



Cisco Catalyst Operating System Software Version 7.5(1) for the Cisco Catalyst 6500 Series and Cisco Catalyst 4000 Family Switches

The Cisco Catalyst[®] Operating System (Catalyst OS) Software Version 7.5(1) for the supervisor engine supports the Cisco Catalyst 6500 Series and Cisco Catalyst 4000/4500 Series multilayer switches (including the Cisco Catalyst 2948G, 4912G, and 2980G-A switches).

Hardware Supported

The Cisco Catalyst OS Software version 7.5(1) supports all the modules that the Cisco Catalyst OS previously supported on the Cisco Catalyst 6500 and Catalyst 4000/4500 series supervisor engines. In addition, the Cisco Catalyst OS Software version 7.5(1) supports the Cisco Catalyst 6500 Series hardware listed in Table 1.

Table 1 Hardware Supported on the Cisco Catalyst 6500 Series Switches in Version 7.5(1)

Hardware	Description
Firewall Services Module (FWSM) WS-SVC-FWM-1-K9	<p>The FWSM is a high-speed integrated firewall module for the Cisco Catalyst 6500 Series switches that provides data throughput up to 5 Gbps, 100,000 connections per second, and 1 million concurrent connections. Up to four firewall modules can be installed in a single chassis providing scalability to 20 Gbps per chassis. As part of the industry-leading Cisco PIX[®] firewalls, the FWSM provides enterprises and service providers with superior security, reliability, and performance.</p> <p>The FWSM is commonly deployed in Internet edge environments and between corporate and Internet data centers, and the LAN and WAN.</p> <p>Notes:</p> <p>Requires Cisco Catalyst 6000 Multilayer Switch Feature Card MSFC2 and Cisco IOS Software for the MSFC2 Release 12.1(13)E3.</p> <p>Currently supported only on Supervisor Engine 2 in hybrid configurations.</p>



Table 1 Hardware Supported on the Cisco Catalyst 6500 Series Switches in Version 7.5(1)

Hardware	Description
Secure Sockets Layer (SSL) Services Module WS-SVC-SSL-1-K9	<p>Integrated service module for the Cisco Catalyst 6500 Series that offloads the processor-intensive tasks related to securing traffic with SSL and thus increases the number of secure connections supported by a Web site. Offering 3000 connection setups per second per module (12,000 per chassis) and 300-Mbps bulk encrypted throughput per module (1.2 Gbps per chassis) while maintaining 60,000 concurrent client connections (200,000 per chassis), the SSL Services Module provides the fastest session setup rates and bulk encrypted throughput in the industry.</p> <p>The SSL module is commonly deployed with a Content Switching Module (CSM) to scale the performance and improve the persistence mechanisms and manageability of a Web site.</p> <p>Notes: Up to four SSL modules supported in a single chassis. Requires Cisco MSFC2 and Cisco IOS for the MSFC2 Software Release 12.1(13)E3.</p> <p>Currently supported only on Supervisor Engine 2 in hybrid configurations.</p> <p>Hardware FCS January, 2003.</p>
CSM WS-X6066-SLB-APC	<p>The CSM integrates advanced Layer 4 – Layer 7 content switching into the Cisco Catalyst 6500 Series to provide high-performance, high-availability load balancing, while taking advantage of the Catalyst support of Layer 2 and Layer 3 switching. With features such as full regular expression support, full stateful redundancy, server and firewall load balancing, configurable network address translation (NAT), virtual private networking (VPN) and IPsec load balancing, HTTP 1.1 persistence support, sticky connections, and many load balancing predictors, the CSM provides the flexibility to improve the performance and reliability of most network infrastructures.</p> <p>The CSM is commonly deployed with the SSL Services Module in the Internet-corporate data center.</p> <p>Note: Requires Cisco MSFC2 and Cisco IOS for the MSFC2 Release 12.1(13)E3.</p>
Intrusion Detection System Module 2 (IDSM2) WS-SVC-IDSM2-BUN-K9	<p>The IDSM2 is an integrated services module for the Cisco Catalyst 6500 Series chassis offering performance speeds of 400 Mbps. The IDSM2 detects unauthorized activity traversing the network by analyzing traffic in real time, helping enable users to quickly respond to security breaches.</p>
ATA Flash Card Support MEM-C6K-ATA-1-64M	<p>Support for 64 MB ATA Flash (Type I and Type II) on Supervisor Engine 2, allowing the storage of more backup images.</p> <p>Note: Requires ROM Monitor (ROMMON) version 7.1 or later.</p>

Note: There is no new hardware for the Cisco Catalyst 4000/4500 Series switches in this release.



Software Features

The Catalyst OS Software version 7.5(1) supports all software features previously supported by the Cisco Catalyst OS Software Version 7.4(1) on the Cisco Catalyst 6500 and 4000/4500 series supervisor engines. In addition, the Cisco Catalyst OS Software version 7.5(1) supports the software features listed in Table 2.

Table 2 Software Features of Cisco Catalyst OS Software Version 7.5(1)

Software Feature	Description	Cisco Catalyst 6500 Feature	Cisco Catalyst 4000 Feature
IEEE 802.1x with Port Security	Allows port security to be configured on an 802.1x-enabled port. If port security is enabled for only one Media Access Control (MAC) address on a port, only that MAC address will authenticate via the Remote Authentication Dial-In User Service (RADIUS) server. All other MAC addresses will be denied access to the network, which eliminates the security risk of additional users attaching to a hub to bypass authentication. When 802.1x and port security are enabled in the multiple authentication mode, all hosts attempting to connect through a switch port will be required to authenticate using 802.1x.	X	
IEEE 802.1x operation with voice VLAN Identification (VVID)	Helps enable organizations to combine the benefits of Cisco AVVID (Architecture for Voice, Video and Integrated Data) voice over IP (VoIP), and dynamic port security. Users can configure the auxiliary VLAN feature on an 802.1x port and vice versa. When the switch recognizes a phone is attached to a port via CDP, it allows phone traffic on the auxiliary VLAN without 802.1x authentication. Then, the PC or Workstation connected (behind the phone) to the 802.1x port of the switch will use the port VLAN ID and authenticate following the dot1x protocol. The IP phone connected to the 802.1x port will use the VVID of the port for its voice traffic independent of whether the 802.1x port status is authorized or unauthorized.	X	
IEEE 802.1x with guest VLAN	Enables organizations to offer restricted "guest" network access. With this feature enabled, users are placed into the Guest VLAN if they fail authentication or if a non-802.1x client is connected to an 802.1x-enabled port. The guest VLAN is configured globally from the normal or extended VLAN range.	X	
High availability for IEEE 802.1x	This feature offers synchronization of runtime information between active and standby supervisors so that the 802.1x port state, either authorized or unauthorized, is maintained during a high-availability switchover.	X	



Table 2 Software Features of Cisco Catalyst OS Software Version 7.5(1)

Software Feature	Description	Cisco Catalyst 6500 Feature	Cisco Catalyst 4000 Feature
High availability for port security	<p>Port security is used to block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC address of the station attempting to access the port is different from any of the MAC addresses specified for that port. Alternatively, it is used to filter traffic destined to or received from a specific host based on the host MAC address.</p> <p>High-availability with port security ensures that the port-security database is synchronized from the active supervisor engine to the standby supervisor engine during a supervisor switchover. This allows the new active supervisor engine to take over from the latest protocol state, rather than restarting.</p>	X	
AutoQoS	<p>AutoQoS is a feature that simplifies quality of service (QoS) configuration for voice-enabled switches. When issued, the autoqos command on the Cisco Catalyst 6500 Series switch will dynamically set QoS parameters on the switch ports according to Cisco best practice recommendations.</p> <p>AutoQoS consists of two macros. The first covers all the related QoS configurations required for implementing the recommended Cisco AVVID settings for a voice port (AutoQoS). The second macro is a superset of the first, configuring all features required for a Cisco IP Phone to work properly on the Catalyst 6500 platform.</p> <p>When the AutoQoS commands are issued, VoIP-QoS configurations are automated and the script intelligence allows voice traffic to be prioritized appropriately.</p>	X	
Rapid PVST+	<p>Per-VLAN Rapid Spanning Tree (PVRST+), also known as Rapid PVST+, provides the ability to apply rapid spanning tree convergence on a per-VLAN basis. Prior to this software release, achieving rapid spanning tree convergence was done by implementing IEEE 802.1s, Multiple Instance Spanning Tree, and IEEE 802.1w, Rapid Spanning Tree, protocols. There was not a means to achieve the Rapid Spanning Tree convergence on a per-VLAN basis prior to Cisco Catalyst OS Software version 7.5(1).</p> <p>This eases the overall deployment for customers familiar with the operation of IEEE 802.1d Spanning Tree and Per VLAN Spanning Tree implementations common in most enterprises and service provider environments.</p>	X	X



Table 2 Software Features of Cisco Catalyst OS Software Version 7.5(1)

Software Feature	Description	Cisco Catalyst 6500 Feature	Cisco Catalyst 4000 Feature
Address Resolution Protocol (ARP) inspection	<p>Prevents ARP spoofing and “man-in-the-middle” attacks by ensuring an attacker cannot hijack the default gateway address of a user so as to intercept all of the user’s data. ARP inspection prevents malicious users from impersonating other hosts or routers by inspecting all ARP packets. It provides the network administrator the ability to configure a set of order-dependent rules within the security access control list (ACL) framework, to prevent the attack described above.</p> <p>If an ARP inspection specific rule exists in the security ACL on a VLAN, all ARP packets will be directed to the CPU (through Access Control Entries, ACEs, in the VACL). These packets would be inspected by the ARP validation task for conformance to the specified rules. Conforming packets will be forwarded, while non-conforming packets will be dropped and possibly logged.</p> <p>Note: Supported only on the Supervisor Engine 2.</p>	X	
SC1 interface	<p>The sc1 interface is a second management interface on the Cisco Catalyst 6500 Series Switch similar to the existing sc0 interface. Using the inband port on the chassis, the sc1 is a valid interface for image downloads, outgoing ping and telnet, and Simple Network Management Protocol (SNMP) functions.</p>	X	
Internet Group Management Protocol v3 (IGMPv3)	<p>IGMP is used by hosts and routers to report their IP multicast group membership to neighboring multicast routers. IGMPv3 adds support for source-based filtering which allows systems to report interest in packets from a specified source, and eliminate the <i>leave group</i> message. IGMPv3 snooping is backward compatible with IGMPv1 and IGMPv2 snooping.</p>	X	



Table 2 Software Features of Cisco Catalyst OS Software Version 7.5(1)

Software Feature	Description	Cisco Catalyst 6500 Feature	Cisco Catalyst 4000 Feature
Network-Based Application Recognition (NBAR) in software	<p>NBAR is used to classify IP unicast traffic into application specific flows. It determines which protocols and applications are currently running on a network so that an appropriate QoS policy can be created based on the current traffic mix and application requirements.</p> <p>NBAR is capable of classifying packets belonging to the following four types of protocols/applications:</p> <ul style="list-style-type: none"> • Non-UDP and non-TCP/IP protocols; for example, ICMP, IPSec • TCP and UDP protocols that use statically assigned port numbers; for example, telnet, HTTP • TCP and UDP protocols that dynamically assign port numbers and require stateful inspection of the flow; for example, FTP, MS Exchange • TCP and UDP protocols that dynamically assign port numbers and require stateful inspection of the flow; for example, FTP, MS Exchange • Heuristic or Holistic classification; for example, Real-Time Transport Protocol (RTP) payload classified by multiple criteria <p>The classification information can be used for several purposes, such as QoS policing, traffic shaping, and Class-based Weighted Fair Queuing and identifying viruses such as NIMDA.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Requires Cisco IOS Software on the MSFC2 Release 12.1(13)E • Traffic on NBAR-enabled interfaces is software switched • Supported only on Supervisor 2 with an MSFC2 	X	
Local username/password	<p>Prior to release 7.5(1), Cisco Catalyst OS provided authentication of users by using TACACS, RADIUS or KERBEROS and local authentication was limited to authentication for normal mode and enable mode.</p> <p>Local username/password provides the switch administrators the ability to create and manage users local to a switch. Users are created with privilege levels of either 0 or 15. Users with privilege level 0 are restricted to access commands in "normal mode" and users with privilege level 15 have access to commands in "enable mode."</p> <p>A maximum of 25 local users can be created. Once this feature is enabled, the console and telnet processes will prompt for "local username" followed by a prompt for "password."</p>	X	X



Table 2 Software Features of Cisco Catalyst OS Software Version 7.5(1)

Software Feature	Description	Cisco Catalyst 6500 Feature	Cisco Catalyst 4000 Feature
Port unicast block	<p>Port Unicast Block enables a user to block unicast flooding on a per-port basis. By default, all Ethernet ports are configured to allow unicast flooding. When port security is enabled and MAC addresses are learned, the unicast flooded packets to this port can be blocked.</p> <p>This is accomplished by configuring the “port security” port to <i>blocking</i> mode. Once the address count on the port reaches the maximum threshold count, and the port is in blocking mode, unicast flooding is blocked.</p>	X	X
High availability for port security	<p>Port Security is used to block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC address of the station attempting to access the port is different from any of the MAC addresses specified for that port. Alternatively, it is used to filter traffic destined to or received from a specific host based on the host MAC address.</p> <p>High availability with port security ensures that the port-security database is synchronized from the active supervisor engine to the standby supervisor engine during a supervisor switchover. This allows the new active supervisor engine to take over from the latest protocol state, rather than restarting.</p>	X	
802.1q all tagged per port	<p>The Dot1q-all-tagged feature command prior to Cisco Catalyst OS Software version 7.5(1) was a <i>global</i> command. It configured a switch to forward all frames from 802.1Q trunks with 802.1Q tagging, including traffic in the native VLAN (default VLAN), and admit only 802.1Q tagged frames on 802.1Q trunks, dropping any untagged traffic, including untagged traffic in the native VLAN.</p> <p>In Cisco Catalyst OS Software version 7.5(1) and later, the <i>dot1q-all-tagged</i> feature can be enabled or disabled on a <i>per port basis</i>, should some network devices, for example customer premise equipment in Metro area deployments, not support tagged packets.</p>	X	
Rate limit log ACL	<p>Prior to Cisco Catalyst OS version 7.5(1), rate limiting was not available for logging router access control list (RACL) denied packets. In that case, all denials were sent to the MSFC and there existed the possibility of overloading the MSFC.</p> <p>With the enhancement in Cisco Catalyst OS Software version 7.5(1) of rate limit log ACL, the user can rate limit the amount of denials that are sent to the MSFC. Those packets that exceed the limit will be dropped.</p>	X	



Table 2 Software Features of Cisco Catalyst OS Software Version 7.5(1)

Software Feature	Description	Cisco Catalyst 6500 Feature	Cisco Catalyst 4000 Feature
NetFlow Version 5	NetFlow Data Export (NDE) is used for collecting accounting statistics on IP flow information for routed and bridged traffic. NDE makes these statistics available for analysis by an external data collector to improve manageability of the network. The NetFlow version 5 format is now supported on the Cisco Catalyst 6500 Series switches.	X	
QoS ACL limit increase	Maximizes Catalyst 6500 series supervisor engine QoS ACL capacity so that 500 interfaces can contain IP, IPX and MAC ACLs for a total of 1500 global ACLs.	X	
New MAC address trap	With this trap, the switch can send an SNMP trap to a pre-defined network management system station if it learns a new MAC address. This occurs when running port security and a new MAC address is learned, and also when a MAC address ages out. This feature also provides a means to specify a time interval for when these traps are sent so that if there are multiple users accessing the network simultaneously, traps aren't continuously traversing the network.	X	
Various MIB support	CISCO-SWITCH-ENGINE-MIB Enhancements CISCO-CATOS-ACL-QOS-MIB Enhancement CISCO-IGMP-SNOOPING-MIB CISCO-PAE-MIB Enhancement CISCO-FLASH-MIB Enhancement CISCO-L2-TUNNEL-CONFIG-MIB CISCO-STP-EXTENSION-MIB Enhancement CISCO-VLAN-MEMBERSHIP-MIB Enhancement CISCO-VTP-MIB Enhancement RFC2665 ETHERLIKE-MIB Enhancement RFC2863 IF-MIB Enhancement	X X X X X X X X X X X X	 X X X X X X

Orderable Software Images

Table 3 lists the software versions and applicable ordering information for the Cisco Catalyst 6500 Series and Cisco Catalyst 4000 Series supervisor engine software.



Caution: Always back up the switch configuration file before upgrading or downgrading the switch software to avoid losing all or part of the configuration stored in nonvolatile RAM (NVRAM). When downgrading switch software, you will lose your configuration. Use the write network command or the copy config tftp command to back up your configuration to a Trivial File Transfer Protocol (TFTP) server. Use the copy config flash command to back up the configuration to a Flash memory device.

Table 3 Software Ordering Information

Orderable Product Number	Description	Image
SC4K-SUPK8-7.5.1 SC4K-SUPK8-7.5.1=	Cisco Catalyst 4000 Supervisor Flash image, version 7.5.1 Spare	cat4000-k8
SC4K-SCVK8-7.5.1 SC4K-SCVK8-7.5.1=	Cisco Catalyst 4000 CiscoView image, version 7.5.1 Spare	cat4000-cv
SC4K-SUPK9-7.5.1 SC4K-SUPK9-7.5.1=	Cisco Catalyst 4000 Supervisor Flash image with SSH, version 7.5.1 Spare	cat4000-k9
SC6K-SUPK8-7.5.1 SC6K-SUPK8-7.5.1=	Catalyst 6000 Supervisor 1 Flash Image, Release 7.5.1 Spare	cat6000-supk8
SC6K-SUP2K8-7.5.1 SC6K-SUP2K8-7.5.1=	Catalyst 6000 Supervisor 2 Flash Image, Release 7.5.1 Spare	cat6000-sup2k8
SC6K-SCVK8-7.5.1 SC6K-SCVK8-7.5.1=	Cat6K Supervisor 1 Flash Image w/CiscoView, Release 7.5.1 Spare	cat6000-supcvk8
SC6K-S2CVK8-7.5.1 SC6K-S2CVK8-7.5.1	Cat6K Supervisor 2 Flash Image w/CiscoView, Release 7.5.1 Spare	cat6000-sup2cvk8
SC6K-SUPK9-7.5.1 SC6K-SUPK9-7.5.1=	Catalyst 6000 Supervisor 1 Flash Image w/SSH, Release 7.5.1 Spare	cat6000-supk9
SC6K-SUP2K9-7.5.1 SC6K-SUP2K9-7.5.1=	Catalyst 6000 Supervisor 2 Flash Image w/SSH, Release 7.5.1 Spare	cat6000-sup2k9
SC6K-SCVK9-7.5.1 SC6K-SCVK9-7.5.1=	Catalyst 6000 Sup 1 Flash Image w/CV and SSH, Release 7.5.1 Spare	cat6000-supcvk9
SC6K-S2CVK9-7.5.1 SC6K-S2CVK9-7.5.1=	Catalyst 6000 Sup 2 Flash Image w/CV and SSH, Release 7.5.1 Spare	cat6000-sup2cvk9

For more detailed information, refer to the Cisco Catalyst 6500 and 4000 Series release notes at:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/index.htm>

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/relnotes/index.htm>

The Cisco Catalyst 6500 and 4000 Series documentation is available at:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm>

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/index.htm>

CISCO SYSTEMS



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands

www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912

www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992-2003, Cisco Systems Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0208R) MH/LW4043 0103