



Text Part Number: 78-6138-05 Rev. -B0

# Release Notes for Cisco AS5200 Universal Access Servers for Cisco IOS Release 12.0 T

---

**January 21, 2000**

These release notes for Cisco AS5200 universal access servers support Cisco IOS Release 12.0 T, up to and including Release 12.0(7)T. These release notes are updated as needed to accommodate memory requirements, new features, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of software caveats that apply to Release 12.0 T, see the *Caveats for Cisco IOS Release 12.0 T* document that accompanies these release notes. The caveats document is updated for every maintenance release, and is location on Cisco Connection Online (CCO) and the Documentation CD-ROM. For more information, refer to the "Caveats" on page 26 of these release notes.

Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.0* located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

## Contents

These release notes discuss the following topics:

- Introduction, page 2
- System Requirements, page 2
- New and Changed Information, page 7
- Limitations and Restrictions, page 20
- Important Notes, page 20
- Caveats, page 26
- Related Documentation, page 26
- Service and Support, page 31
- Cisco Connection Online, page 32
- Documentation CD-ROM, page 32

---

### Corporate Headquarters

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

Copyright © 1999-2000  
Cisco Systems, Inc.  
All rights reserved.

## Introduction

The Cisco AS5200 universal access server is a multifaceted data communications platform that provides all the functions of an access server, a router, modems, and terminal adapters (TAs) in a modular chassis. Mid-sized organizations or service providers requiring centralized processing capabilities for mobile users and telecommuters will benefit the most using the Cisco AS5200 universal access server.

With their optimization for high-speed modem access, the Cisco AS5200 universal access servers are ideally suited for all traditional dial-up applications, such as host access, electronic mail, file transfer, and dial-in access to a local area network.

For information on new features and Cisco IOS commands supported by Release 12.0 T, see the “New and Changed Information” on page 7 and “Related Documentation” on page 26.

## System Requirements

This section describes the system requirements for Release 12.0(7)T:

- Memory Requirements, page 2
- Hardware Supported, page 3
- Determining the Software Version, page 3
- Updating to a New Software Release, page 3
- Modem Code, page 3
- Feature Set Tables, page 4

## Memory Requirements

describes the memory requirements for the Cisco AS5200 platform feature sets supported by Cisco IOS Release 12.0(7)T.

**Table 1** Memory Requirements for the Cisco AS5200 Access Server

Image Name	Software Image	Flash Memory Required	DRAM Memory Required	Runs from
IP	c5200-i-1	16 MB	8 MB	Flash
IP Plus	c5200-is-1	16 MB	16 MB	Flash
Desktop	c5200-d-1	16 MB	8 MB	Flash
Desktop Plus	c5200-ds-1	16 MB h	16 MB	Flash

## Hardware Supported

The following are LAN interfaces supported on the Cisco AS5200 universal access servers:

- Ethernet (AUI)
- MultiChannel Interface (Channelized E1/T1)

The following are WAN data rates supported on the Cisco AS5200:

- 48/56/64 kbps
- 1.544/2.048 Mbps

The following are WAN interfaces supported on the Cisco AS5200:

- EIA/TIA-232
- X.21
- V.35
- EIA/TIA-449
- EIA-530
- ISDN PRI
- E1-G.703/G.704
- Channelized T1
- Channelized E1
- Serial

## Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco AS5200, log in to the Cisco AS5200 and enter the **show version** EXEC command:

```
router>show version
Cisco Internetwork Operating System Software
IOS (tm) AS5200 Software (c5200-i-1), Version 12.0(7)T, RELEASE SOFTWARE
```

## Updating to a New Software Release

For information on upgrading to a new software release, see the product bulletin *Cisco IOS Software Release 12.0 T Upgrade Paths and Packaging Simplification (#819: 1/99)* on CCO at:

**Service & Support: Product Bulletins: Software**

Under **Cisco IOS 12.0**, click **Cisco IOS Software Release 12.0 T Upgrade (#819: 1/99)**.

## Modem Code

Cisco IOS Release 11.2(2) and later releases, including Release 12.0(7)T, include bundled modem code for the Cisco AS5200, which is the firmware or portware that runs on the Microcom 12-port and MICA 6-port modem cards. Modem code is bundled with the Cisco IOS software image to eliminate the need to store separate modem code. When the Cisco AS5200 access server starts, the Cisco IOS software unpacks the modem code and loads the proper code on the modem cards. Table 2 lists the current bundled modem code versions for the Cisco AS5200.

**Table 2 Current Bundled Modem Code Version**

Modem Code Module	Current Bundled Modem Code Version	Cisco IOS Software Releases
Microcom modems	Microcom version 5.1.20	Release 12.0(5)T and later
MICA modems	MICA portware Version 2.7.1.0	Release 12.0(5)T and later

**Note** You could have received a later version of modem code than the one bundled with the Cisco IOS software. The modem code in Flash memory is mapped to the modems. Unless you fully understand how Cisco IOS software uses modem code, it is important to keep the factory configuration.

The *Cisco IOS Software Upgrade Planner* on CCO contains information about downloading software. To access this document from CCO, click **Login** on the CCO home page to access all information. From the CCO home page, go to the Service & Support area menu, click **Software Center**, then **Cisco IOS Software** or **IOS Upgrade Planner**.

The modem code release notes are on CCO and on the Documentation CD-ROM.

On CCO at:

**Technical Documents: Documentation Home Page: Access Servers and Access Routers: Firmware and Portware Information**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Access Servers and Access Routers:Firmware and Portware Information**

## Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images — depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Table 3 lists the Cisco IOS software feature sets available for the Cisco AS5200, including the feature set name, the feature set matrix term, the software image name, and supported platforms.

**Table 3 Feature Sets Supported by Cisco AS5200 Universal Access Servers**

Feature Set	Image Name	Feature Set Matrix Term	Software Image
<b>IP Standard Feature Set</b>	IP	Basic <sup>1</sup>	c5200-i-1
	IP Plus	Basic, Plus <sup>2</sup>	c5200-is-1
<b>Desktop Standard Feature Set</b>	Desktop	Basic	c5200-d-1
	Desktop Plus	Basic, Plus	c5200-ds-1

<sup>1</sup> This feature is offered in the basic feature set.

<sup>2</sup> This feature is offered in the Plus feature set.



**Caution** Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to [export@cisco.com](mailto:export@cisco.com).

Table 4 lists the features and feature sets supported by the Cisco AS5200 for Cisco IOS Release 12.0(7)T and uses the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, (7) means a feature was introduced in 12.0(7)T. If a cell in this column is empty, the feature was included in the initial base release.

**Note** This feature set table contains only a selected list of features. This table is not cumulative — nor complete list of all the features in each image.

**Table 4 Feature List by Feature Set for the Cisco AS5200 Universal Access Server**

Features	In <sup>1</sup>	Software Images by Feature Set			
		IP	IP Plus	Desktop	Desktop Plus
<b>IBM Support</b>					
Bridging Code Rework		Yes	Yes	Yes	Yes
RIF Passthru in DLSw+		No	No	No	No
<b>IP Routing</b>					
Asynch over UDP	(5)	Yes	Yes	Yes	Yes
Easy IP Phase 2-DHCP Server	(1)	Yes	Yes	Yes	Yes
IP Type of Service and Precedence for GRE Tunnels		Yes	Yes	Yes	Yes
OSPF Point to Multipoint		Yes	Yes	Yes	Yes
Per User DNS		Yes	Yes	Yes	Yes
<b>Management</b>					
Cisco IOS File System		Yes	Yes	Yes	Yes
CNS Client for Cisco IOS Software	(4)	No	No	No	No
CNS client for IOS 12.05(t) (aka IPSec Policy Agent II)	(5)	No	No	No	No
Entity MIB		Yes	Yes	Yes	Yes
Expression MIB		Yes	Yes	Yes	Yes
Conditionally Triggered Debugging		Yes	Yes	Yes	Yes
ISDN MIB RFC 2127	(1)	Yes	Yes	Yes	Yes
Generic Filesystem Layer (OS_IFSS)	(4)	Yes	Yes	Yes	Yes

## System Requirements

**Table 4 Feature List by Feature Set for the Cisco AS5200 Universal Access Server (continued)**

Features	In <sup>1</sup>	Software Images by Feature Set			
		IP	IP Plus	Desktop	Desktop Plus
Multicast Routing Monitor	(5)	Yes	Yes	Yes	Yes
Process MIB	(4)	Yes	Yes	Yes	Yes
Show Caller		Yes	Yes	Yes	Yes
SNMP Inform Request		No	No	No	No
SNMP Manager		Yes	Yes	Yes	Yes
Cisco SNMP Version 3	(4)	Yes	Yes	Yes	Yes
Virtual Console	(1)	Yes	Yes	Yes	Yes
VPDN MIB and Syslog Facility		No	Yes	No	Yes
<b>Multimedia</b>					
Protocol-Independent Multicasts (PIM) v2		Yes	Yes	Yes	Yes
<b>Quality of Service</b>					
CLI String Search	(1)	Yes	Yes	Yes	Yes
<b>Scalability</b>					
Airline Product Set (ALPS)		Yes	Yes	Yes	Yes
<b>Security</b>					
Additional Vendor-Proprietary RADIUS Attributes		Yes	Yes	Yes	Yes
Authenticating ACLs		Yes	Yes	Yes	Yes
Automated Double Authentication		Yes	Yes	Yes	Yes
MS-CHAP Support		No	No	No	No
Named Method Lists for AAA Authentication & Accounting		Yes	Yes	Yes	Yes
Parse Bookmarks	(4)	Yes	Yes	Yes	Yes
Subblock Phase 1		Yes	Yes	Yes	Yes
<b>WAN Optimization</b>					
DRP Server Agent Enhancement		Yes	Yes	No	Yes
<b>WAN Services</b>					
Always On/Dynamic ISDN (AO/DI)		No	No	No	No
ATM E.164 Auto Conversion		Yes	Yes	Yes	Yes
Dialer Watch		Yes	Yes	Yes	Yes
ISDN LAPB-TA	(4)	Yes	Yes	Yes	Yes
Large Scale Dialout	(4)	Yes	Yes	No	No
Layer 2 Tunneling Protocol	(1)	No	Yes	No	Yes
Layer 2 Tunneling Protocol Dial Out	(5)	No	Yes	No	Yes
Microsoft Point-to-Point (MPPC)		Yes	Yes	Yes	Yes
MS Callback		Yes	Yes	Yes	Yes
Multiple ISDN Switch Types		Yes	Yes	Yes	Yes

**Table 4 Feature List by Feature Set for the Cisco AS5200 Universal Access Server (continued)**

Features	In <sup>1</sup>	Software Images by Feature Set			
		IP	IP Plus	Desktop	Desktop Plus
National ISDN Switch Types		Yes	Yes	Yes	Yes
Signaling System 7 (SS7)	(4)	No	Yes	No	Yes
Stackable Home Gateway		No	Yes	No	Yes
<b>Miscellaneous</b>					
Cisco Resource Pool Manager	(4)	Yes	Yes	Yes	Yes
Flow Random Early Detection (Flow WRED)	(4)	Yes	Yes	Yes	Yes
Subnetwork Bandwidth Manager	(5)	Yes	Yes	Yes	Yes
<b>New</b>					
Configuring RADIUS for Multiple User Datagram Protocol Ports	(7)	Yes	Yes	Yes	Yes
Dynamic Multiple Encapsulation for Dial-in over ISDN	(7)	Yes	Yes	Yes	Yes
Resource Pool Management Server	(7)	Yes	Yes	Yes	Yes
Resource Pool Management with Direct Remote Services	(7)	Yes	Yes	Yes	Yes
Selecting AAA Server Groups Based on DNIS	(7)	Yes	Yes	Yes	Yes

<sup>1</sup> This column indicates the maintenance release in which the feature was introduced. If this cell is empty in this column, this feature was introduced in the initial base release.

## New and Changed Information

The following sections list the new hardware and software features supported by the Cisco AS5200 universal access servers for Release 12.0 T.

### New Software Features in Release 12.0(7)T

The following new hardware features are supported by the Cisco AS5200 for Release 12.0(7)T:

#### Cisco H.235 Accounting and Security Enhancements for Cisco Gateways

The Cisco H.323 gateway now supports the use of CryptoH323Tokens for authentication. The CryptoH323Token is defined in H.225 Version 2 and is used in a “password-with-hashing” security scheme described in section 10.3.3 of the H.235 specification.

A cryptoToken can be included in any RAS message and is used to authenticate the sender of the message. You can use a separate database for user ID and password verification.

With this release, Cisco H.323 gateways support three levels of authentication:

- **Endpoint**—The RAS channel used for gateway-to-gatekeeper signaling is not a secure channel. To ensure secure communications, H.235 allows gateways to include an authentication key in their RAS messages. This key is used by the gatekeeper to authenticate the source of the messages. At the endpoint level, validation is performed on all messages from the gateway. The cryptoTokens are validated using the password configured for the gateway.

- **Per-Call**—When the gateway receives a call over the telephony leg, it prompts the user for an account number and personal identification number (PIN). These two numbers are included in certain RAS messages sent from the endpoint and are used to authenticate the originator of the call.
- **All**—This option is a combination of the other two. With this option, the validation of cryptoTokens in ARQ messages is based on an the account number and PIN of the user making a call and the validation of cryptoTokens sent in all the other RAS messages is based on the password configured for the gateway.

You can configure the level of authentication for the gateway using the Cisco IOS software command line interface.

CryptoTokens for registration requests (RRQ), unregistration request (URQ), disengage request (DRQ) and the terminating side of admission request (ARQ) messages contain information about the gateway that generated the token, including the gateway ID (which is the H.323 ID configured on the gateway) and the gateway password. CryptoTokens for the originating side ARQ messages contain information about the user that is placing the call, including the user ID and personal identification number (PIN).

### Cisco H.323 Multizone Enhancements

Cisco H.323 Multizone enhancements allow a Cisco gateway to provide information to the gatekeeper with additional fields in the RAS (registration, admission, and status) messages.

Previously, the source gateway attempted to set up a call to a destination IP address as provided by the gatekeeper in an Admission Confirm (ACF) message. If the gatekeeper was unable to resolve the destination E.164 phone number to an IP address, the incoming call was terminated.

This version of the H.323 software adds support to allow a gatekeeper to provide additional destination information and modify the destinationInfo field in the ACF. The gateway will include the canMapAlias associated destination information in setting up the call to the destination gateway.

In conjunction with the canMapAlias functionality, this version includes support for the gatekeeper to indicate to the gateway that the call should be destined to a new E.164 number. The gatekeeper indicates this by sending an Admission Confirm message with an IP address of 0.0.0.0 in the destCallSignalAddress field and the new destination E.164 phone number in the destinationInfo field.

The gateway receiving such an ACF will fall back to routing the call based on this new E.164 address and performing a new lookup of the gateway's configured dial plan. This may result in the call being routed back to the PSTN or to an H.323 endpoint.

### Configuring RADIUS for Multiple User Datagram Protocol Ports

In past Cisco IOS releases, RADIUS hosts were uniquely identified by their IP addresses; therefore, only one definition of a RADIUS server for each IP address was allowed. The Configuring RADIUS for Multiple UDP Ports feature expands RADIUS implementation so that RADIUS security servers are identified by their IP addresses and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

The Configuring RADIUS for Multiple UDP Ports feature also applies to RADIUS server groups—server groups can now include multiple service definitions for host entries for the same server, as long as each entry has a unique identifier.

### Dynamic Multiple Encapsulations for Dial-In over ISDN

The Dynamic Multiple Encapsulations feature allows incoming calls over ISDN to be assigned an encapsulation type such as Frame Relay, PPP, and X.25 based on calling line identification (CLID) or DNIS. It also allows various encapsulation types and per-user configurations on the same ISDN B channel at different times according to the type of incoming call.

The Dynamic Multiple Encapsulations feature allows per-user configuration for each dial-in caller on any ingress ISDN B channel on which encapsulation can be run independently from other B channels on the same ISDN link. The caller is identified by CLID (caller ID) or DNIS to ensure that only incoming calls with authorization and valid user profiles are accepted. When PPP is used, authentication and profile binding can also be done by PPP name.

In addition, a large set of user profiles can be stored in dialer profiles locally or on a remote AAA server. (For large scale dial-in, storing user-specific configurations on a remote server becomes necessary for enhancing expandability and local memory efficiency.) However, whether stored locally or on a remote AAA server, the user-specific encapsulation and configuration can be applied to individual B channels dynamically and independently.

Dynamic multiple encapsulation is especially important in Europe where ISDN is relatively inexpensive and maximum use of all 30 B channels on the same ISDN link is desirable. Further, the feature removes the need to statically dedicate channels to a particular encapsulation and configuration type, and improves channel usage.

### Gateway Support for Alternate Gatekeeper

The Alternate Gatekeeper feature provides redundancy for a gatekeeper in a system where gatekeepers are used. This enhancement allows a gateway to use up to two alternate gatekeepers as a backup in the case of a primary gatekeeper failure.

A gatekeeper manages H.323 endpoints in a consistent manner, allowing them to register with the gateway and to locate another gatekeeper. The gatekeeper provides logic variables for proxies or gateways in a call path, to provide connectivity with the public switched telephone network (PSTN), to improve Quality of Service (QoS), and to enforce security policies. Multiple gatekeepers may be configured to communicate with one another, either by integrating their addressing into Domain Naming System (DNS) or using Cisco IOS configuration options.

### Redundant Link Manager

Part of the Cisco SS7 Dial Access Solution (DAS), the Cisco Redundant Link Manager (RLM) provides link management over multiple IP networks, so that your Cisco SS7 DAS can tolerate a single point of failure.

By using the RLM functionality, the Q.931 signaling protocol and other proprietary protocols are transported on top of multiple redundant links between a telephony controller and the media gateways (MGWs).

A feature enhancement to RLM for this Cisco SS7 DAS release is redundancy at the link and telephony-controller level. When each RLM group has multiple telephony controllers associated with a MGW, a telephony-controller priority and a link priority are examined by the RLM client during failover, ensuring improved control handling. The RLM client is an MGW running RLM software.

The RLM client on the MGW supports both versions of RLM functionality:

- Multiple redundant links between a single telephony-controller and the MGWs (Version 1)
- Multiple redundant links between multiple telephony-controllers and the MGWs (Version 2)

After installation, the RLM client defaults to Version 2; however, you can choose a different version by using a command line interface (CLI) configuration command. Once an RLM version is selected, all RLM groups on a given MGW use the selected version's functionality.

---

**Note** The RLM feature is backwards compatible on the telephony-controller, but only one version of the RLM client can run on a given MGW.

---

### Resource Pool Management Server

Part of the Cisco SS7 Dial Access Solution (DAS), the Cisco Resource Pool Manager Server (RPMS) communicates with the RPM component of the MGWs to enable telephone companies and ISPs to count, control, bill, and manage resources centrally for wholesale and retail dial network services. RPM is configured across multiple MGW stacks using one or more external RPMS.

The Cisco RPMS provides the following:

- Customer shared-resource management
- Advanced wholesale (VPDN) services for enterprise accounts and ISPs
- Efficient use of resources to offer different oversubscription ratios and dial-service agreements
- Combination of retail and wholesale services on the same MGWs

Cisco RPMS offers three major functions:

- Resource management uses the call type and dialed number identification service (DNIS) information to accept or reject the call based on the customer profile session limits associated with the DNIS information. If the call is accepted, the call is assigned to an MGW resource.
- Dial services determines how the call is handled after it is answered. The call can be authenticated locally or sent to a home gateway through a VPDN tunnel (using the DNIS information or a domain name).
- Call discrimination is used to prevent unapproved call types from accessing MGW resources. When a call is placed, the MGW sends the call type and dialed number information service (DNIS) information to the Cisco RPMS. The Cisco RPMS compares this combination to the call discrimination table. If the call type-DNIS combination appears in the table, the call is rejected.

### Resource Pool Management with Direct Remote Services

Cisco Resource Pool Manager (RPM) enables telephone companies and ISPs to share dial resources for wholesale and retail dial network services in a single network access server (NAS) or across multiple NAS stacks. With Cisco RPM, service providers can count, control, and manage dial resources and provide accounting for shared resources when implementing different service-level agreements.

Cisco RPM can be configured in one or more standalone Cisco NASs, or, optionally, across multiple NAS stacks by using one or more external Cisco Resource Pool Manager Servers (RPMSs).

The Cisco RPM is ideal for combining retail and wholesale dial services using Cisco AS5200, AS5300, and AS5800 network access servers. Call management and call discrimination can be configured to occur before the call is answered. Dial customers are differentiated by the use of configurable customer profiles that are based on the Dialed Number Information Service (DNIS) and the call type determined at the time of an incoming call. When a call arrives at the NAS, the DNIS and call type are matched against a table of disallowed calls. If the DNIS and call type match an entry in this table, the call is rejected. Call discrimination can be used to manage the billing of calls to different types of resources.

When management by virtual private dialup network (VPDN) is configured, a VPDN group includes the information needed to set up or reject a VPDN session. VPDN setup can be based on the DNIS received during call setup, or on the domain name after the call is answered. Load balancing is used to achieve full usage of VPDN tunnels. The VPDN group can also serve as the “customer profile” when all calls are answered and sessions are identified and limited by domain name instead of DNIS.

To support data over voice bearer service (DoVBS), service providers use DNIS to direct calls to the appropriate resource. When a digital call arrives at the NAS through the voice network, it terminates on a High-Level Data Link Control (HDLC) controller rather than on a modem.

Direct remote services is an enhancement to Cisco resource pool management (RPM) implemented in Cisco IOS Release 12.0(7)T that enables service providers to implement wholesale dial services without using VPDN tunnels. A customer profile that has been preconfigured with a PPP template to define the unique PPP services for the wholesale dial customer is selected by the incoming DNIS and call type. At the same time, the DNIS is used to select AAA server groups for authentication/authorization and for accounting for the customer.

### Selecting AAA Server Groups Based on DNIS

In past Cisco IOS releases, authentication and accounting services (otherwise referred to as AAA services) have been implemented in one of the following methods:

- Globally—meaning that AAA services were defined using global configuration access list commands and applied in general to all interfaces on a specific network access server
- Per Interface—meaning that AAA services were defined using interface configuration commands and applied specifically to the interface being configured on a specific network access server
- Using the AAA DNIS Map feature as described in the Cisco IOS Release 12.0(2)T *Selecting AAA Servers Using DNIS Numbers* feature module—meaning that you could use DNIS to specify one AAA server to supply AAA services

With Cisco IOS Release 12.0(7)T, you can now select an AAA server group to which authentication and accounting requests will be sent by using DNIS. With this new Selecting AAA Server Groups Based on DNIS feature, you can specify the same server group for AAA services or a separate server group for each AAA service. You can now configure authentication and accounting on different physical devices and provide failover backup support.

This feature obsoletes the previous Cisco IOS Release 12.0(2)T AAA DNIS Map feature.

# New Software Features in Release 12.0(5)T

The following new hardware features are supported by the Cisco AS5200 for Release 12.0(5)T:

### Asynchronous Serial Traffic over UDP

The Asynchronous Serial Traffic over UDP feature provides the ability to encapsulate asynchronous data into UDP packets, and then unreliably send this data without needing to establish a connection with a receiving device.

You load the data you want to send through an asynchronous port, and then send it, optionally, as a multicast or a broadcast. The receiving device(s) can then receive the data whenever it wants. If the receiver ends reception, the transmission is unaffected.

This process is referred to as UDP Telnet (UDPTN), although it does not (and cannot) use the Telnet protocol. UDPTN is similar to Telnet in that both are used to send data, but UDPTN is unique in that it does not require that a connection be established with a receiving device.

### Cisco Resource Pool Manager

The Cisco Resource Pool Manager (RPM) feature enables telephone companies and Internet service providers (ISPs) to share dial resources for wholesale and retail dial network services. With RPM, telcos and ISPs can count, control, and manage dial resources and provide accounting for shared resources when implementing different service-level agreements. Resource pool management can be configured in a single, standalone Cisco network access server using RPM or, optionally, across multiple network access server stacks using one or more external Cisco Resource Pool Manager Servers.

### CNS Client for Cisco IOS Software

Cisco Networking Services (CNS) Client feature for Cisco IOS software enables authenticated directory access. CNS Client for Cisco IOS software includes the following components:

- Lightweight Directing Access Protocol (LDAP) V.3 client
- Support to use Kerberos V.5 as security protocol for LDAP V.3 client
- CNS Event Services Client
- CNS Locator Services Client
- CNS IP Security (IPSec) virtual private network (VPN) Provisioning Agent
- CNS Configuration Change Notification Agent
- CNS Provisioning Agent

LDAP V.3 client functionality enables Cisco IOS software-based applications to securely authenticate to a CNS for Active Directory (CNS/AD) server using Kerberos V.5 as security protocol to retrieve or store information such as policy and configuration data. Cisco IOS software-based applications publish or subscribe to events using CNS event services client, enabling external applications using the application programming interface (API) features of CNS to receive events or publish events to the Cisco IOS device. This Cisco IOS software-based device will use CNS locator services client to locate the nearest directory server using Domain Name System. The administrator need not configure the device to locate the nearest directory server.

All the above-mentioned functionality is intended for use by internal Cisco IOS application developers. CNS IPsec VPN provisioning agent enables the router to retrieve IPsec policies stored in the CNS/AD server and configure itself, automating the provisioning of customer premises equipment devices for IPsec VPN. CNS provisioning agent enables Cisco IOS device to be provisioned using CNS event services.

### Layer 2 Tunneling Protocol Dial-out

The Layer 2 Tunneling Protocol (L2TP) Dial-Out feature enables L2TP Network Servers (LNSs) to tunnel dial-out VPDN calls using L2TP as the tunneling protocol. This feature enables a centralized network to efficiently and inexpensively establish a virtual point-to-point connection with any number of remote offices.

Using the L2TP Dial-Out feature, Cisco routers can carry both dial-in and dial-out calls in the same L2TP tunnels.

Previously, only dial-in VPDN calls were supported.

L2TP dial-out involves two devices: an LNS and an L2TP Access Concentrator (LAC). When the LNS wants to perform L2TP dial-out, it negotiates an L2TP tunnel with the LAC. The LAC then places a PPP call to the client(s) the LNS wants to dial-out to.

### Multicast Routing Monitor

The Multicast Routing Monitor (MRM) feature is a management diagnostic tool that provides network fault detection and isolation in a large multicast routing infrastructure. It is designed to notify a network administrator of multicast routing problems in near real time.

MRM has three components that play different roles: the Manager, the Test Sender, and the Test Receiver. The Manager can reside on the same device as the Test Sender or Test Receiver. You can test a multicast environment using test packets (perhaps before an upcoming multicast event), or you can monitor existing IP multicast traffic.

You create a test based on various test parameters, name the test, and start the test. The test runs in the background and the command prompt returns. If the Test Receiver detects an error (such as packet loss or duplicate packets), it sends an error report to the router configured as the Manager. The Manager immediately displays the error report. Also, by issuing a certain **show** command, you can see the error reports, if any. You then troubleshoot your multicast environment as normal, perhaps using the **mtrace** command from the source to the Test Receiver. If the **show** command displays no error reports, the Test Receiver is receiving test packets without loss or duplicates from the Test Sender.

### Service Assurance Agent

The Service Assurance (SA) Agent is both an enhancement to and a new name for the Response Time Reporter (RTR) feature that was introduced in Cisco IOS Release 11.2. The feature allows you to monitor network performance by measuring key Service Level Agreement metrics such as response time, network resources, availability, jitter, connect time, packet loss, and application performance.

With Cisco IOS Release 12.0(5)T, the SA Agent provides new capabilities that enable you to:

- Monitor the Domain Name Server, DHCP Server, and DLSw peer stack and tunnel performance. Thresholds can be used to trigger additional collection of time delay statistics.
- Monitor network one-way delay variance (jitter) and packet loss.
- Monitor web server response time.

### Subnetwork Bandwidth Manager

Resource Reservation Protocol (RSVP) is a signalling mechanism that supports request of specific levels of service such as reserved bandwidth from the network. RSVP and its service class definitions are largely independent of the underlying network technologies. This independence requires that a user define the mapping of RSVP onto subnetwork technologies.

The Subnetwork Bandwidth Manager (SBM) feature answers this requirement for RSVP in relation to IEEE 802-based networks. SBM specifies a signalling method and protocol for LAN-based admission control for RSVP flows. SBM allows RSVP-enabled routers and Layer 2 and Layer 3 devices to support reservation of LAN resources for RSVP-enabled data flows. The SBM signalling method is similar to that of RSVP itself. SBM protocol entities have the following features:

- Reside in Layer 2 or Layer 3 devices.
- Can manage resources on a segment. A segment is a Layer 2 physical segment shared by one or more senders, such as a shared Ethernet or Token Ring wire.
- Can become candidates in a dynamic election process that designates one SBM as the segment manager. The elected candidate is called the Designated Subnetwork Bandwidth Manager (DSBM). The elected DSBM is responsible for exercising admission control over requests for resource reservations on a managed segment.

## New Software Features in Release 12.0(4)T

The following new software enhancements are supported by the Cisco AS5200 universal access servers in Cisco IOS Release 12.0(4)T.

### Cisco IOS SNMPv3

Cisco IOS Simple Network Management Protocol version 3 (SNMPv3) addresses issues related to the large scale deployment of SNMP for configuration, accounting and fault management. Currently SNMP is predominantly used for monitoring and performance management. The primary goal of SNMPv3 is to define a secure version of the SNMP protocol. SNMPv3 also facilitates remote configuration of the SNMP entities which make remote administration of SNMP entities a much simpler task. SNMPv3 builds on top of SNMPv1 and SNMPv2 to provide a secure environment for the management of systems and networks.

SNMPv3 provides an identification strategy for SNMP devices to facilitate communication only between known SNMP strategy. Each SNMP device has an identifier called the SNMP EngineID which is a copy of SNMP. Each SNMP message contains an SNMP EngineID. SNMP communication is possible only if an SNMP entity knows the identity of its peer SNMP device.

SNMPv3 also contains a security model or security strategy that exists between an SNMP user and the SNMP group to which the user belongs. A security model may define the security policy within an administrative domain or a intranet. The SNMPv3 protocol consists of the specification for the User based Security Model (USM).

Definition of security goals where the goals of message authentication service includes the following protection strategies:

- **Modification of Information** or protection against some unauthorized SNMP entity altering in-transit SNMP messages generated on behalf of an authorized principal)
- **Masquerade** or protection against attempting management operations not authorized for some principal by assuming the identity of another principal that has the appropriate authorizations
- **Message Stream Modification** or protection against messages getting maliciously re-ordered, delayed or replayed in order to effect unauthorized management operations

- **Disclosure** or protection against eavesdropping on the exchanges between SNMP engines. Three different types of communication mechanisms are available for this protection strategy. They are:
  - communication without authentication and privacy (NoAuthNoPriv)
  - communication with authentication and without privacy (AuthNoPriv)
  - communication with authentication and privacy (AuthPriv)

#### Dynamic Multiple Encapsulation for Dial-In over ISDN

The Dynamic Multiple Encapsulations feature allows incoming calls over Integrated Services Digital Network (ISDN) to be assigned an encapsulation type such as Point-to-Point Protocol (PPP), X.25, and ISDN Link Access Procedure, Balanced-Terminal Adapter (LAPB-TA) based on calling line identification (CLID) or Dialed Number Identification Service (DNIS). It also allows various encapsulation types and per-user configurations on the same ISDN B channel at different times according to the type of incoming call.

The Dynamic Multiple Encapsulations feature allows per-user configuration for each dial-in caller on any ingress ISDN B channel on which encapsulation can be run independently from other B channels on the same ISDN link. The caller is identified by CLID or DNIS to make sure that only incoming calls with authorization and valid user profiles are accepted. When PPP is used, authentication and profile binding can also be done by PPP name.

Dynamic multiple encapsulation is especially important in Europe where ISDN is relatively inexpensive and maximum use of all 30 B channels on the same ISDN link is desirable. Further, the feature removes the need to statically dedicate channels to a particular encapsulation and configuration type, and improves channel usage.

#### Flow-Based Weighted Random Early Detection (WRED)

Weighted Random Early Detection (WRED) is a mechanism that helps avoid congestion in packet-switched networks. The transport layer reacts to congestion indications coming from the router, such as in a TCP/IP network. A router can indicate to upper layer protocols that congestion is taking place either by marking the packet or dropping it. WRED drops packets to indicate congestion. In a TCP/IP network, when TCP detects that a packet has been dropped, it goes into a slow start phase that enables it to determine the rate at which it can send traffic through the network without dropping.

WRED allows control of queue size to eliminate long delays and avoid tail-dropping when the queue fills up. When a router tail-drops packets, it drops anything that exceeds the transmit queue limit. WRED uses the time since the last drop and the current queue size to determine whether a packet should be dropped. The time factor prevents WRED from dropping multiple packets from a TCP traffic stream within a short period of time, giving the TCP session enough time to detect that a packet has been dropped and go into a slow start phase. WRED uses the queue size factor to specify different dropping thresholds by IP precedence; IP precedence defines the type of service required. WRED gives a higher discard trigger to RSVP packets.

Flow-based WRED is an extension to WRED that penalizes flows that do not back off or respond to dropping from the network. Adaptive, fragile flows tend to send short bursts of traffic and have fewer packets buffered. Thus, if their packets arrive when the average queue depth is high, they are just as likely to have packets dropped as the rest of the flows. WRED does not recognize the fact that these sessions have fewer packets in the output queue overall. Flow-based WRED adjusts for this by keeping track of which flows are using more than the allowable portion of resources. Non-adaptive flows do not respond to WRED's congestion signals and are therefore more likely to use up the output queue/buffers more greedily. Flow-based WRED recognizes this and penalizes them more aggressively.

Flow-based WRED allows a per-flow threshold for all active flows in the output queue. This threshold allows each flow to have a certain number of packets in the output queue before it is marked for dropping. The effect is that adaptive flows are less likely to experience packet dropping because they have an allocated portion of resources even when the average queue depth is high. Non-adaptive flows are more likely to experience packet dropping because they are more inclined to exceed their resource allowance.

### ISDN LAPB-TA

To carry asynchronous traffic over ISDN, you need a terminal adapter to convert that traffic and forward it over synchronous connections. This is normally implemented by the V.120 protocol, which carries asynchronous traffic over ISDN. (For more information on the V.120 protocol, see “Configuring V.120 Access” in the Dial Solutions Configuration Guide.)

However, several countries in Europe (Germany, Switzerland, and some Eastern European countries) use LAPB (Link Access Procedure, Balanced) as the protocol to forward their asynchronous traffic over synchronous connections.

Cisco routers, therefore, needed to be able to recognize and accept calls from these asynchronous/synchronous conversion devices, which is why LAPB-TA (Link Access Procedure, Balanced-Terminal Adapter) was created. (LAPB is sometimes referred to as “X.75,” because LAPB is the link layer specified in the ITU-T X.75 recommendation for carrying asynchronous traffic over ISDN.)

LAPB-TA allows someone with an ISDN terminal adapter that supports asynchronous traffic over LAPB to call into the router and establish an asynchronous PPP (point to point protocol) session. LAPB supports both local CHAP (challenge handshake authentication protocol) authentication and external RADIUS authorization on the AAA (authentication, authorization and accounting) server.

### Large Scale Dialout

In previous dial-on-demand routing (DDR) networking strategies, only incoming calls could take advantage of features such as dialer and virtual profiles, Multichassis

Multilink PPP (MMP) support, and the ability to use an authentication, authorization, and accounting (AAA) server to store attributes. MMP allows network access servers (NASes) to be stacked together and appear as a single NAS chassis so that if one NAS fails, another NAS in the stack can accept calls. MMP also provides stacked NASes access to a local Internet point of presence (POP) using a single telephone number. This allows for easy expansion and scalability, as well as assured fault tolerance and redundancy. Now with large scale dialout, these features are available for both outgoing and incoming calls.

Large scale dialout eliminates the need to configure dialer maps on every NAS for every destination. Instead, you create remote site profiles containing outgoing call attributes (telephone number, service type, and so on) on the AAA server. The profile is downloaded by the NAS when packet traffic requires a call to be placed to a remote site.

Additionally, large scale dialout addresses congestion management by seeking an uncongested, alternative NAS within the same POP when the designated primary NAS experiences port congestion.

As an added benefit, large scale dialout enables scalable dial-out service to many remote sites across one or more Cisco NASes or Cisco routers. This is especially beneficial to both Internet service providers (ISPs) and large scale enterprise customers because it can simplify network configuration and management. Large scale dialout streamlines activities such as service maintenance and scheduled activities like application upgrades from a centralized location. Large enterprise networks such as those used by retail stores, supermarket chains, and franchise restaurants can use large scale dialout to easily update daily prices and inventory information from a central server to all branch locations in one process, using the same NASes they currently use for dial in functions.

### Multilink Multiplexor

The Multilink Point to Point Protocol (MLP) Inverse Multiplexor feature allows you to combine T1/E1 lines in a Versatile Interface Processor (VIP) into a bundle that has the combined bandwidth of the multiple T1/E1 lines. This is done by using a VIP MLP link. You choose the number of bundles and the number of T1/E1 lines in each bundle. This allows you to increase the bandwidth of your network links beyond that of a single T1/E1 line without having to purchase a T3 line.

### Parse Bookmarks

The Parse Bookmarks feature quickly processes consecutive similar commands, such as **access-lists** and **prefix-lists**—up to five times faster than usual. Parse bookmarks reduce boot and load time for large configurations with many similar consecutive commands. This feature is an enhancement to the parsing algorithm, therefore no configuration changes are needed.

### Process MIB

The addition of the CISCO-PROCESS-MIB and changes to the CISCO-MEMORY-POOL-MIB will allow the retrieval of more CPU and memory statistics. This information will be particularly used by the Device Health Monitor Application.

### Signaling System 7

SS7 is the international standard for the common channel signaling system. SS7 defines the architecture, network elements, interfaces, protocols, and the management (MGMT) procedures for a network which transports control information between network switches and between switches and databases. The North American version is also sometimes referred to as CCS7. SS7 is used between the PSTN switches replacing per-trunk in-band signaling, LEC switches, IEC switches, and between LEC and IEC networks.

The SS7 is implemented on a separate data network within the PSTN and provides call setup and teardown, network management, fault resolution, and traffic management services. The SS7 network is solely used for network control and the only data sent over it is signaling messages. (Note that the term SS7 can be used to refer to the SS7 protocol, the signaling network, or the signaling network architecture.)

The SS7 protocols that convey signaling information between switching systems (called signaling points) in the PSTN are carried on a special overlay network used exclusively for signaling. The signaling points use routing information in the SS7 signals to transfer calls to their final destinations.

### Virtual Console

The Virtual Console feature allows you to access dial and router shelves connected to a system controller. During a system controller session, you can connect to a router or dial shelf at the same privilege level as the current system controller session.

By entering one command, you can Telnet directly to a shelf, provide a username and password, and then go to the same privilege level as the system controller.

### No New Features in Release 12.0(3)T

There are no new features supported by the Cisco AS5200 in Cisco IOS Release 12.0(3)T.

### No New Features in Release 12.0(2)T

There are no new features supported by the Cisco AS5200 in Cisco IOS Release 12.0(2)T.

### New Software Features in Release 12.0(1)T

The following new software features are supported by the Cisco AS5200 universal access servers for Release 12.0(1)T.

#### CLI String Search

The Command Line Interface (CLI) String Search feature allows you to search or filter any **show** or **more** command's output. This is useful when you need to sort through large amounts of output, or if you want to exclude output that you do not need to see. CLI String Search also allows for searching and filtering at --More-- paging prompts.

With the search function, you can begin unfiltered output at the first line that contains a regular expression you specify. You can specify a maximum of one filter per command to either include or exclude output lines that contain the specified regular expression.

A regular expression is any word, phrase, number, etc. that appears in **show** or **more** command output.

#### Easy IP Phase 2-DHCP Server

With the introduction of Easy IP Phase 2, Cisco IOS software also supports Intelligent DHCP Relay functionality. A DHCP Relay Agent is any host that forwards DHCP packets between clients and servers. A DHCP Relay Agent enables the client and server to reside on separate subnets. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its own database, it can forward the DHCP request to one or more secondary DHCP servers defined by the network administrator using standard Cisco IOS IP helper-address functionality.

#### ISDN MIB RFC2127

The new Integrated Services Digital Network (ISDN) Management Information Base (MIB) RFC2127 has been designed to provide useful information in accordance with the IETF's new standard for the management of ISDN interfaces. RFC2127 provides information on the physical Basic Rate interfaces, control and statistical information for B (bearer) and D (signaling) channels, terminal endpoints, and directory numbers.

The ISDN MIB RFC2127 controls all aspects of ISDN interfaces. It consists of five groups:

- ISDN Physical Interface Group
- B (Bearer) Channel Group
- D (Signaling) Channel Group
- Terminal Endpoint Group
- Directory Number Group (optional)

The ISDN MIB RFC2127 enables you to use any commercial SNMP network management application to support ISDN call processing in Cisco IOS software. You can integrate management of dial access products using ISDN with your existing network management systems.

### Layer Two Tunneling Protocol (L2TP)

Layer Two Tunneling Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer Two Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for Access Virtual Private Networks (VPNs). Access VPNs allow mobile users to connect to their corporate intranets or extranets, thus improving flexibility and reducing costs.

Traditional dial-up networking services only supported registered IP address, which limited the types of applications that could be implemented over Virtual Private Networks (VPNs). L2TP supports multiple protocols and unregistered and privately administered IP addresses over the Internet. This allows the existing access infrastructure, such as the Internet, modems, access servers, and ISDN terminal adaptors (TAs), to be used.

L2TP can be initiated wherever PPTP or L2F is currently deployed and can be operated as a client initiated tunnel, such as PPTP, or a network access server (NAS) initiated tunnel, such as L2F.

## Limitations and Restrictions

### MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. Currently, OLD-CISCO-\* MIBs are being converted into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 5:

**Table 5 Depreciated and Replacement MIBs**

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	In development
OLD-CISCO-DECNET-MIB	
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	

### Important Notes

This section contains important information about Cisco IOS Release 12.0 T software that can apply to the Cisco AS5300 universal access server.

### Last Maintenance Release of Cisco IOS Release 12.0 T

Cisco IOS Release 12.0(6)T has been renamed 12.0(7)T to align this release with the 12.0(7) mainline release. The closed caveats for Release 12.0(7)T are identical to the caveats closed in the 12.0(7) mainline release. There was no change in the feature content of the renamed release--the features in 12.0(6)T are the same as 12.0(7)T. Release 12.0(7)T is the last maintenance release of the 12.0 T release train.

Customers needing closure of caveats for the 12.0 T features should migrate to the 12.1 mainline release, which has the complete feature content of Release 12.0 T and will eventually reach General Deployment (GD). Release 12.0 T is a super set of the 12.0 mainline release, so all caveats closed in the 12.0 mainline are also closed in 12.0 T.

## Cisco IOS Syslog Failure

Certain versions of Cisco IOS software can fail when they receive invalid User Datagram Protocol (UDP) packets sent to their syslog ports (port 514). At least one commonly used Internet scanning tool generates packets that cause such problems. This fact has been published on public Internet mailing lists, which are widely read both by security professionals and by security crackers. This information should be considered in the public domain.

Attackers can cause Cisco IOS devices to repeatedly fail and reload, resulting in a completely disabled Cisco IOS device that needs to be reconfigured by its administrator. Some Cisco IOS devices can hang instead of failing when attacked. These devices do not recover until they are manually restarted by reset or power cycling. An administrator must visit the device to restart it, even if the attacker is no longer actively sending any traffic. Some devices have failed without providing stack traces; some devices indicate that they were “restarted by power-on,” even when that was not the case.

Assume that any potential attacker knows the existence of this problem and the ways to exploit it. An attacker can use tools available to the public on the Internet and does not need to write any software to exploit the vulnerability. Minimal skill is required and no special equipment is required.

Despite Cisco specifically inviting such reports, Cisco has received no actual reports of malicious exploitation of this problem.

This vulnerability notice was posted on Cisco’s World Wide Web site:

<http://www.cisco.com/warp/public/770/iossyslog-pub.shtml>

This information was also sent to the following e-mail and USENET news recipients:

- [cust-security-announce@cisco.com](mailto:cust-security-announce@cisco.com)
- [bugtraq@netspace.org](mailto:bugtraq@netspace.org)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [first-info@first.org](mailto:first-info@first.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [nanog@merit.edu](mailto:nanog@merit.edu)

### Affected Devices and Software Versions

Table 6 describes hardware and software that are affected by this problem. Affected versions include Releases 11.3 AA, 11.3 DB, and all 12.0 versions (including 12.0 mainline, 12.0 S, 12.0 T, and any other regular released version whose number starts with 12.0), up to the repaired releases listed in Table 6. Cisco is correcting the problem in certain special releases, will correct it in future maintenance and interim releases, and intends to provide fixes for all affected IOS variants. See Table 6, Affected and Repaired Software Versions for details.

No particular configuration is needed to make a Cisco IOS device vulnerable. It is possible to filter out attack traffic by using access lists. See the “Workarounds” on page 23 for techniques. However, except at Internet firewalls, the appropriate filters are not common in customer configurations. Carefully evaluate your configuration before assuming that any filtering you have protects you against this attack.

The most commonly used or asked-about products are listed below. If you are unsure whether your device is running Cisco IOS software, log in to the device and enter the **show version** command. Cisco IOS software will identify itself simply as “IOS” or “Internetwork Operating System

Software.” Other Cisco devices do not have the **show version** command and identify themselves differently in their output. The most common Cisco devices that run Cisco IOS software include the following:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800, uBR900, 1000, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200 (including the uBR7200), 7500, and 12000 series
- Most recent versions of the LS1010 ATM switch
- Some versions of the Catalyst 2900XL LAN switch
- Cisco DistributedDirector

Affected software versions, which are relatively new, are not necessarily available on every device listed above. If you are not running Cisco IOS software, you are not affected by this problem.

The following Cisco devices are *not* affected:

- 700 dialup routers (750, 760, and 770 series)
- Catalyst 1900, 2800, 2900, 3000, and 5000 LAN switches are not affected, except for some versions of the Catalyst 2900XL. However, optional router modules running Cisco IOS software in switch backplanes, such as the RSM module for the Catalyst 5000 and 5500, are affected.
- WAN switching products in the IGX and BPX lines
- MGX (formerly known as the AXIS shelf)
- Host-based software
- Cisco PIX Firewall
- Cisco LocalDirector
- Cisco Cache Engine

This vulnerability has been assigned Cisco bug ID CSCdk77426.

## Solution

Cisco offers free software updates to correct this vulnerability for all affected customers—regardless of their contract status. However, because this vulnerability information has been disseminated by third parties, Cisco has released this notice before updates are available for all software versions. Table 6 gives Cisco’s projected fix dates.

Make sure that your hardware has adequate RAM to support the new software before installing it. The amount of RAM is seldom a problem when you upgrade within a major release, for example, from 11.2[11]P to 11.2[17]P, but it is often a factor when you upgrade between major releases, for example, from 11.2 P to 11.3 T.

Because fixes will be available for all affected releases, this vulnerability will rarely, if ever, require you to upgrade to a new major release. Cisco recommends that you carefully plan for any upgrade between major releases. Make certain no known bugs will prevent the new software from working properly in your environment.

Further upgrade planning assistance is available on Cisco’s World Wide Web site at:

<http://www.cisco.com>

If you have service contracts, you can obtain new software through your regular update channels (generally through Cisco’s World Wide Web site). You can upgrade to any software release, but you must remain within the boundaries of the feature sets you have purchased.

If you do not have service contracts, you can upgrade to only obtain the bug fixes; free upgrades are restricted to the minimum upgrade required to resolve the defects. You can only upgrade to the software described in one row of Table 6—except when no upgrade within the same row is available in a timely manner.

Obtain updates by contacting one of the following Cisco Technical Assistance Centers (TACs):

- +1 800 553 2447 (toll-free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- [tac@cisco.com](mailto:tac@cisco.com)

Give the URL of this notice (<http://www.cisco.com/warp/public/770/iossyslog-pub.shtml>) as evidence for a free update. Customers with no contracts must request for free updates through the TAC. For software updates, please do not contact either “[psirt@cisco.com](mailto:psirt@cisco.com)” or “[security-alert@cisco.com](mailto:security-alert@cisco.com).”

## Workarounds

You can work around this vulnerability by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to port 514. You can do this by either using packet filtering on surrounding devices, or by using input access list filtering on the affected IOS device itself.

If you use an input access list, apply it to all interfaces to which attackers can send datagrams. Interfaces include not only physical LAN and WAN interfaces but also virtual subinterfaces of those physical interfaces—as well as virtual interfaces and interface templates corresponding to GRE, L2TP, L2F, and other tunneling protocols.

The input access list must block traffic destined for UDP port 514 at any of the Cisco IOS device’s own IP addresses—as well as at any broadcast or multicast addresses on which the Cisco IOS device may be listening. Be sure to block both old-style “all-zeros” broadcasts and new-style “all-ones” broadcasts. It is not necessary to block traffic being forwarded to other hosts—only traffic actually addressed to the Cisco IOS device.

No single input access list works in all configurations. Be sure you know the effect of your access list in your specific configuration before activating it.

The following example shows a possible access list for a three-interface router, along with the configuration commands needed to apply the list. The example assumes input filtering is not needed—other than as a workaround for this problem:

```
! Deny all multicasts, and all unspecified-net broadcasts, to port 514
access-list 101 deny udp any 224.0.0.0 31.255.255.255 eq 514
! Deny old-style unspecified-net broadcasts
access-list 101 deny udp any host 0.0.0.0 eq 514
! Deny network-specific broadcasts. This example assumes that all of
! the local interfaces are on the class B network 172.16.0.0, subnetted
! everywhere with mask 255.255.255.0. This will differ from network
! to network. Note that we block both new-style and old-style broadcasts.
access-list 101 deny udp any 172.16.0.255 0.0.255.0 eq 514
access-list 101 deny udp any 172.16.0.0 0.0.255.0 eq 514
! Deny packets sent to the addresses of our own network interfaces.
access-list 101 deny udp any host 172.16.1.1 eq 514
access-list 101 deny udp any host 172.16.2.1 eq 514
access-list 101 deny udp any host 172.16.3.3 eq 514
! Permit all other traffic (default would be to deny)
access-list 101 permit ip any any

! Apply the access list to the input side of each interface
interface ethernet 0
ip address 172.16.1.1 255.255.255.0
ip access-group 101 in

interface ethernet 2
ip address 172.16.2.1 255.255.255.0
ip access-group 101 in

interface ethernet 3
ip address 172.16.3.3 255.255.255.0
ip access-group 101 in
```

Listing all possible addresses—especially all possible broadcast addresses—to which attack packets can be sent is complicated. If you do not need to forward any legitimate syslog traffic received on an interface, you can block all syslog traffic arriving on that interface. Remember that blocking will affect traffic routed through the Cisco IOS device—as well as traffic destined to the device. If the IOS device is expected to forward syslog packets, you will have to filter in detail. Because input access lists impact system performance, install them with caution—especially on systems running very near their capacity.

### Software Versions and Fixes

Many Cisco software images have been or will be specially reissued to correct this vulnerability. For example, regular released Cisco IOS version 12.0(2) is vulnerable, as are interim versions 12.0(2.1) to 12.0(2.3). The first fixed interim version of Release 12.0 mainline software is Release 12.0(2.4). However, a special release, 12.0(2a), contains only the fix for this vulnerability and does not include any other bug fixes from later 12.0 interim releases.

If you are running Release 12.0(2) and want to fix this problem without risking possible instability presented by installing the 12.0(2.4) interim release, you can upgrade to Release 12.0(2a). Release 12.0(2a) is a “code branch” from the Release 12.0(2) base, which will merge back into the Release 12.0 mainline at Release 12.0(2.4).

Special releases, like 12.0(2a), are one-time spot fixes, and they will not be maintained. Thus, the upgrade path from Release 12.0(2a) is to Release 12.0(3).

---

**Note** All dates within this table are subject to change.

---

Table 6 Affected and Repaired Software Versions

Cisco IOS Major Release	Description	Special Fix <sup>1</sup>	First Fixed Interim Release <sup>2</sup>	Fixed Maintenance Release <sup>3</sup>
<b>Unaffected Releases</b>				
11.2 and earlier releases—all variants	Unaffected early releases (no syslog server)	Unaffected	Unaffected	Unaffected
11.3, 11.3 T, 11.3 DA, 11.3 MA, 11.3 NA, 11.3 WA, 11.3(2)XA	11.3 releases without syslog servers	Unaffected	Unaffected	Unaffected
<b>Releases Based on 11.3</b>				
11.3 AA	11.3 early deployment for AS58xx	11.3(7)AA2, 8-JAN-1999 <sup>4</sup>	11.3(7.2)AA	11.3(8)AA, 15-FEB-1999
11.3 DB	11.3 for Cisco NRP routing blade in Cisco 6400 xDSL DSLAM			11.3(7)DB2, 18-JAN-1999
<b>Releases Based on 12.0</b>				
12.0	12.0 Mainline	12.0(2a), 8-JAN-1999	12.0(2.4)	12.0(3), 1-FEB-1999
12.0 T	12.0 new technology early deployment	12.0(2a)T1, 11-JAN-1999	12.0(2.4)T	12.0(3)T, 15-FEB-1999
12.0 S	ISP support; 7200, RSP, GSR		12.0(2.3)S, 27-DEC-1998	12.0(2)S <sup>5</sup> , 18-JAN-1999
12.0 DB	12.0 for Cisco 6400 universal access concentrator node switch processor (lab use)			12.0(2)DB, 18-JAN-1999
12.0(1)W	12.0 for Catalyst 8500 and LS1010	12.0(1)W5(5a) and 12.0(1a)W5(5b) (LS1010 platform only)	12.0(1)W5(5.15)	12.0(1)W5(6) (platform support for Catalyst 8540M will be in 12.0(1)W5(7))
12.0(0.6)W5	One-time early deployment for CH-OC-12 module in Catalyst 8500 series switches	Unaffected; one-time release	Unaffected	Unaffected; To upgrade use 12.0(1)W5 releases.
12.0(1)XA3	Short-life release; merged to 12/0T at 12.0(2)T	Obsolete	Merged	Upgrade to 12.0(2a)T1 or to 12.0(3)T.
12.0(1)XB	Short-life release for Cisco 800 series; merged to 12.0 T and 12.0 (3)T	12.0(1)XB1	Merged	Upgrade to 12.0(3)T.
12.0(2)XC	Short-life release for new features in Cisco 2600, Cisco 3600, uBR7200, uBR900 series; merged to 12.0 T at 12.0(3)T	12.0(2)XC1, 7-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(2)XD	Short-life release for ISDN voice features; merged to 12.0 T at 12.0(3)T	12.0(2)XD1, 18-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(1)XE	Short-life release	12.0(2)XE, 18-JAN-1999	Merged	Upgrade to 12.0(3)T

- 1 A special fix is a one-time release that provides the most stable immediate upgrade path.
- 2 Interim releases are tested less rigorously than regular maintenance releases; interim releases can contain serious bugs.
- 3 Fixed maintenance releases are on a long-term upgrade path. Other long-term upgrade paths also exist.
- 4 All dates in this table are estimates and are subject to change.
- 5 This entry is not a misprint. The 12.0(2.3)S interim release is available before the 12.0(2)S regular release.

## Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

For information on caveats in Cisco IOS Release 12.0 T, see *Caveats for Cisco IOS Release 12.0 T*.

All caveats in Release 12.0 are also in Release 12.0 T.

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, and is located on CCO and the Documentation CD-ROM.

---

**Note** If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco IOS BugToolkit: Cisco Bug Navigator II**, or at: [http://www.cisco.com/support/bugtools/Bug\\_root.html](http://www.cisco.com/support/bugtools/Bug_root.html).

---

## Related Documentation

The following sections describe the documentation available for the Cisco AS5200 universal access servers. These documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on CCO and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 26
- Platform-Specific Documents, page 27
- Feature Modules, page 28
- Cisco IOS Software Documentation Set, page 28

## Release-Specific Documents

The following documents are specific to Release 12.0 T, and they are located on CCO and the Documentation CD-ROM:

- *Release Notes for Cisco IOS Release 12.0 T*

You can reach the *Cross-Platform Release Notes for Cisco IOS Release 12.0* on CCO at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross Platform Release Notes**

You can reach the *Cross-Platform Release Notes for Cisco IOS Release 12.0* on the Documentation CD-ROM, click on this path:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross Platform Release Notes**

- Product bulletins, field notices, and other release-specific documents

You can reach these documents on CCO at:

**Technical Documents: Product Bulletins**

- *Caveats for Cisco IOS Release 12.0* and *Caveats for Cisco IOS Release 12.0 T*

As a supplement to the caveats listed in “Caveats” in these release notes, see *Caveats for Cisco IOS Release 12.0* and *Caveats for Cisco IOS Release 12.0 T* documents, which contain caveats applicable for all platforms for all maintenance releases of Release 12.0 T.

You can reach the caveat document on CCO at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Caveats**

You can reach the caveat document on the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS 12.0: Caveats**

---

**Note** If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco IOS BugToolkit: Cisco Bug Navigator II**, or at: [http://www.cisco.com/support/bugtools/Bug\\_root.html](http://www.cisco.com/support/bugtools/Bug_root.html).

---

## Platform-Specific Documents

These documents are available for the Cisco AS5200 access server on CCO and on the Documentation CD-ROM.

- *Cisco AS5200 Universal Access Server Installation Guide*
- *Cisco AS5200 Universal Access Server Software Configuration Guide*
- *Cisco AS5200 Manager Guide*
- Modem/Terminal Adapter Information
- *Regulatory Compliance and Safety Information*
- Documentation for Spare Parts
- Release notes

You can reach Cisco AS5200 documentation on CCO at:

**Technical Documents: Documentation Home Page: Access Servers and Access Routers: Access Servers: Cisco AS5200**

You can reach Cisco AS5200 documentation on the Documentation CD-ROM at:

**Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5200**

## Feature Modules

Feature modules describe new features supported by Release 12.0 T and are updated to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the features modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

You can reach the feature modules on CCO at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation: New Features in Release 12.0 T**

You can reach the feature modules on the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation: New Features in Release 12.0 T**

## Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents, which are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

### Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

You can reach these documents on CCO at:

**Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Cisco IOS Release 12.0 Configuration Guides and Command References**

You can reach these documents on the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Cisco IOS Release 12.0 Configuration Guides and Command References**

### Release 12.0 Documentation Set

Table 7 describes the contents of the Cisco IOS Release 12.0 software documentation set, which is available in electronic form and also in printed form upon request.

---

**Note** You can find the most current Cisco IOS documentation on CCO and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the paper documents were printed.

---

You can reach the Cisco IOS documentation set from CCO at:

**Service & Support: Technical Documents: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0**

You can reach the Cisco IOS documentation set on the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0**

**Table 7 Cisco IOS Software Release 12.0 Documentation Set**

<b>Books</b>	<b>Chapter Topics</b>
<ul style="list-style-type: none"> <li>• <i>Configuration Fundamentals Configuration Guide</i></li> <li>• <i>Configuration Fundamentals Command Reference</i></li> </ul>	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> <li>• <i>Bridging and IBM Networking Configuration Guide</i></li> <li>• <i>Bridging and IBM Networking Command Reference</i></li> </ul>	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set
<ul style="list-style-type: none"> <li>• <i>Dial Solutions Configuration Guide</i></li> <li>• <i>Dial Solutions Command Reference</i></li> </ul>	Dial-In Port Setup Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions ISDN X.25 over ISDN VPDN Dial Business Solutions and Examples
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Interface Configuration Guide</i></li> <li>• <i>Cisco IOS Interface Command Reference</i></li> </ul>	Interface Configuration Overview
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 1</i></li> <li>• <i>Network Protocols Command Reference, Part 1</i></li> </ul>	IP Addressing IP Services IP Routing Protocols
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 2</i></li> <li>• <i>Network Protocols Command Reference, Part 2</i></li> </ul>	AppleTalk Novell IPX
<ul style="list-style-type: none"> <li>• <i>Network Protocols Configuration Guide, Part 3</i></li> <li>• <i>Network Protocols Command Reference, Part 3</i></li> </ul>	Apollo Domain Banyan VINES DECnet ISO CLNS XNS

**Table 7 Cisco IOS Software Release 12.0 Documentation Set**

Books	Chapter Topics
<ul style="list-style-type: none"> <li>• <i>Security Configuration Guide</i></li> <li>• <i>Security Command Reference</i></li> </ul>	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Switching Services Configuration Guide</i></li> <li>• <i>Cisco IOS Switching Services Command Reference</i></li> </ul>	Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing
<ul style="list-style-type: none"> <li>• <i>Wide-Area Networking Configuration Guide</i></li> <li>• <i>Wide-Area Networking Command Reference</i></li> </ul>	ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> <li>• <i>Voice, Video, and Home Applications Configuration Guide</i></li> <li>• <i>Voice, Video, and Home Applications Command Reference</i></li> </ul>	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Video Support Universal Broadband Features
<ul style="list-style-type: none"> <li>• <i>Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Quality of Service Solutions Command Reference</i></li> </ul>	Classification Scheduling Packet Drop Traffic Shaping ATM QoS SNA QoS Line Protocols
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Software Command Summary</i></li> <li>• <i>Dial Solutions Quick Configuration Guide</i></li> <li>• <i>System Error Messages</i></li> <li>• <i>Debug Command Reference</i></li> </ul>	

---

**Note** *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco Connection Online. From CCO, click on the following path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**.

---

## Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in “Service and Support” of *Cisco Information Packet* shipped with your product.

---

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

---

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

## Software Configuration Tips from the Cisco Technical Assistance Center

If you have a CCO login account, you can access the following URL, which contains links and tips on configuring your Cisco products:

[http://www.cisco.com/kobayashi/serv\\_tips.shtml](http://www.cisco.com/kobayashi/serv_tips.shtml)

This URL is subject to change without notice. If it changes, point your web browser to CCO and click on this path: **Products & Technologies: Products: Technical Tips.**

The following sections are provided from the Technical Tips page:

- Access Dial Cookbook—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Describes the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Provides technical tips related to specific hardware platforms.
- Hot Tips—Describes popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.
- Internetworking Features—Lists tips on using and deploying Cisco IOS software features and services.
- Sample Configurations—Provides actual configuration examples which are complete with topology and annotations.
- Software Products—Contains Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Applications and Software, Network Management, Network Protection Software Tips, and WAN Switching Products and Software.
- Special Collections—Lists other helpful documents, including Case Studies, References & Requests for Comment (RFCs), and Security Advisories.

## Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can reach CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: [cco.cisco.com](http://cco.cisco.com)
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact [cco-help@cisco.com](mailto:cco-help@cisco.com). For additional information, contact [cco-team@cisco.com](mailto:cco-team@cisco.com).

---

**Note** If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or [tac@cisco.com](mailto:tac@cisco.com). To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or [cs-rep@cisco.com](mailto:cs-rep@cisco.com).

---

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

---

This document is to be used in conjunction with documents mentioned in the "Related Documentation" on page 26.

Access Registrar, AccessPath, Any to Any, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, ConnectWay, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, Kernel Proxy, MGX, MultiPath Data, MultiPath Voice, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, ScriptShare, Secure Script, ServiceWay, Shop with Me, SlideCast, SMARTnet, SVX, *The Cell*, TrafficDirector, TransPath, ViewRunner, Virtual Loop Carrier System, Virtual Service Node, Virtual Voice Line, VisionWay, VlanDirector, Voice LAN, WaRP, Wavelength Router, Wavelength Router Protocol, WebViewer, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9912R)

Copyright © 1999-2000, Cisco Systems, Inc.  
All rights reserved. Printed in USA.

