



Text Part Number: 78-6097-02

Release Notes for the Cisco AS5800 Universal Access Servers for Cisco IOS Release 12.0

August 16, 1999

These release notes for Cisco AS5800 universal access servers support Cisco IOS Release 12.0, up to and including Release 12.0(6). These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of the software caveats that apply to Release 12.0(6), see *Caveats for Cisco IOS Release 12.0* that accompanies these release notes. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

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

Contents

These release notes describe the following topics:

- Introduction, page 2
- System Requirements, page 3
- Feature Sets, page 5
- New and Changed Information, page 9
- Caveats, page 17
- Related Documentation, page 23
- Service and Support, page 28
- Cisco Connection Online, page 29
- Documentation CD-ROM, page 30

Corporate Headquarters

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

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

Introduction

The Cisco AS5800 is a high-density, Integrated Services Digital Network (ISDN) and modem Wide Area Network (WAN) aggregation system that provides digital and analog call termination. It is intended to be used as a service provider dial point-of-presence (POP) or centralized enterprise dial gateway. The Cisco AS5800 consists of a dial shelf, a router shelf, and (optionally) a system controller:

- The Cisco 5814 dial shelf has 14 slots and can support 1 dial shelf controller card and up to 12 feature cards (subject to a limit of 2 trunk cards and 10 modem cards) to provide full analog modem and ISDN coverage. The dial shelf supports up to 720 simultaneous analog and/or digital calls. Analog calls are terminated by a feature card that is loaded with integrated modems. ISDN calls are terminated onboard the trunk card on High-Level Data Link Control (HDLC) controllers. The E1 trunk and the T1 trunk card include channel service units (CSUs) and has either 12 E ports or 12 T1 ports that can operate as Primary Rate Interface (PRI) interfaces or channelized interfaces in any combination.
- The Cisco 7206 router shelf contains a network processing engine, an I/O controller, and the egress interfaces, such as High-Speed Serial Interface (HSSI), Fast Ethernet (FE), Fiber Distributed Data Interface (FDDI), and Asynchronous Transfer Mode (ATM), and supports either 280W AC-input or 280W DC-input redundant power. The router shelf also contains a dial shelf interconnect port adapter with a single RJ-45 receptacle that is used to connect the router shelf to the Cisco 5814 dial shelf. The interconnect port adapter connects directly to the dial shelf controller card on the dial shelf via a single, full-duplex cable. The cable used for this connection is a Cisco-proprietary cable, customized with jack screws to secure the connection. You must use this specially designed cable that ships with your interconnect port adapter.
- The Cisco 3640 system controller includes the Cisco 3640 router running Cisco IOS software. The system controller can be installed at a remote facility so users can access multiple systems through a console port or Web interface. System administrators can download software configurations to any Cisco AS5800 universal access server using Simple Network Management Protocol (SNMP) or Telnet. The system controller monitors Cisco equipment to provide performance data collection, accounting data collection, and logging.

The Cisco 5814 dial shelf and host Cisco 7206 router shelf communicate over a dial shelf interconnect cable (DSIC). This nonblocking interconnect supports 100 Mbps, full-duplex data transfer. Data is converted into packets by the feature cards, transmitted to a hub on the dial shelf controller (DSC) card, and from there sent to the router shelf. Conversely, packets from the router shelf are sent to the DSC card, where they are transmitted over the backplane to the modem and trunk cards.

The AC-input power shelf is an optional component of the Cisco <<series, e.g., 4000 series>> and is used to convert AC-input power into DC-output power for the DC-powered Cisco 5814 dial shelf. The AC-input power shelf contains two AC-input power supplies.

The Cisco <<series, e.g., 4000 series>> accept AC-input power via a separate, self-contained AC-input power shelf, which converts AC-input power into DC-output for use by the DC-powered dial shelf. The AC-input power shelf is rack-mounted and has a safety cover that shields the electrical connections in the power shelf rear.

The AC-input to DC-output connection supplies -48V DC-output power to the dial shelf power entry modules (PEMs). The PEMs receive the -48 volts and transmit power to the filter module. Power flows through the filter module to the backplane where it is distributed to the dial shelf controller card(s) and feature cards.

The AC-input power shelf includes two 2,000-watt, AC-input power supplies that plug into a common power backplane in the AC-input power shelf. A single AC-input power supply is capable of powering a fully configured Cisco 5814 dial shelf. The second power supply provides full redundancy.

For more information on the Cisco AS5800, refer to the *Cisco AS5800 Universal Access Server Software Installation and Configuration Guide* (DOC-5800-SICG) or the *Cisco AS5800 Universal Access Server Software Installation and Configuration Guide* (DOC-5800-HICG) that shipped with your system.

For information on new features and Cisco IOS commands supported by Release 12.0, see the “New and Changed Information” section on page 9 and “Related Documentation” section on page 17.

System Requirements

This section describes the system requirements for Release 12.0(6):

- Memory Requirements, page 3
- Hardware Supported, page 3
- Modem Code, page 4
- Determining Your Cisco IOS Software Release, page 4

Memory Requirements

Table 1 describes the memory requirements for the Cisco AS5800 feature sets supported by Cisco IOS Release 12.0(6). Flash memory is optional for these Cisco AS5800 images.

Table 1 Cisco AS5800 Memory Requirements

System Components	Feature Set	Image Name	Required Flash Memory	Required DRAM Memory	Runs From
Cisco AS5800 Router	IP Plus	c5800-p4-mz	16 MB	64 MB	RAM
Dial Shelf: Cisco 5814	IP Plus	dsc-c5800-mz	8 MB	32 MB	RAM
System Controller: Cisco 3640	IP Plus	c3640-c2is-mz	16 MB	64 MB	RAM

Hardware Supported

The Cisco AS5800 universal access server includes:

Platforms

- Cisco AS5814
- Cisco 7206
- Cisco 3640

Interfaces

- 12 port E1-trunk card
- 12 port T1-trunk cardT1

Modem cards

- 72-modem MICA card
- Dual-density MICA modem

Modem Code

Cisco IOS Release 12.0(1) and later includes bundled modem code, which is the firmware or portware that runs on the Microcom 12-port and MICA 6-port modem cards. Modem code is bundled with the Cisco IOS software image to eliminate the need to store separate modem code. When the access server starts, the Cisco IOS software unpacks the modem code and loads the proper code on the modem cards. Table 2 lists the current bundled modem code versions.

Table 2 Current Modem Versions

Modem Module	Current Bundled Modem Code Version	Minimum Cisco IOS Software Release
Microcom modems	Microcom version 3.1.30	11.3(3)T and later
MICA modems	MICA portware version 2.0.1.7	11.3(3)T and later

The **show modem mapping** command lists all versions of modem code running on the modem modules, residing in system Flash, and bundled with Cisco IOS software. Enter this command to help you decide if you need to update your modem code files.

Note The Cisco factory could have installed a later version of modem code than the one bundled with the Cisco IOS software. When this happens, the factory installs modem code in Flash memory and maps that code to the modems. Unless you fully understand how Cisco IOS software uses modem code, it is important to keep the factory configuration.

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

- Use this path to access the release notes from CCO:

Products and Ordering: Cisco Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5300: Modem Information: Firmware/Portware Release Notes.

- Use this path to access the release notes from the Documentation CD-ROM:

Cisco Product Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5300: Modem Information: Firmware/Portware Release Notes.

Determining Your Cisco IOS Software Release

To determine the version of Cisco IOS software running on your Cisco AS5800 universal access server, log on to the access server and enter the **show version** User EXEC command:

```
router> show version
```

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) 5800 Software (C5800-p4-mz), Version 12.0.....
```

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

The Cisco AS5800 universal access server contains multiple Cisco IOS software images. Four images are required to run the entire system (see Table 3). However, only the first three software images listed require part numbers for ordering.

Filename	Description
c5800-p4-mz	Router shelf image—Cisco IOS software image supporting the Cisco 7206 router shelf functionality, bundled trunk card, and modem card images.
c7200-boot-mz	Router shelf boot image—Boot helper image for the Cisco 7206 router shelf
dsc-c5800-mz	Dial shelf controller image—Special image for the Cisco 5814 dial shelf controller card
das-c5800-m.unicode	Dial shelf feature board image—Cisco 5814 dial shelf feature card image bundled into the router shelf image

For information on upgrading to a new software release, refer to the *Cisco IOS Software Release Upgrade Paths and Packaging Simplification* product bulletin #703 located on CCO. For more information, refer to the “Cisco Connection Online” section later in this document.

On CCO, follow this path:

Products and Ordering: Product Bulletins: Upgrade Paths and Packaging Simplification

Feature Sets

This section lists Cisco IOS software feature sets available for the Cisco AS5800. Table 4 uses the following terms to identify features:

Feature Set Matrix Term	Description
Yes	This feature is offered.
No	This feature is not offered.
In	The “In” column lists the Cisco IOS release that first introduces a feature. For example, (1) means a feature is introduced in 12.0(1). If a cell has a dash in this column, the feature was included in the initial, base release.

Table 4 lists the feature sets supported up to and including Cisco IOS Release 11.3(2)AA. IPSEC listed in this table is an abbreviation for IP Security.

Features	IP Plus	In
IBM Support		
APPN High-Performance Routing	No	-
APPN MIB Enhancements	No	-
APPN over Ethernet LAN Emulation	No	-
APPN Scalability Enhancements	No	-
Bisync Enhancements:	No	-
— Bisync 3780 Support		
— BSC Extended Addressing		
— Block Serial Tunneling (BSTUN) over Frame Relay		
Cisco MultiPath Channel (CMPC)	No	-
DLSw+ Enhancements:	No	-
— Backup Peer Extensions for Encapsulation Types		
— DLSw+ Border Peer Caching		
— DLSw+ MIB Enhancements		
— DLSw+ SNA Type of Service		
— LLC2-to-SDLC Conversion between PU4 Devices		
— NetBIOS Dial-on-Demand Routing		
— UDP Unicast Enhancement		
FRAS Enhancements:	No	-
— FRAS Boundary Network Node Enhancement		
— FRAS Dial Backup over DLSw+		
— FRAS DLCI Backup		
— FRAS Host		
— FRAS MIB		
— SRB over Frame Relay		
RIF Passthru in DLSw+	No	-
SRB over FDDI on Cisco 4000-M, 4500-M, and 4700-M Routers	No	-
TN3270 LU Nailing	No	-
TN3270 Server Enhancements	No	-
Token Ring LANE	No	-
Tunneling of Asynchronous Security Protocols	No	-
Internet		-
DRP Server Agent	No	-
DRP Server Agent Enhancements	No	-
L2TP	No	-
SS7	No	-
IP Routing		-
Easy IP (Phase 1)	Yes	(1)

Features	IP Plus	In
Hot Standby Router Protocol (HSRP) over ISL in Virtual LAN Configurations	No	-
IP Enhanced IGRP Route Authentication	Yes	(1)
OSPF LSA Group Pacing	Yes	(1)
OSPF Point-to-Multipoint Networks with Neighbors	Yes	(1)
Per User DNS	No	-
PIM Version 2	Yes	(1)
TCP Enhancements:	Yes	(1)
— TCP Selective Acknowledgment		
— TCP Timestamp		
LAN Support		
AppleTalk Access List Enhancements	No	-
DECnet Accounting	No	-
IPX Named Access Lists	No	-
IPX SAP-after-RIP	No	-
NLSP Enhancements	No	-
NLSP Multicast Support	No	-
Management		
Cisco Call History MIB Command Line Interface	Yes	(1)
Cisco IOS File System	Yes	(1)
Cisco IOS Internationalization	Yes	(1)
Conditionally Triggered Debugging	Yes	(1)
Entity MIB, Phase 1	Yes	(1)
External Portware Download	No	-
Show Caller Command	No	-
Show Modem Command	No	-
SNMP v2C	Yes	(1)
SNMP Inform Requests	No	-
Virtual Profiles	Yes	(1)
VPDN MIB	No	(1)
VPDN MIB and Syslog Facility	No	-
Multimedia		
IP Multicast Load Splitting across Equal-Cost Paths	Yes	(1)
IP Multicast over ATM Point-to-Multipoint Virtual Circuits	Yes	(1)
IP Multicast over Token Ring LANs	Yes	(1)
Stub IP Multicast Routing	Yes	(1)
Quality of Service		
RTP Header Compression	No	-
Security		

Features	IP Plus	In
AAA Scalability	No	-
Authenticating ACL	No	-
Automated Double Authentication	No	-
Certificate Authority Interoperability	No	-
Double Authentication	Yes	(1)
Encrypted Kerberized Telnet	No	-
HTTP Security	Yes	(1)
Internet Key Exchange Security Protocol	No	-
IPSec Network Security	No	-
MS-CHAP Support	No	-
Named Method Lists for AAA Authentication and Accounting	No	-
Per-User Configuration	Yes	(1)
Reflexive Access Lists	Yes	(1)
TCP Intercept	No	-
Vendor-Proprietary RADIUS Attributes	Yes	(1)
Vendor-Proprietary RADIUS -Additional Attributes	No	-
Switching		
AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs	No	-
CLNS and DECnet Fast Switching over PPP	No	-
DECnet/Vines/XNS over ISL:	No	-
— Banyan VINES Routing over ISL Virtual LANs		
— DECnet Routing over ISL Virtual LANs		
— XNS Routing over ISL Virtual LANs		
Fast-Switched Policy Routing	Yes	(1)
IPX Routing over ISL Virtual LANs	No	-
VIP Distributed Switching Support for IP Encapsulated in ISL	No	-
Terminal Services		
Telnet Extensions for Dialout	No	-
Virtual Templates for Protocol Translation	No	-
WAN Optimization		
ATM MIB Enhancements	No	-
PAD Enhancements	No	-
PAD Subaddressing	Yes	(1)
WAN Services		
Always On/Dynamic ISDN (AO/DI)	No	-
Bandwidth Allocation Control Protocol	Yes	(1)
Channelized T3	No	-
Dialer Watch	Yes	(1)
E1 R2	No	-

Features	IP Plus	In
E1 R1 Support for Taiwan only	No	-
Enhanced Local Management Interface (ELMI)	No	-
Frame Relay Enhancements	Yes	(1)
Frame Relay MIB Extensions	Yes	(1)
Frame Relay Router ForeSight	Yes	(1)
GRE VPN	No	-
ISDN Advice of Charge	Yes	(1)
ISDN Caller ID Callback	Yes	(1)
ISDN NFAS	Yes	(1)
Layer 2 Forwarding—Fast Switching	Yes	(1)
Leased-Line ISDN at 128 kbps	No	-
Microsoft Point-to-Point Compression (MPPC)	No	-
MS Callback	Yes	(1)
Modem Management Enhancements	Yes	(1)
Multiple ISDN Switch Types	No	-
National ISDN Switch Types for BRI and PRI Interfaces (NI2)	No	-
PPP over ATM	No	-
Stackable Home Gateway	No	-
Switched 56K Digital Connections	No	-
Telnet Extensions for Dialout	No	-
X.25 Enhancements	Yes	(1)
X.25 on ISDN	Yes	(1)

New and Changed Information

This section lists the new features supported by the *Cisco AS5800* for Cisco IOS in Release 12.0(1).

New Features in Release 12.0(1)

The following new features for the Cisco AS5800 universal access server are available for Cisco IOS Release 12.0(1). Documentation is also provided for these features.

- Additional Vendor-Proprietary RADIUS Attributes
- Microsoft Point-to-Point Compression (MPPC)
- MS-CHAP Support
- Multiple ISDN Switch Types
- Named Method Lists for AAA Authorization and Accounting
- National ISDN Switch Types for Basic Rate and Primary Rate Interfaces
- Performance Data Collection (for the Cisco 3640 system controller)
- VPDN MIB and Syslog Facility

Additional Vendor-Proprietary RADIUS Attributes

Remote Authentication Dial-In User Server (RADIUS) is an access server authentication, authorization, and accounting protocol originally developed by Livingston, Inc. Although an Internet Engineering Task Force (IETF) draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. In this release, Cisco IOS software introduces support for additional vendor-proprietary RADIUS attributes. Users who have implemented security solutions using a vendor-proprietary implementation of RADIUS can now integrate Cisco access routers into their networks more easily.

Microsoft Point-to-Point Compression (MPPC)

Microsoft Point-to-Point Compression (MPPC) is a scheme used to compress Point-to-Point Protocol (PPP) packets between Cisco and Microsoft client devices. The MPPC algorithm is designed to optimize processor and bandwidth utilization in order to support multiple simultaneous connections. The MPPC algorithm uses a Lempel-Ziv (LZ) based algorithm with a continuous history buffer, called a dictionary.

MS-CHAP Support

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; in this case, authentication occurs between a PC using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server (NAS).

MS-CHAP differs from the standard CHAP as follows:

- MS-CHAP is enabled by negotiating CHAP Algorithm 0x80 in LCP option 3, Authentication Protocol.
- The MS-CHAP Response packet is in a format designed to be compatible with Microsoft Windows NT 3.5 and 3.51, Microsoft Windows 95, and Microsoft LAN Manager 2.x. This format does not require the authenticator to store a clear or reversibly encrypted password.
- MS-CHAP provides an authenticator-controlled authentication retry mechanism.
- MS-CHAP provides an authenticator-controlled change password mechanism.
- MS-CHAP defines a set a “reason-for failure” codes returned in the Failure packet message field.

Depending on the security protocols you have implemented, PPP authentication using MS-CHAP can be used with or without Authentication, Authorization and Accounting (AAA) security services. If you have enabled AAA, PPP authentication using MS-CHAP can be used in conjunction with both TACACS+ and RADIUS.

Multiple ISDN Switch Types

The **Multiple ISDN Switch Types** feature allows you to configure more than one ISDN switch type per router. You can apply an ISDN switch type on a per interface basis, thus extending the existing global **isdn switch-type** command to the interface level. This allows Basic Rate Interfaces (BRI) and Primary Rate Interfaces (PRI) to run simultaneously on platforms that support both interface types.

The **isdn tei** command is also extended to the interface level. Terminal endpoint negotiation (TEI) determines when Layer 2 is activated (powerup or first-call).

Named Method Lists for AAA Authorization and Accounting

In earlier Cisco IOS releases, only named authentication method lists were supported under Cisco's Authentication, Authorization, and Accounting (AAA) network security services. With Cisco IOS Release 11.3(3)T, AAA has been extended to support both authorization and accounting named method lists. Named method lists for authorization and accounting function the same way as those for authentication; they allow you to define different methods for authorization and accounting and apply those methods on a per-interface or per-line basis.

National ISDN Switch Types for Basic Rate and Primary Rate Interfaces

National ISDN Switch Types for Basic Rate and Primary Rate Interfaces introduces changes to ISDN switch types for Primary Rate Interfaces (PRI) and Basic Rate Interfaces (BRI) as follows:

- Adds a new switch type for PRI interfaces (**isdn switch-type primary-ni**).
- Changes the BRI basic-ni1 switch type to basic-ni (**isdn switch-type basic-ni**).
- Removes the ISDN vn2 switch type (**isdn switch-type vn2**) used in France. The existing vn3 switch type (**isdn switch-type vn3**) supports French vn2 switches.
- Removes the ISDN basic-nwnet3 switch type (**isdn switch-type basic-nwnet3**) used in Norway. The basic-net3 switch type (**isdn switch-type basic-net3**) supports Norway NET3 switches.
- Removes the ISDN basic-nznet3 switch type (**isdn switch-type basic-nznet3**) used by New Zealand NET3 switches. The ISDN basic-net3 switch type (**isdn switch-type basic-net3**) supports New Zealand NET3 switches.
- Adds the ability to configure outgoing PRI B channel selection for the T1 controller in ascending order (channel 1 to channel 23) or descending order (channel 23 to channel 1). Previously, the router selected a B channel for outgoing calls from the highest free channel in descending order. The E1 controller channel selection for ascending order is channel 1 to 31, and 31 to 1 for descending order.

Note The command parser will still accept the following switch types: basic-nwnet3, vn2, and basic-net3; however, when viewing the NVRAM configuration using either the **show running configuration** or **write terminal** command, the basic-net3 or vn3 switch types are displayed respectively.

Performance Data Collection

The Performance Data Collection feature allows a system controller, Cisco 3640, to collect and store SNMP MIB data from its managed router and dial shelves. The system controller then serves as a central point for network management data collection. The system controller collects the raw data from the managed shelves periodically, saves the data, and provides a single access point for a central network management application. The data can then be uploaded to a network management station using FTP or TFTP.

VPDN MIB and Syslog Facility

The Virtual Private Dialup Network (VPDN) Management Information Base (MIB) feature is intended to support all the tables and objects defined in "Cisco VPDN Management MIB" for the user sessions of the VPDN features. There are a number of commands which provide information and statistics through the Command Line Interface (CLI) but not Simple Network Management Protocol (SNMP); the Cisco VPDN MIB has been created to satisfy the need to provide information and statistics through SNMP.

New Features in Release 11.3(2)AA

The following new features for the Cisco AS5800 universal access server are available for Cisco IOS Release 11.3(2)AA. Documentation is also provided for these features.

- Cisco AS5800 Universal Access Server Feature Module
- Cisco IOS File System
- Conditionally Triggered Debugging
- AAA Scalability
- OSPF LSA Group Pacing
- OSPF Point-to-Multipoint Networks with Neighbors
- Dialer Watch
- MS Callback
- PIM Version 2
- DRP Server Agent Enhancements
- VPDN MIB
- SNMP Inform Requests
- Modem Management Enhancements

The following features are for the Cisco 3640 system controller:

- Shelf Discovery and Autoconfiguration
- Health Monitor
- Virtual Console
- FTP Server
- Syslog Disk Logging

Cisco AS5800 Universal Access Server Feature Module

This feature module presents the new features for the Cisco AS5800 universal access server and includes a description of the system, supported MIBs and RFCs, and configuration tasks including the following:

- Configuring shelf IDs
- Executing commands on cards
- Configuring busyout
- Upgrading modem firmware
- Commands, with explanations and examples of new and modified commands
- Debug commands, with examples and sample output

Cisco IOS File System

The Cisco IOS File System (IFS) feature provides a single interface to all file systems the router uses:

- Flash memory file systems

- Network file systems (TFTP, rcp, FTP)

Any other endpoint for reading or writing data (NVRAM, the running configuration, ROM, raw system memory, system bundled microcode, Xmodem, Flash load helper log, Lex interfaces, modems, and BRI MUX interfaces).

Conditionally Triggered Debugging

The Conditionally Triggered Debugging feature limits debugging messages based on their related interface or subinterface. When this feature is enabled, the router will generate debugging messages for packets entering or leaving the router on a specified interface. However, the router will not generate debugging output for packets entering or leaving through a different interface. This feature allows you to focus debugging output on the problematic interface or interfaces. You can specify the interfaces explicitly. For example, you may only want to see debugging messages for one interface or subinterface. You can also turn on debugging for all interfaces that meet specified conditions, such as a particular username, calling party number, or called party number. If you specify multiple conditions, the interface must meet at least one of the conditions.

AAA Scalability

The Authentication, Authorization and Accounting (AAA) Scalability feature enables you to configure and monitor the number of background processes allocated by the PPP manager in the network access server (NAS) to deal with AAA authentication and authorization requests. In previous Cisco IOS releases, only one background process was allocated to handle all AAA requests for PPP. This meant that parallelism in AAA servers could not be fully exploited. The AAA Scalability feature enables you to configure the number of processes used to handle AAA requests for PPP, thus increasing the number of users that can be simultaneously authenticated or authorized.

OSPF LSA Group Pacing

The OSPF LSA group pacing feature allows the router to group together OSPF link state advertisements (LSAs) and pace the refreshing, checksumming, and aging functions. The group pacing results in more efficient use of the router.

OSPF Point-to-Multipoint Networks with Neighbors

OSPF has two new features related to point-to-multipoint networks. One feature applies to broadcast networks; the other feature applies to nonbroadcast networks. On point-to-multipoint, broadcast networks, there is no need to specify neighbors. However, you can specify neighbors with the neighbor command, in which case you should specify a cost to that neighbor. On point-to-multipoint, nonbroadcast networks, you now use the neighbor command to identify neighbors. Assigning a cost to a neighbor is optional.

Before this feature, some OSPF point-to-multipoint protocol traffic was treated as multicast traffic. Therefore, the neighbor command was not needed for point-to-multipoint interfaces because multicast took care of the traffic. Hellos, updates, and acknowledgments were sent using multicast. In particular, multicast hellos discovered all neighbors dynamically. Some customers, however, were using point-to-multipoint on nonbroadcast media (such as classic IP over ATM), so their routers could not dynamically discover their neighbors. This feature allows the neighbor command to be used on point-to-multipoint interfaces. On any point-to-multipoint interface (broadcast or not), the Cisco IOS software assumes the cost to each neighbor is equal. The cost is configured with the **ip ospf cost** command. In reality, the bandwidth to each neighbor is different, so the cost should be different. With this feature, you can configure a separate cost to each neighbor. This feature applies to point-to-multipoint interfaces only.

Dialer Watch

Dialer Watch is a backup feature that integrates dial backup with routing capabilities. Prior dial backup implementations used the following conditions to trigger backup:

- Interesting packets were defined at central and remote routers using Dial on Demand routing (DDR).
- Connection loss occurred on a primary interface using a back up interface with floating static routes.
- Traffic thresholds were exceeded using a dialer load threshold.

Prior backup implementations might not have supplied optimum performance on some networks, such as those using Frame Relay multipoint subinterfaces or Frame Relay connections that do not support end-to-end LMI.

Dialer Watch provides reliable connectivity without relying solely on defining interesting traffic to trigger outgoing calls at the central router. Dialer Watch uses the convergence times and characteristics of dynamic routing protocols. Integrating backup and routing features enables Dialer Watch to monitor every deleted route. By configuring a set of watched routes that define the primary interface, you are able to monitor and track the status of the primary interface as watched routes are added and deleted. Monitoring the watched routes is done in the following sequence:

- 1 Whenever a watched route is deleted, Dialer Watch checks to see if there is at least one valid route for any of the watched IP addresses defined.
- 2 If there is no valid route, the primary line is considered down and unusable.
- 3 If there is a valid route for at least one of the defined watched IP addresses, and if the route is pointing to an interface other than the backup interface configured for Dialer Watch, the primary link is considered up.
- 4 In the event that the primary link goes down, Dialer Watch is immediately notified by the routing protocol and the secondary link is brought up.
- 5 Once the secondary link is up, at the expiration of each idle timeout, the primary link is rechecked.
- 6 If the primary link remains down, the idle timer is indefinitely reset.
- 7 If the primary link is up, the secondary backup link is disconnected. Additionally, a disable timer can be set to create a delay for the secondary link to disconnect, after the primary link is reestablished.

MS Callback

The MS Callback feature provides client-server callback services for Microsoft Windows 95 and Microsoft Windows NT clients. MS Callback supports the Microsoft Callback Control Protocol (MSCB). MSCB is a Microsoft proprietary protocol used by Windows 95 and Windows NT clients. MS Callback supports negotiated PPP Link Control Protocol (LCP) extensions initiated and agreed upon by the Microsoft client. MS Callback is added to existing PPP Callback functionality. Therefore, if you configure your Cisco AS5800 to perform PPP Callback using Cisco IOS Release 11.3(2)T or later, MS Callback is automatically available.

MS Callback supports AAA security models using a local database or AAA server. MSCB uses LCP callback options with suboption type 6. The Cisco MS Callback feature supports clients with a user-specified callback number and server-specified (preconfigured) callback number. MS Callback does not affect non-Microsoft machines that implement standard PPP LCP extensions as described in RFC 1570. In this scenario, MS Callback is transparent.

PIM Version 2

Protocol-Independent Multicast (PIM) Version 2 includes the following improvements over PIM Version 1:

- A single, active rendezvous point (RP) exists per multicast group, with multiple backup RPs. This compares to multiple active RPs for the same group in PIM Version 1.
- A bootstrap router (BSR) provides a fault-tolerant, automated RP discovery and distribution mechanism. Thus, routers dynamically learn the group-to-RP mappings.
- Sparse mode and dense mode are properties of a group, as opposed to an interface. Cisco recommends sparse-dense mode, as opposed to either sparse mode or dense mode only.
- PIM Join and Prune messages have more flexible encodings for multiple address families.
- A more flexible Hello packet format replaces the Query packet to encode current and future capability options.
- Register messages to an RP indicate whether they were sent by a border router or a designated router.
- PIM packets are no longer inside IGMP packets; they are stand-alone packets.

PIM Version 1, together with the Auto-RP feature, can perform the same tasks as the PIM Version 2 BSR. However, Auto-RP is a stand-alone protocol, separate from PIM Version 1, and is Cisco proprietary. PIM Version 2 is a standards track protocol in the Internet Engineering Task Force (IETF).

Cisco's PIM Version 2 implementation allows good interoperability and transition between Version 1 and Version 2. You can upgrade to PIM Version 2 incrementally. PIM Versions 1 and 2 can be configured on different routers within one network. Internally, all routers on a shared media network must run the same PIM version. Therefore, if a PIM Version 2 router detects a PIM Version 1 router, the Version 2 router downgrades itself to Version 1 until all Version 1 routers have been shut down or upgraded.

PIM uses the BSR to discover and announce RP-set information for each group prefix to all the routers in a PIM domain. This is the same function accomplished by Auto-RP, but the BSR is part of the PIM Version 2 specification. The BSR mechanism interoperates with Auto-RP.

To avoid a single point of failure, you can configure several candidate BSRs in a PIM domain. A BSR is elected among the candidate BSRs automatically; they use bootstrap messages to discover which BSR has the highest priority. This router then announces to all PIM routers in the PIM domain that it is the BSR.

Routers that are configured as candidate RPs then unicast to the BSR the group range for which they are responsible. The BSR includes this information in its bootstrap messages and disseminates it to all PIM routers in the domain. Based on this information, all routers will be able to map multicast groups to specific RPs. As long as a router is receiving the bootstrap message, it has a current RP map.

DRP Server Agent Enhancements

The DRP Server Agent enhancements are as follows:

- Distributed Director can use BGP Multi-Exit Discriminators in traffic redirection decisions.
- The DRP Server can measure client-to-server link latency (roundtrip time) for use in traffic redirection decisions.

VPDN MIB

For VPDN (Virtual Private Dial Network) sessions, information on active tunnels and sessions will be retrievable by SNMP from the VPDN MIB.

SNMP Inform Requests

The following software enhancement was first introduced in Cisco IOS Release 11.3(1)T, and is now available for the Cisco AS5800. The SNMP Inform Requests feature allows routers to send inform requests to SNMP managers.

Routers can send notifications to SNMP managers when particular events occur. For example, an agent router might send a message to a manager when the agent router experiences an error condition. SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. However, an SNMP manager that receives an inform request acknowledges the message with an SNMP response PDU. If the manager does not receive an inform request, it does not send a response. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

Because they are more reliable, informs consume more resources in the router and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times.

The retries increase traffic and contribute to a higher overhead on the network. Thus, traps and inform requests provide a trade-off between reliability and resources. If it is important that the SNMP manager receives every notification, use inform requests. On the other hand, if you are concerned about traffic on your network or memory in the router and you do not need to receive every notification, use traps.

Modem Management Enhancements

This modem management enhancements feature is available for Cisco AS5800 universal access servers using MICA modems. A snapshot of all the firmware versions running on all modems in the access server can be displayed by using the **show modem mapping** command. This command also shows the source location of each version of firmware (for example, running out of Flash memory, boot Flash memory, or bundled with Cisco IOS software). This command is useful for managing and monitoring multiple versions of modem firmware running in an access server.

Shelf Discovery and Autoconfiguration

The Shelf Discovery and Autoconfiguration feature allows a system controller to automatically discover new shelves and properly configure them to interact with the system controller. The system controller communicates with its managed shelves through the Shelf Discovery Protocol (SDP), which runs on top of UDP.

Health Monitor

The Health Monitor feature monitors key performance attributes of the shelves managed by the system controller. The Health Monitor feature continually polls its managed shelves to obtain the information stored in the Health Monitor MIB. Management stations collect information for all the shelves from the system controller rather than by polling each shelf individually. In addition, you can

configure specific performance thresholds for all managed shelves through simple commands on the system controller. The system controller uses SNMP to automatically configure the following on each managed shelf:

- Expressions in the EXPRESSION-MIB to calculate the attributes
- RMON alarms to poll the attributes at specific intervals
- RMON events to send traps to the system controller when an attribute exceeds its specified threshold

When threshold traps are received by the system controller, they are converted to Health Monitor traps and sent to trap destinations configured in the system controller.

Virtual Console

The Virtual Console feature allows you to access dial and router shelves connected to a system controller. During a system controller session, you can connect to a router or dial shelf at the same privilege level as the current system controller session. By entering one command, you can Telnet directly to a shelf, provide a username and password, and then go to the same privilege level as the system controller.

FTP Server

The FTP Server feature configures a router to act as an FTP server. FTP clients can copy files to and from certain directories on the router. In addition, the router can perform many other standard FTP server functions.

Syslog Disk Logging

The Syslog Disk Logging feature allows you to collect, store, and retrieve all managed shelf syslog messages through the system controller. The system controller receives syslog messages from managed shelves and stores these messages in subfiles on its disk. Each syslog message stored in a subfile contains the following information:

- Host IP address
- Facility
- Severity
- Timestamp (date and time) set by the managed shelf
- Text message

In addition, this feature provides an enhanced method of viewing messages in the logging history table. Messages can be displayed based on host IP address, time received, and order receive

Caveats

This section contains open caveats for the current Cisco IOS maintenance release only. For information on caveats in previous maintenance releases, refer to the *Caveats for Release 11.3*, refer to the “caveates” section in ght *Cross-Platform Release Notes for Cisco IOS Release 12.0(1)* document located on CCO and the Documentation CD-ROM. This section contains caveats affecting all maintenance releases.

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 12.0(1)

This section describes possibly unexpected behavior by Release 12.0(1). This section describes only severity 1 and 2 caveats.

Access Server

- Under heavy stress, a Cisco AS5200 series router may get a bus error and reload. [CSCdk44928]

Basic System Services

- When hardware compression is enabled, packets are normally fastswitched. If the user turns off fastswitching then turns it back on, fastswitching remains disabled.

The workaround is to reconfigure compression (for example, use the **no comp** and **comp stac** commands). [CSCdj14601]

- When configuring more than one traffic shape group on a serial interface, only one of the defined traffic shape groups is used. The additional traffic shape group will not show up in the running configuration or startup configuration displays if the group assignment options are not added to the traffic-shape group command as the first statement. [CSCdk09806]
- Currently Generic Traffic Shaping and Frame Relay Traffic Shaping is not supported with turbo (Optimum/CEF) switching modes. You need to disable these turbo switching modes to make traffic shaping work over the interface. This fix allows turbo switching modes to co-exist with traffic shaping. [CSCdk28278]
- A router becomes unresponsive when a query RTR history is attempted and the history table is empty. [CSCdk36156]
- A problem was seen when a user dialed into a Cisco AS5200: The user was passed to a TACACS+ server and authenticated. However, the access list passed back to the router by the TACACS+ server is not applied to the asynchronous interface by the router. [CSCdk39738]
- An SNMP memory leak was detected when an SNMP ping was enabled. [CSCdk40599]
- A customer using a Cisco 4700-M router reported that running traffic shaping with custom queuing drops too many packets. [CSCdk41472]
- A Cisco MC3810 router has a TDM group configured on the E1 controller. When a cross connect is configured using the TDM group, incorrect time slots are assigned. [CSCdk50968]

IBM Connectivity

- While running DLSw with FST encapsulation, the router might give the following error message along with traceback:

```
00:39:38: %SYS-2-INPUTQ: INPUTQ set, but no IDB, ptr=ADDD9C -Traceback= 148D3A 572A
4DF4 110064 17DAA2 17B0DA 14CC 10005B4 10047DA
```

There is currently no workaround for this problem. [CSCdk25935]

- The input queue on the Token Ring interfaces may overflow and accept no additional packets. The workaround is to increase the interfaces' input queue or reload the router. You could use this command, for example:

```
hold-queue 200 in
[CSCdk36470]
```

- A Cisco 4500 router configured with a Token Ring LE Client adds six extra bytes when fastswitching routed protocol packets from a Token Ring LEC ATM interface to the packets target output interface. Although, this problem is known to occur with IP packets, it potentially exists for other routed protocols that are fastswitched in a TR-LANE interface, and fastswitched to the packets target output interface. [CSCdk48387]

Interfaces and Bridging

- When encapsulation is changed on a PRI interface, B-channel interfaces are set in the UP state. This can cause the first call to the B-channel to fail, but subsequent calls to that channel will work after the first failure.

Workaround: When changing encapsulation on a PRI interface, first shut down the interface before configuring new encapsulation. [CSCdj91477]

- When multiple ATM-Lite port adapters are situated in the same PCI bus on a Cisco 7200 series router, sub-optimal performance is noticed. This is not a recommended configuration. [CSCdk30675]
- A problem occurred when HSSI3 code was waiting for the chip reset to be done at the beginning of the code sequence. However, chip reset is only done at booting or OIR. This problem has not shown up before because, when both the transmit and receive clocks are present, somehow bit 0 of STATUS6 is also set, so the microcode can proceed with no problem. But the microcode sticks at PC=0 when there is only one clock.

The workaround is just to proceed regardless of the reset status, as the old HSSI microcode did. [CSCdk39193]

- A Cisco router can crash when the following events occur: CEF switching is enabled and an IP address is assigned to an ISL sub-interface, then the sub-interface is deleted, but the same IP address is assigned to another interface. [CSCdk46966]
- Removing an ATM Deluxe card from a Cisco 7200 router and inserting an ATM Lite card in the same slot can cause the router to crash. [CSCdk48089]

IP Routing Protocols

- A new configuration command, `ip spd mode aggressive`, is available. When configured, all IP packets that fail sanity check, such as "bad checksum not version 4," and "bad TTL," will be dropped aggressively to guard against bad IP packet spoofing. The `show ip spd` command displays whether aggressive mode is enabled or not. SPD random drop in RSP is supported.

When enabled, SPD now works as follows:

- When the **ip spd mode aggressive** command is issued, IP packets that fail sanity checks are classified as aggressive droppable packets.
- When the IP input queue reaches SPD minimum threshold (specified by **ip spd queue min-threshold n** command), all aggressive droppable packets are dropped immediately, while normal IP packets (not high-priority SPD packets) are dropped with increasing probability as the length of the IP input queue grows.

- When the IP input queue reaches SPD maximum threshold (specified by **ip spd queue max-threshold** *n* command), all normal IP packets are dropped at 100 percent.

The default SPD minimum threshold is 10, while the default maximum threshold is 75. To avoid an input interface that takes too many router resources, new packets (SPD or non-SPD) received from that interface are dropped when the interface has more than the input hold queue limit of input packets floating somewhere in the router. [CSCdj45202]

- A router configured with a policy route map on a BRI interface may not forward packets to the next hop as specified in the `set ip next-hop` statement.

The following conditions must exist for policy routing to fail:

- The **ip policy route-map name** command is configured on a BRI interface.
- The destination exists in the IP cache table of the policy router.

The workaround is to use the **clear ip cache** command, or remove fast-switching by using the `no ip route-cache` command. [CSCdk12537]

- NetBIOS over TCP/IP port 139 is not getting translated. Support for this feature is currently being added by development. [CSCdk26313]
- The system encounters console error messages during periods of high serial line usage. Error messages are of the format:

```
%SYS-3-CPUHOG: Task ran for 2672 msec (87/71), Process = IP Input
```

[CSCdk26388]

- The **clear ip route net** command can remove a connected route from the routing table which will not be properly reinstalled. This is a regression introduced in the 12.0 software by CSCdk01482.

A workaround is to use the `shut` then the `no shut` commands on the interface. [CSCdk40372]

Miscellaneous

- If two Cisco 7500 series routers are connected to many Ethernet interfaces with EIP interface processors, and are running HSRP on many of these interfaces, the HSRP configuration may take several minutes to determine the active and standby routers after a router reloads. During this period of instability, the CPU load on the router approaches 100%.

The workaround is to replace the EIP interface processors with VIP interface processors and Ethernet Port adapters. A less effective workaround is to reduce the number of HSRP groups, or to increase the HSRP hello and hold time. [CSCdj29595]

- Packets might not be forwarded correctly and may cause problems if fancy queuing (for example, fair-queue) is enabled along with the Compression Service Adapter (CSA). [CSCdj64898]
- When using the **physical-layer async** command on low-speed serial interfaces (either asynchronous or synchronous), the fast-switching process increases by approximately 10 percent. [CSCdj80674]
- A Cisco 7200 router configured to route IP packets over ISDN with encryption only works in process-switch mode. [CSCdj82823]
- Encrypted TCP sessions are pausing when passing over an MPP bundle as soon as two or more members in the bundle become active. This behavior is only observed when building a TCP session between hosts on the LAN interface of two routers connected using encrypted MPP.

The current workaround is to disable fastswitching on the LANs. [CSCdj91142]

- A VIP Token Ring interface does not encrypt or decrypt IP packets containing a routing information field (RIF), even though the initial crypto connection setup with the remote router is successful. Encryption and decryption for Token Ring IP packets without a RIF continue to function normally. [CSCdk18888]
- On a Cisco 5800 series router, where the TTY lines are configured with **autoselect ppp** and the asynchronous interfaces are configured with **async mode interactive**, PPP calls to the asynchronous interfaces of the Cisco 5800 router can fail occasionally. [CSCdk21977]
- A router cannot handle TCP flows according to QoS weight defined after a reload or using the `wr mem` or `conf mem` commands. [CSCdk28971]
- Context-Based Access Control (CBAC) fails to create dynamic access control lists that allow FTP data channels to be established because the FTP client sends the command terminated signal with a single carriage return character, instead of the carriage return and line feed character sequence. The symptom is that commands that require the exchange of a port to set up a data channel between client and server, such as the UNIX `ls` command, hang. [CSCdk35745]
- When using an NPE200, the fallback pool uses SRAM and will be triggered on all the time. The NPE150 triggers the fallback pool only when no receive buffer has been detected, to minimize the impact of the DRAM fallback pool on high speed port adapters. [CSCdk38210]
- If only one VIC is installed in the VPN on a Cisco 2600 router, it must be installed in slot 0. Installing only one VIC in slot 1 causes the router to crash. [CSCdk41106]
- There is a limit of 25 crypto maps on any VIP. This limit applies when encrypting many serial lines on the VIP using a fractional T1 or E1 port adapter. [CSCdk41708]
- When the traffic between the PA-12E/2FE port adapter and the CPU is high and the PCI bus is overloaded, a DEC21140 can get underrun and overrun errors. This is due to PCI congestion. The traffic is affected momentarily, then restored. [CSCdk41735]
- Bell 103 communication does not work on the analog Microcom modems in answer mode. [CSCdk43602]
- If a crypto map is applied to a dialer interface, dialer pools are used and a dialup interface (for example, a BRI) is used as the physical interface. When that dialup interface is unbound from the dialer, it can cause a system reload or misalignments. A workaround is to not use dialer pools. [CSCdk46346]
- The length field in the MAC Management Message Header for the SYNC message is computed incorrectly.

The workaround is to use a modem that has the Broadcom Chip set. Since the SYNC message is a well known size, the Broadcom chip set can read the CMTS Timestamp without looking at the length field. [CSCdk46537]

- When enrolling a certificate with Entrust VPN, you may fail to get CA certificates. This has only happened on the Cisco 2500 routers. Currently there is no workaround. [CSCdk46820]
- When configuring encryption using FastEthernet interfaces, if the crypto map is only applied to the main interface, and the IP address is configured in the subinterface, packets might not be switched. If CEF is enabled, the packets might get dropped. [CSCdk46853]
- The RADIUS implementation for MS-CHAP should comply with the latest specification from Microsoft. [CSCdk48214]

- The POET Output drops at low data rates with two port adapters in the VIP2. The use of a sub-rate POET interface together with a full-rate POET on the same VIP, VIP2 or VIP2-50 causes the full-rate POET to drop outbound packets. This occurs with an externally clocked sub-rate POET. There is no workaround except to move the sub-rate POET or clock the sub-rate POET at 44.726 Mbps. [CSCdk48525]
- Packets larger than 1010 bytes are not transmitted on the BRI interface of a Cisco 7200 router when WFQ is enabled (default queuing).

The workaround is to enable FIFO queuing on the interface. [CSCdk50099]

Novell IPX, XNS, and Apollo Domain

- A customer reports memory allocation failure due to SAP general request storms. [CSCdj88812]
- A Cisco 2500 router crashes when an X.25 virtual circuit is opened between the Cisco 2500 router and a Cisco 7500 router. This occurs when the **debug x25 events** command is used in the Cisco 2500 router, and the router is configured for the IPX, XNS, VINES, and DECnet protocols.

The workaround is to disable the debug x25 events command. [CSCdk23276]

TCP/IP Host-Mode Services

- Configuring the **privilege exec level debug ip tcp packet** command causes a Cisco router to crash when the **show running-config** or **write terminal** commands are used. [CSCdk45442]

Wide-Area Networking

- The system is not responding to BECNs correctly when the Frame Relay interface is a channelized interface on a 75xx router. [CSCdj67297]
- When IP Fast-Switch is enabled on a Cisco 1600 router with BRI interfaces, it is possible to cause a router to crash under the following conditions:
 - The ISDN connection is being brought up and down repeatedly;
 - The clear ip cache command is invoked during this period repeatedly, in conjunction with the connection being disconnected. [CSCdj81263]
- Running Frame Relay over ISDN on a Cisco 3640 router initially worked, but started to fail when the interface input queue became full and all incoming packets were dropped. The interface input queue wedge problem cannot be resolved by a lock or unlock, but needs to have the router reloaded. [CSCdj82342]
- The **show CMNS** command is no longer available. [CSCdk22864]
- A Cisco 3640 router rejects incoming calls even though there are free channels and available modems. Both ISDN and analog incoming calls are rejected with the message "Incoming call rejected, exceeded max calls." [CSCdk42780]
- The AAA software has a memory leak. This occurs when AAA, RADIUS, and TACACS+ are configured.

A workaround is to configure the **aaa accounting update periodic x** command at startup time. Set x to a large number to avoid lots of periodic update accounting records. [CSCdk43196]

- The **multilink max-links** command does not work for L2F projected interfaces. This also applies for AAA user profiles which use the **max-links** TACACS+ attribute or Port-Limit and Ascend-Maximum-Channels RADIUS attributes. [CSCdk45216]

- A Cisco router may crash when running VPDN L2F sessions over ISDN with the following stackdump:

```
Enter hex value: 221B763A 22093530 2206C92C FFFFFFFF
0x221B763A: _getbuffer (0x22052d90+0x16487a)+0x30
0x22093530: _L2D_Srq_Task (0x22052d90+0x4049e)+0x302
0x2206C92C: _TaskBegin (0x22052d90+0x19b86)+0x16
0xFFFFFFFF: _etext (0x22052d90+0xa1ae78)+0xdd5923f7 Enter hex value: 221B763A 22093530
2206C92C FFFFFFFF 0x221B763A: _getbuffer (0x22052d90+0x16487a)+0x30
0x22093530: _L2D_Srq_Task (0x22052d90+0x4049e)+0x302
0x2206C92C: _TaskBegin (0x22052d90+0x19b86)+0x16
0xFFFFFFFF: _etext (0x22052d90+0xa1ae78)+0xdd5923f7
```

[CSCdk46784]

- An attempt to switch an incoming call when all outgoing channels are in use causes a memory leak. [CSCdk47523]
- It is not possible to send a break signal to a device connected to the asynchronous port on a Cisco 2511 router through a PAD connection. [CSCdk48335]

Resolved Caveats - Release 12.0(1)

Since Release 12.0(1) is the first maintenance release of Cisco IOS software release 12.0, there is no history of resolved caveats. The next maintenance release of Cisco IOS 12.0(2) will provide a list of resolved caveats.

Related Documentation

This section describes the documentation available for the Cisco AS5000. 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 up-to-date 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. For information on CCO, refer to the "Cisco Connection Online" section later in this document. For more information on to the CD-ROM, refer to the "Documentation CD-ROM" section later in this document.

Release-Specific Documents

Use these release notes with:

- *Release Notes for Cisco IOS Release 12.0(1)* that contain some feature and caveat information applicable to Cisco IOS Release 11.3(6)T, located on Cisco Connection Online (CCO) and the Documentation CD-ROM.
- Product bulletins; the path from Cisco Connection Online follows:
Products and Ordering: More Information: Product Bulletins. Scroll to **Software**. Under **Cisco IOS 12.0**, click the **Upgrade Paths** bulletin. The *Upgrade Paths and Packaging Simplification* bulletin appears.

Feature Modules

The documentation for new Release 12.0(1) features is available online only. This new feature documentation includes configuration tasks and new and changed command reference pages that supplement the Cisco IOS Release 11.3 configuration guide and command reference publications.

Cisco IOS Release 11.3 documentation and Release 11.3 AA feature documentation can be found on CCO and the Documentation CD-ROM:

- On Cisco Connection Online (CCO), <http://www.cisco.com/>, the path is **Products and Ordering: Documentation: Cisco Documentation: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0 New Features**. For more information, refer to “Cisco Connection Online,” page 29.
- On the Documentation CD, the path is **Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0**. For more information, refer to “Documentation CD-ROM,” page 30.

Platform Documents

The Cisco AS5800 universal access server is comprised of the Cisco 5814 dial shelf, the Cisco 7206 router shelf, and an optional AC power supply. To help you manage multiple systems, the Cisco 3640 system controller network management system is available to provide local data gathering and monitoring functions for multiple hardware platforms within a single point of presence (POP).

The Cisco 3640 system controller facilitates the management of AS5800 systems by performing automated monitoring and data collection. The Cisco 3640 has 220 MB of non-volatile storage for the temporary storage of log files, images, and MIB statistics. Because it is based upon the Cisco 3640 modular access router, the Cisco 3640 also provides connectivity and routing for an out-of-band management network while it is performing network management functions.

The Cisco AS5800 universal access server and the Cisco 3640 system controller network management system are available to help you manage your dial POP site efficiently and effectively. Each of these products is supported by documentation listed in Table 1.

Cisco Product	Document Title
Cisco AS5800 universal access server	<ul style="list-style-type: none"> • Cisco AS5800 Universal Access Server Hardware Installation and Configuration Guide • Cisco AS5800 Universal Access Server Regulatory Compliance and Safety Information • Configuration notes, updates, feature modules, and release notes
Cisco 7206 router shelf	<ul style="list-style-type: none"> • Cisco 7206 Installation and Configuration Guide • Regulatory Compliance and Safety Information for the Cisco 7206 • Configuration notes, updates, feature modules, and release notes
Cisco 3640 system controller	<ul style="list-style-type: none"> • Cisco 3640 Router Installation and Configuration Guide • Cisco 3640 System Controller Installation and Configuration Guide • Regulatory Compliance and Safety Information for the Cisco 3640 • Configuration notes, updates, feature modules, and release notes

Cisco Product	Document Title
Cisco IOS software	<ul style="list-style-type: none"> • Configuration guides • Command references • Feature modules, configuration notes, updates, and release notes
Cisco marketing tools	<ul style="list-style-type: none"> • <i>Cisco Information Packet</i> • Cisco Product Catalog • Cisco Product Bulletin 738

This documentation can be found on CCO and the Documentation CD-ROM:

- On Cisco Connection Online (CCO), <http://www.cisco.com/>, the path is **Software & Support: Cisco Documentation: Access Servers and Access Routers: Access Servers: Cisco AS5800**. For more information, refer to “Cisco Connection Online,” page 29.
- On the Documentation CD, the path is **Access Servers and Access Routers: Access Servers: Cisco AS5800**. For more information, refer to “Documentation CD-ROM,” page 30.

Cisco IOS Software Documentation

The following are some of the Cisco IOS Release document types that are available in electronic form, printed form, or both forms:

- Configuration guides and command references (electronic and printed)
- Feature modules (electronic)
- Product-specific release notes (electronic and printed)
- Cisco IOS software caveats (electronic and printed)

Table 6 lists the Cisco IOS software documentation set that contains Cisco IOS configuration guides, command references, and several supporting documents. The document set is available in electronic form, and is also available in printed form if you special order it.

Note The most current Cisco IOS documentation can be found on the Web and the latest Documentation CD-ROM. These electronic documents contain updates and modifications made after the paper documents were printed. See the section “Online Navigation for Software Documentation,” page 25 for more details.

Online Navigation for Software Documentation

You can access the Cisco IOS software electronic documents from Cisco Connection Online (CCO) on the Web and the Cisco Documentation CD-ROM:

- On CCO, click **Software & Support**, scroll down and click **Cisco Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0**.
- On the Documentation CD-ROM, click **Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0**.

The following are some of the types of Cisco IOS Release 12.0 documents available:

- Configuration guides and command references
- Feature descriptions

- Product-specific release notes
- Cisco IOS software caveats

For Product Bulletins on CCO, the path is as follows from Cisco Connection Online: **Products and Ordering: More Information: Product Bulletins**. In the Software area, under Cisco IOS 12.0, click **Cisco IOS Software Release 12.0 Upgrade Paths**.

- Online hot-linked master indexes for configuration guide and command reference documentation sets.

On CCO or the Documentation CD-ROM, go to Cisco IOS Release 12.0 and click *Cisco IOS Release 12.0 Configuration Guides: Command References*. Then click *Configuration Guide Master Index* or *Command Reference Master Index*. To access documentation related to an index entry, click on the page number following the entry.

- Online hot-linked list of features that are new since Release 11.2.

On CCO or the Documentation CD-ROM, go to Cisco IOS Release 11.3 and click *Cisco IOS Release 11.3 Configuration Guides: Command References*. Next, click **Cisco IOS 11.3 New Features**. To access configuration documentation for a feature, do one of the following:

- Click on the page number following the feature name. This takes you to the location where the feature is documented.
- Using your browser search function, search one or more keywords from the feature name. This brings the feature documentation to your screen.

For additional information about the CCO and Documentation CD-ROM, refer to the sections “Cisco Connection Online” and “Documentation CD-ROM” at the end of these release notes.

Documentation Modules

Each module 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. Each configuration guide can be used in conjunction with its corresponding command reference.

Note Due to a production problem, many source-route bridging commands were omitted from the printed version of the Cisco IOS Software Command Summary (part number 78-4746-01). For complete documentation of all source-route bridging commands, refer to the *Bridging and IBM Networking Command Reference* (part number 78-4743-01). You can also obtain the most current documentation on the Documentation CD-ROM or Cisco Connection Online (CCO).

Master Indexes

Two master indexes provide indexing information for the Cisco IOS software documentation set: an index for the configuration guides and an index for the command references. In addition, individual books contain a book-specific index.

The Cisco IOS documentation set consists of the following books and chapter topics:

Books	Chapter Topics
<ul style="list-style-type: none"> • Configuration Fundamentals Configuration Guide • Configuration Fundamentals Command Reference 	<ul style="list-style-type: none"> Configuration Fundamentals Overview Cisco IOS User Interfaces File Management Interface Configuration System Management
<ul style="list-style-type: none"> • Network Protocols Configuration Guide, Part 1 • Network Protocols Command Reference, Part 1 	<ul style="list-style-type: none"> IP Addressing IP Services IP Routing Protocols
<ul style="list-style-type: none"> • Network Protocols Configuration Guide, Part 2 • Network Protocols Command Reference, Part 2 	<ul style="list-style-type: none"> AppleTalk Novell IPX
<ul style="list-style-type: none"> • Network Protocols Configuration Guide, Part 3 • Network Protocols Command Reference, Part 3 	<ul style="list-style-type: none"> Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • Wide-Area Networking Configuration Guide • Wide-Area Networking Command Reference 	<ul style="list-style-type: none"> ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • Security Configuration Guide • Security Command Reference 	<ul style="list-style-type: none"> AAA Security Services Security Server Protocols Traffic Filtering Network Data Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options
<ul style="list-style-type: none"> • Dial Solutions Configuration Guide • Dial Solutions Command Reference 	<ul style="list-style-type: none"> 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

Books	Chapter Topics
<ul style="list-style-type: none">• 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
<ul style="list-style-type: none">• 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
<ul style="list-style-type: none">• 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, go to **Software and Support**; click **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.

Software Configuration Tips on the Cisco TAC Home Page

The following URL contains links to access helpful tips on configuring your Cisco products:

http://www.cisco.com/kobayashi/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your web browser to <http://www.cisco.com/>, and follow this path: Software & Support, Technical Tips (button on left margin).

“Hot Tips” are popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC FAX-on-demand service. To access FAX-on-demand and receive documents at your FAX machine from the USA, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.

The following sections are provided from the Technical Tips page:

- **Field Notices**—Designed to provide notification of any critical issues regarding Cisco products. These include problem descriptions, safety or security issues, and hardware defects.
- **Hardware**—Technical Tips related to specific hardware platforms.
- **Internetworking Features**—Tips on using and deploying Cisco IOS software features and services.
- **Sample Configurations**—Actual configuration examples complete with topology and annotations.
- **Software Products**—MultiNet & Cisco Suite 100, Network Management, Cisco IOS Software Bulletins, and CiscoPro Configurations.
- **Special Collections**—Other Helpful Documents, Frequently Asked Questions, Security Advisories, References & RFCs, Case Studies, and the CiscoPro Documentation CD-ROM.

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 access 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 access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

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

This document is to be used with the documents described in the section "Related Documentation."

AccessPath, Any to Any, AtmDirector, the CCIE logo, CD-PAC, Centri, the Cisco Capital logo, *CiscoLink*, the Cisco NetWorks logo, the Cisco Powered Network logo, the Cisco Press logo, ClickStart, ControlStream, DAGAZ, Fast Step, FireRunner, IGX, JumpStart, Kernel Proxy, LoopRunner, MGX, Natural Network Viewer, NetRanger, NetSonar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RouteStream, Secure Script, SMARTnet, SpeedRunner, Stratum, StreamView, *The Cell*, TrafficDirector, TransPath, VirtualStream, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn and Empowering the Internet Generation are service marks; and BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, Enterprise/Solver, EtherChannel, FastHub, FastPacket, ForeSight, FragmentFree, IPX, LightStream, MICA, Phase/IP, StrataSphere, StrataView Plus, and SwitchProbe are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners.

Copyright © 1998, Cisco Systems, Inc.
All rights reserved. Printed in USA.
9807R