



PRODUCT BULLETIN NO. 2506

NEW CISCO IOS SOFTWARE RELEASE 12.2(20)SE FOR CISCO CATALYST 3750, 3560, AND 2970 SERIES SWITCHES

OVERVIEW

Cisco Systems® announces Cisco IOS® Software updates for the Cisco® Catalyst® 3750, 3560, and 2970 series Intelligent Ethernet switches. This new release furthers Cisco leadership in providing secure, reliable, and easily managed LAN switching solutions.

This product bulletin describes the content and delivery information concerning Cisco IOS Software Release 12.2(20)SE. For more information about the Cisco IOS Software release process, see Product Bulletin 537.

Auto Quality of Service (QoS) 1.5 extends the current Auto QoS function to give preference to softphone traffic. At a high level, Auto QoS 1.5 functions by trusting differentiated services code point markings on VoIP traffic from an ingress port that has been configured to indicate that a softphone is attached.

Dynamic Address Resolution Protocol (ARP) Inspection is used to verify the validity of ARP requests and the responses sent by hosts connected to a switch. Today, widely available software tools enable “man in the middle” attacks by poisoning the ARP caches of hosts and routers. These attacks can be devastating because users can eavesdrop for unencrypted passwords or even record voice over IP conversations. Dynamic ARP Inspection helps prevent these attacks by not relaying invalid ARP requests and responses to other ports.

IP Source Guard is a security feature which restricts IP traffic on untrusted Layer 2 ports to clients with an assigned IP address. In other words, any IP traffic with a source IP address other than that assigned via DHCP or static configuration will be filtered out on the untrusted Layer 2 ports. This would prevent a malicious host from attacking the network by taking over its neighbor host’s IP address. IP source guard provides an IP and a MAC filter to restrict traffic on Dynamic Host Configuration Protocol from snooping untrusted ports, allowing network administrators to prevent end users from spoofing or stealing IP addresses. Similar to DHCP snooping, this feature is enabled on DHCP snooping untrusted Layer 2 ports, which include both access and trunk ports.

The **Private VLAN** feature partitions regular VLAN domains into sub-domains. There are two kinds of sub-domains—isolated and community. Ports within an isolated sub-domain cannot talk to one another and are known as “isolated ports”. Ports within a community VLAN sub-domain talk to one another but cannot talk to other community VLANs within the same private VLAN domain. Such ports are known as “community ports”. A promiscuous port can talk to both isolated and community ports.

Fixed configuration Cisco Catalyst switches currently support private VLAN edge (protected port). However, Private VLAN functions have been added to the Cisco Catalyst 3750 Series switches going forward. Private VLAN functions have been implemented on all access promiscuous, isolated, and community (limited to only one VLAN) ports.

With the widespread adoption of IEEE 802.1x and Identity Based Networking Services, customers have been anticipating support for **802.1x MIB and 802.1x Accounting** feature sets. This further extends the Cisco Catalyst switch platform security and manageability functions. With 802.1x Accounting, the switch provides accounting and security audit tracking and reports it to the secure access control server (ACS). After the user is authenticated, the username, IP address, and port information are logged. This information is passed to the ACS server using RADIUS audiovisual pair. If the user is rejected, the attempted trial information is logged along with the cause of rejection. After the session is terminated, the cause of termination also is logged.

As an alternative to Spanning Tree, **Flex Links** (also known as backup interface) provide the capability for sub-second failover across two uplinks to maintain resiliency in the network. Flex Links allows users to configure one of the switchport interfaces to backup the another

switchport interface. This feature is only supported on Layer 2 ports. At any time, only one of the ports (either active or backup) can pass traffic but not both. The other interface will be in standby mode, ready for sub-second take over when the interface that is currently passing traffic goes down.

Gigabit Interface Converter/Small Form-Factor Pluggable (GBIC/SFP) Diagnostic Management Interface allows real-time access to device parameters such as transceiver temperature, laser bias current, transmitted optical power, received optical power, and transceiver supply voltage. It also defines a system of alarms and warnings that can alert end users.

With enhancements being added by way of **Smartports** to further simplify the configuration of Cisco Catalyst switches, a global macro has been embedded in Cisco IOS Software for each of the switching platforms to optimize default switch settings. This macro can be applied using a command-line interface or using Cisco Cluster Management Suite (CMS) to apply global macros across multiple switches simultaneously. For implementation specific details, go to <http://www.cisco.com/go/smartports>. In addition, implementers can benefit from newly added dynamic help functions on parameters specified during the creation of Smartports macros via CLI.

100BASE-FX SFPs are now supported on Cisco Catalyst 3750, 3560 and 2970 switches with SFP slots, allowing these switches to support 100BASE-FX in various deployment scenarios.

With the “**Show StackWise Stats**,” users are able to track CPU utilization, memory usage, and backplane use for the Cisco Catalyst 3750 switch stack.

With **Switch Pre-provisioning** implemented on the Cisco Catalyst 3750 platform, the need to apply the startup configuration goes away in the event that some systems join the stack late. Switch pre-provisioning solves the problem directly, by parsing the startup configuration, including the parts of it that correspond to switches that currently are not present in the stack.

The **CiscoWorks MIB work** involves fixing problems as outlined in direct digital telephone service entries CSCin47528 and CSCin48923. This is crucial to an ongoing effort to enhance and optimize the interface for Catalyst switches using CiscoWorks.

NEW FEATURES IN CISCO IOS SOFTWARE RELEASE 12.2(20)SE

The features shown in Table 1 will be delivered in Cisco IOS Software Release 12.2(20)SE.

Table 1. Cisco IOS Software Release 12.2(20)SE New Features

Feature	Cisco Catalyst 3750-EMI	Cisco Catalyst 3750-SMI	Cisco Catalyst 3560-EMI	Cisco Catalyst 3560-SMI	Cisco Catalyst 2970-E
Auto QoS 1.5	X	X	X	X	X
IP Source Guard	X		X		
Dynamic ARP Inspection	X		X		
Private VLAN	X		X		
802.1x MIB	X	X	X	X	X
802.1x Accounting	X	X	X	X	X
Flex Links	X	X	X	X	X
GBIC/SFP Diagnostic Management Interface	X	X	X	X	X
Smartports III	X	X	X	X	X


Feature	Cisco Catalyst 3750-EMI	Cisco Catalyst 3750-SMI	Cisco Catalyst 3560-EMI	Cisco Catalyst 3560-SMI	Cisco Catalyst 2970-E
100BASE-FX SFP Support	X	X	X	X	X
HTTP Software Upgrade	X	X	X	X	X
Show StackWise Stats	X	X			
Switch Pre-provisioning	X	X			
CiscoWorks MIB Work	X	X	X	X	X

SMI—Standard Multi-Layer Image

EMI—Enhanced Multi-Layer Image

Feature enhancements made to Cisco Cluster Management Suite (CMS) Software with this new software release are highlighted in Table 2 below.

Table 2. New Features in Cisco CMS Software

Feature	Description
HTTP Software Upgrade	The new software upgrade supports: <ul style="list-style-type: none"> • Simultaneously upgrading multiple devices in the cluster regardless of their device families • Both Trivial File Transfer Protocol (TFTP) and HTTP protocols. The HTTP upgrade is supported only on Cisco IOS Software Release 12.2. An advantage with the HTTP upgrade is that it allows users to upgrade devices without having to use a TFTP server.
Smartports III	The feature gives the ability to apply Smartports global macro on multiple switches simultaneously. The menu path for device macros is Device->Smartports Device Macros.
Online Help Dialog Enhancements	This enhancement provides an optimized organization of the help content common to all the switches. With this feature, the help content scrolls automatically to the selected item if the help dialog is launched with a preselected node in the table of the content.
Support Unknown Devices in Views	Both the topology view and front panel view will display unknown devices in a cluster with the following icon 
Additional Feature Support	Rapid Per VLAN Spanning Tree Plus (PVRST+) and Port Security are added to CMS. IEEE 802.1s Multiple Spanning Tree Protocol currently is not supported in CMS. Port Security is enhanced to support Port Security aging, and trunk and dot1q tunnel ports.

The fixed configuration Catalyst switches supported with this software release are listed in Table 3 below.

Table 3. Catalyst Switches Supported with this Release

Cisco Catalyst 3750 Series Enhanced Multilayer Software Image Models	Cisco Catalyst 3750 Series Standard Multilayer Software Image Models	Cisco Catalyst 3560 Series Enhanced Multilayer Software Image Models	Cisco Catalyst 3560 Series Standard Multilayer Software Image Models	Cisco Catalyst 2970 Series Software Models
3750-48TS-E	3750-48TS-S	3560-48PS	3560-48PS	2970G-24T-E

Cisco Catalyst 3750 Series Enhanced Multilayer Software Image Models	Cisco Catalyst 3750 Series Standard Multilayer Software Image Models	Cisco Catalyst 3560 Series Enhanced Multilayer Software Image Models	Cisco Catalyst 3560 Series Standard Multilayer Software Image Models	Cisco Catalyst 2970 Series Software Models
3750-24TS-E	3750-24TS-S	3560-24PS	3560-24PS	2970G-24TS-E
3750G-24T-E	3750G-24T-S			
3750G-24TS-E	3750G-24TS-S			
3750G-12S-E	3750G-12S-S			
3750G-16TD	3750G-16TD			
3750-48PS	3750-48PS			
3750-24PS	3750-24PS			

ADDITIONAL RESOURCES

Software Download—Software available May 2004

Cisco Catalyst 3750 Series software download—<http://www.cisco.com/cgi-bin/tablebuild.pl/cat3750>

Cisco Catalyst 3560 Series software download—<http://www.cisco.com/cgi-bin/tablebuild.pl/cat3560>

Cisco Catalyst 2970 Series software download—<http://www.cisco.com/cgi-bin/tablebuild.pl/cat2970>

Due to export restrictions on strong cryptography software, a separate image is required for the cryptographic features (Secure Shell Protocol, Simple Network Management Protocol Version 3, and Kerberos Protocol). These software images can be downloaded from the corresponding 3DES area of the links provided above.

Additional product information is available at the following Websites:

Catalyst 3750 Series product information:

<http://www.cisco.com/go/catalyst3750>

Catalyst 3560 Series product information:

<http://www.cisco.com/go/catalyst3560>

Catalyst 2970 Series product information:

<http://www.cisco.com/go/catalyst2970>

Catalyst 3750, 3560, 3550, 2970, 2955/2950/2950 LRE, and 2940 release notes:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/c3750/index.htm>

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3560/index.htm>

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2970/index.htm>

Support

Cisco IOS Software Release 12.2(20)SE follows the standard Cisco support policy as indicated at

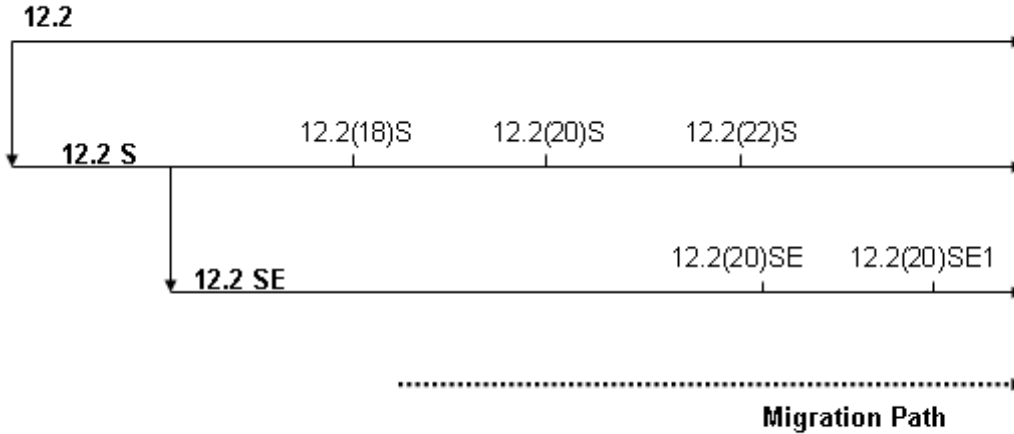
http://www.cisco.com/en/US/products/products_end-of-life_policy.html.

Software Image Migration Guide

Figure 1 displays Cisco IOS Software Release 12.2(20)SE functions relative to the 12.2S and 12.2SE releases. This diagram identifies the recommended migration path. For more information about the Cisco IOS Software release process, please see Product Bulletin 537.

Figure 1

Cisco IOS Software Release 12.2 Release Train



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.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 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 • Cyprus • 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

Copyright © 2004 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 United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0403R)
204064_ETMG_WH_08.04