



Release Notes for Catalyst 4000 Family Layer 3 Services Module for Cisco IOS Release 12.0W5

June 16, 2004

Current Release:
12.0(25)W5(27b)

Previous release: 12.0(25)W5(27a), 12.0(25)W5(27), 12.0(18)W5(22b), 12.0(18)W5(22a), 12.0(10)W5(18g), 12.0(14)W5(20), 12.0(10)W5(18f), 12.0(7)W5(15d)

These release notes describe the features, modifications, and caveats for the Catalyst 4000 family Layer 3 Services Module (WS-X4232-L3). These release notes apply to the 12.0(25)W5(27a) Cisco IOS release. For features, modifications, and caveats for the Catalyst 4000 family supervisor engine software, refer to the *Release Notes for Catalyst 4000 Family Software Release 6.x*.



Note

The Catalyst 4000 family includes the Catalyst 4003 and the Catalyst 4006 switches. Throughout this publication and all Catalyst 4000 family documents, the phrase *Catalyst 4000 family switches* refers to all Catalyst 4000 family switches, unless otherwise noted.



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Contents

This document consists of the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New Features and Changed Information, page 3](#)
- [Limitations and Restrictions, page 8](#)
- [Caveats, page 9](#)
- [Related Documentation, page 20](#)
- [Service and Support, page 22](#)
- [Obtaining Documentation and Submitting a Service Request, page 23](#)
- [Obtaining Technical Assistance, page 22](#)
- [Obtaining Additional Publications and Information, page 23](#)

Introduction

The Catalyst 4003 and 4006 Layer 3 Services Module provides multiprotocol switching and routing for the Catalyst 4000 family switches.

The 32 10/100 Ethernet interfaces on the module provide full Layer 2 feature support and are configurable from the Catalyst 4000 family switch supervisor engine. Refer to the *Catalyst 4500 Series, 2980G, and 2948G Switches Software Configuration Guide*, Software Release 6.1, for information on feature support for the Catalyst 4000 family switches.

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.0(18)W5(22b), see the “[New Features and Changed Information](#)” section on [page 3](#) and the “[Related Documentation](#)” section on [page 20](#).

System Requirements

This section describes the system requirements for Release 12.0(18)W5(22b) and includes the following topics:

- [Memory Requirements, page 3](#)
- [Software Release Requirement, page 3](#)
- [Software Ordering Information, page 3](#)
- [New Features and Changed Information, page 3](#)

Memory Requirements

The Layer 3 Services Module has a 64-MB synchronous dynamic random-access memory (SDRAM) and requires 16-MB Flash memory.

Software Release Requirement

The Catalyst 4000 family Layer 3 Services Module is shipped with Cisco IOS software installed. However, before this module can run in your Catalyst 4000 family switch, ensure that the Catalyst 4000 family supervisor engine has the minimum required software release of 5.5(1). We recommend that you run software release 6.1(1) or later. Software images are available through Cisco.com; see the [“Cisco.com” section on page 21](#) for more information.

To determine the version of the Cisco IOS software currently running on the Catalyst 4000 Layer 3 Service Module, log on to the switch and enter the **show version EXEC** command.

Software Ordering Information

[Table 1](#) lists the software version and applicable ordering information for the Layer 3 Services Module software.

Table 1 Software Version and Orderable Product Number

Software Version	Filename	Orderable Product Number for Flash on System	Orderable Product Number for Spare Upgrade (Floppy Media)
12.0(10)W5(18g)	cat4232-in-mz.bin	SC42Z-12.0.10W	SC42Z-12.0.10W=
12.0(18)W5(22a)	cat4232-in-mz.bin	SC42Z-12.0.18W	SC42Z-12.0.18W=
12.0(18)W5(22b)	cat4232-in-mz.bin	SC42Z-12.0.18W	SC42Z-12.0.18W=
12.0(25)W5(27)	cat4232-in-mz.bin	SC42Z-12.0.25W	SC42Z-12.0.25W=
12.0(25)W5(27a)	cat4232-in-mz.bin	SC42Z-12.0.25W	SC42Z-12.0.25W=
12.0(25)W5(27b)	cat4232-in-mz.bin	SC42Z-12.0.25W	SC42Z-12.0.25W=

New Features and Changed Information

This section lists the new features available in this release and in previous releases.

Features in Release 12.0(25)W5(27b)

There are no new features in Cisco IOS Release 12.0(25)W5(27b).

Features in Release 12.0(25)W5(27a)

There are no new features in Cisco IOS Release 12.0(25)W5(27a).

Features in Release 12.0(25)W5(27)

There are no new features in Cisco IOS Release 12.0(25)W5(27).

Features in Release 12.0(18)W5(22b)

There are no new features in Cisco IOS Release 12.0(18)W5(22b).

The 12.0(18)W5(22b) release contains important fixes. If you are currently running 12.0(18)W5(22a) or any earlier release you should migrate to the 12.0(18)W5(22b) release.

Features in Release 12.0(18)W5(22a)

Software release 12.0(18)W5(22a) supports the following new features:

- [Local Proxy ARP, page 4](#)
- [RADIUS Server, page 4](#)
- [CEF Load Balancing on Gigabit Ethernet Ports, page 5](#)

Local Proxy ARP

The Local Proxy Address Resolution Protocol (ARP) feature allows the route processor to respond to ARP requests for IP addresses within a subnet where routing is not normally required. When the local proxy ARP feature is enabled, the route processor responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only in subnets in which the hosts are prevented from directly communicating within the subnet by the configuration on the switch to which they are connected.

By default, the local proxy ARP feature is disabled. Use the **ip local-proxy-arp** interface configuration command to enable the local proxy ARP feature on an interface. Use the **no ip local-proxy-arp** interface configuration command to disable the local proxy ARP feature. Internet Control Message Protocol (ICMP) redirects are disabled on interfaces where the local proxy ARP feature is enabled.

To use the local proxy ARP feature, the IP proxy ARP feature must be enabled. The IP proxy ARP feature is enabled by default. Refer to “IP Addressing and Services,” “Configuring IP Addressing,” and “Configure Address Resolution Methods” in the *Cisco IOS Release 12.0 Network Protocols Configuration Guide Part 1*.

RADIUS Server

The RADIUS feature is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

RADIUS is a fully open protocol, distributed in source code format, that can be modified to work with any security system currently available on the market.

Cisco supports RADIUS under its AAA security paradigm. RADIUS can be used with other AAA security protocols, such as TACACS+, Kerberos, or local username lookup. RADIUS is supported on all Cisco platforms. Refer to the *Cisco IOS Release 12.0 Security Configuration Guide*, “Security Server Protocols,” “Configuring RADIUS.”

CEF Load Balancing on Gigabit Ethernet Ports

Cisco Express Forwarding (CEF) load balancing is based on a combination of source and destination packet information; it allows you to optimize resources by distributing traffic over multiple paths for transferring data to a single destination.

You can configure CEF load balancing on a per-destination basis. Load distortions can occur across multiple switches when the same CEF load balancing algorithm is used on every switch. You can resolve these distortions by selecting a specific CEF load balancing algorithm, based on your network environment.

Features in Release 12.0(10)W5(18g)

There are no new features in Cisco IOS Release 12.0(10)W5(18g).

The 12.0(10)W5(18g) release contains important fixes. If you are currently running 12.0(10)W5(18f) you should migrate to the 12.0(10)W5(18g) release or to the recommended 12.0(14)W5(20) release because 12.0(10)W5(18f) has been deferred.

Features in Release 12.0(14)W5(20)

There are no new features in Cisco IOS Release 12.0(14)W5(20).

Features in Release 12.0(10)W5(18f)

The following features were new in Cisco IOS Release 12.0(10)W5(18f):

- Border Gateway Protocol (BGP)
- AppleTalk access lists (ACLs)
- IPX standard ACLs
- IP standard and extended ACLs
- Per-port QOS traffic conditioning features, such as, rate-limiting and shaping
- AppleTalk routing

Features in Release 12.0(7)W5(15d)

The Layer 3 Services Module provides multiprotocol switching and routing for Catalyst 4000 family switches.

The 32 10/100 Ethernet ports on the module provide full Layer 2 feature support and are configurable from the Catalyst 4000 family switch supervisor engine. Refer to the *Software Configuration Guide—Catalyst 4000 Family, Catalyst 2948G and Catalyst 2980G Switches*, Software Release 6.1(1) for information on feature support on the Catalyst 4000 family switches.

[Table 2](#) lists the Cisco IOS features available for the Layer 3 Services Module.

Table 2 Cisco IOS Features**Layer 2 Bridging Features**

Layer 2 transparent bridging

Layer 2 MAC learning, aging, and switching by hardware

Spanning Tree Protocol (IEEE 802.1D) on each bridge group

A maximum of 16 active bridge groups

Up to 4000 MAC addresses

24-Kb CAM¹ shared by Layer 2 entries, IP routing, IP multicast routing, and Novell IPX routing**VLAN Features**ISL²-based VLAN trunking on the front panel Gigabit Ethernet ports

IEEE 802.1Q-based VLAN trunking on all ports

Layer 3 Routing, Switching, and Forwarding

IP, IPX, and IP multicast routing and switching between Ethernet ports

Constrained multicast flooding (CMF)

Load balancing on a per-destination basis

Load balancing among equal cost paths, based on source and destination IP and IPX³ addresses

CEF load balancing on Gigabit Ethernet ports using tunnel and universal load balancing algorithms

Layer 3 Routing, Switching, and Forwarding (continued)

24-Kb CAM shared by Layer 2 entries, IP routing, IP multicast routing, and Novell IPX routing

Up to 18,000 IP routes

Up to 20,000 IP host entries

Up to 20,000 IPX routes

Up to 20,000 IPX host entries

Up to 128,000 IP multicast route entries

Supported Routing ProtocolsRIP⁴ and RIP IIIGRP⁵EIGRP⁶OSPF⁷

IPX RIP and EIGRP

PIM⁸—sparse and dense mode

Secondary addressing

Static routes

GEC Features

Bundling of up to two Gigabit Ethernet ports

Load balancing among equal cost paths, based on source and destination IP and IPX⁹ addresses

CEF load balancing on Gigabit Ethernet ports using tunnel and universal load balancing algorithms

Load sharing for bridge traffic based on MAC address

Table 2 Cisco IOS Features (continued)

ISL trunking supported on the external GEC
802.1Q trunking supported on the external and internal GEC
Two active GEC ¹⁰ port channels
Additional Protocols and Features
Layer 3 QoS ¹¹
SDM ¹²
BOOTP ¹³
CDP ¹⁴ support on Ethernet ports
CGMP ¹⁵ server support
DHCP ¹⁶ relay
HSRP ¹⁷
ICMP ¹⁸
IGMP ¹⁹
SAP and IPX SAP ²⁰ filtering
SNMP ²¹
TACACS+ ²²

1. CAM = content addressable memory
2. ISL = Inter-Switch Link
3. IPX = Internet Packet Exchange
4. RIP = Routing Information Protocol
5. IGRP = Interior Gateway Routing Protocol
6. EIGRP = Enhanced Interior Gateway Routing Protocol
7. OSPF = Open Shortest Path First
8. PIM = Protocol Independent Multicast
9. IPX = Internet Packet Exchange
10. GEC = Gigabit EtherChannel
11. QoS = Quality of Service
12. SDM = Switching Database Manager
13. BOOTP = Bootstrap Protocol
14. CDP = Cisco Discovery Protocol
15. CGMP = Cisco Group Management Protocol
16. DHCP = Dynamic Host Configuration Protocol
17. HSRP = Hot Standby Router Protocol
18. ICMP = Internet Control Message Protocol
19. IGMP = Internet Group Management Protocol
20. IPX SAP = Internet Packet Exchange Service Advertisement Protocol
21. SNMP = Simple Network Management Protocol
22. TACACS+ = Terminal Access Controller Access Control System Plus

Unsupported Features

The following features are not supported on the Layer 3 Services Module:

- Multilayer switching
- IPX extended access lists
- Named IPX SAP access lists
- 48-bit MAC access lists
- 48-bit MAC extended access lists
- Integrated routing and bridging, and concurrent routing and bridging
- ISL trunking on the internal Gigabit Ethernet ports
- Generic Routing Encapsulation (GRE)

If a feature is not listed in the supported features section for a release, that feature is not supported on the Layer 3 Services Module.

Limitations and Restrictions

This section provides usage guidelines for the Catalyst 4000 family Layer 3 Services Module hardware and software:

- The internal IP address used by the Catalyst 4000 family supervisor engine to communicate with the Layer 3 Services Module will be listed in the BGP routing table as the 127.0.0.0 network. To prevent the address from appearing in the BGP routing table, use the **distribute-list** command to filter the 127.0.0.0 network by entering the following commands:

```
Router(config)#router bgp 1
Router(config-router)#redistribute connected
Router(config-router)#distribute-list 10 out connected
Router(config)#access-list 10 deny 127.0.0.0 0.255.255.255
Router(config)#access-list 10 permit any
Router(config)#
```

Enter the **show ip bgp** command to verify that network 127.0.0.0 is filtered:

```
Router(config)#show ip bgp
      Network      Next Hop          Metric LocPrf Weight Path
Router(config)#
```

- Do not configure the 10/100 management port for Hot Standby Router Protocol (HSRP). Doing so could make the Layer 3 Services Module the active router in the network.
- The **show ip route** command always shows one more router connection than is displayed in the routing table. This additional route reflects the internal IP address that is assigned for the Catalyst 4000 family Layer 3 Services Module and Catalyst 4000 family supervisor engine communications.
- Under normal circumstances, heavy data traffic is routed by the XPIFs within the switch fabric without involving the CPU but when the XPIFs receive packets they are unable to route, they forward those packets to the main CPU. Such packets include CDP packets, unreachable network packets, and packets coming in on a native VLAN on an IEEE 802.1Q trunk interface. When the CPU receives too much traffic, packets can be lost, causing CDP to fail and the Layer 3 Services Module to become unreachable using the **session** command.
- When the **no negotiation auto** command is used on a Layer 3 Gigabit Ethernet port, the link status of that port shows up, regardless of the presence of a cable or GBIC on that port.
- An invalid value is returned for SNMP requests for the CiscoFlashDeviceCard MIB object.

- CDP will fail on an external Layer 3 Gigabit port when trunking is enabled. The switch will not send CDP packets on a trunk port connected to a Catalyst 4000 family switch when CDP packets are coming on a VLAN for which a subinterface is not configured. To receive CDP packets, configure a dummy VLAN subinterface on the trunk port connected to the Catalyst 4000 family switch.
- The CLI command **no qos switching** is not supported on the Layer 3 Gigabit Ethernet ports. Use the **qos mapping precedence value wrr-weight weight** command to configure the same WRR weight for all the precedence values globally, using the CLI.
- If the interface encapsulation is changed to ISL or 802.1Q on an external Layer 3 Gigabit Ethernet port while there is traffic on the port, runs and input error counters might increase. However, after the link is stable and normal operation resumes, these counters should not continue to increase.
- Catalyst 2948G-L3 and Catalyst 4908G-L3 switches do not block SNAP encapsulated ARP packets, even though there is switching support for ARPA- encapsulated IP packets. Because of this, ARP entries for unsupported IP encapsulations can be in the ARP table.
- When spanning tree is disabled in a bridge group, dynamically learned MAC entries will not be immediately deleted from the CAM. If the interface on which the MAC entries were learned goes down, the entries will be aged-out and removed.

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

For information on caveats in Cisco IOS Release 12.0, see “Caveats for Cisco IOS Release 12.0,” which lists severity 1 and 2 caveats for Release 12.0 on Cisco.com and the Documentation CD-ROM.



Note

Caveats about Fast Ethernet interfaces do not apply to the Catalyst 4908G-L3 switch, which has only Gigabit Ethernet interfaces.

Open Caveats in Release 12.0(25)W5(27b)

This section describes open caveats in Cisco IOS Release 12.0(25)W5(27b):

- Cisco IOS does not update the IPX routing table when more than two equal hop paths are available and one of them is shut down. For example, a switch with three interfaces (I1, I2, and I3) might have an IPX network configured on each interface, as N1, N2, and N3, respectively. A remote IPX network (R) is accessible through N1, N2, and N3 interfaces. The maximum equal hop paths is set to 2. The IOS routing table will show two destination paths (N1 and N2) in the IPX routing table, the interface I2 will shut down. Because all the three paths are equal hop, the IOS routing table should show N1 and N3 as two equal hop paths. However, the routing table shows only N1 as the destination path.

Workaround: Enter the `clear ipx route` command. The routing table will show N1 and N3 as the destination next hop paths. (CSCdp13515)

Resolved Caveats in Release 12.0(25)W5(27b)

This section describes the resolved caveats in Cisco IOS Release 12.0(25)W5(27b):

- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at:

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at:

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>. (CSCed27956 and CSCed38527)

- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

Cisco has made free software available to address this problem. For more details, refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml>. (CSCdu53656 and CSCea28131)

Open Caveats in Release 12.0(25)W5(27a)

This section describes open caveats in Cisco IOS Release 12.0(25)W5(27a):

- Cisco IOS does not update the IPX routing table when more than two equal hop paths are available and one of them is shut down. For example, a switch with three interfaces (I1, I2, and I3) might have an IPX network configured on each interface, as N1, N2, and N3, respectively. A remote IPX network (R) is accessible through N1, N2, and N3 interfaces. The maximum equal hop paths is set to 2. The IOS routing table will show two destination paths (N1 and N2) in the IPX routing table, the interface I2 will shut down. Because all the three paths are equal hop, the IOS routing table should show N1 and N3 as two equal hop paths. However, the routing table shows only N1 as the destination path.

Workaround: Enter the **clear ipx route** command. The routing table will show N1 and N3 as the destination next hop paths. (CSCdp13515)

Resolved Caveats in Release 12.0(25)W5(27a)

This section describes the resolved caveats in Cisco IOS Release 12.0(25)W5(27a):

- When the Layer 3 Services Module is configured as a relay agent, it sends DHCP discover packets (with their primary IP address) to the DHCP server that is requesting an IP address for the DHCP client in the same subnet. If the primary pool of IP addresses is excluded and only the secondary pool is available on the DHCP server, the DHCP discover packet with the primary IP address should be rejected, but it is not. The functionality to resend DHCP requests with the secondary IP address when the primary IP address fails will be available in a later release. (CSCdr23558)
- When the Layer 3 Services Module is configured as a DHCP relay agent, it fails to drop DHCP packets with hop counts over 16. (CSCdr21806)
- IRB and CRB are not supported. (CSCdr31970)
- Appletalk stops working when you load the cat4232-in-mz.120-25.W5.27.bin software, and the router stops responding to “GETNETINFO” requests during an Appletalk clients’ startup.

Workaround: Downgrading to an earlier version of the software solves the problem. (CSCeb70373)

Open Caveats in Release 12.0(25)W5(27)

This section describes open caveats in Cisco IOS Release 12.0(25)W5(27):

- Cisco IOS does not update the IPX routing table when more than two equal hop paths are available and one of them is shut down. For example, a switch with three interfaces (I1, I2, and I3) might have an IPX network configured on each interface, as N1, N2, and N3, respectively. A remote IPX network (R) is accessible through N1, N2, and N3 interfaces. The maximum equal hop paths is set to 2. The IOS routing table will show two destination paths (N1 and N2) in the IPX routing table, the interface I2 will shut down. Because all the three paths are equal hop, the IOS routing table should show N1 and N3 as two equal hop paths. However, the routing table shows only N1 as the destination path.

Workaround: Enter the **clear ipx route** command. The routing table will show N1 and N3 as the destination next hop paths. (CSCdp13515)

- When the Layer 3 Services Module is configured as a relay agent, it sends DHCP discover packets (with their primary IP address) to the DHCP server that is requesting an IP address for the DHCP client in the same subnet. If the primary pool of IP addresses is excluded and only the secondary pool is available on the DHCP server, the DHCP discover packet with the primary IP address should be rejected, but it is not. The functionality to resend DHCP requests with the secondary IP address when the primary IP address fails will be available in a later release. (CSCdr23558)
- When the Layer 3 Services Module is configured as a DHCP relay agent, it fails to drop DHCP packets with hop counts over 16. (CSCdr21806)
- IRB and CRB are not supported. (CSCdr31970)

Resolved Caveats in Release 12.0(25)W5(27)

This section describes the resolved caveats in Cisco IOS Release 12.0(25)W5(27):

- Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

Cisco has made software available, free of charge, to correct the problem.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml>. (CSCea02355)

- The RME tool should look at the “chassisType” in the OLD-CISCO-CHASSIS MIB to find the chassis type for a Catalyst 4000 family Layer 3 Services Module, and the RHINO MIB should return a chassis type of “other” instead of “c2948g”. (CSCin29900)
- When the Catalyst 4000 family Layer 3 Services Module is loaded with Cisco IOS Release 12.0(18)W5(22b), you cannot confirm that SDM autolearns disabled by using the **show running-config** command.

Workaround: There is no workaround. (CSCdy32831)

- You cannot configure IP addresses on GigabitEthernet3 and GigabitEthernet4 interfaces when using port channels trunking 802.1q. CDP will not use any of the IP addresses configured on the Layer 3 interface as source address and CDP will use the 127.0.0.X inband IP address as the source address. The 127.0.0.X inband IP address is not accessible to the Campus management software, and ANI cannot discover the routing module.

Workaround: Add the Layer 3 interface as a seed device. (CSCdx14326)

- When more than 27 subinterfaces are created on the backplane ports of the same bridge group, the following memory allocation error message is displayed:

```
%SYS-2-MALLOCFAIL: Memory allocation of 692 bytes failed from 0x6006C9 08, pool
I/O, alignment 32 -Process= "Exec", ipl= 6, pid= 2 -Traceback= 6009DA2C
6009EE20 6006C910 6006CC90 6006D160 602EA0B8 602EA340 602EA 3D8 6007684C
603EB2E8 603EB434 6051F528 6051FB28 6051FE0C 6040F180 60085254
```

This condition may occur during configuration without the presence of any traffic. There is no workaround. (CSCdu61768)

- When configuring more than 256 subinterfaces, the following error messages are displayed:

```
Sep  3 21:59:40.247: %AUTOSTATE-6-SHUT_DOWN: Putting interface
GigabitEthernet4.382 into Autostate mode

Sep  3 22:20:11.303: %SYS-5-CONFIG_I: Configured from console by vty0
(127.0.0.2)

Sep  3 22:21:19.055: lss_myip full, 10.15.4.65 not added

Sep  3 22:22:09.443: deletion of 10.15.4.65 not in MY_IP list

Sep  3 22:22:09.443: lss_myip full, 10.15.4.65 not added

Sep  3 22:23:53.699: deletion of 10.15.4.65 not in MY_IP list
```

Workaround: You must limit the number of subinterfaces because the Catalyst 4000 family Layer 3 Services Module supports only 256 subinterfaces. (CSCdy55551)

Open Caveats in Release 12.0(18)W5(22b)

This section describes open caveats in Cisco IOS Release 12.0(18)W5(22b):

- When the Layer 3 Services Module is configured as a DHCP relay agent, it fails to drop DHCP packets with hop counts over 16. (CSCdr21806)
- IRB and CRB are not supported. (CSCdr31970)
- Cisco IOS does not update the IPX routing table when more than two equal hop paths are available and one of them is shut down. For example, a switch with three interfaces (I1, I2, and I3) might have an IPX network configured on each interface, as N1, N2, and N3, respectively. A remote IPX network (R) is accessible through N1, N2, and N3 interfaces. The maximum equal hop paths is set to 2. The IOS routing table will show two destination paths (N1 and N2) in the IPX routing table, the interface I2 will shut down. Because all the three paths are equal hop, the IOS routing table should show N1 and N3 as two equal hop paths. However, the routing table shows only N1 as the destination path.
Workaround: Enter the **clear ipx route** command. The routing table will show N1 and N3 as the destination next hop paths. (CSCdp13515)
- When the Layer 3 Services Module is configured as a relay agent, it sends DHCP discover packets (with their primary IP address) to the DHCP server that is requesting an IP address for the DHCP client in the same subnet. If the primary pool of IP addresses is excluded and only the secondary pool is available on the DHCP server, the DHCP discover packet with the primary IP address should be rejected, but it is not. The functionality to resend DHCP requests with the secondary IP address when the primary IP address fails will be available in a later release. (CSCdr23558)

Resolved Caveats in Release 12.0(18)W5(22b)

This section describes the resolved caveats in Cisco IOS Release 12.0(18)W5(22b):

- An error can occur with management protocol processing. You can use the following URL for further information:
<http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903>

Open Caveats in Release 12.0(18)W5(22a)

This section describes open caveats in Cisco IOS Release 12.0(18)W5(22a):

- Cisco IOS does not update the IPX routing table when more than two equal hop paths are available and one of them is shut down. For example, a switch with three interfaces (I1, I2, and I3) might have an IPX network configured on each interface, as N1, N2, and N3, respectively. A remote IPX network (R) is accessible through N1, N2, and N3 interfaces. The maximum equal hop paths is set to 2. The IOS routing table will show two destination paths (N1 and N2) in the IPX routing table, the interface I2 will shut down. Because all the three paths are equal hop, the IOS routing table should show N1 and N3 as two equal hop paths. However, the routing table shows only N1 as the destination path.

Workaround: Enter the **clear ipx route** command. The routing table will show N1 and N3 as the destination next hop paths. (CSCdp13515)

- When the Layer 3 Services Module is configured as a DHCP relay agent, it fails to drop DHCP packets with hop counts over 16. (CSCdr21806)
- IRB and CRB are not supported. (CSCdr31970)
- When the Layer 3 Services Module is configured as a relay agent, it sends DHCP discover packets (with their primary IP address) to the DHCP server that is requesting an IP address for the DHCP client in the same subnet. If the primary pool of IP addresses is excluded and only the secondary pool is available on the DHCP server, the DHCP discover packet with the primary IP address should be rejected, but it is not. The functionality to resend DHCP requests with the secondary IP address when the primary IP address fails will be available in a later release. (CSCdr23558)

Resolved Caveats in Release 12.0(18)W5(22a)

This section describes the resolved caveats in Cisco IOS Release 12.0(18)W5(22a):

- An ARP packet received by the router that has the router's own interface address but with a different MAC address can overwrite the router's own MAC address in the ARP table, causing that interface to stop sending and receiving traffic. This attack is successful only against interfaces on the Ethernet segment that is local to the attacking host.

Workaround: Hardcode the interface's ARP table entry by using the *arp ip-address hardware-address type [alias]* command. This entry will remain in the ARP table until you enter the **clear arp** command.

Refer to the advisory at the following URL:

<http://www.cisco.com/warp/public/707/IOS-arp-overwrite-vuln-pub.shtml>

This vulnerability does not apply to switches running Cisco CatOS software, only to switches running Cisco IOS software. (CSCdu81936)

- A CPU HOG condition occurs on the switch after you enter the **no ipx router eigrp** command for routes learned through IEEE 802.1Q encapsulation on the Gigabit Ethernet port. After approximately 15 seconds the console prompt returns. (CSCdp37972)

Open Caveats in Release 12.0(10)W5(18g)

This section describes open caveats in Cisco IOS Release 12.0(10)W5(18g):

- A CPU HOG condition occurs on the switch after you enter the **no ipx router eigrp** command for routes learned through IEEE 802.1Q encapsulation on the Gigabit Ethernet port. After approximately 15 seconds, the console prompt returns. (CSCdp37972)
- Cisco IOS does not update the IPX routing table when more than two equal hop paths are available and one of them is shut down. For example, a switch with three interfaces (I1, I2, and I3) might have an IPX network configured on each interface, as N1, N2, and N3, respectively. A remote IPX network (R) is accessible through N1, N2, and N3 interfaces. The maximum equal hop paths is set to 2. The IOS routing table will show two destination paths (N1 and N2) in the IPX routing table, the interface I2 will shut down. Because all the three paths are equal hop, the IOS routing table should show N1 and N3 as two equal hop paths. However, the routing table shows only N1 as the destination path.
Workaround: Enter the **clear ipx route** command. The routing table will show N1 and N3 as the destination next hop paths. (CSCdp13515)
- When the Layer 3 Services Module is configured as a DHCP relay agent, it fails to drop DHCP packets with hop counts over 16. (CSCdr21806)
- When the Layer 3 Services Module is configured as a relay agent, it sends DHCP discover packets (with their primary IP address) to the DHCP server that is requesting an IP address for the DHCP client in the same subnet. If the primary pool of IP addresses is excluded and only the secondary pool is available on the DHCP server, the DHCP discover packet with the primary IP address should be rejected, but it is not. The functionality to resend DHCP requests with the secondary IP address when the primary IP address fails will be available in a later release. (CSCdr23558)
- IRB and CRB are not supported. (CSCdr31970)
- When accessed through SNMP, the QoS mapping table lists an entry with an incorrect precedence index value of 4. This value must be in a range from 0 to 3. (CSCdr24893)

Resolved Caveats in Release 12.0(10)W5(18g)

This section describes the resolved caveats in Cisco IOS Release 12.0(14)W5(18g):

- A Border Gateway Protocol (BGP) UPDATE contains Network Layer Reachability Information (NLRI) and attributes that describe the path to the destination. Each path attribute is a type, length, value (TLV) object.

The type is a two-octet field that includes the attribute flags and the type code. The fourth high-order bit (bit 3) of the attribute flags is the Extended Length bit. It defines whether the attribute length is one octet (if set to 0) or two octets (if set to 1). The extended length bit is used only if the length of the attribute value is greater than 255 octets.

The AS_PATH (type code 2) is represented by a series of TLVs (or path segments). The path segment type indicates whether the content is an AS_SET or AS_SEQUENCE. The path segment length indicates the number of autonomous systems (ASes) in the segment. The path segment value contains the list of ASes (each AS is represented by two octets).

The total length of the attribute depends on the number of path segments and the number of ASes in them. For example, if the AS_PATH contains only an AS_SEQUENCE, then the maximum number of ASes (without having to use the extended length bit) is 126 [= (255-2)/2]. If the UPDATE is propagated across an AS boundary, then the local Abstract Syntax Notation (ASN) must be appended and the extended length bit used.

The caveat was caused by the mishandling of the operation during which the length of the attribute was truncated to only one octet. Because of the internal operation of the code, the receiving border router would not be affected, but its iBGP peers would detect the mismatch and issue a NOTIFICATION message (update malformed) to reset their session.

The average maximum AS_PATH length in the Internet is between 15 and 20 ASes, so there is no need to use the extended length. The failure was discovered because of a malfunction in the BGP implementation of another vendor. There is no workaround.

[Part of the text was taken from RFC 1771.] (CSCdr54230)

- When BGP sessions get reset, currently, with `log neighbor-changes`, the event is not logged. However, to find out the reasons as to why there was a reset, one has to turn on the debugs. This fix will automatically log the NOTIFICATION message when the sessions are reset. This feature will be turned on by the same `log neighbor-changes` knob. (CSCdr54231)
- BGP configuration with route-map configured is susceptible to memory corruption. (CSCdt79947)
- Cisco Security Advisory:

Cisco IOS Software TCP Initial Sequence Number Randomization Improvements

Revision 1.0: INTERIM

For Public Release 2001 February 27 20:00 US/Eastern (UTC+0500)

Summary

Cisco IOS software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers.

This vulnerability is present in all released versions of Cisco IOS software running on Cisco routers and switches. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts.

To remove the vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is described in DDTS record CSCds04747.

Workarounds are available that limit or deny successful exploitation of the vulnerability by filtering traffic containing forged IP source addresses at the perimeter of a network or directly on individual devices.

This notice will be posted at <http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml>. (CSCds04747)

Open Caveats in Release 12.0(14)W5(20)

This section describes open caveats in Cisco IOS Release 12.0(14)W5(20):

- A CPU HOG condition occurs on the switch after you enter the **no ipx router eigrp** command for routes learned through IEEE 802.1Q encapsulation on the Gigabit Ethernet port. After approximately 15 seconds, the console prompt returns. (CSCdp37972)
- When the Layer 3 Services Module is configured as a DHCP relay agent, it fails to drop DHCP packets with hop counts over 16. (CSCdr21806)
- IRB and CRB are not supported. (CSCdr31970)

- Cisco IOS does not update the IPX routing table when more than two equal hop paths are available and one of them is shut down. For example, a switch with three interfaces (I1, I2, and I3) might have an IPX network configured on each interface, as N1, N2, and N3, respectively. A remote IPX network (R) is accessible through N1, N2, and N3 interfaces. The maximum equal hop paths is set to 2. The IOS routing table will show two destination paths (N1 and N2) in the IPX routing table, the interface I2 will shut down. Because all the three paths are equal hop, the IOS routing table should show N1 and N3 as two equal hop paths. However, the routing table shows only N1 as the destination path.

Workaround: Enter the **clear ipx route** command. The routing table will show N1 and N3 as the destination next hop paths. (CSCdp13515)

- When the Layer 3 Services Module is configured as a relay agent, it sends DHCP discover packets (with their primary IP address) to the DHCP server that is requesting an IP address for the DHCP client in the same subnet. If the primary pool of IP addresses is excluded and only the secondary pool is available on the DHCP server, the DHCP discover packet with the primary IP address should be rejected, but it is not. The functionality to resend DHCP requests with the secondary IP address when the primary IP address fails will be available in a later release. (CSCdr23558)

Resolved Caveats in Release 12.0(14)W5(20)

This section describes the resolved caveats in Cisco IOS Release 12.0(14)W5(20):

- A Border Gateway Protocol (BGP) UPDATE contains Network Layer Reachability Information (NLRI) and attributes that describe the path to the destination. Each path attribute is a type, length, value (TLV) object.

The type is a two-octet field that includes the attribute flags and the type code. The fourth high-order bit (bit 3) of the attribute flags is the Extended Length bit. It defines whether the attribute length is one octet (if set to 0) or two octets (if set to 1). The extended length bit is used only if the length of the attribute value is greater than 255 octets.

The AS_PATH (type code 2) is represented by a series of TLVs (or path segments). The path segment type indicates whether the content is an AS_SET or AS_SEQUENCE. The path segment length indicates the number of autonomous systems (ASes) in the segment. The path segment value contains the list of ASes (each AS is represented by two octets).

The total length of the attribute depends on the number of path segments and the number of ASes in them. For example, if the AS_PATH contains only an AS_SEQUENCE, then the maximum number of ASes (without having to use the extended length bit) is 126 [= (255-2)/2]. If the UPDATE is propagated across an AS boundary, then the local Abstract Syntax Notation (ASN) must be appended and the extended length bit used.

The caveat was caused by the mishandling of the operation during which the length of the attribute was truncated to only one octet. Because of the internal operation of the code, the receiving border router would not be affected, but its iBGP peers would detect the mismatch and issue a NOTIFICATION message (update malformed) to reset their session.

The average maximum AS_PATH length in the Internet is between 15 and 20 ASes, so there is no need to use the extended length. The failure was discovered because of a malfunction in the BGP implementation of another vendor. There is no workaround.

[Part of the text was taken from RFC 1771.] (CSCdr54230)

- When accessed through SNMP, the QoS mapping table lists an entry with the wrong precedence index value of 4. This value must be in a range from 0 to 3. (CSCdr24893)

- When BGP sessions get reset, currently, with `log neighbor-changes`, the event is not logged. However, to find out the reasons as to why there was a reset, one has to turn on the debugs. This fix will automatically log the NOTIFICATION message when the sessions are reset. This feature will be turned on by the same `log neighbor-changes` knob. (CSCdr54231)
- Cisco Security Advisory:
Cisco IOS Software TCP Initial Sequence Number Randomization Improvements
Revision 1.0: INTERIM
For Public Release 2001 February 27 20:00 US/Eastern (UTC+0500)

Summary

Cisco IOS software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers.

This vulnerability is present in all released versions of Cisco IOS software running on Cisco routers and switches. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts.

To remove the vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is described in DDTS record CSCds04747.

Workarounds are available that limit or deny successful exploitation of the vulnerability by filtering traffic containing forged IP source addresses at the perimeter of a network or directly on individual devices.

This notice will be posted at <http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml>. (CSCds04747)

Open Caveats in Release 12.0(10)W5(18f)

This section describes open caveats in Cisco IOS Release 12.0(10)W5(18f):

- When the Layer 3 Services Module is configured as a DHCP relay agent, it fails to drop DHCP packets with hop counts over 16. (CSCdr21806)
- When the Layer 3 Services Module is configured as a relay agent, it sends DHCP discover packets (with their primary IP address) to the DHCP server that is requesting an IP address for the DHCP client in the same subnet. If the primary pool of IP addresses is excluded and only the secondary pool is available on the DHCP server, the DHCP discover packet with the primary IP address should be rejected, but it is not. The functionality to resend DHCP requests with the secondary IP address when the primary IP address fails will be available in a later release. (CSCdr23558)
- IRB and CRB are not supported. (CSCdr31970)
- When accessed through SNMP, the QoS mapping table lists an entry with an incorrect precedence index value of 4. This value must be in a range from 0 to 3. (CSCdr24893)
- A CPU HOG condition occurs on the switch after you enter the **no ipx router eigrp** command for routes learned through IEEE 802.1Q encapsulation on the Gigabit Ethernet port. After approximately 15 seconds, the console prompt returns. (CSCdp37972)

- Cisco IOS does not update the IPX routing table when more than two equal hop paths are available and one of them is shut down. For example, a switch with three interfaces (I1, I2, and I3) might have an IPX network configured on each interface, as N1, N2, and N3, respectively. A remote IPX network (R) is accessible through N1, N2, and N3 interfaces. The maximum equal hop paths is set to 2. The IOS routing table will show two destination paths (N1 and N2) in the IPX routing table, the interface I2 will shut down. Because all the three paths are equal hop, the IOS routing table should show N1 and N3 as two equal hop paths. However, the routing table shows only N1 as the destination path.

Workaround: Enter the **clear ipx route** command. The routing table will show N1 and N3 as the destination next hop paths. (CSCdp13515)

Resolved Caveats in Release 12.0(10)W5(18f)

This section describes the resolved caveats in Cisco IOS Release 12.0(10)W5(18f):

- Packets are switched out on the native VLAN, leading to routing by the CPU. Untagged packets coming in on the 802.1Q native VLAN are not processed by the microcode. Instead they are given to the CPU, and the CPU does the processing. This means that high CPU utilization will be seen if untagged packets are received at a high rate on the native VLAN subinterfaces. (CSCdp33630)
- If the native VLAN on a port is cleared from the allowed range of VLANs for the port's trunk link, the port will not appear to be in the native VLAN in the configuration file. (CSCdr31412)
- Address Resolution Protocol (ARP) packets are consumed and flooded by IOS even though IP routing is turned off globally. (CSCdr39535)
- Border Gateway Protocol (BGP) is not supported. (CSCdr32464)
- AppleTalk routing is not supported. (CSCdr30658)

Open Caveats in Release 12.0(7)W5(15d)

This section describes open caveats in Cisco IOS Release 12.0(7)W5(15d):

- If the native VLAN on a port is cleared from the allowed range of VLANs for the port's trunk link, the port will not appear to be in the native VLAN in the configuration file. (CSCdr31412)
- When the Layer 3 Services Module acts as a relay agent, it sends DHCP discover packets (with its primary IP address) to the DHCP server requesting an IP address for the DHCP client in the same subnet. If the primary pool of IP addresses is excluded and only the secondary pool is available on the DHCP server, the DHCP discover packet with the primary IP address should be rejected, but it is not. The functionality to resend DHCP requests with the secondary IP address when the primary IP address fails will be available in a later release. (CSCdr23558)
- When the Layer 3 Services Module is configured as a DHCP relay agent, it fails to drop DHCP packets with hop counts over 16. (CSCdr21806)
- TACACS+ authentication does not work properly if a banner is configured. The banner is either not displayed or the banner is displayed but does not prompt for the username and password, which causes the authentication to fail.

Workaround: Do not configure TACACS+ authentication with a banner. (CSCdr46740)



Note This problem has not been seen in later versions of software.

- IRB and CRB are not supported. (CSCdr31970)
- Border Gateway Protocol (BGP) is not supported. (CSCdr32464)
- AppleTalk routing is not supported. (CSCdr30658)

Resolved Caveats in Release 12.0(7)W5(15d)

There were no resolved caveats in 12.0(7)W5(15d).

Related Documentation

Although their Release Notes are unique, the 4 platforms (Catalyst 4500, Catalyst 4900, Catalyst ME 4900, and Catalyst 4900M) use the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide*. Refer to the following home pages for additional information:

- Catalyst 4500 Series Switch Documentation Home
<http://www.cisco.com/go/cat4500/docs>
- Catalyst 4900 Series Switch Documentation Home
<http://www.cisco.com/go/cat4900/docs>
- Cisco ME 4900 Series Ethernet Switches Documentation Home
http://www.cisco.com/en/US/products/ps7009/tsd_products_support_series_home.html

Hardware Documents

Installation guides and notes including specifications and relevant safety information are available at the following URLs:

- *Catalyst 4500 Series Switches Installation Guide*
<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/installation/guide/78-14409-08/4500inst.html>
- *Catalyst 4500 E-series Switches Installation Guide*
<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/catalyst4500e/installation/guide/Eseries.html>
- For information about individual switching modules and supervisors, refer to the *Catalyst 4500 Series Module Installation Guide* at:
http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/module/guide/mod_inst.html
- *Regulatory Compliance and Safety Information for the Catalyst 4500 Series Switches*
http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/regulatory/compliance/78_13233.html
- Installation notes for specific supervisor engines or for accessory hardware are available at:
http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_installation_guides_list.html
- Catalyst 4900 and 4900M hardware installation information is available at:

http://www.cisco.com/en/US/products/ps6021/prod_installation_guides_list.html

- Cisco ME 4900 Series Ethernet Switches installation information is available at:
http://www.cisco.com/en/US/products/ps7009/prod_installation_guides_list.html

Software Documentation

Software release notes, configuration guides, command references, and system message guides are available at the following URLs:

- Catalyst 4500 release notes are available at:
http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_release_notes_list.html
- Catalyst 4900 release notes are available at:
http://www.cisco.com/en/US/products/ps6021/prod_release_notes_list.html
- Cisco ME4900 4900 Series Ethernet Switch release notes are available at:
http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_11511.html

Software documents for the Catalyst 4500 Classic, Catalyst 4500 E-Series, Catalyst 4900, and Cisco ME 4900 Series Ethernet Switches are available at the following URLs:

- *Catalyst 4500 Series Software Configuration Guide*
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- *Catalyst 4500 Series Software Command Reference*
http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_command_reference_list.html
- *Catalyst 4500 Series Software System Message Guide*
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_system_message_guides_list.html

Cisco IOS Documentation

Platform-independent Cisco IOS documentation may also apply to the Catalyst 4500 and 4900 switches. These documents are available at the following URLs:

- Cisco IOS configuration guides, Release 12.x
http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html
- Cisco IOS command references, Release 12.x
http://www.cisco.com/en/US/products/ps6350/prod_command_reference_list.html

You can also use the Command Lookup Tool at:

<http://tools.cisco.com/Support/CLILookup/cltSearchAction.do>

- Cisco IOS system messages, version 12.x
http://www.cisco.com/en/US/products/ps6350/products_system_message_guides_list.html

You can also use the Error Message Decoder tool at:

<http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi>

- For information about MIBs, refer to:
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

Service and Support

For service and support for a product purchased from a reseller, contact the reseller. Resellers offer a wide variety of Cisco service and support programs, which are described in the “Service and Support” section in the information packet that was shipped with your product.



Note

If you purchased your product from a reseller, you can access Cisco.com as a guest. Cisco.com is Cisco Systems’ primary real-time support channel. Your reseller offers programs that include direct access to Cisco.com services.

For service and support for a product purchased directly from Cisco, use Cisco.com.

Software Configuration Tips on the Cisco TAC Home Page

For helpful tips on configuring Cisco products, follow this path on Cisco.com:

Service & Support: Technical Assistance Center

“Software Technical Tips” are popular tips and hints gathered from Cisco’s Technical Assistance Center (TAC). Most of these documents are also available from the TAC’s Fax-on-Demand service. To access Fax-on-Demand and receive documents at your fax machine, call 888-50-CISCO (888-502-4726). From international areas, call 650-556-8409.

In addition to “Software Technical Tips,” the following sections are on the Technical Documents page:

- Cisco Product Catalog—MultiNet & Cisco Suite 100, Network Management, Cisco IOS Software Bulletins, CiscoPro Configurations.
- Field Notices—Notification of critical issues regarding Cisco products. These include problem descriptions, safety or security issues, and hardware defects.
- Hardware Technical Tips—Technical tips related to specific hardware platforms.
- Hot Tips—Popular tips and hints for a range of product suites, gathered from Cisco’s Technical Assistance Center (TAC).
- Internetworking Technical Tips—Tips for using and deploying Cisco IOS software features and services.
- Sample Configurations—Actual configuration examples complete with topology and annotations.
- Special Collections—Other helpful documents: Frequently Asked Questions, Security Advisories, References & RFCs, Case Studies, and the CiscoPro Documentation CD-ROM.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0711R)

Copyright © 2001—2004 Cisco Systems, Inc. All rights reserved.