



# Release Notes for Cisco 1400 Series for Cisco IOS Release 12.0 T

---

**December 13, 1999**

These release notes for Cisco 1400 series support Cisco IOS Release 12.0 T, up to and including Release 12.0(7)T. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of the software caveats that apply to Release 12.0(7)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 located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

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

## Contents

These release notes describe the following topics:

- System Requirements, page 2
- New and Changed Information, page 7
- Important Notes, page 9
- Caveats, page 16
- Related Documentation, page 16
- Obtaining Documentation, page 21
- Obtaining Technical Assistance, page 22



---

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

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

# System Requirements

This section describes the system requirements for Release 12.0 T:

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

## Memory Requirements

**Table 1** Memory Requirements for the Cisco 1400 Series

Feature Set	Software Image	Required Flash Memory	Required DRAM Memory	Runs from	In <sup>1</sup>
IP/IPX	c1400-ny-mz	4 MB	16 MB	RAM	
IP/IPX Plus	c1400-nsy-mz	4 MB	16 MB	RAM	
IP/IPX/FW Plus	c1400-nosy-mz	6 <sup>2</sup> MB	16 MB	RAM	(3) <sup>3</sup>
IP/FW Plus IPSec 56	c1400-osy56i-mz	6 MB	16 MB	RAM	(7)

1. The number in the “In” column indicates the Cisco IOS release when the image was first introduced. For example, (7) means an image was introduced in Release 12.0(7)T. If a cell in this column is empty, the interface was included in the initial base release.
2. 4 MB in Release 12.0(5)T and earlier releases.
3. This feature set was initially introduced in Release 12.0(2)T for the Cisco 1401 router only.

## Hardware Supported

Cisco IOS Release 12.0 T supports the Cisco 1400 series:

- Cisco 1401
- Cisco 1417

For detailed descriptions of the new hardware features, see the “New and Changed Information” section on page 7.

Following are some of the key features of the Cisco 1400 series:

- ATM-25 port (Cisco 1401 router)---For connecting through a DSL modem over an ADSL line to a central service provider.
- ADSL port (Cisco 1417 router)---For connecting directly over an ADSL line to a central service provider.
- Console port---For connecting a terminal or PC to configure and manage the router. Supports up to 9600 bps (up to 115.2 kbps for software download).
- Supports IP, IPX, PPP over ATM, and firewall security.
- Supports ATM features such as ATM Adaption Layer 5, ATM PVCs, and RFC 1483.

- Supports SNMP for management over an SNMP network.
- Supports Cisco ATM Management Information Base (MIB).

## Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 1400 series, log in to the router and enter the **show version EXEC** command:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 1400 Software (C1400-NY-MZ), Version 12.0(7)T, RELEASE SOFTWARE
```

## Upgrading 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:

**Technical Documents: Product Bulletins: Software**

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

## 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.

Release 12.0 T supports the same feature sets as Release 12.0, but Release 12.0 T can include new features supported by the Cisco 1400 series.

**Table 2** Feature Sets Supported by the Cisco 1400 Series

Feature Sets	Image Names	Feature Set Matrix Term	Software Image	Platforms	In <sup>1</sup>
IP Feature Sets	IP/IPX	Basic <sup>2</sup>	c1400-ny-mz	Cisco 1400 series	
	IP/IPX Plus	Plus <sup>3</sup>	c1400-nsy-mz	Cisco 1400 series	
	IP/IPX/FW	Basic	c1400-nosy-mz	Cisco 1400 series	(3) <sup>4</sup>
	IP/FW Plus IPSec 56	Plus, IPSec 56 <sup>5</sup>	c1400-osy56i-mz	Cisco 1400 series	(7)

1. The number in the “In” column indicates the Cisco IOS release when the image was first introduced. For example, (3) means an image was introduced in Release 12.0(3)T. If a cell in this column is empty, the interface was included in the initial base release.
2. This feature set is offered in the basic feature set.
3. This feature set is offered in the Plus feature set.
4. This feature set was initially introduced in Release 12.0(2)T for the Cisco 1401 router only.
5. This feature set is offered in the encryption feature sets, which consist of IPSec 56-bit (Plus IPSec 56) data encryption feature sets.

**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 may require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, the purchaser or the user must obtain local import and use authorizations for all encryption strengths. Contact your sales representative or distributor for more information, or send an e-mail to [export@cisco.com](mailto:export@cisco.com).

Table 3 lists the features and feature sets supported by the Cisco 1400 series in Cisco IOS Release 12.0 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.

**Note**

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

**Table 3** Feature List by Feature Set for the Cisco 1400 Series

Features	Feature Set			
	IP/IPX	IP/IPX Plus	IP/IPX/FW Plus <sup>1</sup>	IP/FW Plus IPsec 56 <sup>2</sup>
<b>IP Routing</b>				
EIGRP	Yes	Yes	Yes	Yes
IGRP	Yes	Yes	Yes	Yes
OSPF	Yes	Yes	Yes	Yes
RIP	Yes	Yes	Yes	Yes
<b>LAN Support</b>				
Virtual Private Network (VPN)	No	Yes	Yes	Yes
<b>Management</b>				
ATM MIB	Yes	Yes	Yes	Yes
CDP MIB	Yes	Yes	Yes	Yes
Chassis MIB	Yes	Yes	Yes	Yes
Configuration/Management MIB	Yes	Yes	Yes	Yes
Flash MIB	Yes	Yes	Yes	Yes
IP Multicast MIBs	No	Yes	Yes	Yes
Image MIB	Yes	Yes	Yes	Yes
IP MIB	Yes	Yes	Yes	Yes
IP Multicast Route MIB	No	Yes	Yes	Yes
IPX MIB	Yes	Yes	Yes	No
NLSP MIB	No	Yes	Yes	Yes

**Table 3 Feature List by Feature Set for the Cisco 1400 Series (continued)**

Features	Feature Set			
	IP/IPX	IP/IPX Plus	IP/IPX/FW Plus <sup>1</sup>	IP/FW Plus IPsec 56 <sup>2</sup>
OSPF MIB	Yes	Yes	Yes	Yes
Queue MIB	Yes	Yes	Yes	Yes
Remote Monitoring	Yes	Yes	Yes	Yes
RSVP MIB	No	Yes	Yes	Yes
Round Trip Time Monitor	Yes	Yes	Yes	Yes
Transparent Bridging MIB	Yes	Yes	Yes	Yes
IP Static Route MIB	Yes	Yes	Yes	Yes
VPN MIB	No	Yes	Yes	Yes
UPD MIB	Yes	Yes	Yes	Yes
SNMP	Yes	Yes	Yes	Yes
<b>Miscellaneous</b>				
Compression	Yes	Yes	Yes	Yes
Multicast Source Discovery Protocol <sup>3</sup>	No	No	No	No
NetFlow Policy Routing	No	Yes	Yes	Yes
<b>Protocols</b>				
Border Gateway Protocol (BGP)	No	Yes	Yes	Yes
Cisco Discovery Protocol (CDP)	Yes	Yes	Yes	Yes
ConnectionLess Network Services (CLNS)	No	Yes	Yes	Yes
DHCP Relay	Yes	Yes	Yes	Yes
DHCP Server	Yes	Yes	Yes	Yes
HTTP	Yes	Yes	Yes	Yes
IP CDP	Yes	Yes	Yes	Yes
IP Compression	Yes	Yes	Yes	Yes
IP Multicast	No	Yes	Yes	Yes
IP Multicast NAT	No	Yes	Yes	Yes
IP NAT	Yes	Yes	Yes	Yes
IP NHRP	Yes	Yes	Yes	Yes
IPX	Yes	Yes	Yes	No
IPX Compression	Yes	Yes	Yes	No
IPX EIGRP	Yes	Yes	Yes	No
IPX NHRP	No	Yes	Yes	No
IPX NLSP	No	Yes	Yes	No
Network Address Translation (NAT)	Yes	Yes	Yes	Yes

**Table 3 Feature List by Feature Set for the Cisco 1400 Series (continued)**

Features	Feature Set			
	IP/IPX	IP/IPX Plus	IP/IPX/FW Plus <sup>1</sup>	IP/FW Plus IPSec 56 <sup>2</sup>
Next Hop Reservation Protocol (NHRP)	Yes	Yes	Yes	Yes
Network Time Protocol (NTP)	No	Yes	Yes	Yes
Resource Reserve Protocol (RSVP)	No	Yes	Yes	Yes
Simple Network Time Protocol (SNTP)	Yes	Yes	Yes	Yes
Serial Tunneling (STP)	Yes	Yes	Yes	Yes
Source Route Bridging (SRB)	Yes	Yes	Yes	Yes
Transparent Bridging	Yes	Yes	Yes	Yes
<b>Security</b>				
Access Lists	Yes	Yes	Yes	Yes
Cisco IOS Firewall: Context-Based Access Control	No	No	Yes	Yes
IPX Access Lists	Yes	Yes	Yes	No
NETBIOS Access Lists	Yes	Yes	Yes	Yes
Radius	Yes	Yes	Yes	Yes
TACACS	Yes	Yes	Yes	Yes
TACACS+	Yes	Yes	Yes	Yes
<b>WAN Services</b>				
Cisco Discovery Protocol over PPP (CCP)	Yes	Yes	Yes	Yes
IPX over WAN	Yes	Yes	Yes	No
Layer 2 Forwarding (L2F)	No	Yes	Yes	Yes
Layer Tunnel Protocol (L2TP)	No	Yes	Yes	Yes
PPP over ATM	Yes	Yes	Yes	Yes
Traffic Shaping	Yes	Yes	Yes	Yes
Virtual Profiles	Yes	Yes	Yes	Yes
Virtual Template	Yes	Yes	Yes	Yes

1. This feature set was introduced for the Cisco 1401 in Release 12.0(2)T, and for the Cisco 1400 series in Release 12.0(3)T.
2. This feature set was introduced for the Cisco 1400 series in Release 12.0(7)T.
3. This feature was introduced in Release 12.0(7)T.

# New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 1400 series for Release 12.0 T:

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

The following new software enhancements are supported by the Cisco 1400 series for Release 12.0(7)T and later releases.

### One New Feature Set

One new feature set has been created for the Cisco 1400 series in Release 12.0(7)T:

- IP/FW Plus IPSec 56—c1400-osy56i-mz

### Multicast Source Discovery Protocol

Multicast Source Discovery Protocol (MSDP) connects multiple PIM sparse-mode (SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP runs MSDP over TCP to discover multicast sources in other domains.

An RP in a PIM-SM domain has an MSDP peering relationship with MSDP-enabled routers in another domain. The peering relationship occurs over a TCP connection, where primarily a list of sources sending to multicast groups is exchanged. The TCP connections between RPs are achieved by the underlying routing system. The receiving RP uses the source lists to establish a source path.

The purpose of this topology is to have domains discover multicast sources in other domains. If the multicast sources are of interest to a domain that has receivers, multicast data is delivered over the normal, source-tree building mechanism in PIM-SM.

MSDP is also used to announce sources sending to a group. These announcements must originate at the domain's RP.

MSDP depends heavily on (M)BGP for interdomain operation. You should run MSDP in your domain's RPs that act as sources, sending to global groups for announcement to the Internet.

## New Hardware Features in Release 12.0(5)T

The following new hardware enhancements are supported by the Cisco 1400 series for Release 12.0(5)T and later releases.

### Cisco 1417 Routers

The Cisco 1417 is one in a family of low-end routers providing Ethernet-based CPE devices with an ADSL link to a telco Central Office. It is designed to provide high speed WAN access over regular copper phone lines for small remote branch offices or home offices; it provides data communications services for one or more Ethernet nodes, while at the same time allowing voice communications to a telephone. The Cisco 1417 is the second of the Cisco 1400 family of CPE routers. It is based on the Cisco 1401 1E1ATM25, and incorporates the ADSL interface using an Alcatel chip set.

## No New Features in Release 12.0(4)T

There are no new features supported by the Cisco 1400 series in Cisco IOS Release 12.0(4)T.

## New Software Features in Release 12.0(3)T

The following new software enhancement is supported by the Cisco 1400 series for Release 12.0(3)T and later releases.

### One New Feature Set

The following feature set is now available for the Cisco 1400 series in Release 12.0(3)T:

- IP/IPX/FW Plus—c1400-nosy-mz



**Note**

---

This feature set is available for the Cisco 1401 router beginning in Release 12.0(2)T.

---

## New Software Features in Release 12.0(2)T

The following new software enhancement is supported by the Cisco 1401 router for Release 12.0(2)T and later releases.

### One New Feature Set

One new feature set is now available for the Cisco 1401 router *only* in Release 12.0(2)T and later releases:

- IP/IPX/FW Plus—c1400-nosy-mz

## No New Features in Release 12.0(1)T

There are no new features supported by the Cisco 1400 series in Cisco IOS Release 12.0(1)T.

## Important Notes

The following sections contain important notes about Cisco IOS Release 12.0 that can apply to the Cisco 1400 series.

### 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.

### Caveat CSCdr91706 and IOS HTTP Vulnerability

A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled, browsing to `http://router-ip/anytext?/` is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.

The vulnerability, identified as Cisco bug ID CSCdr91706, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 12.0 through 12.1, inclusive. This is not the same defect as CSCdr36952.

The vulnerability has been corrected and Cisco is making fixed releases available for free to replace all affected IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect as shown in detail below.

This vulnerability can only be exploited if the enable password is known or not set.

You are strongly encouraged to read the complete advisory, which is available at <http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml>.

### Cisco IOS Syslog Failure

Certain versions of Cisco IOS software may fail or hang 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 have been observed to hang instead of failing when attacked. These devices do not recover until they are manually restarted by reset or power cycling. An administrator must personally visit an attacked, hung 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 may indicate that they were “restarted by power-on,” even when that is not the case.

Assume that any potential attacker is likely to know that 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

Vulnerable devices and software versions are specified in Table 4, *Affected and Repaired Software Versions*. 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 4. Cisco is correcting the problem in certain special releases and will correct it in future maintenance and interim releases. See Table 4, *Affected and Repaired Software Versions* for details. Cisco intends to provide fixes for all affected IOS variants.

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” section on page 12 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 issue the **show version** command. Cisco IOS software will identify itself simply as “IOS” or “Internetwork Operating System Software”. Other Cisco devices will not have the **show version** command, or they will 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 4 gives Cisco's projected fix dates.

Make sure 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 (say, from 11.2[11]P to 11.2[17]P), but it is often a factor when you upgrade between major releases (say, from 11.2 P to 11.3 T).

Because fixes will be available for all affected releases, this vulnerability will rarely, if ever, require an upgrade to a new major release. Cisco recommends very careful planning 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 obtain only the bug fixes; free upgrades are restricted to the minimum upgrade required to resolve the defects. In general, you will be restricted to upgrading within a single row of Table 4, 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. Non-contract customers must request free updates through the TAC. Please do not contact either “psirt@cisco.com” or “security-alert@cisco.com” for software updates.

## Workarounds

You can work around this vulnerability by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to its port 514. This can be done 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 that list to all interfaces to which attackers may be able to send datagrams. Interfaces include—not only physical LAN and WAN interfaces—but 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 is of interest.

No single input access list works in all configurations. 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 vulnerability:

```
! 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 do the detailed filtering. 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 version 12.0(2) is vulnerable, as are interim versions 12.0(2.1) through 12.0(2.3). The first fixed interim version of 12.0 mainline software is 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 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 12.0(2a). Release 12.0(2a) is a “code branch” from the 12.0(2) base, which will merge back into the 12.0 mainline at 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 12.0(2a) is to 12.0(3).

specifies information about affected and repaired software versions.



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

**Table 4** *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—all variants	Unaffected early releases (no syslog server)	Unaffected	Unaffected	Unaffected
11.3, 11.3T, 11.3DA, 11.3MA, 11.3NA, 11.3WA, 11.3(2)XA	11.3 releases without syslog servers	Unaffected	Unaffected	Unaffected
<b>Releases based on 11.3</b>				
11.3AA	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
11.3DB	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
12.0T	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

**Table 4** *Affected and Repaired Software Versions (continued)*

<b>Cisco IOS Major Release</b>	<b>Description</b>	<b>Special Fix<sup>1</sup></b>	<b>First Fixed Interim Release<sup>2</sup></b>	<b>Fixed Maintenance Release<sup>3</sup></b>
12.0S	ISP support; 7200, RSP, GSR		12.0(2.3)S, 27-DEC-1998	12.0(2)S <sup>5</sup> , 18-JAN-1999
12.0DB	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-OC12 module in Catalyst 8500 series switches.	Unaffected; one-time release	Unaffected	Unaffected; general upgrade path is via 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 and/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 may 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 in which the vulnerability is fixed.

## Flash defaults to Flash:1 on Multipartition Flash

When using a multipartition flash card, the various flash partitions are referred to as “flash:1:”, “flash:2:”, etc. If you specify only “flash” in a multipartition flash, the parser assumes “flash:1:.” For example, if you enter **show flash all** the parser defaults to “show flash:1: all” and only the flash information for the first partition displays. To see information for all flash partitions, enter **show flash ?**. This will list all of the valid partitions. Then enter **show flash:xx: all** on each valid partition.

## Traffic Shaping

On the ATM25 interface of the Cisco 1400 series there are two types of traffic shaping: hardware-based and software-based. Hardware-based traffic shaping is provided by the ATM SAR chip and is enabled on a per-pvc basis by one of the following IOS PVC configuration commands:

```
ubr      <peak-cell-rate>
ubr+    <peak-cell-rate> <minimum-guaranteed-cell-rate>
vbr-nrt <peak-cell-rate> <sustainable-cell-rate> <maximum-burst-size>
```

The SAR chip has “rate counters” that control the rate at which the current buffer up for segmentation is going to be transmitted. Ideally, the SAR chip could be programmed with values for all of the above command parameters. Unfortunately, it only has the rate counters, which specify a divisor of the basic line rate of 25 Mbps and which really sets the maximum transmission rate (peak-cell-rate) for the channel. Note that with the **ubr** and **ubr+** commands, the rate counter for the PVC is obtained from the <peak-cell-rate> parameter. With the **vbr-nrt** command, the rate counter is obtained from the <sustainable-cell-rate> parameter. While the <minimum-guaranteed-cell-rate> parameter in the **ubr+** command and the <peak-cell-rate> parameter in the **vbr-nrt** command can be specified by the user, they are ignored by the ATM25 driver.

Software-based traffic shaping is enabled on a per-interface basis via the **traffic-shape** interface configuration command. For performance reasons, and since for ATM interfaces you most likely want to do shaping on a per-pvc basis, the ATM driver does not support software-based traffic shaping while fastswitching. However, if fast-switching is disabled and the **traffic-shape** interface configuration command is enabled, then software traffic shaping will occur. (See CSCdk28377 for more information.)

## Image Deferral, Cisco IOS Release 12.0(4)XI

Cisco IOS Release 12.0(4)XI was deferred to Release 12.0(4)XI1 on all software images for the Cisco 1417, uBR7200, and uBR924.

For the Cisco 1417 router, the IP/IPX/FW Plus feature set, c1400-nosy-mz, was deferred due to the firewall not working. This image is now available in Release 12.0(5)T.

# Caveats

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

This section only contains open and resolved caveats for the current Cisco IOS maintenance release.

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

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

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

## Related Documentation

The following sections describe the documentation available for the Cisco 1400 series. 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 16
- Platform-Specific Documents, page 17
- Feature Modules, page 17
- Cisco IOS Software Documentation Set, page 18

## Release-Specific Documents

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

- *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**

On the Documentation CD-ROM at:

**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 on CCO at:

**Service & Support: Technical Documents**

- *Caveats for Cisco IOS Release 12.0 T*

This document contains caveats applicable to all platforms for all maintenance releases of Release 12.0 T.

On CCO at:

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

On the Documentation CD-ROM at:

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

## Platform-Specific Documents

These documents are available for the Cisco 1400 series on CCO and the Documentation CD-ROM:

- *Installing Your Cisco 1401 Router*
- *Installing Your Cisco 1417 Router*
- *Cisco 1400 Series Router Installation and Configuration Guide*
- *Regulatory Compliance and Safety Information*
- *Upgrading DRAM SIMMs in Cisco 1400 Series Routers*
- Release notes for Cisco 1400 series routers

On CCO at:

**Technical Documents: Documentation Home Page: DSL Products: Cisco 1400 Series Routers**

On the Documentation CD-ROM at:

**Cisco Product Documentation: DSL Products: Cisco 1400 Series Routers**

## Feature Modules

Feature modules describe new features supported by Release 12.0 T and are updates 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 feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On CCO at:

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

On the Documentation CD-ROM at:

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

## 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 that 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.

On CCO and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On CCO at:

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

On the Documentation CD-ROM at:

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

### Release 12.0 Documentation Set

Table 5 describes the contents of the Cisco IOS Release 12.0 software documentation set, which is available in electronic form and 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 hard-copy documents were printed.

---

On CCO at:

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

On the Documentation CD-ROM at:

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

**Table 5 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>	X.25 over ISDN Appletalk Remote Access Asynchronous Callback, DDR, PPP, SLIP Bandwidth Allocation Control Protocol ISDN Basic Rate Service ISDN Caller ID Callback PPP Callback for DDR Channelized E1 & T1 Dial Backup for Dialer Profiles Dial Backup Using Dialer Watch Dial Backup for Serial Lines Peer-to-Peer DDR with Dialer Profiles DialOut Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Dialup Networks 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 LAN Interfaces Logical Interfaces Serial Interfaces

**Table 5 Cisco IOS Software Release 12.0 Documentation Set (continued)**

<b>Books</b>	<b>Chapter Topics</b>
<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 Overview IP Addressing and 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>	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<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 Services 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>	Wide-Area Network Overview 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 Frame Relay-ATM Internetworking Synchronized Clocks Video Support Universal Broadband Features

**Table 5** Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
<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>	Policy-Based Routing QoS Policy Propagation via BGP Committed Access Rate Weighted Fair Queueing Custom Queueing Priority Queueing Weighted Random Early Detection Scheduling Signaling RSVP Packet Drop Frame Relay Traffic Shaping Link Fragmentation RTP Header Compression
<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.**

## Obtaining Documentation

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.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 is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

## Ordering Documentation

Registered Cisco.com users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at <http://www.cisco.com/cgi-bin/subcat/kaojump.cgi>.

Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed documents, or by sending mail to Cisco.

## Cisco.com

Cisco continues to revolutionize how business is done on the Internet. Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through Cisco.com, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access Cisco.com in the following ways:

- WWW: [www.cisco.com](http://www.cisco.com)
- Telnet: [cco.cisco.com](telnet://cco.cisco.com)
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using Cisco.com to [cco-team@cisco.com](mailto:cco-team@cisco.com).

## Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use [www.cisco.com/techsupport](http://www.cisco.com/techsupport).

To contact by e-mail, use one of the following:

Language	E-mail Address
English	<a href="mailto:tac@cisco.com">tac@cisco.com</a>
Hanzi (Chinese)	<a href="mailto:chinese-tac@cisco.com">chinese-tac@cisco.com</a>
Kanji (Japanese)	<a href="mailto:japan-tac@cisco.com">japan-tac@cisco.com</a>
Hangul (Korean)	<a href="mailto:korea-tac@cisco.com">korea-tac@cisco.com</a>
Spanish	<a href="mailto:tac@cisco.com">tac@cisco.com</a>
Thai	<a href="mailto:thai-tac@cisco.com">thai-tac@cisco.com</a>

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site:  
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

## Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a Cisco.com log-in account, you can access the following URL, which contains links and tips on configuring your Cisco products:

[http://www.cisco.com/public/technotes/tech\\_sw.html](http://www.cisco.com/public/technotes/tech_sw.html)

This URL is subject to change without notice. If it changes, point your Web browser to Cisco.com, press **Login**, and click on this path: **Technical Assistance Center: 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 Cisco IOS software features and services.
- **Sample Configurations**—Provides actual configuration examples that are complete with topology and annotations.

## Documentation Feedback

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

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.  
Document Resource Connection  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate and value your comments.

---

This document is to be used in conjunction with the documents listed in the “Related Documentation” section on page 16.

AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptShare, SlideCast, SMARTnet, TransPath, Voice LAN, Wavelength Router, WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, IOS, IP/TV, LightStream, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0011R)

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