Text Part Number: 78-5214-06

Release Notes for the Cisco AS5100 and AS5200 Access Servers for Cisco IOS Release 11.2 P

January 18, 1999

These release notes identify the new features and significant software components for the Cisco AS5100 and Cisco AS5200 access servers for Cisco IOS Release 11.2, up to and including Release 11.2(17)P.

For more detailed information about the features and caveats in these release notes, refer to the *Cross-Platform Release Notes for Cisco IOS Release 11.2,* which contains features and caveats for all Release 11.2 platforms. The electronic documentation can be found on Cisco Connection Online (CCO) and on the Documentation CD-ROM. Refer to the "Related Documentation" section on page 25)

Contents

These release notes discuss the following topics:

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

Introduction

The Cisco AS5100 universal access server is a versatile data communications platform that combines all the functions of an access server, a router, and analog and digital modems into one chassis. Organizations requiring centralized processing capabilities for mobile users and telecommuters will benefit the most using the Cisco AS5100 universal access server.

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 AS5100 and 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.

System Requirements

This section describes the system requirements for Cisco IOS Release 11.2 P and includes the following subsections:

Memory Requirements

Table 1 describes the memory requirements of the Cisco IOS features sets for the Cisco AS5100 for Cisco IOS Release 11.2 P, and Table 2 describes the memory requirements of the Cisco IOS features sets for the Cisco AS5200 for Cisco IOS Release 11.2 P.

Note Beginning with Cisco IOS Release 10.3, some software image sizes exceed 4 MB and, when compressed, exceed 2 MB. Also, some systems now require more than 1 MB of main system memory for data structure tables.

Table 1 Cisco AS5100 Memory Requirements

Feature Set	Image Name	Required Flash Memory	Required DRAM Memory	Release 11.2 Runs from[1]
IP	c2500-i-l	8 MB Flash	6 MB DRAM	Flash
Desktop	c2500-d-l	8 MB Flash	6 MB DRAM	Flash
Enterprise	c2500-j-l	8 MB Flash	6 MB DRAM	Flash

1 When a system is running from Flash memory, you cannot update the system while it is running. You must use the Flash memory load helper.

Table 2 Cisco AS5200 Memory Requirements

Feature Set	Image Name	Required Flash Memory	Required DRAM Memory	Release 11.2 Runs from[1]
IP	c5200-i-l	8 MB Flash	8 MB DRAM	Flash
IP Plus[2]	c5200-is-l	8 MB Flash	8 MB DRAM	Flash
Desktop	c5200-d-l	8 MB Flash	8 MB DRAM	Flash
Desktop Plus	c5200-ds-l	8 MB Flash	8 MB DRAM	Flash
Enterprise	c5200-j-l	16 MB Flash	8 MB DRAM	Flash
Enterprise Plus	c5200-js-l	16 MB Flash	8 MB DRAM	Flash

1 When a system is running from Flash memory, you cannot update the system while it is running. You must use the Flash memory load helper.

2 IP Plus for the Cisco AS5200 includes protocol translation, MMP, VPDN, V.120, RMON, Managed Modems, and IBM (if IBM is not already included).

Hardware Supported

Table 3 lists the LAN and WAN interfaces and modem cards supported by the Cisco AS5100 and AS5200 access servers:

Table 3 Supported Interfaces and Modem Cards

Supported LAN/WAN Interfaces
Ethernet (AUI)
EIA/TIA-232
X.21
V.35
EIA/TIA-449
EIA-530
ISDN PRI
E1-G.703/G.704
Channelized T1
Channelized E1
Synchronous serial

Modem Cards
56K (Cisco AS5200)
V.34 Modems (Cisco AS5100 and AS5200)
V.110 terminal adapter (TA) (Cisco AS5200)
V.90 modems (Cisco AS5200)

Note The V.110 terminal adapters are not supported in Cisco IOS Release 11.2(12)P through Release 11.2(15)P.

Determining Your Software Release

To determine the version of Cisco IOS software currently running on your device, log in to the access server and use the **show version** EXEC command. The following is sample output from the **show version** command. The version number is indicated on the second line as shown below:

```
Cisco Internetwork Operating System Software
IOS (tm) 5100 Software (C5100-JS-L), Version 11.2(17)P, RELEASE SOFTWARE
```

Additional command output lines include more information, such as processor revision numbers, memory amounts, hardware IDs, and partition information.

Upgrading to a New Software Release

For information on upgrading to a new software release, refer to the *Cisco IOS Software Release Upgrade Paths and Packaging Simplification Product Bulletin #539*. You can reach this bulletin from CCO or from the Documentation CD-ROM.

- To reach it from CCO, follow this path:

Products & Ordering: **More Information**: **Product Bulletins**: **Cisco IOS Release 11.2**: **Cisco IOS Software Release 11.2 Changes in Packaging and Upgrade Paths (#539: 10/96)**.

- To reach it from the Documentation CD-ROM, follow this path:

  Products & Ordering: **More Information**: **Product Bulletins**: **Cisco IOS Release 11.2**: **Cisco IOS Software Release 11.2 Changes in Packaging and Upgrade Paths (#539: 10/96)**.

Feature Set Tables

Cisco IOS software is packaged in feature sets (also called software images) depending on the platform. Each feature set contains a specific set of Cisco IOS features. Table 4 lists the feature set matrix terms used in Table 6.

Table 4 Feature Set Matrix Terms

Feature Set Matrix Term	Description
Basic	This feature is offered in the basic feature set.
Plus	This feature is offered in the Plus feature set.
Encrypt	This feature is offered in the encryption feature sets, which consist of 40-bit (Plus 40) or 56-bit (Plus 56) data encryption features sets.

Caution Cisco IOS images with strong encryption (including, but not limited to, 56-bit data encryption feature sets) are subject to U.S. government export controls, and have a limited distribution. Images to be installed outside the U.S. require an export license. Customer orders might be denied or subject to delay due to U.S. government regulations. Contact your sales representative or distributor for more information, or send e-mail to export@cisco.com.

Table 5 Feature Set Matrix for the Cisco AS5100 and AS5200

Standard Feature Sets	Cisco AS5100	Cisco AS5200
IP Routing	Basic	Basic and Plus
Desktop (IP/IPX/AppleTalk/DEC)	Basic	Basic and Plus
Enterprise	Basic	Basic and Plus
Remote Access Server	Basic	–

Table 6 lists the features and feature sets supported by the Cisco IOS Release 11.2 P for the Cisco AS5100 and Cisco AS5200:

Table 6 Cisco AS5100 and AS5200 Access Server Software Feature Sets

	Feature Set			
Features Contained in Features Sets	**IP Routing**	**Desktop (IP/IPX/AppleTalk/DEC)**	**Enterprise[1]**	**Remote Access Server[2]**
LAN Support				
Apollo Domain	No	No	Basic	Basic
AppleTalk 1 and 2[3]	No	Basic	Basic	Basic
Banyan VINES	No	No	Basic	No
Concurrent routing and bridging (CRB)	Basic	Basic	Basic	No
DECnet IV	No	Basic	Basic	No
DECnet V	No	No	Basic	Basic
GRE	Basic	Basic	Basic	Basic
Integrated routing and bridging (IRB)[4]	Basic	Basic	Basic	Basic
IP	Basic	Basic	Basic	Basic
LAN extension host	Basic	Basic	Basic	Basic
Multiring	Basic	Basic	Basic	Basic
Novell IPX[5]	No	Basic	Basic	
OSI	No	No	Basic	Basic
Source-route bridging (SRB)	No	No	Basic	No
Transparent and translational bridging	Basic	Basic	Basic	Basic
XNS	No	No	Basic	Basic
WAN Services				
Combinet Packet Protocol (CPP)	Basic	Basic	Basic	Basic
Dialer profiles	Basic	Basic	Basic	Basic
Frame Relay	Basic	Basic	Basic	Basic

Table 6 Cisco AS5100 and AS5200 Access Server Software Feature Sets (continued)

Features Contained in Features Sets	Feature Set			
	IP Routing	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise[1]	Remote Access Server[2]
Frame Relay SVC Support (DTE)	No	No	Basic	Basic
Frame Relay traffic shaping	Basic	Basic	Basic	Basic
Half bridge/half router for CPP and PPP	Basic	Basic	Basic	Basic
HDLC	Basic	Basic	Basic	Basic
IPXWAN 2.0	No	Basic	Basic	Basic
ISDN[6]	Basic	Basic	Basic	No
Multichassis Multilink PPP (MMP)	Plus	Plus	Plus	Plus
PPP[7]	Basic	Basic	Basic	Basic
SMDS	Basic	Basic	Basic	No
Switched 56	Basic	Basic	Basic	Basic
Virtual Private dialup Network (VPDN)	Plus	Plus	Plus	Plus
X.25[8]	Basic	Basic	Basic	Basic
WAN Optimization				
Bandwidth-on-demand	Basic	Basic	Basic	Basic
Custom and priority queuing	Basic	Basic	Basic	Basic
Dial backup	Basic	Basic	Basic	Basic
Dial-on-demand	Basic	Basic	Basic	Basic
Header[9], link and payload compression[10]	Basic	Basic	Basic	Basic
Snapshot routing	Basic	Basic	Basic	Basic
Weighted fair queuing	Basic	Basic	Basic	Basic
IP Routing				
BGP	Basic	Basic	Basic	Basic
BGP4[11]	Basic	Basic	Basic	—
EGP	Basic	Basic	Basic	—
Enhanced IGRP	Basic	Basic	Basic	Basic
Enhanced IGRP Optimizations	Basic	Basic	Basic	Basic
ES-IS	No	No	Basic	No
IGRP	Basic	Basic	Basic	Basic
IS-IS	No	No	Basic	Basic
Named IP Access Control List	Basic	Basic	Basic	Basic
Network Address Translation (NAT)	Plus	Plus	Plus	Basic
NHRP	Basic	Basic	Basic	

Table 6 Cisco AS5100 and AS5200 Access Server Software Feature Sets (continued)

Features Contained in Features Sets	Feature Set			
	IP Routing	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise[1]	Remote Access Server[2]
On Demand Routing (ODR)	Basic	Basic	Basic	Basic
OSPF	Basic	Basic	Basic	No
OSPF Not-So-Stubby-Areas (NSSA)	Basic	Basic	Basic	No
OSPF On Demand Circuit (RFC 1793)	Basic	Basic	Basic	No
PIM	Basic	Basic	Basic	Basic
Policy-based routing	Basic	Basic	Basic	Basic
RIP	Basic	Basic	Basic	Basic
RIP Version 2	Basic	Basic	Basic	Basic
Other Routing				
AURP	No	Basic	Basic	Basic
IPX RIP	No	Basic	Basic	Basic
NLSP	No	Basic	Basic	No
RTMP	No	Basic	Basic	Basic
SMRP	No	Basic	Basic	Basic
SRTP	No	No	Basic	Basic
Multimedia and Quality of Service				
Generic traffic shaping	Basic	Basic	Basic	Basic
Random Early Detection (RED)	Basic	Basic	Basic	Basic
Resource Reservation Protocol (RSVP)	Basic	Basic	Basic	Basic
Management				
AutoInstall	Basic	Basic	Basic	Basic
Automatic modem configuration	Basic	Basic	Basic	Basic
HTTP Server	Basic	Basic	Basic	Basic
Modem Management	Plus	Plus	Plus	Basic
RMON events and alarms[12]	Basic	Basic	Basic	Basic
RMON full	Plus	Plus	Plus	
SNMP	Basic	Basic	Basic	Basic
Telnet	Basic	Basic	Basic	Basic
Security				
Access lists	Basic	Basic	Basic	Basic
Access security	Basic	Basic	Basic	Basic
Extended access lists	Basic	Basic	Basic	Basic
Kerberized login	No	No	Basic	Basic

Table 6 Cisco AS5100 and AS5200 Access Server Software Feature Sets (continued)

Features Contained in Features Sets	Feature Set			
	IP Routing	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise[1]	Remote Access Server[2]
Kerberos V client support	No	No	Basic	No
Lock and key	Basic	Basic	Basic	Basic
MAC security for hubs	Basic	Basic	Basic	No
MD5 routing authentication	Basic	Basic	Basic	Basic
RADIUS	Basic	Basic	Basic	Basic
TACACS+[13]	Basic	Basic	Basic	Basic
IBM Support (Optional)				
APPN (optional)[2]	No	No	No	No
BAN for SNA Frame Relay support	Plus	Plus	Basic	No
Bisync	Plus	Plus	Basic	No
Caching and filtering	Plus	Plus	Basic	
DLSw+ [14]	Plus	Plus	Basic	Basic
Downstream PU concentration (DSPU)	Plus	Plus	Basic	Basic
Frame Relay SNA support (RFC 1490)	Plus	Plus	Basic	No
Native Client Interface Architecture (NCIA) Server	Plus	Plus	Basic	No
NetView Native Service Point	Plus	Plus	Basic	No
QLLC	Plus	Plus	Basic	No
Response Time Reporter (RTR)	Plus	Plus	Basic	
SDLC integration	Plus	Plus	Basic	No
DLSw (RFC 1795)	Plus	Plus	Basic	No
SDLC transport (STUN)	Plus	Plus	Basic	No
SDLC-to-LAN conversion (SDLLC)	Plus	Plus	Basic	No
SNA and NetBIOS WAN optimization via local acknowledgment	Plus	Plus	Basic	No
SRB/RSRB[15]	Plus	Plus	Basic	Basic
SRT	Plus	Plus	Basic	Basic
TG/COS	No	No	Basic	No
TN3270	No	No	Basic	Basic
Protocol Translation				
LAT	No	No	Basic	Basic
Rlogin	No	No	Basic	Basic

Table 6 Cisco AS5100 and AS5200 Access Server Software Feature Sets (continued)

Features Contained in Features Sets	Feature Set: IP Routing	Feature Set: Desktop (IP/IPX/AppleTalk/DEC)	Feature Set: Enterprise[1]	Feature Set: Remote Access Server[2]
Remote Node[16]				
ARAP 1.0/2.0	No	Basic	Basic	Basic
Asynchronous master interfaces	Basic	Basic	Basic	Basic
ATCP	No	Basic	Basic	Basic
CPPP	Basic	Basic	Basic	Basic
CSLIP	Basic	Basic	Basic	Basic
DHCP	Basic	Basic	Basic	Basic
IP pooling	Basic	Basic	Basic	Basic
IPX and ARAP on virtual async interfaces	No	No	Basic	Basic
IPXCP	No	Basic	Basic	
MacIP	No	Basic	Basic	Basic
NASI	No	Basic	Basic	No
NetBEUI over PPP	No	No	Basic	No
SLIP	Basic	Basic	Basic	Basic
Terminal Services[16]				
LAT[17]	No	No	Basic	Basic
Rlogin	Basic	Basic	Basic	Basic
Telnet	Basic	Basic	Basic	Basic
TN3270	No	No	Basic	Basic
X.25 PAD	Basic	Basic	Basic	Basic
Xremote	No	No	Basic	Basic

1 Enterprise is available with APPN in a separate feature set. APPN includes APPN Central Registration (CRR) and APPN over DLSw+.
2 This feature set applies to the Cisco AS5100 only.
3 This feature includes AppleTalk load balancing.
4 IRB supports IP, IPX, and AppleTalk; it is supported for transparent bridging, but not for SRB; it is supported on all media-type interfaces except X.25 and ISDN bridged interfaces; IRB and concurrent routing and bridging (CRB) cannot operate at the same time.
5 The Novell IPX feature includes SAP display by name, IPX Access Control List violation logging, and plain-English IPX access lists.
6 ISDN support includes calling line identification (ANI), X.25 over the B channel, ISDN subaddressing, and applicable WAN optimization features.
7 PPP includes support for LAN protocols supported by the feature set, address negotiation, PAP and CHAP authentication, PPP compression, and Multilink PPP.
8 X.25 includes X.25 switching.
9 IPX header compression (RFC 1553) is available in the feature sets that support IPX.
10 X.25 and Frame Relay payload compression are supported.
11 BGP4 includes soft configuration, multipath support, and prefix filtering with inbound route maps.
12 The RMON events and alarms groups are supported on all interfaces. Full RMON support is available with the Plus feature sets.
13 TACACS+ Single Connection and TACACS+ SENDAUTH enhancements are supported.
14 Cisco IOS Release 11.2 introduces several DLSw+ enhancements available in the Plus, Plus 40, and Plus 56 feature sets.
15 SRB/RSRB is fast switched. This enhancement is on by default, but can be disabled.
16 Terminal services are supported on access servers (with limited support on router auxiliary ports).
17 Use of LAT requires terminal license (FR-L8-10.X= for an 8-user license or FR-L16-10.X= for a 16-user license).

New and Changed Information

The following sections list the new features that are available for the Cisco AS5100 and Cisco AS5200 in the maintenance releases of Cisco IOS Release 11.2 P. Features are detailed in the documentation listed in the "Related Documentation" section on page 25.

New Features in Releases 11.2(11)P through Release 11.2(17)P

There are no new features for the Cisco AS5100 or Cisco AS5200 in Cisco IOS Release 11.2(11)P through Release 11.2(17)P.

Bundled Modem Code for the Cisco AS5200

Bundled modem code version 3.3.20 was provided in Cisco IOS Releases 11.2(15)P and 11.2(16)P.

New Features in Release 11.2(10)P

The following new features are supported by the Cisco AS5200 only and are available in Cisco IOS Release 11.2(10)P and later; these features are not available on the Cisco AS5100.

Modem Pooling for the Cisco AS5200

Modem pooling allows service providers to define, select, and use separate pools of modems within a single access server or router to provide different dial-in services. Modem allocation is based on the dialed number identification service (DNIS) and a predetermined number of modem ports based on DNIS.

There are a number of applications for using the call setup information, including DNIS/ANI, processing incoming call requests with CallerID, and selecting services to set up "automatically" for specified calls. These uses generally fall into two categories: those requiring allocation of a specific number of modems for a specific service, and those requiring allocation of specific physical modems.

Note For step-by-step software configuration information, refer to the online feature module *Modem Pooling for the Cisco AS5200*, which is part of the online publication *Feature Guide for Cisco IOS Release 11.2 P*. For instructions on how to reach this publication via CCO or the Documentation CD-ROM, refer to the "Related Documentation" section on page 25.

Web Cache Control Protocol for the Cisco AS5200

The Web Cache Control Protocol (WCCP) feature allows you to use a Cisco Cache Engine to handle web traffic, thus reducing transmission costs and downloading time. This traffic includes user requests to view pages and graphics on World Wide Web servers, whether internal or external to your network, and the replies to those requests.

Web caches reduce transmission costs and the amount of time required to download web files. If a client requests a web page that is already cached, the request and data only have to travel between the Cisco Cache Engine and the client. Without a web cache, the request and reply must travel over the Internet or wide-area network.

Cisco IOS support of WCCP provides a transparent web cache solution. Users can benefit from web proxy caches without having to configure clients to contact a specific proxy server in order to reach web resources. Many web proxy caches require clients to reach web resources through a specific proxy web server rather than using the originally requested web server URL. With WCCP, the clients send web requests to the desired web server URL. Cisco IOS routers intelligently intercept HTTP requests and transparently redirect them to a Cisco Cache Engine.

Note For step-by-step software configuration information, refer to the online feature module *Web Cache Control Protocol*, which is part of the online publication *Cisco IOS Release 11.2(10+)P New Feature Documentation*. For instructions on how to reach this publication via CCO or the Documentation CD-ROM, refer to the "Related Documentation" section on page 25.

Flash Load Helper for the Cisco AS5200

This feature enables you to upgrade the system software on run-from-Flash memory systems that have a single bank of Flash memory. It is a lower-cost software upgrade solution than dual-bank Flash memory, which requires two banks of Flash memory on one SIMM.

Flash Load Helper is an automated procedure that reloads the ROM-based image, downloads the software to Flash memory, and reboots to the system image in Flash memory. Flash Load Helper performs checks and validations to maximize the success of a Flash memory upgrade and to minimize the chance of leaving Flash memory either in an erased state or with a file that cannot boot.

Fastboot for the Cisco AS5200

This feature speeds up the boot process by using the system image directly from the system bootstrap image without accessing the boot image. To enable this feature, perform a write memory by entering the **copy running-config startup-config command** when running Cisco IOS Release 11.2(10)P or later.

Note If you run an image earlier than Cisco IOS Release 11.2(7)P or perform a write memory with Release 11.2(7)P to 11.2(9)P, the feature will automatically disable itself.

Bundled Modem Code for the Cisco AS5200

For 56K modems, bundled modem code version 3.1.30 was provided. The modem code filename is:

mcom-modem-code-3.1.30.bin

New Features in Releases 11.2(6)P through Release 11.2(9)P

There are no new features for the Cisco AS5100 or AS5200 in Cisco IOS Release 11.2(6)P though Release 11.2(9)P.

New Features in Release 11.2(5)P

The following new feature is supported by the Cisco AS5200 only and are available in Cisco IOS Release 11.2(5)P and later; these features are not available on the Cisco AS5100.

Channelized E1 Signaling for the Cisco AS5200

Cisco IOS Release 11.2(5)P and later support channel-associated signaling for channelized E1 lines, which are commonly deployed in networks in Latin America, Asia, and Europe.

After this feature is configured on a single E1 controller, up to 30 remote users can simultaneously dial in to the Cisco AS5200 through networks running the R2 protocol. Typically, all 30 channels of a channelized E1 line are used for analog calls. However, a signal converter is still needed to perform conversions between R2 signaling and ear and mouth signaling (also known as E&M). Because the Cisco AS5200 has two physical E1 ports on its dual E1 Primary Rate Interface (PRI) board, up to 60 simultaneous connections can be made through the dual E1 PRI board.

These service adapters provide high-performance, hardware-based data compression capabilities via simultaneous stacker compression data compression algorithms with independent full-duplex compression and decompression capabilities on Point-to-Point Protocol (PPP) encapsulated packets.

Note For step-by-step software configuration information, refer to the feature module *Channelized E1 Signaling for the Cisco AS5200*, which is published in the *Feature Guide for Cisco IOS Release 11.2 P*. For instructions on how to reach this publication via CCO or the Documentation CD-ROM, refer to the "Related Documentation" section on page 25.

New Features in Releases 11.2(3)P through Release 11.2(4)P

There are no new features for the Cisco AS5100 or AS5200 in Cisco IOS Release 11.2(3)P through Release 11.2(4)P.

New Features in Releases 11.2(1)P through 11.2(2)P

The following new features are supported by the Cisco AS5200 only and are available in Cisco IOS Release 11.2(1)P and later; these features are not available on the Cisco AS5100.

Robbed-Bit Signaling for the Cisco AS5200

Ground-start and loop-start signaling was provided for channelized T1. This new signaling is set using the **cas-group** controller configuration command.

Note For step-by-step software configuration information, refer to the feature module *Channelized E1 Signaling for the Cisco AS5200*, which is published in the *Feature Guide for Cisco IOS Release 11.2 P*. For instructions on how to reach this publication via CCO or the Documentation CD-ROM, refer to the "Related Documentation" section on page 25.

Dual E1 PRI for the Cisco AS5200

A new E1 PRI card providing physical termination for two E1 PRI lines was introduced. Unlike most controller E1 configurations, the Cisco AS5200's E1 PRI controllers require a clock source, which is set with the **clock source** command.

Note For step-by-step software configuration information, refer to the feature module *Channelized E1 Signaling for the Cisco AS5200*, which is published in the *Feature Guide for Cisco IOS Release 11.2 P*. For instructions on how to reach this publication via CCO or the Documentation CD-ROM, refer to the "Related Documentation" section on page 25.

Additional Features Supported for the Cisco AS5200

Release 11.2(2)P also supports features in the following categories:

- Routing Protocols
- Desktop Protocols
- Wide-Area Networking Features
- IBM Functionality
- Security Features
- Network Management

Important Notes

This section lists important information for this and previous releases.

Some 40-bit Encryption Images Are Unavailable

Cisco is conducting an internal review of the build and distribution processes associated with its 40-bit Cisco IOS cryptographic products. To provide seamless access to Cisco IOS 40-bit encryption capability, Cisco will provide access to the most current 40-bit encryption images, beginning with Cisco IOS Release 11.2 (12), 11.2(12)P, and 11.3(2). The following 40-bit encryption images will be indefinitely unavailable:

- 11.2(1)–11.2(11.2)
- 11.2(2)P–11.2(11.1)P
- 11.2(1)F–11.2(4)F
- 11.3(1)

This review is not related to any new or previously unreported bugs. The information gathered in the review will be used to implement new automated development and order processing applications.

Some V.110 Terminal Adapters are Unavailable

The V.110 terminal adapters are not supported in Cisco IOS Release 11.2(12)P through 11.2(15)P.

Caveats

This section contains the open and resolved caveats for the current Cisco IOS maintenance release only. For a list of software caveats that apply to previous maintenance releases (for example, Release 11.2(14)P), refer to the *Caveats for Cisco IOS Release 11.2P* document that accompanies these release notes. The caveats document is also 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. Bug Navigator II can be found at **http://www.cisco.com/support/bugtools**, or from CCO, select **Software & Support: Technical Tools: Bug Toolkit II**.

Open Caveats - Release 11.2(17)P

This section describes possibly unexpected behavior by Release 11.2(17)P. Unless otherwise noted, these caveats apply to all 11.2 releases, up to and including Release 11.2(17)P.

Access Server

- CSCdk79534

  A Cisco AS5200 access server might restart with a bus error. The PC is in main memory, but the address to which the access server points is not. This address can be anywhere. There is no workaround.

Basic System Services

- CSCdj14601

  When hardware compression is enabled, packets are normally fast-switched. If you disable fast switching and then reenable fast switching, fast switching remains disabled.

  Workaround: Reconfigure hardware compression by issuing the **no compression** command followed by the **compression stac** command.

- CSCdj68910

  When you have two simultaneous accesses to NVRAM (for example, one access from the console and another access from a Telnet session), one session might attempt to issue the **show configuration** command and might pause at the More prompt while the other session issues the **write memory** command. This problem is unlikely during normal router usage. There is no workaround.

- CSCdj79890

  A Cisco 7200 series router running Cisco IOS Release 11.2(9)P reloads with a software forced error in abort every two or three days. There is no workaround.

- CSCdj80100

  The Cisco 3640 router configured to write a core dump using FTP or RCP is only writing main memory and not writing the I/O memory. There is no workaround.

- CSCdk12199

  NetFlow statistics are not counted for flows sourced from or destined to Frame Relay interfaces on a Cisco 7200 series router running Release 11.2(8)P. There is no workaround.

- CSCdk28664

  The router may experience a stack reload when running general traffic shaping and priority queueing simultaneously on the same interface. This problem is not seen with later images. There is no workaround.

- CSCdk48207

  A Cisco 1601 router running Cisco IOS Release 11.2(15a)P that is configured for asynchronous MPPP dialing might experience memory corruption. This situation will cause the router to reload. There is no workaround.

- CSCdk57892

  A Cisco 1600 series router might fail a loopback test when setting the service-module t1 clock source to **internal** and **looopback dte**, on the WIC-DSU-T1 card.

  Workaround: Execute the **ignore-dcd** and **service-module t1 lbo -7.5db** commands and clear the interface manually.

- CSCdk66459

  A Cisco router might send false packets on the LCP level when starting a file transfer over an asynchronous PPP link. The following is a sample of the LCP debug output:

  ```
  *Mar 1 04:42:45.317: Se0 UNKNOWN(0x0000): I VENDORS [Not negotiated] id 0 len 0 *Mar 1
  04:42:45.321: Se0 LCP: O PROTREJ [Open] id 146 len 1500 protocol UNKNOWN(0x0000) *Mar 1
  04:42:45.325: Se0 LCP: (0x00000000000000000000000000000000) *Mar 1 04:42:45.325: Se0
  LCP: (0x00000000000000000000000000000000) *Mar 1 04:42:45.329: Se0 LCP:
  (0x00000000000000000000000000000000) or even
  *Mar 1 00:50:12: Se0 LCP: (0x1313131313131212) *Mar 1 00:50:12: Se0 UNKNOWN(0x1212): I
  UNKNOWN(17) [Not nego tiated] id 17 len 4369 *Mar 1 00:50:12: Se0 LCP: O PROTREJ [Open]
  id 196 len 1500 protocol UNKNOWN(0x1 212)
  ```

  This condition continues until the asynchronous line disconnects. There is no workaround.

- CSCdk74692

  A Cisco 1605R router running Cisco IOS Release 11.2(15a)P will allow excess UDP packets to be sent inside a firewall. If the **ip inspect max-incomplete high** command is set to 10 half-open sessions, you can send more than 10 UDP packets inside the firewall and they are not denied. There is no workaround.

- CSCdk77783

  The Cisco 1005 and Cisco 1600 series routers do not support the serial interface configuration command **ignore-dcd** properly. The Cisco 1005 router will not accept the command at all, and the Cisco 1600 series routers will accept the command, but will not operate properly if it is issued. Certain external modems and CSU/DSU devices require the ability of the DTE to ignore the DCD signal, and use of such devices is not possible until a fix is available.

  Workaround: Do a shunt at the cable level to bring DCD high on the cisco side.

- CSCdk81558

  If **service compress-config** is configured, you cannot write to the NVRAM after 30 seconds. This condition continues to exist even if **service compress-config** is removed and **wr** is executed.

  Workaround: Remove the **service compress-config** command and reload the router.

IBM Connectivity

- CSCdk30352

  Cross-domain session drops might occur when you configure **stun-tg** on the routers to connect two front-end processes. When the session drop occurs, a "%SYS-2-BADSHARE:Bad refcount in datagram_done" message might be reported by the router. There is no workaround.

Interfaces and Bridging

- CSCdj54192

  Mueslix based HSSI port adaptors (PA-1H revB and PA-2H rev B) might experience "STOPFAIL/STARTFAIL" error messages. The customer should tell their Cisco technical support personnel that the detailed instructions to debug this problem are in the DDTs release note enclosure. The Cisco technical support personnel can also contact the development team (currently rharagan-group) for further support.

- CSCdj71794

  Inbound telnet sessions across asynchronous lines on a Cisco 3640 router might cause the router to reload. The router will reload to the "ROMMON" state.

  Workaround: Connect to the console port and issue the **initialize** command.

- CSCdj91521

  A Cisco router might report interface descriptions for interfaces 38—40, which are T1 ports for channelized T1 cards. The MIB data for all subsequent interfaces after the T1 is off by four interfaces (the number of channels). There is no workaround.

- CSCdk21038

  On an ATM backbone, the following types of errors occur on all Cisco 7200 and 7500 series routers:

  `TI1570-3-FAILSETUPVC`, `ATM-3-FAILCREATEVC`, and `CBUS-3-CATMREJCMD`

  This then causes the LANE connection to fail, and these messages appear:

  ```
  2 %LINK-3-BADMACREG: Interface ATM1/0.2,
  non-existent MACADDR registry for link 0 Jun 30 07:30:11 [10.81.1.5.20.189] 1595:
  -Process= "<interrupt level", ipl= 1
  Jun 30 07:30:15 [10.81.1.5.20.189] 1596: -Traceback= 6000A0F0 600FB8F8 6022D4C0
  600DF48C 601E2A90 601E2BF0 601E2ECC 600C2BBC 600C2C9C 6023BCC8 600C8868 600CB71C
  ```

  LANE is attempting to create an excessive number of virtual circuits, and the core ATM Cisco IOS software code is allowing the setup calls to be passed to the driver.

  The output of the **show atm int atm X** command shows that the current virtual circuit connections are exceeding the maximum number of virtual circuits for that interface. However, the output of the **show atm vc** command shows that this is not the cause. There is no workaround.

- CSCdk41802

  Enabling policy routing may cause FDDI transitions. This problem has only been seen in one location. There is no workaround.

- CSCdk42931

  A Cisco 7513 router running 11.1(20)CA1 Enterprise feature set with an FEIP fails to bridge the MOP load packets when the MAC filter list for the Fast Ethernet interface exceeds 26 entries.

  Workaround: Use a Fast Ethernet Port Adaptor on a VIP2 card.

- CSCdk51747

  The "TBRIDGE-4-GIANT" error message might be seen on the routed PA-F-MM interfaces with Cisco IOS Release 11.2(15a)P. This situation occurs when a Cisco router interface that is configured as a bridge interface receives a packet larger than the specification. For example, when using Ethernet, the condition might arise when the packets are larger than approximately 1540 bytes. The problem is caused by high CPU and ICMP redirects and very slow FDDI ring performance. There is no workaround.

- CSCdk60571

  Serial interfaces and line protocols on high-end Cisco routers might be down with all physical control signals up, including data carrier detect (DCD).

  Workaround: A microcode reload fixes the problem.

- CSCdk66019

  Under normal conditions, If **no keepalive** or **keepalive** *0* is configured on Fast Ethernet, the line stays up when the media-independent interface (MII) is removed or the cable is disconnected. However, If the interface is then reconfigured with **keepalive** *non-zero value* while the physical media stays down, the link still indicates that it is up.

  Workaround: Issue the **shut** command followed by the **no shut** command, or issue the **clear interface** command.

- CSCdk80751

  When helpering to a broadcast address on a VIP ethernet port, you might experience a small amount of UDP packet drops (approximately 6 in 3000) with Cisco IOS Release 11.2.

  Workaround: Use Cisco IOS Release 11.1(21)CC or an EIP.

IP Routing Protocols

- CSCdk37681

  When you use dynamic address translation, the same global inside address might be used by two or more different inside hosts. In this case, NAT will not work for these hosts.

  Workaround: Clear the translation table.

- CSCdk57480

  A corrupted Enhanced Interior Gateway Routing Protocol (EIGRP) topology table between mutually redistributed autonomous systems might cause a race condition of the routes. The **show ip route** command output for certain routes always shows up as "00:00:00." There is no workaround.

- CSCdk57801

  Corrupted router link state advertisements might cause following error messages:

  ```
  %SYS-2-GETBUF: Bad getbuffer , bytes= 65583 -Traceback= 601E3940 603C7684 603C7420
  603AAF00 6 0203E48 60203E34 -Process= "OSPF Router", ipl= 0, pid= 61
  %SYS-2-GETBUF: Bad getbuffer, bytes= 65583 -Process= "OSPF Hello", ipl= 0, pid= 2
  -Traceback= 601E3940 603C7684 603B4098 603AB38C 603AB644 60203E48 60203E34
  ```

  Workaround: Reload the router.

- CSCdk78845

  When the prune-timers in the oil list are not identical, the mroute will still go to a "forwarding" status even when there is no listener. There is no workaround.

Miscellaneous

- CSCdj53849

  A Cisco 4700 series router running Cisco IOS Release 11.2(8)P might reload in the SSCOP timer process. There is no workaround.

- CSCdj64290

  Under heavy loading by a Netcom Smartbit, the route switch module might experience the following error message:

  ```
  >Dec 2 17:02:29.659: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan41, chn >Dec 2
  17:02:37.355: %RSP-2-QAERROR: bad buffer header address error, write at ) > log
  06019000, data FFFF0000 00000000 >Dec 2 17:02:42.911: %CBUS-3-CMDTIMEOUT: Cmd timed
  out, CCB 0x5800FF20, slot 0,2 >-Traceback= 601C8314 601C8624 601C1CD0 601C03F4 601417AC
  601419A4 60154F08 60154
  ```

  There is no workaround.

- CSCdj64898

  Packets might not be forwarded correctly if fancy queuing (for example, fair-queue) is enabled along with the Compression Service Adapter (CSA) on a Cisco 7200 router. This condition also occurs when fancy queuing is enabled along with the Compression Network Module (CNM) on a Cisco 3600 router.

  Workaround: Disable fancy queueing. Instead, use FIFO queueing.

- CSCdj80674

  When the **physical-layer async** command is used on low-speed serial interfaces (either asynchronous or synchronous), the fast switching process time increases by approximately 10 percent. There is no workaround.

- CSCdj89070

  The command **show crypto card** on a Cisco 7500 series router does not return any information. The command should provide output similar to the following:

  ```
  Router# show crypto card 1
  Crypto card in slot: 1
  Tampered: No
  Xtracted: No
  Password set: Yes
  DSS Key set: Yes
  Router#
  ```

  To verify that the card is recognized by the software, use the command **show diag** or **show crypto engine brief**. There is no workaround.

- CSCdk12532

  The VIP crypto engine might not reload into a VIP after online insertion and removal of any interface processor on the router.

  Workaround: Reload the microcode.

- CSCdk41289

  All logging to terminals and buffers halts.

  Workaround: Remove **logging synchronous** from the configuration of **line console** *0*.

- CSCdk43192

  A router inspection might reload because of a bus error at list_enqueue_default.

  Workaround: Turn off fast path by configuring **no ip route-cache** on all interfaces where an inspected packet might cross. For example, if a packet comes in from Ethernet 0/0, and goes out to s0, inspection (CBAC) is configured on s0. In this situation, the user must configure **no ip route-cache** on both e0/0 and s0.

- CSCdk46853

  For Cisco IOS Release 11.2 P or Cisco IOS Release 11.3, if Fast Ethernet subinterfaces are configured for encryption over encapsulation ISL, and the crypto map is only applied to the main interface, and the IP address is configured in the subinterface, the packets could be switched in the clear. The packets might be dropped when using a Cisco IOS Release 12.0 image while enabling CEF. There is no workaround.

- CSCdk47359

  The VIP controllers on a Cisco 7500 series router configured for encryption reload with the following error message:

  ```
  %VIP2-1-MSG: slot1 System Reload called from 0x6009F374, context=0x60246810
  %VIP2-1-MSG: slot1 System exception: sig=10, code=0x4, context=0x60246810 [...]
  %VIP2-1-MSG: slot1 EPC : 0x6016B2D8, SREG : 0x3400C103, Cause : 0x00000004 %VIP2-1-MSG:
  slot1 ErrorEPC : 0x8000861C %VIP2-1-MSG: slot1 Attempting traceback with FP=0x6029C178,
  PC=0x6016B2D8 %VIP2-1-MSG: slot1 Traceback= 0x60096FE4 0x6013D738 0x6013D898 0x60146E44
  0x6013 8A44 0x6012A894 0x6012B0BC 0x6009F278 %DBUS-3-DBUSINTERR: Slot 1, Internal Error
  ```

  The VIP may reload after a manual change of a crypto map or during a periodic IPC. There is no workaround.

- CSCdk65092

  When you use the RSP platform with ESA installed, crypto sessions might stop encrypting data, but the access-lists will continue to see matches. A **show crypto engine connections** *slot* command shows the interface as "???" instead of the physical interface through which the packets should be going. The symptom is that although the crypto session appears to be up according to the **sh crypto conn** command, you are unable to send any data to the other side if it is to be encrypted according to the crypto map.

  Workaround: Remove the crypto map from the interface and then remove the corresponding sequence number from the crypto map. Re-create the sequence into the map (using the same configuration commands) and apply it back to the interface.

- CSCdk65533

  I/O memory might get fragmented on a Cisco 3640 router.

  Workaround: Reload the router.

- CSCdk68408

  A Cisco 7200 router that uses GRE with encryption and runs IP and IPX with an ESA card might reload. There is no workaround.

- CSCdk68700

  Encryption over dialer profiles might cause a Cisco router to reload when fast switching is turned on. This situation results in a "get alignment fatal" error.

  Workaround: Disable fast switching on the dialer profile interfaces.

- CSCdk69415

  An RSP based router running Cisco IOS Release 11.2(15a)P might stop IP traffic that passes through two FDDI port adaptors and is encrypted and decrypted on the VIP2-40.

  Workaround: A microcode reload momentarily fixes the problem.

- CSCdk69456

  The ESA Crypto engine of a Cisco 7507 router with a VIP2 installed might be limited to 25 connections. In this situation, new connections are established after key exchange, but no encryption and traffic flow take place. There is no workaround.

- CSCdk75458

  A Cisco 3600 series router may experience slow switching behavior when a packet is received with a bad checksum. The **debug ip packet error** command shows:

  ```
  *Mar 30 17:45:34.238: IP: s=10.32.0.1 (BRI0/0), d=10.32.1.230, len 193, dispose
  ip.checksumerr
  ```

  There is no workaround.

- CSCdk75496

  When you send a break to a reverse Telnetted session using a Cisco 3640 router, you must press **Break** before pressing **Enter**. There is no workaround.

- CSCdk77654

  An encryption session setup might not setup properly if the **access-list** command applied to a **crypto map** includes **deny** statements before **permit** statements.

  Workaround: Remove the **deny** statements in the **access-list** commands. A ramification of the workaround is that more packets may match the encryption policy than originally configured.

- CSCdk79281

  When you run NAT and encryption, FTP fails, but Telnet and ping work. FTP login is possible, but **get** and **dir** commands are hanging.

  Workaround: Remove NAT or encryption.

- CSCdk79511

  A Cisco 4700 series router repeatedly produces the following error message:

  ```
  System was restarted by processor memory parity error at PC 0x6081D860, address 0x0
  ```

  There is no workaround.

- CSCdk79568

  If you have turned on fast switching on the dialer interface as well as on the interface where the host is connected, and you have configured OSPF to do authentication, the router will reload with a bus error. Both the calling and the called router are using hardware encryption.

  Workaround: Turning off fast switching helps to resolve the issue. Please see CSCdj82823 and CSCdk68700

TCP/IP Host-Mode Services

- CSCdk34313

  A Cisco router might reload with the following message:

  ```
  %SYS-6-STACKLOW: Stack for process TCP Timer running low, 0/600
  ```

  The message indicates that the TCP timer process has a full stack and that subsequent use of this stack will cause an overflow. There is no workaround.

- CSCdk49133

  A system with all of the following conditions might not operate: one Token Ring card, one ISDN BRI, two serial interfaces, a Cisco 2504 router, RSRB configured, IPX configured, NAT configured, EIGRP configured, and SNMP configured.

  Workaround: Upgrade to Cisco IOS Release 11.3 (Changes were made to TCP driver in Cisco IOS Release 11.3 to overcome the previous limitations of the TCP driver in Cisco IOS Release 11.2).

Wide-Area Networking

- CSCdj17959

  The asynchronous interfaces on Cisco 3600 series routers may drop calls under heavy traffic conditions when running PPP Multilink bundles. There is no workaround.

- CSCdj82342

  When Cisco IOS Release 11.3 or Cisco IOS Release 11.3T is running on a Cisco 3640 series router, Frame Relay over the ISDN connection works initially but starts to fail because the interface input queue is full and all incoming packets are dropped.

  Workaround: Disable fast switching on the interface.

- CSCdj93398

  A Cisco 2513 router running Cisco IOS Release 11.2(12.3)P might display the following error message when a manual reload is performed:

  ```
  %SYS-3-MGDTIMER: Timer has parent, timer link, timer = 279DC -Process= "traffic_shape",
  ipl= 6, pid= 41 -Traceback= 317DAEC 318353A 31B116
  ```

  There is no workaround.

- CSCdk39736

  A Cisco AS5200 series access server running Cisco IOS Release 11.2(13)P1 is not dialing out from one random dialer map.

  Workaround: Reloading the router will temporarily fix the problem.

- CSCdk51616

  On routers with asynchronous serial interfaces running PPP encapsulation, the router might reload with the following error message from a **show stack** command:

  ```
  System was restarted by unexpected interrupt at PC 0x2218AC58, address 0x2218AC58
  ```

  This problem is unlikely during normal router usage. There is no workaround.

- CSCdk66665

  The Cisco 4500 ATM reports high output drops on the ATM interface . If you are seeing "output queue" drops incrementing that are not affected by load, output queue size, and traffic shaping config, you might be experiencing this caveat. The problem appears to be caused by the small VC queue size for buffering the packets.The proposed solution is to make the VC queue size configurable to higher values.

  Workaround: Increasing the **burst-cell-no** in the traffic shape configuration to high values around 2000 stops these output drops.

- CSCdk72052

  A Cisco router might reload when IP multicast is configured. There is no workaround.

- CSCdk72493

  A Cisco AS5200 access server might experience a bus error at "_level4_pan_e1." There is no workaround.

Resolved Caveats—Release 11.2(17)P

All the caveats listed in this section are resolved in Release 11.2(17)P. This section describes only severity 1 and 2 caveats.

Access Server

- CSCdk44928

  Under heavy stress, Cisco AS5200 series access servers might display a bus error and reload. There is no workaround.

Basic System Services

- CSCdk08376

  Significant numbers of subinterfaces (ATM or Frame Relay) cause "CPUHOG" messages.

  Workaround: A partial workaround is to use the command **no snmp-server sparse-table**. This reduces the number of "CPUHOG" messages.

- CSCdk11908

  A Cisco 1005 router running IOS 10.3(17) repeatedly reports the following errors:

  ```
  %ETHERNET-1-TXERR: Ethernet0: Fatal transmit error. Restarting... %QUICC-5-COLL: Unit
  0, excessive collisions. Retry limit 15 exceeded
  ```

  All hardware attached to the router was tested and replaced, but the router kept on reporting errors.

- CSCdk33318

  The Cisco 7206 router might experience a memory leak. There is no workaround.

- CSCdk41472

  If a Cisco 4700M router runs Release 11.2(14)P and also runs traffic shaping with custom queuing, GTS drops are counted as CQ queue drops. There is no workaround.

IBM Connectivity

- CSCdk28549

  Configuring source route translational bridging and data-link switching (DLSw) to the same bridge group at the same time results in traceback messages and ultimately might cause the router to restart unexpectedly. The problem can be prevented by deconfiguring source route translational bridging or by deconfiguring the DLSw connection to the bridge group. There are no other known workarounds.

Interfaces and Bridging

- CSCdj85213

  The primary SDLC interface may send out an erroneous frame causing a secondary device to send a frame reject (FRMR). There is no workaround.

- CSCdk11808

  Certain types of terminal adapters (for example, NEC adapters) may toggle control lines during DTR pulsing. These line status changes will interrupt the 8T/4T+ port adaptor controller and cause a reset of the line by the Cisco IOS driver. Thus the DTR pulse is shortened. There is no workaround.

- CSCdk20550

  The 10 Mbps full duplex capability of the Cisco 3600 NM-1FE-TX in CiscoIOSRelease11.2 P does not operate properly. The speed toggles between 10 Mbps and 100 Mbps. This affects the connectivity. There is no workaround.

- CSCdk39193

  When the RX or TX clock is missing, the HSSI3 code waits for the chip reset to be completed at the beginning of the code. A problem exists because chip reset is only done at booting or online insertion and removal. Previously, the problem did not appear because when both TX/RX clocks were present, bit 0 of STATUS6 was set and microcode could proceed with no difficulties. The microcode, however, stuck at PC=0 when the system possessed only one clock.

  Workaround: Proceed regardless of reset status.

- CSCdk53401

  When you net boot a Cisco 3640 router over the Fast Ethernet port, the IOS proceeds to interactive setup without trying to load configurations from the network. This has been traced to an autonegotiation race condition where the Fast Ethernet port momentarily appears to be in a down state. There is no workaround.

IP Routing Protocols

- CSCdj49045

  The C programming language print function “Printf” can suspend the current process if the calling process inhibits a process context switch to protect its processing. The router reloads. There is no workaround.

- CSCdk20424

  When the original V.110 modem management protocol was implemented for NEC modems, NEC firmware did not have ACKs for RI and DI messages. At that time it was decided to distinguish between the older and newer firmware with the revision number byte in a cookie. For commands without ACKs, Tx complete is treated as an ACK and an appropriate message is sent

to the sender. However, this mechanism was not restricted to the specific V.110 units. It was done unconditionally resulting in enqueue errors. When the enqueue errors were fixed, this feature stopped working for the older revision V.110 from NEC. This commit fixes the problem with older revision NEC V.110 and avoids the earlier pitfalls of enqueue errors by restricting the ACKs to older NEC V.110 ports only.

- CSCdk23751

  If there is no router at the end of a connection and you attempt to encrypt to the missing (phantom) side, problems in the connection setup code will occur. There is no workaround.

- CSCdk34128

  On an M4T or M8T adapter, the router might experience a depletion in packet memory after generating enough network traffic to saturate a serial interface. The only method of recovering the memory is reloading the router. There is no workaround.

Miscellaneous

- CSCdk47147

  On the Cisco AS5200 access server and Cisco AS5300 access server a problem has been observed with MICA modems with the configuration of **async mode dedicated** as well as **async mode interactive**. The routers reload with bus errors. On the Cisco AS5300 the reload is preceded by a "%ALIGN-1-FATAL" log message on the console. The cause seems to be that many PPP calls are connecting and disconnecting. There is no workaround.

- CSCdk53807

  The ESA does not work with pregeneration.

  Workaround: Turn off pregeneration functionality with the **no crypto pregen-dh-pairs** command.

- CSCdk64463

  When bridging is configured on an RSM VLAN interface that runs Cisco IOS Release 11.2P or Cisco IOS Release 11.3, NetFlow or optimum switching does not occur. When bridging is configured on an RSM VLAN interface that runs Cisco IOS Release 12.0, CEF switching does not occur. IP packets are processed by fast switching instead of flow/optimum/CEF switching, causing a significant decrease in the IP packet forwarding rate. The Net Flow Collector might also fail. There is no workaround.

Wide-Area Networking

- CSCdj81263

  When IP fast switching is enabled on a Cisco 1600 series router with BRI interface(s), a router reload is possible under the following conditions: (1) the ISDN connection is being brought up and down repeatedly and (2) the **clear ip cache** command is invoked repeatedly in conjunction with the connection being disconnected. There is no workaround.

Related Documentation

The following sections describe the documentation available for the Cisco AS5100 and Cisco AS5200. Typically, these documents consist of hardware installation guides, software installation guide guides, Cisco IOS configuration and command references, system error messages, and feature modules, which are updates to the Cisco IOS documentation. Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online only.

The most current documentation can be found on the Web via Cisco Connection Online (CCO) and on the latest Documentation CD-ROM. These electronic documents might contain updates and modifications made after the paper documents were printed.

Use these release notes in conjunction with the documents in the following sections:

- Release-Specific Documents, page 25
- Platform-Specific Documents, page 26
- Feature Modules, page 26
- Cisco IOS Software Documentation, page 27

Release-Specific Documents

The following documents are specific to Release 11.2 P. They are located on CCO and the Documentation CD-ROM:

- *Release Notes for Cisco IOS Release 11.2 P*

  To reach the cross-platform *Release Notes for Cisco IOS Release 11.2 P* on CCO, follow this path:

  Software & Support: Cisco Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.2: Release Notes for Cisco IOS Release 11.2

  To reach the cross-platform *Release Notes for Cisco IOS Release 11.2* on the Documentation CD-ROM, follow this path:

  Software & Support: Cisco Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.2: Product Specific Release Notes for Cisco IOS Release 11.2: Cross-Platform Release Notes for Cisco IOS Release 11.2: Release Notes for Cisco IOS Release 11.2(1)P through 11.2(7)P

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

  To reach these documents, refer to the Software Center at this path on CCO:

  Software & Support: Software Center: Cisco IOS Software

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. Bug Navigator II can be found at **http://www.cisco.com/support/bugtools**, or from CCO, select **Software & Support: Technical Tools: Bug Toolkit II**.

Platform-Specific Documents

Cisco AS5100 Documents

The following documents are specific to the Cisco AS5100:

- *Cisco Access Server 5100 User Guide*
- *Cisco Access Server 5100 Public Network Certification*
- *AS5100 Dual E1/PRI Application Card Configuration Note*
- *AS5100 Dual T1/PRI Application Card Configuration Note*

To reach Cisco AS5100 documentation on CCO, follow this path:

Products & Ordering: **Cisco Documentation**: **Access Servers and Access Routers**: **Access Servers**: **Cisco AS5100**.

To reach Cisco AS5100 documentation on the Documentation CD-ROM, follow this path:

Cisco Product Documentation: **Access Servers and Access Routers**: **Access Servers**: **Cisco AS5100**.

Cisco AS5200 Documents

The following documents are specific to the Cisco AS5200:

- *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*

To reach Cisco AS5200 documentation on CCO, follow this path:

Products & Ordering: **Cisco Documentation**: **Access Servers and Access Routers**: **Access Servers**: **Cisco AS5200**.

To reach Cisco AS5200 documentation on the Documentation CD-ROM, follow this path:

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

Feature Modules

Feature modules describe new features supported by Release 11.2 P and are an update to the Cisco IOS documentation set. They consist of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the features modules are available online only. The feature module information is included in the next printing of the Cisco IOS documentation set.

To reach the feature modules on CCO, follow this path:

Products & Ordering: **Cisco Documentation**: **Cisco IOS Software Configuration: Cisco IOS Release 11.2**: **Feature Guide for Cisco IOS Release 11.2 P**.

To reach the feature modules on the Documentation CD-ROM, follow this path:

Cisco Product Documentation: **Cisco IOS Software Configuration: Cisco IOS Release 11.2**: **Feature Guide for Cisco IOS Release 11.2 P**.

Cisco IOS Software Documentation

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

Table 7 details the contents of the Cisco IOS Release 11.2 software documentation set. The document set is available in electronic form, and also in printed form upon request.

Note The most current Cisco IOS documentation can be found on the latest Documentation CD-ROM and on the Web. These electronic documents might contain updates and modifications made after the paper documents were printed.

To reach the Cisco IOS documentation set on CCO, follow this path:

Products & Ordering: **Cisco Documentation**: **Cisco IOS Software Configuration**: **Cisco IOS Release 11.2**: **Cisco IOS Release 11.2 Configuration Guide/Command References**

To reach the Cisco IOS documentation set on the Documentation CD-ROM, follow this path:

Cisco IOS Software Configuration: **Cisco IOS Release 11.2**: **Configuration Guides and Command References**

Table 7 Cisco IOS Software Release 11.2 P Documentation Set

Books	Chapter Topics
• *Configuration Fundamentals Configuration Guide* • *Configuration Fundamentals Command Reference*	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management Interface Configuration System Management
• *Network Protocols Configuration Guide, Part 1* • *Network Protocols Command Reference, Part 1*	IP Addressing IP Services IP Routing Protocols
• *Network Protocols Configuration Guide, Part 2* • *Network Protocols Command Reference, Part 2*	AppleTalk Novell IPX
• *Network Protocols Configuration Guide, Part 3* • *Network Protocols Command Reference, Part 3*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS

Books	Chapter Topics
• *Wide-Area Networking Configuration Guide* • *Wide-Area Networking Command Reference*	ATM Frame Relay SMDS X.25 and LAPB
• *Security Configuration Guide* • *Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering Network Data Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options
• *Dial Solutions Configuration Guide* • *Dial Solutions Command Reference*	Dial Business Solutions and Examples Dial-In Port Setup DDR and Dial Backup Remote Node and Terminal Service Cost-Control and Large-Scale Dial Solutions VPDN
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Switching Paths for IP Networks Fast Switching Autonomous Switching NetFlow Switching Optimum Switching Virtual LAN (VLAN) Switching and Routing Inter-Switch Link Protocol Encapsulation IEEE 802.10 Encapsulation LAN Emulation
• *Bridging and IBM Networking Configuration Guide* • *Bridging and IBM Networking Command Reference*	Transparent Bridging Source-Route Bridging 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 NCIA Client/Server Topologies IBM Channel Attach

Books	Chapter Topics
• *Cisco IOS Software Command Summary* • *Dial Solutions Quick Configuration Guide* • *System Error Messages* • *Debug Command Reference*	

Note The *Cisco Management Information Base (MIB) User Quick Reference* publication is no longer being published. For the latest list of MIBs supported by Cisco, see the Cisco Network Management Toolkit on Cisco Connection Online (CCO). On CCO, follow this path: **Software & Support**: **Software Center**: **Network Management Products**: **Cisco Network Management Toolkit**: **Cisco MIBs**.

Service and Support

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

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

- 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. For additional information, contact 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. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or 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 reach 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 the documents listed in the "Related Documentation" section.