



Doc. No. 78-4827-03 Rev C0

Release Notes for the Cisco AS5300 for Cisco IOS Release 11.2(9) XA

May 8, 2001

These release notes describe the new features and significant software components for Cisco IOS Release 11.2(9) XA2 for the Cisco AS5300 access server.

Introduction

These release notes discuss the following topics:

- Cisco IOS Release 11.2 Paradigm, page 2
- Cisco AS5300 Access Servers, page 3
- Cisco IOS Documentation, page 4
- Software Features in Release 11.2(9) XA2, page 6
- Cisco IOS Feature Sets for the Cisco AS5300 Access Servers, page 19
- Upgrading Your Cisco IOS Software or Firmware Release, page 24
- Memory Requirements, page 26
- Important Notes, page 27
- Open Caveats for Release 11.2(9), page 27
- Open Caveats for Release 11.2(9) XA2, page 32
- Cisco.com, page 34
- Documentation CD-ROM, page 35

Corporate Headquarters

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

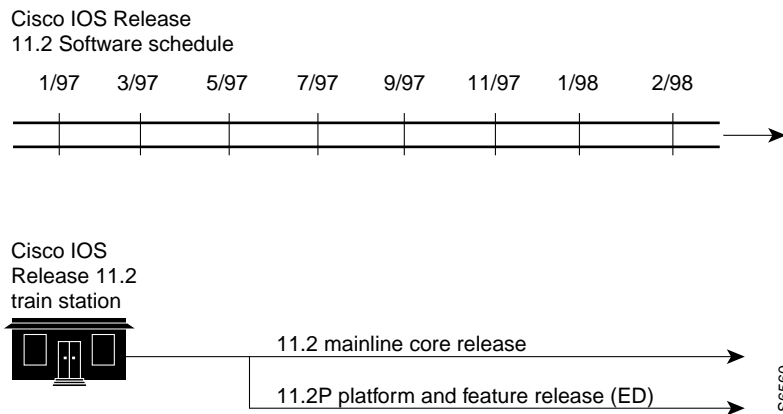
Copyright © 1997–2001
Cisco Systems, Inc.
All rights reserved.

Cisco IOS Release 11.2 Paradigm

Before Cisco IOS Release 11.2, maintenance releases of major Cisco IOS software releases were used to deliver additional new features. Beginning with Cisco IOS Release 11.2, Cisco Systems provides as many as two software release “trains” based on a single version of Cisco IOS software. Similar to a train rolling down the track and picking up passengers, after a release of Cisco IOS software is released to customers, it continues to pick up software fixes along the way and is rereleased as maintenance releases. Maintenance releases provide the most stable software for your network, for the features you need. In addition to the major train, there is typically an early deployment (ED) train. The ED train—Release 11.2 P—delivers fixes to software defects and support for new Cisco platforms. Figure 1 shows the Cisco IOS 11.2 and the 11.2 P software releases.

Note The Release 11.2(9) XA2 software is not included in Figure 1.

Figure 1 Cisco IOS Release 11.2 Software Releases



Note The Cisco AS5300 access server runs only Release 11.2(9) XA2 software.

To determine which version of Cisco IOS software is running on your Cisco AS5300 series access server, log on to the server and enter the **show version** User EXEC command:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 5300 Software (C5300-JS-M), Version 11.2(0.12.0), CISCO DEVELOPMENT TEST VERSION
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Thu 11-Sep-97 08:23 by jng
Image text-base: 0x600088F0, data-base: 0x60792000

ROM: System Bootstrap, Version 11.2(19970311:165032) [rmeadows-easy 116], INTERIM
SOFTWARE
BOOTFLASH: 5300 Software (C5300-BOOT-M), Version 11.2(9), CISCO DEVELOPMENT TEST VERSION

crashsite-t5 uptime is 2 minutes
System restarted by reload
System image file is "flash:c5300-js-mz.0.12.0", booted via flash
```

```

cisco AS5300 (R4K) processor (revision A.14) with 32768K/8192K bytes of memory.
Processor board ID 05433580
R4700 processor, Implementation 33, Revision 1.0 (512KB Level 2 Cache)
Bridging software.
SuperLAT software copyright 1990 by Meridian Technology Corp).
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
TN3270 Emulation software.
Primary Rate ISDN software, Version 1.0.
Backplane revision 2
Manufacture Cookie Info:
  EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x30,
  Board Hardware Version 1.0, Item Number 73-2414-2,
  Board Revision ^@3, Serial Number 05433580,
  PLD/ISP Version 255.255, Invalid Date code.
1 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
96 Serial network interface(s)
96 terminal line(s)
4 Channelized T1/PRI port(s)
128K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash partition 1 (Read/Write)
8192K bytes of processor board System flash partition 2 (Read/Write)
4096K bytes of processor board Boot flash (Read/Write)

Configuration register is 0x2102

```

Cisco AS5300 Access Servers

This section describes the new features for Cisco AS5300 access servers.

Channelized E1 Signaling for the Cisco AS5300

The Cisco AS5300 access server now supports channel associated signaling for channelized E1 lines, which are commonly deployed in networks in Latin America, Asia, and Europe.

After this feature is configured on a single E1 controller, up to 30 remote users can simultaneously dial in to the Cisco AS5300 through networks running the R2 protocol. Typically, all 30 channels of a channelized E1 line are used for analog calls. Because the Cisco AS5300 has four physical E1 ports on its quad E1 Primary Rate Interface (PRI) board, up to 120 simultaneous connections can be made through the quad E1/PRI board.

Robbed Bit Signaling for the Cisco AS5300

New types of signaling provided for a channelized T1 include ground start and loop start support. This new signaling is set using the **cas-group** controller configuration command.

Quad E1 PRI for the Cisco AS5300

This new E1 PRI card has four E1 controllers, which provide physical termination for four E1 PRI lines. Unlike most controller E1 configurations, the Cisco AS5300's E1 PRI controllers require a clock source, which is set with the **clock source** command.

In addition, the quad E1 card can be software-configured for channelized or PRI operation. An additional hardware selector switch is provided for configuration for balanced 75-ohm or unbalanced 120-ohm operation.

Interfaces Supported on Cisco AS5300 Access Servers

The following LAN and WAN interfaces are supported on Cisco AS5300 access servers:

- Ethernet RJ45
- Ethernet/Fast Ethernet (RJ45)
- ISDN PRI
- E1-G.703/G.704
- Channelized T1
- Channelized E1

The following modem cards are supported on the Cisco AS5300 access server:

- MICA modems with speeds up to 33.6K
- Microcom 56K and V.34 modems

Cisco IOS Documentation

For Cisco IOS Release 11.2, the Cisco IOS documentation set consists of eight modules, each module consisting of a configuration guide and a command reference. The documentation set also includes five supporting documents.

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

The books and chapter topics are as follows:

Books	Chapter Topics
<ul style="list-style-type: none">• <i>Configuration Fundamentals Configuration Guide</i>• <i>Configuration Fundamentals Command Reference</i>	Access Server and Router Product Overview User Interface System Images and Configuration Files Using ClickStart, AutoInstall, and Setup Interfaces System Management
<ul style="list-style-type: none">• <i>Security Configuration Guide</i>• <i>Security Command Reference</i>	Network Access Security Terminal Access Security Accounting and Billing Traffic Filters Controlling Router Access Network Data Encryption with Router Authentication

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Access Services Configuration Guide</i> • <i>Access Services Command Reference</i> 	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
<ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> 	ATM Dial-on-Demand Routing (DDR) Frame Relay ISDN LANE PPP for Wide-Area Networking SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 1</i> • <i>Network Protocols Command Reference, Part 1</i> 	IP IP Routing
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 2</i> • <i>Network Protocols Command Reference, Part 2</i> 	AppleTalk Novell IPX
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 3</i> • <i>Network Protocols Command Reference, Part 3</i> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS

Books	Chapter Topics
<ul style="list-style-type: none">• <i>Bridging and IBM Networking Configuration Guide</i>• <i>Bridging and IBM Networking Command Reference</i>	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
<ul style="list-style-type: none">• <i>Cisco IOS Software Command Summary</i>• <i>Access Services Quick Configuration Guide</i>• <i>System Error Messages</i>• <i>Debug Command Reference</i>• <i>Cisco Management Information Base (MIB) User Quick Reference</i>• <i>New and Changed IOS Commands for Cisco AS5300 Access Servers</i>	

All the documents mentioned are available as printed manuals or electronic documents.

For electronic documentation of Cisco IOS Release 11.2 router and access server software features, refer to the Cisco IOS Release 11.2 configuration guides and command references, which are located in the Cisco IOS Release 11.2 database, on the Documentation CD-ROM.

You can also access Cisco technical documentation on the World Wide Web at <http://www.cisco.com>.

Software Features in Release 11.2(9) XA2

The features described in this section are supported in all Cisco IOS Release 11.2 images or feature sets. This section is divided into the following subjects:

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

Routing Protocols

This section describes routing protocol features that are new in the initial release of Cisco IOS Release 11.2.

IP Protocol and Feature Enhancements

The following new IP protocol software features are available:

- **On Demand Routing**—On Demand Routing (ODR) is a mechanism that provides minimum-overhead IP routing for stub sites. The overhead of a general dynamic routing protocol is avoided, without incurring the configuration and management overhead of using static routing.

A stub router is the peripheral router in a hub-and-spoke network topology. Stub routers commonly have a WAN connection to the hub router and a small number of LAN network segments (stub networks) that are connected directly to the stub router. To provide full connectivity, the hub routers can be statically configured to know that a particular stub network is reachable via a specified access router. However, if there are multiple hub routers, many stub networks, or asynchronous connections between hubs and spokes, the overhead required to statically configure knowledge of the stub networks on the hub routers becomes too great.

ODR simplifies installation of IP stub networks in which the hub routers dynamically maintain routes to the stub networks. This is accomplished without requiring the configuration of an IP routing protocol at the stub routers. With ODR, the stub advertises IP prefixes corresponding to the IP networks that are configured on its directly connected interfaces. Because ODR advertises IP prefixes, rather than IP network numbers, ODR is able to carry Variable Length Subnet Mask (VLSM) information.

After ODR is enabled on a hub router, the router begins installing stub network routes in the IP forwarding table. The hub router can also be configured to redistribute these routes into any configured dynamic IP routing protocols. IP does not need to be configured on the stub router. With ODR, a router is automatically considered to be a stub when no IP routing protocols have been configured on it.

The routing protocol that ODR generates is propagated between routers using Cisco Discovery Protocol (CDP). Thus, ODR is partially controlled by the configuration of CDP:

- If CDP is disabled, the propagation of ODR routing information will stop.
- By default, CDP sends updates every 60 seconds. This update interval might not be frequent enough to provide fast reconvergence of IP routers on the hub router side of the network. A faster reconvergence rate might be necessary if the stub connects to several hub routers via asynchronous interfaces (such as modem lines).
- ODR might not work well with dial-on-demand routing (DDR) interfaces, because CDP packets will not cause a DDR connection to be made.

We recommend that IP filtering be used to limit the network prefixes that the hub router will permit to be learned dynamically through ODR. If the interface has multiple logical IP networks configured (via the IP secondary command), only the primary IP network is advertised through ODR.

Open Shortest Path First Enhancements

The following features have been added to Cisco's Open Shortest Path First (OSPF) software:

- **OSPF On-Demand Circuit**—OSPF On-Demand Circuit is an enhancement to the OSPF protocol, as described in RFC 1793, that allows efficient operation over demand circuits such as ISDN, X.25 Switched Virtual Circuits (SVCs), and dialup lines. Previously, the period nature of OSPF

routing traffic mandated that the underlying data-link connection needed to be open constantly, resulting in unwanted usage charges. With this feature, OSPF Hellos and the refresh of OSPF routing information is suppressed for on-demand circuits (and reachability is presumed), allowing the underlying data-link connections to be closed when not carrying application traffic.

The feature allows the consolidation on a single routing protocol and the benefits of the OSPF routing protocol across the entire network, without incurring excess connection costs.

If the router is part of a point-to-point topology, only one end of the demand circuit needs to be configured for OSPF On-Demand Circuit operation. In point-to-multipoint topologies, all appropriate routers must be configured with OSPF On-Demand Circuit. All routers in an area must support this feature—that is, be running Cisco IOS Software Release 11.2 or greater.

- **OSPF Not-So-Stubby Areas (NSSAs)**—As part of the OSPF protocol's support for scalable, hierarchical routing, peripheral portions of the network can be defined as "stub" areas, so that they do not receive and process external OSPF advertisements. Stub areas are generally defined for low end routers with limited memory and CPU, that have low-speed connections, and are in a default route configuration.

OSPF NSSAs defines a more flexible, hybrid method, whereby stub areas can import external OSPF routes in a limited fashion, so that OSPF can be extended across the stub-to-backbone connection.

NSSA enables OSPF to be extended across a stub-to-backbone connection to become logically part of the same network.

Border Gateway Protocol version 4 (BGP4) Enhancements

The following features have been added to Cisco's BGP4 software:

- **BGP4 Soft Configuration**—BGP4 soft configuration allows BGP4 policies to be configured and activated without clearing the BGP session (without invalidating the forwarding cache). This enables policy reconfiguration without causing short-term interruptions to traffic being forwarded in the network.
- **BGP4 Multipath Support**— BGP4 Multipath Support provides BGP load balancing between multiple Exterior BGP (EBGP) sessions. If there are multiple EBGP sessions between the local autonomous system and the neighboring autonomous system, multipath support allows BGP to load balance among these sessions. Depending on the switching mode, per packet or per destination load balancing is performed. BGP4 Multipath Support can support up to six paths.
- **BGP4 Prefix Filtering with Inbound Route Maps**—This feature allows prefix-based matching support to the inbound neighbor route map. This feature allows an inbound route map to be used to enforce prefix-based policies.

Network Address Translation

Network Address Translation (NAT) provides a mechanism for a privately addressed network to access registered networks, such as the Internet, without requiring a registered subnet address. This eliminates the need for host renumbering and allows the same IP address range to be used in multiple intranets.

With NAT, the privately addressed network (designated as "inside") continues to use its existing private or obsolete addresses. These addresses are converted into legal addresses before packets are forwarded onto the registered network (designated as "outside"). The translation function is compatible with standard routing; the feature is required only on the router connecting the inside network to the outside domain.

Translations can be static or dynamic in nature. A static address translation establishes a one-to-one mapping between the inside network and the outside domain. Dynamic address translations are defined by describing the local addresses to be translated and the pool of addresses from which to allocate outside addresses. Allocation is done in numeric order and multiple pools of contiguous address blocks can be defined.

NAT offers these advantages:

- Eliminates readdressing overhead. NAT eliminates the need to readdress all hosts that require external access, saving time and money.
- Conserves addresses through application port-level multiplexing. With NAT, internal hosts can share a single registered IP address for all external communications. In this type of configuration, relatively few external addresses are required to support many internal hosts, thus conserving IP addresses.
- Protects network security. Because private networks do not advertise their addresses or internal topology, they remain reasonably secure when used in conjunction with NAT to gain controlled external access.

Because the addressing scheme on the inside network may conflict with registered addresses already assigned within the Internet, NAT can support a separate address pool for overlapping networks and translate as appropriate.

Applications that use raw IP addresses as a part of their protocol exchanges are incompatible with NAT. Typically, these are less common applications that do not use fully qualified domain names.

Named IP Access Control List

The named IP Access Control List (ACL) feature gives network managers the option of using names for their access control lists. Named IP ACLs function the same as to their numbered counterparts, except that they use names instead of numbers.

This feature also includes a new configuration mode, which supports addition and deletion of single lines in a multiline access control list.

This feature eliminates some of the confusion associated with maintaining long access control lists. Meaningful names can be assigned, making it easier to remember which service is controlled by which access control list. Moreover, this feature removes the limit of 100 extended and 99 standard access control lists, so that additional IP access control lists can be configured.

The new configuration feature allows a network manager to edit access control lists, rather than recreating the entire list.

Currently, only packet and route filters can use named IP ACLs. Also, named IP ACLs are not backward-compatible with earlier releases of Cisco IOS software.

Named IP ACLs are not currently supported with Distributed Fast Switching.

Multimedia and Quality of Service

The following features have been added to Cisco's multimedia and quality of service software:

- Resource Reservation Protocol—Resource Reservation Protocol (RSVP) enables applications to dynamically reserve necessary network resources from end-to-end for different classes of service. An application, which acts as a receiver for a traffic stream, initiates a request for reservation of resources (bandwidth) from the network, based on the application's required quality of service. The first RSVP-enabled router that receives the request informs the requesting host whether the requested resources are available or not. The request is forwarded to the next

router, toward the sender of the traffic stream. If the reservations are successful, an end-to-end pipeline of resources is available for the application to obtain the required quality of service. RSVP enables applications with real-time traffic needs, such as multimedia applications, to coexist with bursty applications on the same network. RSVP works with both unicast and multicast applications.

RSVP requires both a network implementation and a client implementation. Applications need to be RSVP-enabled to take advantage of RSVP functionality. Currently, Precept provides an implementation of RSVP for Windows-based PCs. Companies such as Sun and Silicon Graphics have demonstrated RSVP on their platforms. Several application developers are planning to take advantage of RSVP in their applications.

- **Random Early Detection**—Random Early Detection (RED) helps eliminate network congestion during peak traffic loads. RED uses the characteristics of a robust transmission control protocol (TCP) to reduce transmission volume at the source when traffic volume threatens to overload a router's buffer resources. RED is designed to relieve congestion on TCP/IP networks.

RED is enabled on a per-interface basis. It “throttles back” lower-priority traffic first, allowing higher-priority traffic (as designated by an RSVP reservation or the IP precedence value) to continue unabated.

RED works with RSVP to maintain end-to-end quality of service during peak traffic loads. Congestion is avoided by selectively dropping traffic during peak load periods. This is performed in a manner designed to damp out waves of sessions going through TCP slow start.

Existing networks can be upgraded to better handle RSVP and priority traffic. Additionally, RED can be used in existing networks to manage congestion more effectively on higher-speed links where fair queuing is expensive.

Exercise caution when enabling RED on interfaces that support multiprotocol traffic (in addition to TCP/IP), such as IPX or AppleTalk. RED is not designed for use with these protocols and could have deleterious effects.

RED is a queuing technique; it cannot be used on the same interface as other queuing techniques, such as Standard Queuing, Custom Queuing, Priority Queuing, or Fair Queuing.

- **Generic Traffic Shaping**—Generic Traffic Shaping (also called Interface Independent Traffic Shaping) helps reduce the flow of outbound traffic from a router interface into a backbone transport network when congestion is detected in the downstream portions of the backbone transport network or in a downstream router. Unlike the Traffic Shaping over Frame Relay features which are specifically designed to work on interfaces to Frame Relay networks, Generic Traffic Shaping works on interfaces to a variety of Layer 2 data-link technologies (including Frame Relay, SMDS, Ethernet, etc.)

Topologies that have high-speed links feeding into lower-speed links—such as a central site to a remote or branch sites—often experience bottlenecks at the remote end because of the speed mismatch. Generic Traffic Shaping helps eliminate the bottleneck situation by throttling back traffic volume at the source end.

Routers can be configured to transmit at a lower bit rate than the interface bit rate. Service providers or large enterprises can use the feature to partition, for example, T1 or T3 links into smaller channels to match service ordered by customers.

Generic Traffic Shaping implements a weighted fair queuing on an interface or subinterface to allow the desired level of traffic flow. The feature consumes router memory and CPU resources, so it must be used judiciously to regulate critical traffic flows while not degrading overall router performance.

Multiprotocol Routing

The following enhancement has been made to Cisco's multiprotocol routing:

- **Enhanced IGRP Optimizations**—With the wide-scale deployment of Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) in increasingly large and complex customer networks, Cisco has been able to continuously monitor and refine Enhanced IGRP operation, integrating several key optimizations. Optimizations have been made in the allocation of bandwidth, use of processor and memory resources, and mechanisms for maintaining information about peer routers, as described below.
 - **Intelligent Bandwidth Control**—In network congestion scenarios, packet loss, especially the dropping of routing protocol messages, adversely affects convergence time and overall stability. To prevent this problem, Enhanced IGRP now takes into consideration the available bandwidth (at a granularity of per subinterface/virtual circuit if appropriate) when determining the rate at which it will transmit updates. Interfaces can also be configured to use a certain (maximum) percentage of the bandwidth, so that even during routing topology computations, a defined portion of the link capacity remains available for data traffic.
 - **Improved Processor and Memory Utilization**—Enhanced IGRP derives the distributed routing tables from topology databases that are exchanged between peer routers. This CPU computation has now been made significantly more efficient as has the protocol's queuing algorithm, resulting in improved memory utilization. The combination of these factors further increases Enhanced IGRP's suitability for deployment, particularly on low-end routers.
 - **Implicit Protocol Acknowledgments**—Enhanced IGRP running within a router maintains state and reachability information about other neighboring routers. This mechanism has been modified so that it no longer requires explicit notifications to be exchanged but rather will accept any traffic originating from a peer as a valid indication that the router is operational. This provides greater resilience under extreme load.
 - **IPX Service Advertisement Interleaving**—Large IPX environments are typically characterized by many Service Advertisements, which can saturate lower-speed links at the expense of routing protocol messages. Enhanced IGRP now employs an interleaving technique to ensure that both traffic types receive sufficient bandwidth in large IPX networks.

These enhancements are particularly applicable in networking environments having many low-speed links (typically in hub-and-spoke topologies); in Non-Broadcast-Multiple-Access (NBMA) wide-area networks such as Frame Relay, ATM, or X.25 backbones; and in highly redundant, dense router-to-router peering configurations. It should be noted that the basic Enhanced IGRP routing algorithm that exhibits very fast convergence and guaranteed loop-free paths has not changed, so there are no backward compatibility issues with earlier versions of Cisco IOS software.

Switching Features

The following feature has been added to Cisco's switching software:

- **Integrated Routing and Bridging**—Integrated routing and bridging (IRB) delivers the functionality to extend VLANs and Layer 2 bridged domains across the groups of interfaces on Cisco IOS software-based routers and interconnect them to the routed domains within the same router.

The ability to route and bridge the same protocol on multiple independent sets of interfaces of the same Cisco IOS software-based router makes it possible to route between these routed and bridged domains within that router. IRB provides a scalable mechanism for integration of Layer 2 and Layer 3 domains within the same device.

Integrated routing and bridging provides:

- Scalable, efficient integration of Layer 2 and Layer 3 domains—The IRB functionality allows you to extend the bridge domains or VLANs across routers while maintaining the ability to interconnect them to the routed domains through the same router.
- Layer 3 address conservation—You can extend the bridge domains and the VLAN environments across the routers to conserve the Layer 3 address space and still use the same router to interconnect the VLANs and bridged domains to the routed domain.
- Flexible network reconfiguration—Network administrators gain the flexibility of being able to extend the bridge domain across the router's interfaces to provide temporary solution for moves, adds, and changes. This can be useful during migration from a bridged environment to a routed environment, or when making address changes on a scheduled basis.

Note that:

- IRB currently supports three protocols: IP, IPX, and AppleTalk, in both fast switching and process switching modes.
- IRB is not supported on ciscoBus bus platforms (the AGS+ and Cisco 7000 series).
- IRB is supported for transparent bridging, but not for source-route bridging.
- IRB is supported on all media-type interfaces except X.25 and ISDN bridged interfaces.
- IRB and concurrent routing and bridging (CRB) cannot operate at the same time.

Desktop Protocols

This section describes the desktop protocol features that are new in the initial release of Cisco IOS Release 11.2.

AppleTalk Features

The following feature has been added to Cisco's AppleTalk software:

- AppleTalk Load Balancing—This feature allows AppleTalk data traffic to be distributed more evenly across redundant links in a network.

AppleTalk load balancing can reduce network costs by allowing more efficient use of network resources. Network reliability is improved because the chance that network paths between nodes will become overloaded is reduced. For convenience, load balancing is provided for networks using native AppleTalk routing protocols such as Routing Table Maintenance Protocol (RTMP) and Enhanced IGRP.

AppleTalk load balancing operates with process and fast switching.

Novell Features

The following features have been added to Cisco's Novell software:

- **Display by Service Advertisement Protocol Name**—This feature allows network managers to display Service Advertisement Protocol (SAP) entries that match a particular server name or other specific value. The current command that displays IPX servers has been extended to allow the use of any regular expression (including supported special characters) for matching against the router's SAP table.
- **IPX Access Control List Violation Logging**—With this feature, routers can use existing router logging facilities to log IPX access control list (ACL) violations whenever a packet matches a particular access-list entry. The first packet to match an entry is logged immediately; updates are sent at intervals of approximately five minutes.

This feature allows logging of:

- Source and destination addresses
- Source and destination socket numbers
- Protocol (or packet) type (for example, IPX, SPX, or NCP)
- Action taken (permit/deny)

Matching packets and logging-enabled ACLs are sent at the process level. Router logging facilities use the IP protocol.

- **Plain English IPX Access List**—Through the use of this feature, the most common protocol and socket numbers used in IPX extended ACLs can be specified by either name or number instead of numbers, as required previously.

Protocol types supported include RIP, SAP, NCP, and NetBIOS. Supported socket types include Novell Diagnostics Packet Enhanced IGRP, and NLSP.

Plain English IPX Access Lists greatly reduce the complexity and increase the readability of IPX extended access control lists, reducing network management expense by making it easier to build and analyze the access control mechanisms used in IPX networks.

Wide-Area Networking Features

This section describes the wide-area networking features that are new in the initial release of Cisco IOS Release 11.2.

ISDN/DDR Enhancements

The following features have been added to Cisco's ISDN and DDR software:

- **Multichassis Multilink PPP**—Multichassis Multilink Point-to-Point Protocol (MMP) extends Multilink PPP (MLP) by providing a mechanism to aggregate B-channels transparently across multiple routers or access servers. MMP defines the methodology for sharing individual links in an MLP bundle across multiple, independent platforms. The primary application for MMP is the ISDN dialup pool; however, it can also be used in a mixed technology environment.

MMP is based on the concept of a *stackgroup*—a group of routers or access servers that operate as a group when receiving MLP calls. Any member of the stackgroup can answer any call into the single access number applied to all WAN interfaces. Typically, the access number corresponds to a telco hunt group.

Cross-platform aggregation is performed via tunneling between members of a stackgroup using the Level 2 Forwarding (L2F) protocol, a draft Internet Engineering Task Force (IETF) standard.

MMP is flexible and scalable. Because the L2F protocol is IP-based, members of a stackgroup can be connected over many types of LAN or WAN media. Stackgroup size can be increased by increasing the bandwidth available to the L2F protocol—for example, by moving from shared to switched Ethernet.

With Multichassis Multilink PPP:

- New devices can be added to the dialup pool at any time.
- The load for reassembly and resequencing can be shared across all devices in the stackgroup. MMP is less CPU-intensive than MLP.
- MMP provides an interoperable multivendor solution because it does not require any special software capabilities at the remote sites. The only remote requirement is support for industry standard MLP (RFC 1717).

Note This feature is documented in the PPP for wide-area networking chapters of the *Wide-Area Networking Configuration Guide* and the *Wide-Area Networking Command Reference*.

- Virtual Private Dialup Network— Virtual Private Dialup Network (VPDN) allows users from multiple disparate domains to gain secure access to their corporate home gateways via public networks or the Internet. This functionality is based on the Layer 2 Forwarding (L2F) specification which Cisco has proposed as an industry standard to the IETF.

Service providers who wish to offer private dial-up network services can use VPDN to provide a single telephone number for all their client organizations. A customer can use dial-up access to a local point of presence where the access server identifies the customer by PPP user name. The PPP username is also used to establish a home gateway destination. Once the home gateway is identified, the access server builds a secure tunnel across the service provider's backbone to the customer's home gateway. The PPP session is also transported to this home gateway, where local security measures can ensure the person is allowed access to the network behind the home gateway.

Of special interest to service providers is VPDN's independence of WAN technology. Since L2F is TCP/IP-based, it can be used over any type of service provider backbone network.

Note This feature is documented in the PPP for wide-area networking chapters of the *Wide-Area Networking Configuration Guide* and the *Wide-Area Networking Command Reference*.

- Dialer Profiles—Dialer profiles allow the user to separate the network layer, encapsulation, and dialer parameters portion of the configuration from that of the interface used to place or receive calls.

Dialer profile extends the flexibility of current dial-up configurations. For example, on a single ISDN PRI or PRI rotary group, it is now possible to allocate separate profiles for different classes of user. These profiles may define normal DDR usage or backup usage.

Each dialer profile uses an Interface Descriptor Block (IDB) distinct from the IDB of the physical interface used to place or receive calls. When a call is established, both IDBs are bound together so that traffic can flow. As a result, dialer profiles use more IDBs than normal DDR.

This initial release of dialer profiles does not support Frame Relay, X.25, or LAPB encapsulation on DDR links or Snapshot Routing capabilities.

- **Combinet Packet Protocol Support**—Combinet Packet Protocol (CPP) is a proprietary encapsulation used by legacy Combinet products for data transport. CPP also defines a methodology for performing compression and load sharing across ISDN links. The Cisco IOS software implementation of CPP supports both compression and load sharing using this proprietary encapsulation.

A large installed base of early Combinet product users cannot upgrade to later software releases that support interoperability standards such as PPP. With CPP support, these users can integrate their existing product base into new Cisco IOS-based internetworks.

CPP does not provide many of the functions available in Cisco's implementation of the PPP standards. These functions include address negotiation and support for protocols like AppleTalk. Where possible, Cisco recommends that customers migrate to software that supports PPP.

- **Half Bridge/Half Router for CPP and PPP**—Half bridge/half router allows low-end, simply configured bridge devices to bridge either PPP or CPP encapsulated data to a Cisco IOS core network router. Half bridge/half router is designed for networks that have small remote Ethernet segments, each with a single PPP- or CPP-compatible bridging device connected to a core network. The serial or ISDN interface on the core network router appears as a virtual Ethernet port to the network. Layer 3 data packets transported across this type of link are first encapsulated within an Ethernet encapsulation. A PPP or CPP bridging header is then added. This facility allows bridged traffic arriving at the core device to be routed from that point on. This feature is process switched.

IBM Functionality

This section describes the IBM network software features and support that are new in the initial release of Cisco IOS Release 11.2.

New Features

The following new IBM software features are available:

- **Native Client Interface Architecture Server**—The Native Client Interface Architecture (NCIA) server, introduced by Cisco Systems for access of IBM SNA applications over routed internetworks, has been enhanced to be more flexible and scalable. The NCIA Client, implemented in the client workstation, encapsulates the full SNA stack inside TCP/IP packets. These packets are sent to the NCIA Server implemented in Cisco IOS software. The NCIA Server de-encapsulates the TCP/IP packet and sends the LLC data to the host processor via RSRB or DLSw+.

The NCIA Server supports SNA and NetBIOS sessions over a variety of LAN and WAN connections, including dial-up connections. The NCIA architecture supports clients with full SNA stacks—providing all advanced SNA capabilities, unlike some split-stack solutions.

NCIA Server enhancements provide:

- **Simplified client configuration:** It is no longer necessary to predefine ring numbers, and the NCIA Server supports optional dynamic assignment of MAC addresses. There is no Logical Link Control, type 2 (LLC2), at the client. The client is configured as an end station, not a router peer.
- **Scalability:** The limit is based on the number of LLC connections in the central site router rather than RSRB peer connections.

- **Fast Switched Source-Route Translational Bridging (SR/TLB)**—With Cisco IOS Release 11.2, SR/TLB is fast switched. No queuing is done and resource utilization is low. This enhancement is on by default, but can be disabled. It is supported across all router platforms.
- **Response Time Reporter**—The Response Time Reporter (RTR) feature allows you to monitor network performance, network resources, and applications by measuring response times and availability. RTR statistics can be used to perform troubleshooting, problem notifications and pre-problem analysis. RTR offers enhanced functionality over a similar IBM product, NetView Performance Monitor.

RTR enables the following functions to be performed:

- Troubleshoot problems by checking the time delays between devices (such as a router and an MVS host) and the time delays on the path from the source device to the destination device at the protocol level.
- Send SNMP traps and/or SNA Alerts/Resolutions when one of the following has occurred: a user-configured threshold is exceeded, a connection is lost and reestablished, or a timeout occurs and clears. Thresholds can also be used to trigger additional collection of time delay statistics.
- Perform pre-problem analysis by scheduling the RTR and collecting the results as history and accumulated statistics. The statistics can be used to model and predict future network topologies.

The RTR feature is currently available only with feature sets that include IBM support. A CiscoWorks Blue network management application will be available to support the RTR feature. Both the CiscoWorks Blue network management application and the router use the Cisco Round Trip Time Monitor (RTTMON) MIB. This MIB is also available with Cisco IOS Release 11.2.

APPN Enhancements

The following features have been added to Cisco's APPN software:

- **APPN Central Resource Registration**—APPN Central Resource Registration (CRR) support allows a Cisco IOS software-based router acting as a network node to register the resources of end nodes to the Central Directory Service (CDS) on Advanced Communication Facility/Virtual Telecommunication Access Method (ACF/VTAM). A Cisco IOS NN will now register resource names with a VTAN CDS as soon as it establishes connectivity with it. Prior to this enhancement, the router acting as a NN could not register end-node resources. ACF/VTAM could, however, query the router to find these resources.

The CDS reduces broadcast traffic in the network. Without an active CDS on ACF/VTAM, the NN must send a broadcast message to the network to locate nonlocal resources required for a session. With an active CDS, the network node sends a single request directly to the CDS for the location of the resource. A network broadcast is used only if the resource has not registered with the CDS.

ACF/VTAM must be configured as a CDS. The Cisco IOS network node learns of the capability when network topology is exchanged. To most effectively use the CDS, end nodes should register the resources with the network node. Depending on the end node implementation, registration might occur automatically, might require configuration on the end node, or may not be a function of the end node.

- **APPN DLUR MIB**—The existing APPN Management Information Base (MIB) does not contain information about Dependent Logical Units (DLUs) accessing the APPN network through the DLU Requester (DLUR) function in the Cisco IOS network node. A standard MIB for DLUR has been defined by the APPN Implementers Workshop (AIW), the standards body for APPN, and is implemented in this release of the Cisco IOS software.

With the APPN DLUR MIB, users have access to information collected about the DLUR function in the Cisco IOS network node and the DLUs attached to it for more complete network management information.

Data Link Switching+ Features and Enhancements

The following features have been added to Cisco's Data Link Switching (DLSw+) software. These features had previously been available with Remote Source-Route Bridging (RSRB). To provide these features for DLSw+, the Cisco IOS software uses a component known as Virtual Data Link Control (VDLC) that allows one software component to use another software component as a data link.

- LAN Network Manager over DLSw+—LAN Network Manager (LNM) over DLSw+ allows DLSw+ to be used in Token Ring networks that are managed via IBM's LNM software.

With this feature, LNM can be used to manage Token Ring LANs, Control Access Units (CAUs), and Token Ring attached devices over a DLSw+ network. All management functions continue to operate as they would in an RSRB network or source-route bridged network.

- Native Service Point over DLSw+—Native Service Point (NSP) over DLSw+ allows Cisco's NSP feature to be used in conjunction with DLSw+ in the same router.

With this feature, NSP can be configured in remote routers, and DLSw+ can provide the path for the remote service point physical unit to communicate with NetView. This allows full management visibility of resources from a NetView 390 console, while concurrently offering the value-added features of DLSw+ in an SNA network.

- Downstream Physical Unit over DLSw+—Downstream physical unit (DSPU) over DLSw+ allows Cisco's DSPU feature to operate in conjunction with DLSw+ in the same router. DLSw+ can be used either upstream (towards the mainframe) or downstream (away from the mainframe) of DSPU.

DSPU concentration consolidates the appearance of up to 255 physical units into a single physical unit appearance to VTAM, minimizing memory and cycles in central site resources (VTAM, NCP, and routers) and speeding network startup. Used in conjunction with DLSw+, network availability and scalability can be maximized.

- Advanced Peer-to-Peer Networking over DLSw+—Advanced Peer-to-Peer Networking (APPN) over DLSw+ allows Cisco's APPN feature to be used in conjunction with DLSw+ in the same router.

With this feature, DLSw+ can be used as a low-cost way to access an APPN backbone or APPN in the data center. In addition, DLSw+ can be used as a transport for APPN, providing nondisruptive recovery from failures and high speed intermediate routing. In this case, the DLSw+ network appears as a connection network to the APPN network nodes.

- Source-Route Bridging (SRB) over FDDI to DLSw+—This feature allows access to DLSw+ over source-route bridged FDDI LANs. In the past, the supported local DLCs were only Token Ring, Ethernet, or SDLC. With this extension, Token Ring-attached devices can access a DLSw+ router using source-route bridging over an FDDI backbone. At the remote site, the device can be attached over Token Ring, Ethernet, SDLC, or FDDI. This feature allows SRB over FDDI to provide the highest speed access among campus resources, while concurrently allowing DLSw+ for access to remote resources.

Security Features

This section describes the security features that are new in the initial release of Cisco IOS Release 11.2.

New Features

- Router Authentication and Network-Layer Encryption—This feature provides a mechanism for secure data transmission. It consists of two components:
 - Router Authentication—Prior to passing encrypted traffic, two routers perform a one-time, two-way authentication by exchanging Digital Signature Standard (DSS) public keys. The hash signatures of these keys are compared to authenticate the routers.
 - Network-Layer Encryption—For IP payload encryption, the routers use Diffie-Hellman key exchange to securely generate a DES 40- or 56-bit session key. New session keys are generated on a configurable basis. Encryption policy is set by *crypto-maps* that use extended IP Access Lists to define which network, subnet, host, or protocol pairs are to be encrypted between routers.

This feature can be used to build multiprotocol virtual private networks (VPNs), using encrypted generic routing encapsulation (GRE) tunnels. It can also be used to deploy secure telecommuting services, Intranet privacy, and virtual collaborative or community-of-interest networks.

All components of this feature are subject to U.S. Department of Commerce export regulations. Encryption is currently IP only, though it does support multiprotocol GRE tunnels. This feature is most appropriately deployed in a relatively small number of routers, with a logically flat or star-shaped encryption topology. Load-sharing of the encryption/decryption function is not supported. Without a Certification Authority (CA), the one-time authentication effort increases exponentially with the number of routers. Router authentication requires the network administrator to compare the hashes produced by the routers, once during initial configuration. This version of encryption is not IPSEC compliant.

- Kerberos V Client Support—This feature provides full support of Kerberos V client authentication, including credential forwarding. Systems with existing Kerberos V infrastructures can use their Key Distribution Centers (KDCs) to authenticate end-users for network or router access. This is a client implementation, not a Kerberos KDC. Kerberos is generally considered a legacy security service and is most beneficial in networks already using Kerberos.

TACACS+ Enhancements

The following features have been added to Cisco's TACACS+ software:

- TACACS+ Single Connection—Single Connection is an enhancement to the network access server that increases the supported number of transactions per second. Prior to this enhancement, separate TCP connections would be opened and closed for each of the TACACS+ services: authentication, authorization, and accounting. This became a bottleneck for improving throughput on authentication services for large networks.

Single Connection is an optimization whereby the network access server maintains a single TCP connection to one or more TACACS+ daemons. The connection is maintained in an open state for as long as possible, instead of being opened and closed each time a session is negotiated. It is expected that Single Connection will yield performance improvements on a suitably constructed daemon.

Currently, only the CiscoSecure daemon V1.0.1 supports Single Connection. The network access server must be explicitly configured to support a Single Connection daemon. Configuring Single Connection for a daemon that does not support this feature will generate errors when TACACS+ is used.

- TACACS+ SENDAUTH Function—SEDAUTH is a TACACS+ protocol change to increase security. SENDAUTH supersedes SENDPASS. SENDAUTH and SENDPASS are documented in Version 1.63 of the TACACS+ protocol specification, which is available from Cisco.com or via anonymous FTP from ftp-eng.cisco.com.

The network access server can support both SENDAUTH and SENDPASS simultaneously. It detects if the daemon is able to support SENDAUTH and, if not, will use SENDPASS instead. This negotiation is virtually transparent to the user, with the exception that the down-rev daemon may log the initial SENDAUTH packet as unrecognized.

SEDAUTH functionality requires support from the daemon, as well as the network access server.

Network Management

This section describes the network management features that are new in the initial release of Cisco IOS Release 11.2.

MIBs Supported

The following MIB support has been added:

- POPM MIB
- Cisco Modem Management MIB
- Cisco SYSLOG MIB

Cisco IOS Feature Sets for the Cisco AS5300 Access Servers

This section lists Cisco IOS software feature sets available in Cisco IOS Release 11.2(9) XA2. These features are available in specific features sets on specific platforms.

Table 1 and Table 2 use these feature set matrix symbols to identify features:

Feature Set Matrix Symbol	Description
Basic	This feature is offered in the basic feature set.
—	This feature is not offered in the feature set.
Plus	This feature is offered in the Plus feature set, not in the basic feature set.
Encrypt	This feature is offered in the encryption feature sets, which consist of 40-bit (Plus 40) or 56-bit (Plus 56) data encryption feature sets.

Cisco IOS images with 40-bit Data Encryption Standard (DES) support may legally be distributed to any party eligible to receive Cisco IOS software. The 40-bit DES is not a cryptographically strong solution and should not be used to protect sensitive data.

Cisco IOS images with 56-bit DES are subject to International Traffic in Arms Regulations (ITAR) controls and have a limited distribution. Images to be installed outside the United States, require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. Contact your sales representative or distributor for more information, or send e-mail to export@cisco.com.

Table 1 and Table 2 list the standard feature sets supported in Release 11.2.

Table 1 Feature Set Matrix for High-End Access Servers

Standard Feature Sets	Cisco AS5300
IP	Basic
IP Plus	Basic
Desktop (IP/IPX/AppleTalk/DEC)	Basic
Desktop (IP/IPX/AppleTalk/DEC) Plus	Basic
Enterprise	Basic
Enterprise Plus	Basic

Table 2 Cisco AS5300 Access Server Software Feature Sets

Features Contained in Features Sets	Feature Set		
	IP Routing	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise ¹
LAN Support			
Apollo Domain	—	—	Basic
AppleTalk 1 and 2 ²	—	Basic	Basic
Banyan VINES	—	—	Basic
Concurrent routing and bridging (CRB)	Basic	Basic	Basic
DECnet IV	—	Basic	Basic
DECnet V	—	—	Basic
GRE	Basic	Basic	Basic
Integrated routing and bridging (IRB) ³	Basic	Basic	Basic
IP	Basic	Basic	Basic
LAN extension host	Basic	Basic	Basic
Multiring	Basic	Basic	Basic
Novell IPX ⁴	—	Basic	Basic
Open System Interconnect (OSI)	—	—	Basic
Source-route bridging (SRB)	—	—	Basic
Transparent and translational bridging	Basic	Basic	Basic
XNS	—	—	Basic

Table 2 Cisco AS5300 Access Server Software Feature Sets (Continued)

Features Contained in Features Sets	Feature Set		
	IP Routing	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise ¹
WAN Services			
Combinet Packet Protocol (CPP)	Basic	Basic	Basic
Dialer profiles	Basic	Basic	Basic
Half bridge/half router for CPP and PPP	Basic	Basic	Basic
HDLC	Basic	Basic	Basic
IPXWAN 2.0	—	Basic	Basic
ISDN ⁵	Basic	Basic	Basic
Multichassis Multilink PPP (MMP) ⁶	—	—	—
PPP ⁷	Basic	Basic	Basic
Virtual Private Dial-up Network (VPDN)	Plus	Plus	Plus
WAN Optimization			
Bandwidth-on-demand	Basic	Basic	Basic
Custom and priority queuing	Basic	Basic	Basic
Dial backup	Basic	Basic	Basic
Dial-on-demand	Basic	Basic	Basic
Header, link and payload compression	Basic	Basic	Basic
Snapshot routing	Basic	Basic	Basic
Weighted fair queuing	Basic	Basic	Basic
IP Routing			
BGP	Basic	Basic	Basic
BGP4 ⁸	Basic	Basic	Basic
EGP	Basic	Basic	Basic
Enhanced IGRP	Basic	Basic	Basic
Enhanced IGRP Optimizations	Basic	Basic	Basic
ES-IS	—	—	Basic
IGRP	Basic	Basic	Basic
IS-IS	—	—	Basic
Named IP Access Control List	Basic	Basic	Basic
Network Address Translation (NAT)	Plus	Plus	Plus
NHRP	Basic	Basic	Basic
On Demand Routing (ODR)	Basic	Basic	Basic
OSPF	Basic	Basic	Basic

Table 2 Cisco AS5300 Access Server Software Feature Sets (Continued)

Features Contained in Features Sets	Feature Set		
	IP Routing	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise ¹
OSPF Not-So-Stubby-Areas (NSSA)	Basic	Basic	Basic
OSPF On Demand Circuit (RFC 1793)	Basic	Basic	Basic
PIM	Basic	Basic	Basic
Policy-based routing	Basic	Basic	Basic
RIP	Basic	Basic	Basic
RIP Version 2	Basic	Basic	Basic
Other Routing			
AURP	—	Basic	Basic
IPX RIP	—	Basic	Basic
NLSP	—	Basic	Basic
RTMP	—	Basic	Basic
SMRP	—	Basic	Basic
S RTP	—	—	Basic
Multimedia and Quality of Service			
Generic traffic shaping	Basic	Basic	Basic
Resource Reservation Protocol (RSVP)	Basic	Basic	Basic
Management			
HTTP Server	Basic	Basic	Basic
Modem Management	Plus	Plus	Plus
RMON events and alarms ⁹	Basic	Basic	Basic
RMON full	Plus	Plus	Plus
SNMP	Basic	Basic	Basic
Telnet	Basic	Basic	Basic
Security			
Access lists	Basic	Basic	Basic
Access security	Basic	Basic	Basic
Extended access lists	Basic	Basic	Basic
Kerberized login	—	—	Basic
Kerberos V client support	—	—	Basic
Lock and key	Basic	Basic	Basic
MAC security for hubs	Basic	Basic	Basic
MD5 routing authentication	Basic	Basic	Basic
RADIUS	Basic	Basic	Basic

Table 2 Cisco AS5300 Access Server Software Feature Sets (Continued)

Features Contained in Features Sets	Feature Set		
	IP Routing	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise ¹
TACACS+ ¹⁰	Basic	Basic	Basic
IBM Support (Optional)			
APPN (optional)	—	—	—
BAN for SNA Frame Relay support	Plus	Plus	Basic
Bisync	Plus	Plus	Basic
Caching and filtering	Plus	Plus	Basic
DLSw+ ¹¹	Plus	Plus	Basic
Downstream PU concentration (DSPU)	Plus	Plus	Basic
Native Client Interface Architecture (NCIA) Server	Plus	Plus	Basic
NetView Native Service Point	Plus	Plus	Basic
QLLC	Plus	Plus	Basic
Response Time Reporter (RTR)	Plus	Plus	Basic
SDLC integration	Plus	Plus	Basic
DLSw (RFC 1795)	Plus	Plus	Basic
SDLC transport (STUN)	Plus	Plus	Basic
SDLC-to-LAN conversion (SDLLC)	Plus	Plus	Basic
SNA and NetBIOS WAN optimization via local acknowledgment	Plus	Plus	Basic
SRB/RSRB ¹²	Plus	Plus	Basic
SRT	Plus	Plus	Basic
TG/COS	—	—	Basic
TN3270	—	—	Basic
Protocol Translation			
LAT	—	—	Basic
Rlogin	—	—	Basic
Remote Node¹³			
ARAP 1.0/2.0	—	Basic	Basic
Asynchronous master interfaces	Basic	Basic	Basic
ATCP	—	Basic	Basic
CHAP	Basic	Basic	Basic
CSLIP	Basic	Basic	Basic
DHCP	Basic	Basic	Basic
IP pooling	Basic	Basic	Basic

Table 2 Cisco AS5300 Access Server Software Feature Sets (Continued)

Features Contained in Features Sets	Feature Set		
	IP Routing	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise ¹
IPX and ARAP on virtual async interfaces	—	—	Basic
IPXCP	—	Basic	Basic
MacIP	—	Basic	Basic
NASI	—	—	—
NetBEUI over PPP	—	—	—
SLIP	Basic	Basic	Basic
Terminal Services¹³			
LAT ¹⁴	—	—	Basic
Rlogin	Basic	Basic	Basic
Telnet	Basic	Basic	Basic
TN3270	—	—	Basic
Xremote	—	—	Basic

1. Enterprise is available with APPN in a separate feature set. APPN includes APPN Central Registration (CRR) and APPN over DLSw+.
2. 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. In Plus images only
7. PPP includes support for LAN protocols supported by the feature set, address negotiation, PAP and CHAP authentication, and PPP compression, and Multilink PPP.
8. BGP4 includes soft configuration, multipath support, and prefix filtering with inbound route maps.
9. The RMON events and alarms groups are supported on all interfaces. Full RMON support is available with the Plus feature sets.
10. TACACS+ Single Connection and TACACS+ SENDAUTH enhancements are supported.
11. Cisco IOS Release 11.2 introduces several DLSw+ enhancements available in the Plus, Plus 40, and Plus 56 feature sets.
12. SRB/RSRB is fast switched. This enhancement is on by default, but can be disabled.
13. Supported on access servers (with limited support on router auxiliary ports).
14. 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).

Upgrading Your Cisco IOS Software or Firmware Release

When you upgrade Cisco IOS software from an earlier release, remember to save your current configuration file before configuring your access server with the newer software. An unrecoverable error could occur during download or configuration

Note For modem firmware release notes, see the Documentation CD. The most current version is available on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

Modem Firmware Update Procedure for the Cisco AS5300 Access Server

To update your modem firmware using the Web, if you have a maintenance contract (SMARTnet), launch Netscape Navigator and go to the following URL:

<http://www.cisco.com/kobayashi/sw-center>

The Software Center window is displayed.

- Step 1** Click **Access Products**. The Access Products window is displayed.
- Step 2** Click **5300 Series Software**. The Cisco 5300 Series Software window is displayed.
- Step 3** To download modem firmware, select **Download Microcom Modem Firmware** or **Download MICA Modem Firmware**. The Cisco 5300 Series Software Images window is displayed.
- Step 4** Click **Execute**. The modem firmware is downloaded to your desktop computer.
- Step 5** Transfer the firmware release to a local TFTP server on your network, using a terminal emulation application, such as TCP Connect.
- Step 6** Log on to your router. Copy the firmware release from your TFTP server to your router using the **copy tftp** command.

Cisco IOS Upgrade Procedure for the Cisco AS5300 Access Server

For instructions on downloading a current Cisco IOS release from the Cisco.com Trivial File Transfer Protocol (TFTP) server, if you have a maintenance contract (SMARTnet), go to the following URL:

<http://www.cisco.com/kobayashi/sw-center>

The Software Center window is displayed.

- Step 1** Click **Cisco IOS Software**. The Cisco IOS Software window is displayed.
- Step 2** Click **Cisco IOS 11.2**. The Cisco 11.2 Software Upgrade Planner window is displayed.
- Step 3** Click **Download Cisco IOS 11.2 Software**. The Software Checklist window is displayed.
- Step 4** Select the appropriate information in each section of the Software Checklist window.
 - Hardware
 - Release
 - Software and hardware release
- Step 5** Click **Execute**. The software release is downloaded to your desktop computer.
- Step 6** Transfer the software release to a local TFTP server on your network.
- Step 7** Log on to your router. Copy the software release from your TFTP server to your router, using the **copy tftp** command.

Note These URLs are subject to change without notice. Refer to Cisco's Technical Assistance Center (TAC) if you have problems locating software.

Memory Requirements

Table 3 describes the memory requirements for the Cisco AS5300 series access server platform's feature set supported by Cisco IOS Release 11.2.

Table 3 Cisco AS5300—Memory Requirements

Feature Set	Required Flash Memory	Required DRAM Memory	Release 11.2 Runs from
IP	8 MB Flash	32 MB DRAM	DRAM
IP/Plus	8 MB Flash	32 MB DRAM	DRAM
Desktop	8 MB Flash	32 MB DRAM	DRAM
Desktop Plus	8 MB Flash	32 MB DRAM	DRAM
Enterprise	8 MB Flash	32 MB DRAM	DRAM
Enterprise Plus	8 MB Flash	32 MB DRAM	DRAM

Important Notes

Deferral of AS5300 Boot Image

The c5300-boot-mz image has been deferred in Cisco IOS Release 11.2(9)XA because of a severe defect. This defect has been assigned Cisco Caveat ID CSCdu10569. The software solution for this defect is the c5300-boot-mz image in Cisco IOS Release 12.0(4)T1.

In order to increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Caution Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Open Caveats for Release 11.2(9)

This section describes possibly unexpected behavior by Cisco IOS Release 11.2(9). Unless otherwise noted, these caveats apply to 11.2(9). The caveats listed here describe only the serious problems. For the complete list of caveats against Cisco IOS Release 11.2, use the Documentation CD-ROM or access Cisco.com as described in the section “Cisco.com” later in this document.

AppleTalk

- When using ARAP 2.1 on routers running Cisco IOS Release 11.2, the client connects, the authentication negotiates, and then the connection drops with a message indicating that the server called is not a valid remote access server. As a workaround, use Cisco IOS Release 11.1, which works with both ARAP 2.0.1 and 2.1. [CSCdi91670]
- When using the ARAP client 2.1, the user is not able to dial in to an AS5200 with Cisco IOS Release 11.1 if the AS5200 has autoselect configured.

To work around this problem, do one of the following:

- Remove autoselect and use ARAP dedicated.
- Use the ARAP 2.0.1 client instead.
- Turn on MNP10 on the ARAP 2.1 client.
- Modify the client CCL script to extend the pause to 3 seconds before exiting. [CSCdj09817]

- Mounting an AFP volume fails with the following error in ARAP 3.0:

```
%ARAP-6-MAXRESENDS: TTY 1 %ARAP-6-BADEXIT: TTY 1: exited user cisco: ARAP
connection was terminated. TTY1: Line reset by "ARAP" [CSCdj39623]
```

Basic System Services

- The router might reload when trying to process the **show accounting** command. [CSCdi69364]

- The **show stacks** command fails to report the correct version of code running at the time of the last reload. This problem occurs when the Flash version of the Cisco IOS software does not match the running version of code. [CSCdi74380]
- Fast switching and optimum switching counters should be broken out separately in the output of the **show interface switching** command. [CSCdi87008]
- Traffic shaping is not currently supported over tunnels of any type or switching mode. The feature is currently under development. [CSCdi88997]
- When a router is configured with the command **ip identd** and with **aaa authentication login default tacacs+ enable** the router will reload itself under these conditions:
 - The router is resolving host names via an external DNS server.
 - The TACACS server is down.
 - The user gains access to the router via the backup “enable” method.
 - The user attempts to Telnet from the router to a host on the network.After the Telnet is initiated, the router will immediately reload.

The workaround for this problem is to not configure the **ip identd** command or to disable the identd process with the global command **no ip identd** (which is the default). [CSCdj19961]
- Boot Flash devices are not recognized when formatting boot Flash type A7, A6, or AA.

To run type A7, A6, or AA boot Flash devices and use images prior to this bug fix, format boot Flash with an image containing this bug fix. Then load an older image onto the newly formatted boot Flash SIMM. [CSCdj20651]
- The **tacacs-server directed-request restricted** command only applies to authentication, not to accounting or authorization. Therefore, there is no way to restrict a user’s authorization or accounting to a given set of servers, which can lead to inconsistencies. For example, authentication for a directed user can be attempted only on the restricted servers, whereas authorization or accounting can be attempted on non-restricted servers as well. This inconsistency can cause authentication to pass while authorization fails for a given user. [CSCdj37496]
- When issuing the **no snmp trap link-status** command on an ISDN interface on both the Virtual-Template and the D channel, the router still sends traps whenever a B channel changes state. [CSCdj38266]

IBM Connectivity

- The **dlsw remote-peer frame-relay interface serial** command does not work on a point-to-point subinterface. The workaround is to use multipoint and to do LLC mapping. [CSCdi55085]
- On a router running Cisco IOS Release 11.2, Enhanced IGRP fails to connect fully to other Enhanced IGRP routers across a single Token Ring interface, when source-route bridging is configured on the interface but source bridge spanning is not enabled. The workaround is to enable source bridge spanning on the Token Ring interface. [CSCdi70297]
- A bus error occurred at PC0x169a46. The stack trace indicates a problem in the LNX process. This problem occurs on X.25. [CSCdi73516]
- When the fast source-route translational bridging feature is configured, packets are corrupted. The workaround is to issue the **no source-bridge fastest ring-group fastest** command, which disables the fast source-route translational bridging feature. [CSCdi87612]

- A small window exists in which it is possible after a transmission group reinstallation that only one CP-CP session is established between the router and a neighboring node. In this case, the contention winner session from the perspective of the router is not activated. Once this occurs, the CP-CP contention winner session will only activate if the APPN subsystem is stopped and started.

There is no known workaround. [CSCdj25859]

- An APPN router may display the following “Unanticipated CP_STATUS” message when the conloser CP-CP session goes down and comes back up without the conwinner session being deactivated:

```
%APPN-6-APPNSENDMSG: Ended DLUR connection with DLUS NETA.SJMVS1
%APPN-7-MSALERT: Alert LU62004 issued with sense code 0x8A00008 by XXXSMPUN
%APPN-6-APPNSENDMSG: Starting DLUR connection with DLUS NETA.SJMVS4
%APPN-7-APPNETERROR: CP_STATUS FSM: Unanticipated CP_STATUS message received
```

Each subsequent broadcast locate received by the router causes the following messages to be displayed and about 1920 bytes of APPN memory to be leaked:

```
%APPN-7-APPNETERROR: MAP_INPUT_SET_TO_ROW: invalid input value=0x80200080
%APPN-7-APPNETERROR: State Error lcb: 60C05CC0 pcid: DA839C70FB1548CB row: 22
col: 0
```

This problem occurs when two links are active to the same node and the CP-CP sessions are split between these two links and the link with conloser is stopped.

The APPN subsystem should be stopped and restarted to clear this problem. If the CP-CP sessions are between the router and the host, terminating either CP-CP session on the host will also clear this problem. [CSCdj33718]

- There may be intermittent failures when trying to link to bridges over the DLSw remote peers when running LNM over DLSw. The workaround is to reload the router that is directly attached to the LNM device. [CSCdj34112]
- When testing FRAS BAN for SDLC attached PU 2.1 and PU 2.0 and using RSRB backup over PSTN, the PUs failed to connect after the Frame Relay interface was brought back up after a link failure.

The output of the **show fras** command showed ls-reset backup enabled. In order to reconnect the PUs, the **fras backup rsrb** statement had to be removed or the serial interfaces configuration had to be deleted and then readded. [CSCdj39306]

Interfaces and Bridging

- When connecting a Canary Fast Ethernet transceiver to the MII connector on VIP port adapters requires a microcode reload before the port will function properly. [CSCdi64606]
- On an RSP router, the “%CBUS-3-CTRUCHECK” error message is displayed and the Token Ring interface resets. To correct this problem, upgrade to RSP TRIP Microcode Version 20.1. [CSCdi74639]
- The error “%CBUS-3-CTRUCHECK: Unit 0, Microcode Check Error” occurs on Token Ring interfaces, causing the interface to reset. [CSCdj08654]
- An RSP2 router configured with a Fast Ethernet interface and a slow-speed serial interface may experience output packet drops on the serial interface, with incoming traffic on the Fast Ethernet interface. This problem occurs even with less traffic, such as during a regular ping.

To work around this problem, disable fast switching on the serial interface. [CSCdj17962]

- IBM RPL fails to load from a server with IPX routing enabled on a Cisco 3620 router. SMC RPL does not exhibit this behavior. A Cisco 2500 series router does not cause this behavior.
A LANalyzer trace indicates that the router is forwarding RPL requests out the same Token Ring interface port on which it received the packet. [CSCdj18835]
- The **pos specify-sls0** and **pos specify-c2** POS interface specific configuration commands do not work correctly. [CSCdj25166]
- Input from some interfaces is not reaching the processor on a Cisco 7000 router. Although the cards are connected to the correct Ethernet and serial interfaces, no input is received from these interfaces. To recover from this situation, reboot the router. The output from the **show controllers cbus** command shows rql greater than 0. Using the **show interface** command does not indicate input traffic or hangup issues. [CSCdj29154]
- dot5StatsTable does not return any value in Cisco IOS 11.2. [CSCdj32372]
- An NFS transmission problem and FDDI corruption occurred after installing 10.3(9)+ or 11.1(9)+ 11.2(1)+. [CSCdj38715]

IP Routing Protocols

- A routing node is removed from the IP cache Radix tree and then the buffer is freed but somehow it can still be traversed from the treetop and cause a crash (access after free). [CSCdj17314]
- EIGRP failed to advertise a directly connected network. [CSCdj37728]
- If the **summary-address** statement is removed on a remote router that advertises summary-address routes on only one path, then the core router sees both equal cost paths. This problem occurs on OSPF with NSSA. [CSCdj38067]
- If two routing protocols with mutual redistribution cause a routing loop, it is possible that the loop will remain even after updates have been filtered. The problem usually occurs after a **clear ip route *** command is issued after applying the filters. If the routes are allowed to age out the normal way the problem does not occur. If OSPF is running, the workaround is to issue the **clear ip ospf redistribution** command. [CSCdj38397]
- When configured for UDP flooding, a router routes “all nets” broadcast to the default gateway. For example, 150.215.255.255 should get flooded but gets routed instead.
A workaround is to put a static route to 150.215.255.0 to null0. [CSCdj38570]

ISO CLNS

- If secondary addresses are configured on an unnumbered interface, the interface routes corresponding to these addresses are not advertised in IS-IS. A workaround is to number the interface. [CSCdi60673]
- A crash was caused by an AVL node that was freed but was still accessed during tree traversing. This problem was a result of the node being deleted and freed in the middle of tree walk. This is an IS-IS (using AVL tree) specific problem. [CSCdj18685]

Novell IPX, XNS, and Apollo Domain

- Adding XNS back into a router’s configuration after it has been removed may cause a system to restart by bus error. This may only be a one time event if it occurs at all. [CSCdj16694]
- XNS routes may get deleted on serial interfaces at boot time. The workaround is to issue the **shut** and **no shut** commands on the affected interface. [CSCdj25806]

VINES

- In Cisco IOS Release 11.2, a router may unexpectedly reload when VINES SRTP routing is configured. The workaround is to remove the **vines srtp-enabled** command. [CSCdj37888]

Wide-Area Networking

- The AIP cannot be configured to issue idle cells instead of unassigned cells. [CSCdi48069]
- When traffic prioritization is configured on a Frame Relay interface with the command **frame-relay priority-dlci-group**, the command **no fair-queuing** should be also configured on the serial interface to achieve effective traffic prioritization. [CSCdi52067]
- When configuring PVCs on the AIP, you may observe a failure to create more PVCs when the number of VCCs configured is well below the maximum allowed. This failure occurs when the number of VPI values used exceeds a limit. The messages that occur due to this type of failure include the following:

```
%AIP-3-AIPREJCMD: Interface ATM5/0, AIP driver rejected Setup VC command (error code 0x0008)
```

```
%ATM-3-FAILCREATEVC: ATM failed to create VC(VCD=1500, VPI=10, VCI=257) on Interface ATM5/0, (Cause of the failure: Failed to have the driver to accept the VC)
```

The limit to the number of VPI values used depends on the configuration of the **vc-per-vp** configuration parameter. When **vc-per-vp** is 1024 (the default), 33 VPI values can be used. To work around this limitation, implement the **atm vc-per-vp** command on the particular ATM interface, which lowers the number of VCs per VP. This results in a corresponding increase in the number of VPI values that can be used. [CSCdi67839]

- The “%SYS-2-GETBUF” error message may appear. [CSCdi92482]
- A virtual access interface does not inherit the username from its parent interfaces when it hosts a PPP multilink session. Therefore, the **show user** command does not display the username associated with a virtual access interface, and SLIPON requests in Extended TACACS do not contain the username, resulting in possible authentication failures with Extended TACACS. [CSCdj04600]
- When using DLCI prioritization on a point-to-point Frame Relay subinterface and one of the DLCIs fail, the subinterface may bounce once or continually bounce during LMI full status reports, depending on whether LMI reports the DLCI as being DELETED or INACTIVE. This behavior is the same for every DLCI defined in the **priority-dlci-group**.

During normal behavior, the point-to-point subinterface should go down when the primary DLCI fails. If a secondary DLCI fails, the subinterface stays up but traffic destined only for that DLCI will fail. [CSCdj11056]

- A Cisco router running Cisco IOS Release 11.1(6.1) can experience an input queue wedge on the serial interface. The symptoms are dropped packets on the interface. The only way to clear this problem is to reload or power cycle the router. [CSCdj17547]
- A router may randomly and intermittently reload because of an MTU mismatch and generate system error messages similar to the following:

```
%SYS-3-OVERRUN: Block overrun at 4029DEA8 (redzone 743D3334) [CSCdj19105]
```

- Although a router configured for HSRP on LANE replies correctly with the HSRP MAC address in an ARP reply, all packets issued by the router with a virtual IP address use the BIA MAC address as the source address. This makes it difficult for switches to know the forwarding port. [CSCdj28865]

- The BREAK sequence may not be received properly on platforms that use the Cirrus Logic asynchronous controllers. This includes the Cisco AS5100 and AS5200 routers. You may have to send the BREAK sequence multiple times before it is interpreted correctly. [CSCdj32121]
- When you configure dial-backup in a Legacy DDR environment, the primary link does not take over and does not clear the ISDN backup link whenever the kickout-load is reached on the primary interface. This works well in a dialer-profile or in a rotary-group environment. [CSCdj33786]
- When a dialer-profile is in standby mode, backing up a serial interface with the **backup interface dialer** command still allows incoming calls to this profile. Since the profile is in standby-mode this should not be possible. [CSCdj34108]
- IP problems may be experienced when multiple PRIs are set up in a rotary and using a dialer interface. There may be a problem pinging the dialin user since one PRI will be working and another PRI will not be working. There is no known workaround. [CSCdj34245]
- Configuration of a dialer interface for load backup (either with dialer profiles or legacy rotaries) could give rise to a flapping ISDN connection. This problem occurs especially when the bandwidth is configured on the primary for less than actual bandwidth. [CSCdj39723]

Open Caveats for Release 11.2(9) XA2

This section describes possibly unexpected behavior by Cisco IOS Release 11.2(9) XA2. Unless otherwise noted, these caveats apply only to Cisco IOS Release 11.2(9) XA2. The caveats listed here describe only the serious problems. For the complete list of caveats against Cisco IOS Release 11.2, use the Documentation CD-ROM or access Cisco.com as described in the section “Cisco.com” later in this document.

Wide-Area Networking

- Country code t1-default allows the tx level to be set to -6 dBm. When connecting two Cisco AS5300 MICA modems with the country code set for t1-default, the modems connect but the tx levels recorded T-1 test set indicate -1dBm (as do the Cisco AS5300 MICA modem receive level readings). When calling ax S/A 8840, the MICA mode and S/A fail to connect. If you set s39 to 15, the transmit level drops to -8 dBm which will then allow the Cisco AS5300 MICA modem and the standalone to go into steady state. The workaround is to use the USA country code for T1 configurations. [CSCdj38943]
- When connecting multiple modems, there are connection problems with the V.42bis interoperability between Multitech MT2836DZ and portware. The calls are not being connected or only connected at 19.2 kbps. The workaround is to upgrade the Multitech modem firmware to V.314C. [CSCdj38465]
- Sometimes the Cisco AS5300 connects at low connect rates such as (12 kbps or 14.4 kbps) when dialing into an Ascend Max. [CSCdj38945]
- Sometimes when the Cisco AS5300 dials into an Ascend Max 4002, no connection occurs. The Ascend box sends a tone prior to ABT which the AS5300 detects as a BUSY signal. [CSCdj32717]
- Autoselect failed on the Cisco AS5300 with Microcom. The PPP “Autoselect failed” occurred on some of the modems due to autoselect sampling failure. This failure was observed sporadically on some of the Microcom modems in the pool. Sometimes PPP protocol samples some other hex values like “8f, 58, 9c” instead of “7e, ff, 7d”. This wrong sample value varies on each modem. Due to this wrong autoselect sample, PPP negotiation fails and disconnects the modem link. This problem was observed with Microcom modems. The workaround is configuring at&f1 on the client modems. [CSCdj28916]

- Portware 2010a disconnects FTP put without compression. Call disconnects running FTP “puts” with certain USR Sportster modems. The problem does not occur during “gets.” This problem is prevalent if the USR modem has compression turned off. However, the likelihood of the call dropping in the default setting with compression turned on, is lower. This problem is related to the USR Sportster modem family as a whole. It is not a Cisco AS5300-specific problem. [CSCdj31483]
- The system crashed, bus error appeared 0x600FD0A0, address 0xC, illegal access. Adding the rotary-group to the PRI D-channel caused the system crashed. This only occurs when there are a lot of activities on the PRI such as call establishments. The work around is ensure to shutdown the PRI interface prior to adding the dialer rotary-group. [CSCdj35360]
- Need to use command **service password-encryption** to add new user. User has to issue the command **service password-encryption** in order to enable password encryption while adding new users for authentication purposes. This feature was enabled by default in previous releases. The workaround is to configure for **service password-encryption** prior to adding new users and passwords. [CSCdj33310]
- Tcp-ppp protocol translation is broken with xtacacs. Async interface fails to come up while continuously sending CHAP challenge to the peer device even though the peer responds to the Cisco AS5300 as expected. [CSCdj24462]
- Heavy traffic from user (PRI to FE) causes a Cisco AS5300 to drop calls. If a Cisco AS5300 is configured for PRI and receives a packet that is not fast switched on one of its B channels, this packet is moved from the input interface queue say serial 0:0 to the D-channel input interface queue serial 0:15 (for E1). If many of these kinds of packets are received, the D-channel interface drops the packets. Also, the isdn q921 and q931 messages are not able to be received since there is no room on the input queue. This causes the ISDN calls to be dropped on that interface. [CSCdj33571]
- ISDN needs to inform the CSM whenever it transmits a RELEASE_COMP, so that the CSM will enable the modem to go onhook. Otherwise, the modem still thinks it is busy and will remain in offhook state for about 210 seconds, until CSM_EVENT_WDT_TIMEOUT timer expires and makes the modem go onhook. [CSCdj40761]
- Spurious memory access during in dialer code, can occur when calls are torn down by shutting down async groups. The following message might appear on the console:

```
%ALIGN-3-Spurious memory access made at 0x60790FA8 reading 0X0".
```

[CSCdj45375]
- The Cisco AS5300 might crash after an extended period when the layer 2 are going up and down on all the PRIs. [CSCdj43873]
- When the current called number is shorter than the previous called #, the Cisco AS5300 gets incorrect DNIS for CAS/R2. This can affect modem pooling. This can happen as users call from within the local zone, from another state or even country. If it's not a 800 number, length of dialed number may not be constant. The AS5300 remembers the longest dialed number on that modem. [CSCdj46326]
- Simultaneous calls sends R2 analog signaling into a state where it can not make any further calls until the controllers are shut. If 120 calls are made in 4 or more bursts, all calls are completed. It happens for all the country codes and either when the Cisco AS5300s are connected via a converter or back to back. [CSCdj46082]

Closed and Resolved Caveats for Release 11.2(9) XA2

This section describes closed and resolved caveats for Cisco IOS Release 11.2(9) XA2. For the complete list of caveats against Cisco IOS Release 11.2, use the Documentation CD-ROM or access Cisco.com as described in the section “Cisco.com” later in this document.

- CSCdp11863

Cisco IOS software releases based on versions 11.x and 12.0 contain a defect that allows a limited number of SNMP objects to be viewed and modified without authorization using a undocumented ILMI community string. Some of the modifiable objects are confined to the MIB-II system group, such as “sysContact”, “sysLocation”, and “sysName”, that do not affect the device's normal operation but that may cause confusion if modified unexpectedly. The remaining objects are contained in the LAN-EMULATION-CLIENT and PNNI MIBs, and modification of those objects may affect ATM configuration. An affected device might be vulnerable to a denial-of-service attack if it is not protected against unauthorized use of the ILMI community string.

The vulnerability is only present in certain combinations of IOS releases on Cisco routers and switches. ILMI is a necessary component for ATM, and the vulnerability is present in every IOS release that contains the supporting software for ATM and ILMI without regard to the actual presence of an ATM interface or the physical ability of the device to support an ATM connection.

To remove this vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is documented in DDTS record CSCdp11863.

In lieu of a software upgrade, a workaround can be applied to certain IOS releases by disabling the ILMI community or “*ilmi” view and applying an access list to prevent unauthorized access to SNMP. Any affected system, regardless of software release, may be protected by filtering SNMP traffic at a network perimeter or on individual devices.

This notice will be posted at

<http://www.cisco.com/warp/public/707/ios-snmp-ilmi-vuln-pub.shtml>.

This caveat is resolved in Cisco IOS Release 11.2(9) XA2.

Cisco.com

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

Available 24 hours a day, 7 days a week, Cisco.com provides a wealth of standard and value-added services to Cisco's customers and business partners. Cisco.com 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.

Cisco.com 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 Cisco.com 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 Cisco.com provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access Cisco.com in the following ways:

- WWW: <http://www.cisco.com>
- Telnet: [cco.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 Cisco.com'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, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM is available as a single unit or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>.

This document is to be used in conjunction with the *Cisco IOS Release 11.2 Configuration Guides and Command References*.

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

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0102R)

Copyright © 1997–2001, Cisco Systems, Inc.
All rights reserved. Printed in USA.