
WS-X6524-100FX-MM	Cisco Catalyst 6500 24-port, CEF256 100BASE-FX Interface Module, multimode fiber, MT-RJ field-upgradable to support distributed forwarding with the addition of the distributed forwarding daughter card (part number WS-F6K-DFC= or WS-F6K-DFC3A= or WS-F6K-DFC3B= or WS-F6K-DFC3BXL=)
WS-X6324-100FX-MM	Cisco Catalyst 6500 24-port 100BASE-FX Classic Interface Module, multimode fiber, MT-RJ

WS-X6324-100FX-SM	Cisco Catalyst 6500 24-port, 100BASE-FX Classic Interface Module, single-mode fiber, MT-RJ
WS-X6024-10FL-MT	Cisco Catalyst 6500 24-port 10BASE-FL Classic Interface Module, multimode fiber, MT-RJ

Ethernet Interface Modules

Cisco Catalyst 6500 Series Ethernet interface modules, designed for wiring closet, distribution and core, and data center applications, as well as service provider and Metro Ethernet environments, use one of the following types of Ethernet interfaces:

- 10/100 Mbps over copper-For wiring closets providing 10/100-Mbps performance with autonegotiation and support for IEEE 802.3af PoE (inline power); up to 96 ports per module; includes Classic and CEF256 interface modules.
- 10/100/1000 Mbps Gigabit over copper-For wiring closets and data centers providing 10/100/1000-Mbps performance with autonegotiation and support for IEEE 802.3af PoE (inline power); up to 48 ports/module; includes Classic, CEF256, and CEF720 interface modules.
- 100 Mbps over fiber-For secure wiring closets and long-haul router and switch interconnects; up to 24 ports per module; includes Classic and CEF256 interface modules.
- 1 Gbps-For distribution and core layers and for data centers providing 1 Gbps performance; up to 48 ports per module; includes Classic, CEF256, dCEF256, and CEF720 interface modules.
- 10 Gbps-For distribution and core layers providing 10 Gbps performance in 2-port or 4-port modules; includes CEF256 and dCEF720 interface modules.

Product Number	**Description**
WS-X6748-SFP	48 port High Performance Mixed Media Gigabit Ethernet interface module, Requires SFPCEF720
WS-X6724-SFP	24 port High Performance Mixed Media Gigabit Ethernet interface module, Requires SFP CEF720
WS-F6700-DFC3BXL	Distributed Forwarding Card-3BXL Upgrade for WS-X67xx linecards using WS-SUP720-3BXL
WS-F6700-DFC3B	Distributed Forwarding Card-3B Upgrade for WS-X67xx linecards using WS-SUP720-3B
WS-F6700-DFC3A	Distributed Forwarding Card-3A Upgrade for WS-X67xx linecards using WS-SUP720
WS-X6816-GBIC	16 port dCEF256 Gigabit Ethernet interface module for the Cisco Catalyst 6500 Series switches with dual fabric channel interfaces and distributed forwarding requires GBICs and distributed forwarding card
WS-F6K-DFC3A	Distributed forwarding Card-3A for 65xx, 6816 Modules used with SUP720

Product Number	Description
WS-F6K-DFC	Distributed forwarding Card for 65xx, 6816 Modules used with SUP2

Product Number	Description
10/100/1000	
WS-X6748-GE-TX	Cisco Catalyst 6500 Series 48-Port 10/100/1000 RJ-45 Cisco Express Forwarding 720 Interface Module; field-upgradeable to support distributed forwarding with the addition of the distributed forwarding daughter card (part number WS-F6700-DFC3A=)
WS-X6548-GE-TX	Cisco Catalyst 6500 Series 48-Port 10/100/1000 RJ-45 Cisco Express Forwarding 256 Interface Module; field-upgradable to support Cisco Prestandard PoE daughter card (part number WS-F6K-VPWR-GE=) or 802.3af PoE daughter card (part number WS-F6K-GE48-AF=)
WS-X6548-GE-45AF	Cisco Catalyst 6500 Series 48-Port 10/100/1000 RJ-45 Cisco Express Forwarding 256 Interface Module with 802.3af PoE daughter card (that is, includes daughter card [part number WS-F6K-GE48-AF=])
WS-X6548V-GE-TX	Cisco Catalyst 6500 Series 48-Port 10/100/1000 RJ-45 Cisco Express Forwarding 256 Interface Module with Cisco Prestandard PoE Daughter Card (that is, includes daughter card [part number WS-F6K-VPWR-GE=])
WS-X6516-GE-TX	Cisco Catalyst 6500 Series 16-Port 10/100/1000 RJ-45 Cisco Express Forwarding 256 Interface Module; field-upgradable to support distributed forwarding with the addition of the distributed forwarding daughter card (part number WS-F6K-DFC= or DFC3)
WS-X6148A-GE-TX	Cisco Catalyst 6500 Series 48-Port 10/100/1000 RJ-45 Classic Interface Module; field-upgradable to support 802.3af PoE daughter card (part number WS-F6K-GE48-AF=)
WS-X6148-GE-TX	Cisco Catalyst 6500 Series 48-Port 10/100/1000 RJ-45 Classic Interface Module; field-upgradable to support Cisco Prestandard PoE Daughter Card (part number WS-F6K-VPWR-GE=) or 802.3af PoE daughter card (part number WS-F6K-GE48-AF=)
WS-X6148A-GE-45AF	Cisco Catalyst 6500 Series 48-Port 10/100/1000 RJ-45 Classic Interface Module with 802.3af PoE daughter card (that is, includes daughter card (part number WS-F6K-GE48-AF=)
WS-X6148-GE-45AF	Cisco Catalyst 6500 Series 48-Port 10/100/1000 RJ-45 Classic Interface Module with 802.3af PoE daughter card (that is, includes daughter card (part number WS-F6K-GE48-AF=)
WS-X6148V-GE-TX	Cisco Catalyst 6500 Series 48-Port 10/100/1000 RJ-45 Classic Interface Module with Cisco Prestandard PoE Daughter Card (that is, includes daughter card (part number WS-F6K-VPWR-GE=)
10/100	

Product Number	Description
WS-X6548-RJ-45	Cisco Catalyst 6500 Series 48-Port Cisco Express Forwarding 256 10/100 RJ-45 Interface Module; field-upgradable to support distributed forwarding with the addition of the distributed forwarding daughter card (part number WS-F6K-DFC= or DFC3)
WS-X6548-RJ-21	Cisco Catalyst 6500 Series 48-Port, Cisco Express Forwarding 256 10/100 RJ-21 Interface Module; field-upgradable to support distributed forwarding with the addition of the distributed forwarding daughter card (part number WS-F6K-DFC= or DFC3)
WS-X6348-RJ45	Cisco Catalyst 6500 Series 48-Port 10/100 RJ-45 Classic Interface Module; field-upgradable to support Cisco Prestandard PoE Daughter Card (part number WS-F6K-VPWR=)
WS-X6348-RJ45V	Cisco Catalyst 6500 Series 48-Port 10/100 RJ-45 Classic Interface Module with Cisco Prestandard PoE Daughter Card (that is, includes daughter card [part number WS-F6K-VPWR=])
WS-X6348-RJ21V	Cisco Catalyst 6500 Series 48-Port 10/100 RJ-21 Classic Interface Module with Cisco Prestandard PoE Daughter Card (that is, includes daughter card [part number WS-F6K-VPWR=])
WS-X6148X2-RJ-45	Cisco Catalyst 6500 Series 96-Port 10/100 RJ-45 Classic Interface Module; field-upgradable to support 802.3af PoE daughter card (part number WS-F6K-FE48X2-AF=)
WS-X6148X2-45AF	Cisco Catalyst 6500 Series 96-Port 10/100 RJ-45 Classic Interface Module with 802.3af PoE daughter card (that is, includes daughter card [part number WS-F6K-FE48X2-AF=])
WS-X6196-RJ-21	Cisco Catalyst 6500 Series 48-Port 10/100 RJ-21 Classic Interface Module; field-upgradable to support 802.3af PoE daughter card (part number WS-F6K-FE48X2-AF=)
WS-X6196-21AF	Cisco Catalyst 6500 Series 96-Port 10/100 RJ-21Classic Interface Module with 802.3af PoE daughter card (that is, includes daughter card [part number WS-F6K-FE48X2-AF=])
WS-X6148A-RJ-45	Cisco Catalyst 6500 Series 48-Port 10/100 RJ-45 Classic Interface Module; field-upgradable to support 802.3af PoE daughter card (part number WS-F6K-GE48-AF=)
WS-X6148-RJ-45	Cisco Catalyst 6500 Series 48-Port 10/100 RJ-45 Classic Interface Module; upgradable to support Cisco Prestandard PoE Daughter Card (part number WS-F6K-VPWR=) or to IEEE 802.3af PoE daughter card (part number WS-X6148-45AF-UG=)
WS-X6148A-45AF	Cisco Catalyst 6500 Series 48-Port 10/100 RJ-45 Classic Interface Module with IEEE 802.3af PoE daughter card
WS-X6148-45AF	Cisco Catalyst 6500 Series 48-Port 10/100 RJ-45 Classic Interface Module with IEEE 802.3af PoE daughter card
WS-X6148-RJ45V	Cisco Catalyst 6500 Series 48-Port 10/100 RJ-45 Classic Interface Module with Cisco Prestandard PoE Daughter Card (that is, includes daughter card [part number WS-F6K-VPWR=])

Product Number	Description
WS-X6148-RJ-21	Cisco Catalyst 6500 Series 48-Port 10/100 RJ-21 Classic Interface Module; upgradable to support Cisco Prestandard PoE Daughter Card (part number WS-F6K-VPWR=) or to IEEE 802.3af PoE daughter card (part number WS-X6148-21AF-UG=)
WS-X6148-21AF	Cisco Catalyst 6500 Series 48-Port 10/100 RJ-21 Classic Interface Module with IEEE 802.3af PoE daughter card
WS-X6148-RJ21V	Cisco Catalyst 6500 Series 48-Port 10/100 RJ-21 Classic Interface Module with Cisco Prestandard PoE Daughter Card (that is, includes daughter card [part number WS-F6K-VPWR=])

Cisco Catalyst 6500 Series Power Over Ethernet Daughter Cards

Part Number	Description
WS-F6K-GE48-AF=	Cisco Catalyst 6500 Series 802.3af PoE Daughter Card for 10/100/1000 modules (part numbers WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6548-GE-TX, and WS-X6548V-GE-TX)
WS-F6K-FE48X2-AF=	Cisco Catalyst 6500 Series 802.3af PoE Daughter Card for WS-X6148X2-RJ-45) module
WS-X6148-45AF-UG=	Cisco Catalyst 6500 Series 802.3af PoE Advanced Upgrade for (part number WS-X6148-RJ45 or WS-X6148-RJ45V)
WS-X6148-21AF-UG=	Cisco Catalyst 6500 Series 802.3af PoE Advanced Upgrade for (part number WS-X6148-RJ21 or WS-X6148-RJ21V)
WS-F6K-VPWR=	Cisco Catalyst 6500 Series Cisco Prestandard PoE Daughter Card for 10/100 modules (for WS-X6148-RJxx and WS-X6348-xx)
WS-F6K-VPWR-GE=	Cisco Catalyst 6500 Series Cisco Prestandard PoE Daughter Card for 10/100/1000 modules (part numbers WS-X6148-GE-TX and WS-X6548-GE-TX)

Cisco Catalyst 6500 Series 10/100 and 100/1000 Distributed Forwarding Cards

Part Number	Description
WS-F6K-DFC	Cisco Catalyst 6500 Series DFC3A for Cisco Catalyst 6500 Series; Cisco Catalyst 6816 modules used with Supervisor Engine 2
WS-F6K-DFC3A	Cisco Catalyst 6500 Series DFC3A for Cisco Catalyst 6500; Cisco Catalyst 6816 modules used with Supervisor Engine 720
WS-F6K-DFC3B	Cisco Catalyst 6500 Series DFC3B for Cisco Catalyst 6500; Cisco Catalyst 6816 modules used with Supervisor Engine 720
WS-F6K-DFC3BXL	Cisco Catalyst 6500 Series DFC3BXL for Cisco Catalyst 6500; Cisco Catalyst 6816 modules used with Supervisor Engine 720
MEM-DFC-256MB	256 MB DRAM option for DFC
MEM-DFC-512MB	512 MB DRAM option for DFC

Part Number	Description
WS-F6700-DFC3A	Cisco Catalyst 6500 Series DFC3A for Cisco Catalyst 6700 Series modules
WS-F6700-DFC3B	Cisco Catalyst 6500 Series DFC3B for Cisco Catalyst 6700 Series modules
WS-F6700-DFC3BXL	Cisco Catalyst 6500 Series DFC3BXL for Cisco Catalyst 6700 Series modules

WAN Interface Modules

The Cisco Catalyst 6500 Series and Cisco 7600 Series support several WAN interfaces using two technologies:

- FlexWAN module-Accepts up to two plug-in port adapters that provide numerous WAN/MAN protocols and features
- Optical services module (OSM)-A dedicated line card that provides several interfaces, including OC-3/STM-1, OC-12/STM-4, OC-48/STM-16, Channelized T3, Channelized OC-12/STM-4 PoS, Gigabit Ethernet, OC-12/STM-4 ATM, and OC-48/STM-16 DPT

FlexWAN Module

The FlexWAN module fits inside Cisco Catalyst 6500 Series and Cisco 7600 Series systems and uses Cisco 7200 Series and 7500 Series port adapters for several WAN/MAN protocols, including Frame Relay, ATM, PoS, Point-to-Point Protocol (PPP), and High-Level Data Link Control (HDLC). Additionally, the FlexWAN module provides media options such as clear channel and Channelized T1/E1, T3/E3, High-Speed Serial Interface (HSSI), OC-3 PoS, and ATM.