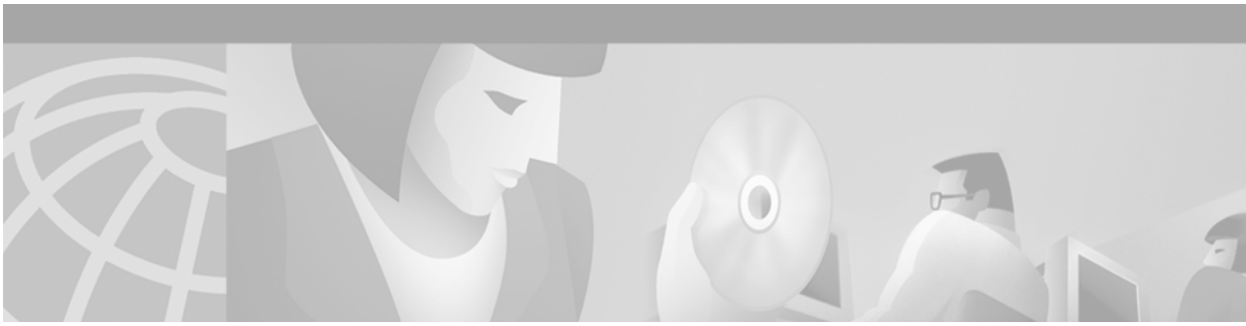

Release Notes for Cisco AS5200 Universal Access Servers for Cisco IOS Release 11.2

April 9, 2001

Note You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

These release notes for the Cisco AS5200 universal access servers support Cisco IOS Release 11.2(26). These release notes are updated to describe new 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 Cisco IOS Release 11.2(26), see the "Caveats" section on page 9 and *Caveats for Cisco IOS Release 11.2*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 11.2*, located on Cisco.com and the Documentation CD-ROM.

Contents

These release notes describe the following topics:

- Introduction, page 2
- System Requirements, page 2
- New and Changed Information, page 9
- Caveats, page 9
- Related Documentation, page 15
- Obtaining Documentation, page 20
- Obtaining Technical Assistance, page 21

Cisco Systems

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

78-4610-19

Introduction

The Cisco AS5200 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. Midsized organizations or service providers requiring centralized processing capabilities for mobile users and telecommuters will benefit the most using the Cisco AS5200.

With its optimization for high-speed modem access, the Cisco AS5200 is 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:

- Memory Recommendations, page 2
- Supported Hardware, page 3
- Determining the Software Version, page 3
- Upgrading to a New Software Release, page 3
- Feature Set Tables, page 4

Memory Recommendations

Table 1 lists the memory recommendations for the Cisco AS5200.

Table 1 Memory Recommendations for the Cisco AS5200

Image Name	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From[1]
IP	c5200-i-l	8 MB	8 MB	Flash
IP Plus[2]	c5200-is-1	8 MB	8 MB	Flash
Desktop	c5200-d-1	8 MB	8 MB	Flash
Desktop Plus	c5200-ds-1	8 MB	8 MB	Flash
Enterprise	c5200-j-1	8 MB	8 MB	Flash
Enterprise Plus	c5200-js-1	8 MB	8 MB	Flash

1. When a system is running from Flash memory, you cannot update the system while it is running. You must use the Flash load helper.
2. IP Plus for the Cisco AS5200 includes protocol translation, V.120, RMON, Managed Modems, and IBM (if IBM is not already included).

Supported Hardware

Cisco IOS Release 11.2 supports the Cisco AS5200. Table 2 lists the supported interfaces for the Cisco AS5200.

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 9.

Table 2 Supported Interfaces for the Cisco AS5200

LAN/WAN Interfaces And Modem Cards	Product Description
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
	V.34 Modems
	V.110 terminal adapter (TA)
	V.90 modems

Determining the Software Version

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

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 11.2 Software (c5200-i-l), Version 11.2(26), RELEASE SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *Upgrading the Cisco IOS Software Release in Cisco Routers and Modems* located at:

http://www.cisco.com/warp/public/620/6.html

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.

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

Table 3 lists the features and feature sets supported by the Cisco AS5200 in Cisco IOS Release 11.2 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 table might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hardcopy documents were printed. If you have a Cisco.com login account, you can find image and release information regarding features prior to Cisco IOS Release 11.2(26) by using the Feature Navigator tool at: http://www.cisco.com/go/fn.

Table 3 Feature List by Feature Set for the Cisco AS5200

	Feature Set					
Features Contained in Feature Sets	**IP**	**IP Plus**	**Desktop**	**Desktop Plus**	**Enterprise[1]**	**Enterprise Plus**
LAN Support						
Apollo Domain	No	No	No	No	Yes	Yes
AppleTalk 1 and 2[2]	No	No	Yes	Yes	Yes	Yes
Banyan VINES	No	No	No	No	Yes	Yes
Concurrent Routing and Bridging (CRB)	Yes	Yes	Yes	Yes	Yes	Yes
DECnet IV	No	No	Yes	Yes	Yes	Yes
DECnet V	No	No	No	No	Yes	Yes
GRE	Yes	Yes	Yes	Yes	Yes	Yes
Integrated Routing and Bridging (IRB)[3]	Yes	Yes	Yes	Yes	Yes	Yes
IP	Yes	Yes	Yes	Yes	Yes	Yes
LAN Extension Host	Yes	Yes	Yes	Yes	Yes	Yes
Multiring	Yes	Yes	Yes	Yes	Yes	Yes
Novell IPX[4]	No	No	Yes	Yes	Yes	Yes
OSI	No	No	No	No	Yes	Yes

Table 3 Feature List by Feature Set for the Cisco AS5200 (continued)

Features Contained in Feature Sets	Feature Set					
	IP	IP Plus	Desktop	Desktop Plus	Enterprise[1]	Enterprise Plus
Source-Route Bridging (SRB)	No	No	No	No	Yes	Yes
Transparent and Translational Bridging	Yes	Yes	Yes	Yes	Yes	Yes
XNS	No	No	No	No	Yes	Yes
WAN Services						
Combinet Packet Protocol (CPP)	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Profiles	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay SVC Support (DTE)	No	No	No	No	Yes	Yes
Frame Relay Traffic Shaping	Yes	Yes	Yes	Yes	Yes	Yes
Half Bridge/Half Router for CPP and PPP	Yes	Yes	Yes	Yes	Yes	Yes
HDLC	Yes	Yes	Yes	Yes	Yes	Yes
IPXWAN 2.0	No	No	Yes	Yes	Yes	Yes
ISDN[5]	Yes	Yes	Yes	Yes	Yes	Yes
Multichassis Multilink PPP (MMP)	No	Yes	No	Yes	No	Yes
PPP[6]	Yes	Yes	Yes	Yes	Yes	Yes
SMDS	Yes	Yes	Yes	Yes	Yes	Yes
Switched 56	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Private Dialup Network (VPDN)	No	Yes	No	Yes	No	Yes
X.25[7]	Yes	Yes	Yes	Yes	Yes	Yes
WAN Optimization						
Bandwidth-on-demand	Yes	Yes	Yes	Yes	Yes	Yes
Custom and Priority Queuing	Yes	Yes	Yes	Yes	Yes	Yes
Dial Backup	Yes	Yes	Yes	Yes	Yes	Yes
Dial-on-Demand	Yes	Yes	Yes	Yes	Yes	Yes
Header[8], Link and Payload Compression[9]	Yes	Yes	Yes	Yes	Yes	Yes
Snapshot Routing	Yes	Yes	Yes	Yes	Yes	Yes
Weighted Fair Queuing	Yes	Yes	Yes	Yes	Yes	Yes
IP Routing						
BGP	Yes	Yes	Yes	Yes	Yes	Yes
BGP4[10]	Yes	Yes	Yes	Yes	Yes	Yes
EGP	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced IGRP	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced IGRP Optimizations	Yes	Yes	Yes	Yes	Yes	Yes
ES-IS	No	No	No	No	Yes	Yes
IGRP	Yes	Yes	Yes	Yes	Yes	Yes

Table 3 Feature List by Feature Set for the Cisco AS5200 (continued)

Features Contained in Feature Sets	Feature Set					
	IP	IP Plus	Desktop	Desktop Plus	Enterprise[1]	Enterprise Plus
IS-IS	No	No	No	No	Yes	Yes
Named IP Access Control List	Yes	Yes	Yes	Yes	Yes	Yes
Network Address Translation (NAT)	No	Yes	No	Yes	No	Yes
NHRP	Yes	Yes	Yes	Yes	Yes	Yes
On Demand Routing (ODR)	Yes	Yes	Yes	Yes	Yes	Yes
OSPF	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Not-So-Stubby-Areas (NSSA)	Yes	Yes	Yes	Yes	Yes	Yes
OSPF on Demand Circuit (RFC 1793)	Yes	Yes	Yes	Yes	Yes	Yes
PIM	Yes	Yes	Yes	Yes	Yes	Yes
Policy-Based Routing	Yes	Yes	Yes	Yes	Yes	Yes
RIP	Yes	Yes	Yes	Yes	Yes	Yes
RIP Version 2	Yes	Yes	Yes	Yes	Yes	Yes
Other Routing						
AURP	No	No	Yes	Yes	Yes	Yes
IPX RIP	No	No	Yes	Yes	Yes	Yes
NLSP	No	No	Yes	Yes	Yes	Yes
RTMP	No	No	Yes	Yes	Yes	Yes
SMRP	No	No	Yes	Yes	Yes	Yes
SRTP	No	No	No	No	Yes	Yes
Multimedia and Quality of Service						
Generic Traffic Shaping	Yes	Yes	Yes	Yes	Yes	Yes
Random Early Detection (RED)	Yes	Yes	Yes	Yes	Yes	Yes
Resource Reservation Protocol (RSVP)	Yes	Yes	Yes	Yes	Yes	Yes
Management						
AutoInstall	Yes	Yes	Yes	Yes	Yes	Yes
Automatic Modem Configuration	Yes	Yes	Yes	Yes	Yes	Yes
HTTP Server	Yes	Yes	Yes	Yes	Yes	Yes
Modem Management	No	Yes	No	Yes	No	Yes
RMON events and alarms[11]	Yes	Yes	Yes	Yes	Yes	Yes
RMON Full	No	Yes	No	Yes	No	Yes
SNMP	Yes	Yes	Yes	Yes	Yes	Yes
Telnet	Yes	Yes	Yes	Yes	Yes	Yes
Security						
Access Lists	Yes	Yes	Yes	Yes	Yes	Yes
Access Security	Yes	Yes	Yes	Yes	Yes	Yes

Table 3 Feature List by Feature Set for the Cisco AS5200 (continued)

Features Contained in Feature Sets	Feature Set					
	IP	IP Plus	Desktop	Desktop Plus	Enterprise[1]	Enterprise Plus
Extended Access Lists	Yes	Yes	Yes	Yes	Yes	Yes
Kerberized Login	No	No	No	No	Yes	Yes
Kerberos V Client Support	No	No	No	No	Yes	Yes
Lock and Key	Yes	Yes	Yes	Yes	Yes	Yes
MAC Security for Hubs	Yes	Yes	Yes	Yes	Yes	Yes
MD5 Routing Authentication	Yes	Yes	Yes	Yes	Yes	Yes
RADIUS	Yes	Yes	Yes	Yes	Yes	Yes
TACACS+[12]	Yes	Yes	Yes	Yes	Yes	Yes
IBM Support (Optional)						
APPN (optional)[2]	No	No	No	No	No	No
BAN for SNA Frame Relay Support	No	Yes	No	Yes	Yes	Yes
Bisync	No	Yes	No	Yes	Yes	Yes
Caching and Filtering	No	Yes	No	Yes	Yes	Yes
DLSw+ [13]	No	Yes	No	Yes	Yes	Yes
Downstream PU Concentration (DSPU)	No	Yes	No	Yes	Yes	Yes
Frame Relay SNA Support (RFC 1490)	No	Yes	No	Yes	Yes	Yes
Native Client Interface Architecture (NCIA) Server	No	Yes	No	Yes	Yes	Yes
NetView Native Service Point	No	Yes	No	Yes	Yes	Yes
QLLC	No	Yes	No	Yes	Yes	Yes
Response Time Reporter (RTR)	No	Yes	No	Yes	Yes	Yes
SDLC Integration	No	Yes	No	Yes	Yes	Yes
DLSw (RFC 1795)	No	Yes	No	Yes	Yes	Yes
SDLC Transport (STUN)	No	Yes	No	Yes	Yes	Yes
SDLC-to-LAN Conversion (SDLLC)	No	Yes	No	Yes	Yes	Yes
SNA and NetBIOS WAN Optimization via Local Acknowledgment	No	Yes	No	Yes	Yes	Yes
SRB/RSRB[14]	No	Yes	No	Yes	Yes	Yes
SRT	No	Yes	No	Yes	Yes	Yes
TG/COS	No	No	No	No	Yes	Yes
TN3270	No	No	No	No	Yes	Yes
Protocol Translation						
LAT	No	No	No	No	Yes	Yes
Rlogin	No	No	No	No	Yes	Yes

Table 3 Feature List by Feature Set for the Cisco AS5200 (continued)

Features Contained in Feature Sets	Feature Set					
	IP	IP Plus	Desktop	Desktop Plus	Enterprise[1]	Enterprise Plus
Remote Node[15]						
ARAP 1.0/2.0	No	No	Yes	Yes	Yes	Yes
Asynchronous Master Interfaces	Yes	Yes	Yes	Yes	Yes	Yes
ATCP	No	No	Yes	Yes	Yes	Yes
CPPP	Yes	Yes	Yes	Yes	Yes	Yes
CSLIP	Yes	Yes	Yes	Yes	Yes	Yes
DHCP	Yes	Yes	Yes	Yes	Yes	Yes
IP pooling	Yes	Yes	Yes	Yes	Yes	Yes
IPX and ARAP on Virtual Async Interfaces	No	No	No	No	Yes	Yes
IPXCP	No	No	Yes	Yes	Yes	Yes
MacIP	No	No	Yes	Yes	Yes	Yes
NASI	No	No	Yes	Yes	Yes	Yes
NetBEUI over PPP	No	No	No	No	Yes	Yes
SLIP	Yes	Yes	Yes	Yes	Yes	Yes
Terminal Services[16]						
LAT[16]	No	No	No	No	Yes	Yes
Rlogin	Yes	Yes	Yes	Yes	Yes	Yes
Telnet	Yes	Yes	Yes	Yes	Yes	Yes
TN3270	No	No	No	No	Yes	Yes
X.25 PAD	Yes	Yes	Yes	Yes	Yes	Yes
Xremote	No	No	No	No	Yes	Yes

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

There are no new hardware and software features supported by the Cisco AS5200 for Cisco IOS Release 11.2(26).

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

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

For information on caveats in Cisco IOS Release 11.2, see "Important Notes and Caveats for Release 11.2" in *Cross-Platform Release Notes for Cisco IOS Release 11.2* on Cisco.com and the Documentation CD-ROM. These release notes contain caveats affecting all maintenance releases, and list severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 11.2(26).

Open Caveats—Cisco IOS Release 11.2

This section describes possibly unexpected behavior by Cisco IOS Release 11.2 and describes only severity 1 and 2 caveats:

Basic System Services

- CSCdk09959

  Traffic shaping was found to be broken in 11.2(7.2)P onwards due to another bug fix. The fix was tested in the lab and was working fine with traffic passing through the router but if ping was used from both routers on each side, traffic shaping was seen to be broken again. This was later fixed and tested in the lab. In customer's production environment, there were still some UPC violations but there was a vast improvement from the earlier case where traffic shaping seemed to be not working at all. The exact cause for UPC violations in production environment could not be identified.

  There is no workaround.

  Customer agreed to have these fixes incorporated in the standard release train so they can use these features.

- CSCdp73519

  Router hangs at **usecdelay**.

  There is no workaround.

- CSCdr11715

  On very rare occasions a router will crash when being managed via the http console.

  Workaround: Disable the http server on the router.

IBM Connectivity

- CSCdp20000

  Several platforms are crashing with bus error, in 11.2(15a) and 11.2(15a)P.

  There is no workaround.

Interfaces and Bridging

- CSCdi81407

  The FDDI interface driver can interact poorly with OSPF during OIR, causing SPF recalculations. This occurs only when OSPF is running on an FDDI interface that is not being inserted or removed. This fix eliminates the spurious indication from the driver that the SPF recalculation needs to take place.

IP Routing Protocols

- CSCdm16194

  EIGRP does not trigger the selection of a new route when one of the less desirable or equal paths is removed from the routing table. The route disappears, but no new route is selected from the topology table.

  There is no workaround.

- CSCdp18448

  Static route to null is not redistributed to EIGRP neighbors when there is also manual summarization, configured on one of the interfaces, for the same network and prefix-length.

  There is no workaround.

- CSCdp36272

  If a BGP peer's route to a BGP next-hop is learned via BGP, then a route flapping condition can occur in certain circumstances.

  Workaround: Give the BGP peer a route to the next-hop via the IGP.

- CSCdp44951

  Router might experience a reload by bus error in **rsvp_dump_object**.

  There is no workaround.

Miscellaneous

- CSCdj06368

  The SH VER output on an RSP router with an HSA configuration fails to differentiate between a reload caused by a power-cycle on the router and a user initiated reload. The router identified both situations with the following text string:

  ```
  System restarted by reload
  ```

  In addition, if the reload failure is caused by the failure of Master RSP such that the router reloads using the former Slave RSP, then the failure cause from the master is not visible unless one looks at the SH STACK output.

  There is no workaround.

- CSCdj73079

  Packet OC-3 Interface Processor does not work with encryption GRE tunnel.

  There is no workaround.

- CSCdk12891

  A crypto key exchange cannot be aborted while telnetted into the router.

  Workaround: Until the problem is resolved, sessions can be cleared as follows using the **show tcp bri** followed by the **clear tcp tcb <value>**:

```
didi(config)# crypto key-ex passive
Enter escape character to abort if connection does not complete.
Wait for connection from peer[confirm]
Waiting ....
telnet> quit
Connection closed.
srowles@srowles-ultra:/users/srowles> telnet didi
Trying 172.21.114.199...
Connected to didi.cisco.com.
Escape character is '^]'.

User Access Verification

Password:
didi>en
Password:

didi#conf t
Enter configuration commands, one per line. End with CNTL/Z.
didi(config)#crypto key-ex passive
TCP bind failed: Address already in use

didi(config)#exit
didi#show tcp bri
TCB Local Address Foreign Address (state)
60C3DF74 didi.cisco.com.23 srowles-ultra.ci.43972 ESTAB
60A23A24 didi.cisco.com.23 srowles-ultra.ci.43971 CLOSEWAIT
didi#clear tcp tcb 60A23A24
[confirm]
[OK]
didi#conf t
Enter configuration commands, one per line. End with CNTL/Z.
didi(config)#crypto key-ex passive
Enter escape character to abort if connection does not complete.
Wait for connection from peer[confirm]n
didi(config)#
```

- CSCdk17443

  A Cisco router configured to route IPX traffic through an encrypted Tunnel interface may reset unexpectedly.

  There are two workarounds:

  – Disable IPX fast-switching by entering the following interface-level command on the Tunnel Interfaces.

    no ipx route-cache

  - Disable Fast Tunneling by enabling a Tunnel ID key by entering the following interface-level command on the Tunnel interfaces.

    tunnel key key-number

    where key-number is any number in the range 0-4294967295

    The Tunnel key ID MUST match on each end of the Tunnel.

- CSCdk85414

  Receiving data while running encryption on a Cisco 2500 Series router running Cisco IOS Release 11.2 causes the router to reload.

  There is no workaround.

- CSCdp97179

  Memory corruption occurs with c4500.

- CSCdr13668

  A Cisco 4000 running 11.2(21) has no I/O memory 10h. After reload, the following errors occur:

```
Mar 23 07:05:54: %SYS-2-MALLOCFAIL: Memory allocation of 756 bytes failed from 0
xC475C, pool I/O, alignment 0
-Process= "Exec", ipl= 6, pid= 33
-Traceback= E1900 E2630 C4764 C492A C4C66 57399C 70430 70A1C 80F46 8141A A92BE
Mar 23 07:06:28: %SYS-2-MALLOCFAIL: Memory allocation of 756 bytes failed from 0
xC475C, pool I/O, alignment 0
-Process= "Exec", ipl= 6, pid= 33
-Traceback= E1900 E2630 C4764 C492A C4C66 57399C 70430 70A1C 70FF8 810BE 8141A A 92BE
Mar 23 07:07:01: %SYS-2-MALLOCFAIL: Memory allocation of 756 bytes failed from 0
xC475C, pool I/O, alignment 0
-Process= "Exec", ipl= 6, pid= 33
-Traceback= E1900 E2630 C4764 C492A C4C66 57399C 70430 70A1C 70FF8 810BE 8141A A 92BE
Mar 23 07:07:44: %SYS-2-MALLOCFAIL: Memory allocation of 756 bytes failed from 0
xC475C, pool I/O, alignment 0
-Process= "TACACS+", ipl= 6, pid= 39
-Traceback= E1900 E2630 C4764 C492A C4C66 11E0FE 11E2FE 2E0B6E 2E0CFE 2E0E02 2E0 EFA
```

  There is no workaround.

Novell IPX, XNS, and Apollo Domain

- CSCdm47697

  There has been a problem with IPX connectivity since upgrading router from Cisco IOS Release 10.3 to Cisco IOS Release 11.2 between FDDI and other interfaces (serial and fastethernet). The City Hall router was upgraded. Rconsole from client on FDDI ring fails to servers on Ethernet segments, either local or remote, and cannot browse NDS server object for those servers. Clients on remote Ethernet segment can rconsole and browse FDDI servers.

- CSCdm50939

  The NLSP update process is pegged at 99% and will not decrease. A **show ipx traffic** indicates the partial route calculation process is incrementing rapidly.

  Workaround: Issue **clear ipx nlsp ***

Protocol Translation

- CSCdm74340

  In 9.0, SUN HACK was added to the translations code, allowing SUN machines that only used LF for a carriage return. In the code, the first LF seen before a CR is converted to a CR and sent along. In 11.2, the HACK is in Cisco IOS software but does not work.

Wide-Area Networking

- CSCdm94730

  If an ARP is received on an incorrect interface (that is, a source IP address belonging to a subnet on another subinterface) on a router running Cisco IOS Release 11.2 and performing inter-ELAN routing, the router will update its ARP table with this incorrect information. Connectivity to that IP address in the correct subnet will then be lost until that IP address sends out an ARP on the correct subinterface.

  There is no workaround. However, this problem is not present in Cisco IOS Release 12.0.

- CSCdp43242

  If a subinterface is configured with an encapsulation different from the encapsulation defined under the main interface, then the bridging will fail. The routing, however, will be correct. This appears in Cisco IOS Releases 11.0, 11.1, 11.2 and 11.3, but not in Cisco IOS Release 10.3.

Resolved Caveats—Cisco IOS Release 11.2

All the caveats listed in this section are resolved in Cisco IOS Release 11.2. This section only describes severity 1 and 2 caveats:

IBM Connectivity

- CSCdp17578

  An Advanced Peer-to-Peer Networking (APPN) router might experience a memory leak if you save the Routing Information Field during link activation.

- CSCdp63998

  A Cisco router that is running Advanced Peer-to-Peer Networking (APPN) might reload after the operator enters the **show appn dlur-pu host-pu** command.

- CSCdp36862

  A Cisco 7200 series router with a PA-4R port adapter might accept a packet with an invalid frame check sequence (FCS) and pass it on to remote source-route bridging (RSRB). This situation does not occur in the PA-4R-DTR port adapter.

IP Routing Protocols

- CSCdk37681

  The same global inside address is used for three different inside hosts—using dynamic address translation / 11.2.9 Cisco IOS software.

- CSCdp05306

  After a link flap, the summary route might not appear in the routing table although it appears in the OSPF topology table.

ISO CLNS

- CSCdm42127

  Under certain conditions, Cisco 7000 running Cisco IOS Release 11.2(18) may corrupt CLNS packets received on an ATM interface. This happens only when the packets are fast switched.

Miscellaneous

- CSCdk41197

  A Multiport Basic Rate Interface (MBRI) might pause indefinitely in "awaiting establishment" and "tei assigned" modes. Entering the **clear interface bri** *interface number* command establishes multiple frames on the port and allows another ISDN call to be made.

- CSCdk51490

  A crypto Access Control List (ACL) with a DENY ACE that specifies a TCP or User Datagram Protocol (UDP) port might cause fragments to be dropped.

  Workaround: Arrange the crypto ACLs to have permits only when specifying ports. For example, instead of the following:

  ```
  access-list 101 deny udp 200.200.20.0 0.0.0.255 200.200.30.0 0.0.0.255 eq 19
  access-list 101 deny udp 200.200.20.0 0.0.0.255 eq 19 200.200.30.0 0.0.0.255
  access-list 101 permit udp 200.200.20.0 0.0.0.255 200.200.30.0 0.0.0.255
  ```

  use:

  ```
  access-list 101 permit udp 200.200.20.0 0.0.0.255 ne 19 200.200.30.0 0.0.0.255 ne 19
  access-list 101 deny udp 200.200.20.0 0.0.0.255 200.200.30.0 0.0.0.255 eq 19
  access-list 101 deny udp 200.200.20.0 0.0.0.255 eq 19 200.200.30.0 0.0.0.255
  ```

- CSCdk64756

  Router's DHCP proxy agent lets the same IP address to two users on different ports but with the same username.

- CSCdk66567

  If Token Ring is the endpoint of an encrypted tunnel, extra packets are generated. The symptoms are a high CPU load (mainly taken by the Crypto Engine) and inaccurate addresses when enabling the **debug tunnel** command.

- CSCdp36078

  Lock and Key idle-timers will not reset when there are packets that match the dynamic ACLs created by Lock and Key.

- CSCdp37597

  For c75xx running 112-18 code may crash with a segV exception in encryption processing.

- CSCdp60101

  When configured to provide access control, the Kerberos client on Cisco products will fail all authentications when the expiration of the credential falls between January and February of a leap year.

- CSCdr02376

  When HSRP is configured between two NM-1FE-TXs connected to any Cisco switch, both routers become active and the interface on the router with the lower HSRP priority will flap.

Security

- CSCdr36952

  A defect in multiple versions of Cisco IOS software will cause a Cisco router or switch to stop and reload if the Cisco IOS http service is enabled and an attempt is made to browse to http://<router-ip. This defect can be exploited to produce a denial of service (DoS) attack. This defect has been discussed on public mailing lists and should be considered public information.

  The vulnerability, identified as Cisco bug ID CSCdr36952, affects virtually all mainstream Cisco routers and switches running Cisco IOS Release 11.1 through Release 12.1. The vulnerability has been corrected and Cisco is making fixed versions available to replace all affected Cisco IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect.

  Please see http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml for the latest complete version of this security advisory.

Wide-Area Networking

- CSCdk23860

  Routers experience high CPU utilization during business hours (about 95% and more) and quite high (20-30%) anytime when the traffic is low. Alignment errors are causing high CPU load on Cisco 4700 routers running on Cisco IOS Release 11.2. This also occurs on Cisco 3600s and Cisco 7200s running Cisco IOS Release 12.0. This happens when Frame Relay Traffic Shaping is configured with priority or custom queuing with classification based on tcp/udp port number or ip fragmentation.

- CSCdm44286

  Cisco 7200 running 11.1(20)CA1 is affected by a memory leak. The process Critical Bkgnd is taking up all the available memory.

Related Documentation

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

Documentation is available as printed manuals or electronic documents.

Use these release notes with these documents:

- Release-Specific Documents, page 16
- Platform-Specific Documents, page 16
- Feature Navigator, page 17
- Cisco IOS Software Documentation Set, page 17

Release-Specific Documents

The following documents are specific to Cisco IOS Release 11.2 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 11.2*

  On Cisco.com at:

  Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 11.2: Product Specific Release Notes for Cisco IOS Release 11.2**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 11.2: Release Notes**: **Cross-Platform Release Notes**

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

  Technical Documents

  Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, log in to Cisco.com and click **Software Center: Cisco IOS Software: Bug Toolkit: Bug Navigator II**. Another option is to go to http://www.cisco.com/support/bugtools/.

Platform-Specific Documents

These documents are available for the Cisco AS5200 on Cisco.com and the Documentation CD-ROM:

- *Cisco AS5200 Universal Access Server Installation Guide*
- *Cisco AS5200 Universal Access Server Software Configuration Guide*
- *Cisco AS5200 Universal Access Server Manager Guide*
- Port Information
- *Regulatory Compliance and Safety Information*
- Documentation for Spare Parts
- Cisco IOS Software
- *Quick Start Guide: Cisco AS5200 Universal Access Server Install and Configure*

  On Cisco.com at:

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

  On the Documentation CD-ROM at:

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

These documents are available for the Cisco AS5200 on Cisco.com and the Documentation CD-ROM:

- *Cisco IOS Release 11.2 Configuration Guides/Command References*
- *Cisco IOS Software Command Summary*
- *System Error Messages*
- *Cisco Management Information Base (MIB) User Quick Reference*

- *Debug Command Reference*
- *Access Services Quick Configuration Guide*
- *Release Notes for Cisco IOS Release 11.2*
- *Product-Specific Release Notes for Cisco IOS Release 11.2*
- *Channel Interface Processor Microcode Release Note and Microcode Upgrade Requirements*
- *Feature Pack Information*
- *LU Pooling and Response Time MIB*

  On Cisco.com at:

  Technical Documents: Documentation Home Page: IOS Software Configuration: Cisco IOS Release 11.2

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 11.2**

Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

http://www.cisco.com/go/fn

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

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.2: Configuration Guides and Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.2: Configuration Guides and Command References

Cisco IOS Release 11.2 Documentation Set Contents

Table 4 describes the contents of the Cisco IOS Release 11.2 software documentation set, which is available in electronic form and in printed form if ordered.

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

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.2: Cisco IOS Release 11.2 Configuration Guides/Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.2

Table 4 Cisco IOS Release 11.2 Documentation Set

Books	Major Topics
• *Configuration Fundamentals Configuration Guide* • *Configuration Fundamentals Command Reference*	Access Server and Router Product Overview User Interface System Images and Configuration Files Using ClickStart, AutoInstall, and Setup Interfaces System Management
• *Security Configuration Guide* • *Security Command Reference*	Network Access Security Terminal Access Security Accounting and Billing Traffic Filters Controlling Router Access Network Data Encryption with Router Authentication

Table 4 Cisco IOS Release 11.2 Documentation Set (continued)

Books	Major Topics
• *Access Services Configuration Guide* • *Access Services Command Reference*	Terminal Lines and Modem Support Network Connections AppleTalk Remote Access SLIP and PPP XRemote LAT Telnet TN3270 Protocol Translation Configuring Modem Support and Chat Scripts X.3 PAD Regular Expressions
• *Wide-Area Networking Configuration Guide* • *Wide-Area Networking Command Reference*	ATM Dial-on-Demand Routing (DDR) Frame Relay ISDN LANE PPP for Wide-Area Networking SMDS X.25 and LAPB
• *Network Protocols Configuration Guide, Part 1* • *Network Protocols Command Reference, Part 1*	IP IP Routing
• *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

Table 4 Cisco IOS Release 11.2 Documentation Set (continued)

Books	Major Topics
• *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 Support SNA Frame Relay Access Support APPN NCIA Client/Server Topologies IBM Channel Attach
• *Cisco IOS Software Command Summary* • *Access Services Quick Configuration Guide* • *System Error Messages* • *Debug Command Reference* • *Cisco Management Information Base (MIB) User Quick Reference*	

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

The most current Cisco documentation is available on the World Wide Web at http://www.cisco.com. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

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 and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

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.

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 your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

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 provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, 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 can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 15.