



Doc. No. 78-4611-04

Release Notes for the 1600 Series for Cisco IOS Release 11.2P

January 12, 1998

These release notes describe the new features and significant software components for Cisco IOS Release 11.2 P up to and including Release 11.2(11) P for Cisco 1600 series routers.

Introduction

These release notes discuss the following topics:

- Cisco IOS Release 11.2 Paradigm, page 2
- Cisco 1600 Series Routers, page 3
- Cisco IOS Documentation, page 3
- New Features in Release 11.2(11) P for the Cisco 1600 Series Routers, page 5
- New Features in Release 11.2(10) P for the Cisco 1600 Series Routers, page 6
- New Features in Release 11.2(9) P for the Cisco 1600 Series Routers, page 8
- New Features in Release 11.2 P for the Cisco 1600 Series Routers, page 8
- Cisco IOS Feature Sets for Cisco 1600 Series Routers, page 20
- Upgrading to a New Software Release, page 23
- Memory Requirements, page 24
- Caveats for Release 11.2(1) Through 11.2(11) P, page 25
- Caveats for Release 11.2(1) Through 11.2(10), page 40
- Caveats for Release 11.2(1) Through 11.2(9), page 48
- Caveats for Release 11.2(1) Through 11.2(8), page 54

Corporate Headquarters

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

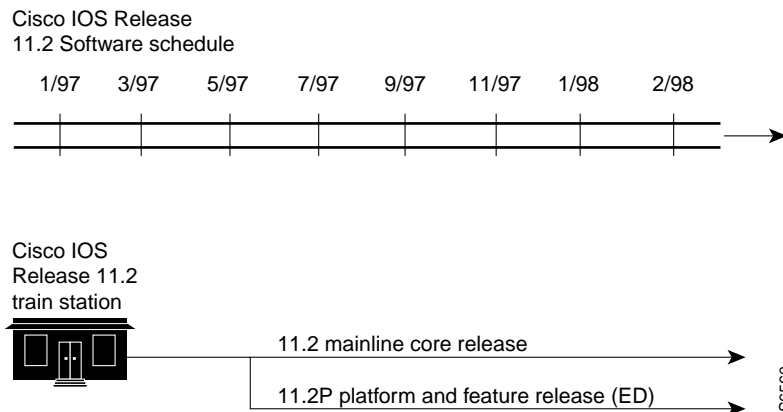
Copyright © 1997,1998
Cisco Systems, Inc.
All rights reserved.

- Caveats for Release 11.2(1) Through 11.2(4), page 61
- Cisco Connection Online, page 63
- Documentation CD-ROM, page 64

Cisco IOS Release 11.2 Paradigm

Similar to a train rolling down a track and picking up passengers, after a release of Cisco IOS software is released to customers it picks 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 mainline software “train,” there is an early deployment (ED) train. The ED train-Release 11.2 P-delivers fixes to software defects and support for new Cisco platforms and features. Figure 1 shows the Cisco IOS 11.2 and 11.2 P train software releases.

Figure 1 Cisco IOS Release 11.2 Software Releases



Note Cisco 1600 series routers run only Release 11.2 P software.

Release 11.2 P includes all the functionality of the features described in Table 1 and Table 2 in the section “Cisco IOS Feature Sets for Cisco 1600 Series Routers”, all the features described in the section “Additional Software Features for the Cisco 1600 series”, and the software caveat information for Release 11.2.

To determine which Cisco IOS maintenance release is running on your Cisco 1600 series router, log on to the router and enter the **show version** User EXEC command, as shown below:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 1600 Software (C1600-Y-L), Version 11.2(8.5)P, MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Fri 12-Sep-97 00:36 by ccai
Image text-base: 0x0200544C, data-base: 0x023028C0

ROM: System Bootstrap, Version 11.1(10)AA, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
ROM: 1600 Software (C1600-BOOT-R), Version 11.1(10)AA, EARLY DEPLOYMENT RELEASE SOFTWARE
(fc1)
router uptime is 1 minute
```

```
System restarted by reload
System image file is "master/cl600-y-1.112-8.5.P", booted via tftp from 223.255.254.254

cisco 1601 (68360) processor (revision C) with 9728K/512K bytes of memory.
Processor board ID 05681524, with hardware revision 00000000
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface(s)
1 serial(sync/async) network interface(s)
System/IO memory with parity disabled
2048K bytes of DRAM onboard 8192K bytes of DRAM on SIMM
System running from RAM
8K bytes of non-volatile configuration memory.
8192K bytes of processor board PCMCIA flash (Read/Write)
Configuration register is 0x0
```

Cisco 1600 Series Routers

The Cisco 1600 series routers deliver the next-generation set of features and benefits for small-office Internet and intranet access: WAN flexibility, end-to-end security, end-to-end quality of service, ease of use, deployment, and management. The Cisco 1600 series routers connect small offices with Ethernet LANs to the public Internet and to a company's internal intranet or corporate LAN through several WAN connections such as ISDN, asynchronous serial, and synchronous serial. The Cisco 1600 series routers include the following models: Cisco 1601, Cisco 1602, Cisco 1603, Cisco 1604, and Cisco 1605-R.

Cisco 1601 through Cisco 1604 router models include one Ethernet port, one built-in WAN port, and one WAN interface card expansion slot for additional connectivity and flexibility. The Cisco 1601 includes a built-in serial WAN port; the Cisco 1602 has an onboard 56-kbps four-wire channel service unit/data service unit (CSU/DSU); the Cisco 1603 has an ISDN BRI S/T port; and the Cisco 1604 includes an ISDN BRI U interface with a built-in NT1 device. The Cisco 1605-R has two Ethernet LAN interfaces and one WAN interface card slot.

The following WAN interface cards are supported by the Cisco 1600 series routers:

- 1-port serial
- 1-port ISDN BRI with S/T interface
- 1-port ISDN BRI with NT1 and U interface
- 1-port ISDN Leased Line BRI S/T WAN interface (Cisco 1603 and Cisco 1604 routers only)
- 1-port 56/64kbps DSU/CSU WAN interface

Cisco IOS Documentation

For Cisco IOS Release 11.2, the Cisco IOS documentation set consists of eight documentation modules. Each documentation module has a configuration guide, a command reference, and 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
<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

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 3</i> • <i>Network Protocols Command Reference, Part 3</i> 	<ul style="list-style-type: none"> Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Bridging and IBM Networking Configuration Guide</i> • <i>Bridging and IBM Networking Command Reference</i> 	<ul style="list-style-type: none"> 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> 	

These documents are available as printed manuals or electronic documents. For electronic documentation of Release 11.2 router and access server software features, refer to the Cisco IOS Release 11.2 configuration guides and command references 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>.

New Features in Release 11.2(11) P for the Cisco 1600 Series Routers

This section describes the new Cisco IOS Firewall feature set and Context-Based Access Control feature, available only in software release 11.2(11) P and above.

The Cisco IOS Firewall Feature Set: Context-Based Access Control

The Cisco IOS Firewall feature set combines existing Cisco IOS firewall technology and the new context-based access control feature to provide an effective, robust firewall.

The Cisco IOS Firewall feature set is designed to prevent unauthorized, external individuals from gaining access to your internal network, and to block attacks on your network, while at the same time allowing authorized users to access network resources.

You can use the Cisco IOS Firewall feature set to configure your Cisco IOS device as:

- An Internet firewall or part of an Internet firewall
- A firewall between groups in your internal network
- A firewall providing secure connections to branch offices
- A firewall between your company's network and your company's partners' networks

The Cisco IOS Firewall feature set provides the following capabilities:

- Protects internal networks from intrusion.
- Monitors traffic through network perimeters
- Enables network commerce via the World Wide Web.

Context-based access control (CBAC) is a new feature which provides intelligent filtering of packets through the firewall. CBAC creates temporary openings in the firewall to permit packets that are part of a permissible session. (These packets are normally blocked at the firewall.) A permissible session is one that originates from within your protected internal network.

New Features in Release 11.2(10) P for the Cisco 1600 Series Routers

Cisco IOS software Release 11.2(10) P and above supports the following features in Cisco 1600 router plus feature sets:

- Virtual Private Dial-up Networks (VPDN)
- RADIUS

Virtual Private Dial-up Networks

Virtual private dial-up networks (VPDN) allow separate and autonomous protocol domains to share common access infrastructure including modems, access servers, and ISDN routers. VPDN uses the Level 2 Forwarding protocol (L2F) which permits the tunneling of link level frames.

Using L2F tunneling, an Internet Service Provider (ISP) or other access service can create a virtual tunnel to link a customer's remote sites or remote users with corporate home networks. In particular, a network access server at the ISP point of presence (POP) exchanges PPP messages with the remote users, and communicates by L2F requests and responses with the customer's home gateway to set up tunnels. L2F passes protocol-level packets through the virtual tunnel between endpoints of a point-to-point connection.

Frames from the remote users are accepted by the ISP POP, stripped of any linked framing or transparency bytes, encapsulated in L2F, and forwarded over the appropriate tunnel. The customer's home gateway accepts these L2F frames, strips the L2F encapsulation, and process the incoming frames for the appropriate interface.

Note This implementation of VPDN supports PPP dial-up only.

To configure virtual private dial-up networks, see the “PPP for Wide-Area Networking” section of the *Wide-Area Networking Configuration Guide*. This information is also available at the following URL on the Documentation CD-ROM and on CCO (as described in the section “Cisco Connection Online” later in this document):

http://www.cisco.com/univercd/data/doc/software/11_2/cwan/4cppp.htm#INDEX11038

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server, which contains all user authentication and network service access information. RADIUS is a fully open protocol, distributed in source code format, that can be modified to work with any security system currently available on the market.

Cisco supports RADIUS under its Authentication, Authorization, and Accounting (AAA) security paradigm. RADIUS can be used with other AAA security protocols, such as TACACS+, Kerberos, or local username lookup. RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS—For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendor's access servers, dialin users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.
- Turn-key network security environments in which applications support the RADIUS protocol—For example, in an access environment that uses a “smart card” access control system. In one case, RADIUS has been used with Enigma's security cards to validate users and grant access to network resources.
- Networks already using RADIUS—You can add a Cisco router with RADIUS to the network. This might be the first step when you transition to a Terminal Access Controller Access Control System (TACACS+).
- Networks in which a user must only access a single service—Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to a single protocol such as Point-to-Point Protocol (PPP). For example, when a user logs in, RADIUS identifies this user as having authorization to run PPP using IP address 1.2.3.4 and access-list N is started.
- Networks that require resource accounting—You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

RADIUS is not suitable in the following network security situations:

- Multiprotocol access environments—RADIUS does not support the following protocols:
 - AppleTalk Remote Access Protocol (ARAP)
 - NetBIOS Frame Protocol Control Protocol (NBFCP)
 - NetWare Asynchronous Services Interface (NASI)
 - X.25 PAD connections

- Router-to-router situations—RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one router to a non-Cisco router if the non-Cisco router requires RADIUS authentication.
- Networks using a variety of services—RADIUS generally binds a user to one service model.

To configure RADIUS on a Cisco 1600 router, see the “Configuring Network Access Security” section of the *Security Configuration Guide*. This information is also available at the following URL on the Documentation CD-ROM and on CCO (as described in the section “Cisco Connection Online” later in this document):

http://www.cisco.com/univercd/data/doc/software/11_2/csecur/2caaa.htm

New Features in Release 11.2(9) P for the Cisco 1600 Series Routers

This section provides information about the new Cisco 1600 hardware introduced with Cisco IOS software Release 11.2(9) P:

- Cisco 1605-R Router—This new router provides two Ethernet LAN interfaces and one WAN interface card slot. One Ethernet interface can be dedicated to an internal LAN while a second perimeter LAN allows users from an untrusted network (such as the Internet) to access resources such as Web and FTP servers.
- ISDN Leased Line BRI S/T WAN Interface Card—This card is supported on Cisco 1603 and 1604 routers. The card provides an additional ISDN 64 kbps leased line on the B1 channel that supports Frame Relay encapsulation, PPP encapsulation, and PPP compression.
- 56/64kbps DSU/CSU WAN Interface Card—This 4-wire, SNMP-manageable DSU/CSU card supports 56- or 64-kbps Digital Data Service (DDS) and Leased Line and Switched 56 kbps. The following synchronous serial WAN services/protocols are supported: Frame Relay, SMDS, X.25, PPP, LAPB, and HDLC. Card diagnostics can be retrieved using Telnet or the console port.

New Features in Release 11.2 P for the Cisco 1600 Series Routers

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 P.

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.

Once 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. Specifically,

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

It is recommended 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 (OSPF) Enhancements

The following features have been added to Cisco's 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 SVCs, and dial-up 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 (NSSA)**—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 Not-So-Stubby-Areas (NSSA) 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 area to backbone area connection to become logically part of the same network.

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:

- 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.

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, towards 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 transport 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 affects.

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 (WFQ) 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-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 backwards 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 the 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:

- Currently, IRB 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 SAP by 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 approximately 5-minute intervals.

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

- **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.

Frame Relay Enhancements

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

- **Frame Relay SVC Support (DTE)**—Currently, access to Frame Relay networks is through private leased lines at speeds ranging from 56 kbps to 45 Mbps. Bandwidth within the Frame Relay network is permanently committed to providing permanent virtual circuits (PVCs) between the endpoints. Switched virtual circuits (SVCs) allow access through a Frame Relay network by setting up a path to the destination endpoints only when the need arises. This is similar to X.25 SVCs, which allow connections to be set up and torn down based upon data traffic requirements. Although SVCs entail overhead for setting up and tearing down links, the VC is only established when data must be transferred, so the number of VCs is proportional to the number of actual conversations between sites rather than the number of sites.

Frame Relay SVCs offer cost savings via usage-based pricing instead of fixed pricing for a PVC connection, dynamic modification of network topologies with any-to-any connectivity, dynamic network bandwidth allocation or bandwidth-on-demand for large data transfers such as FTP traffic, backup for PVC backbones, and conservation of resources in private networks.

To use Frame Relay SVCs, Frame Relay SVC must be supported by the Frame Relay switches used in the network. Also, a Physical Local Loop Connection, such as a leased or dedicated line, must exist between the router (DTE) and the local Frame Relay switch.

- **Traffic Shaping over Frame Relay**

Note Traffic shaping over Frame Relay is not available in Release 11.2(1). This feature will be available in a subsequent maintenance release of Release 11.2. Refer to software defect ID CSCdi60734.

The Frame Relay protocol defines several parameters that are useful for managing network traffic congestion. These include Committed Information Rate (CIR), Forward/Backward Explicit Congestion Notification (FECN/BECN), and Discard Eligibility (DE) bit. Cisco already provides

support for FECN for DECnet and OSI, BECN for SNA traffic using direct LLC2 encapsulation via RFC 1490, and DE bit support. The Frame Relay Traffic Shaping feature builds upon this support by providing the following three capabilities:

- Rate Enforcement on a per virtual circuit (VC) basis: A peak rate can be configured to limit outbound traffic to either the CIR or some other defined value such as the Excess Information Rate (EIR).
- Generalized BECN support on a per VC basis: The router can monitor BECNs and throttle traffic based upon BECN marked packet feedback from the Frame Relay network.
- Priority/Custom/First In, First Out Queuing (PQ/CQ/FIFO) support at the VC level: This allows for finer granularity in the prioritization and queuing of traffic, providing more control over the traffic flow on an individual VC.

Frame Relay Traffic Shaping:

- Eliminates bottlenecks in Frame Relay network topologies with high-speed connections at the central site, and low-speed connections at the branch sites. Rate Enforcement can be used to limit the rate at which data is sent on the VC at the central site.
- Provides a mechanism for sharing media by multiple VCs. Rate Enforcement allows the transmission speed used by the router to be controlled by criteria other than line speed, such as the CIR or EIR. The Rate Enforcement feature can also be used to pre-allocate bandwidth to each VC, creating a Virtual Time Division Multiplexing network.
- Dynamically throttles traffic, based on information contained in BECN-tagged packets received from the network. With BECN based throttling, packets are held in the router's buffers to reduce the data flow from the router into the Frame Relay network. The throttling is done on a per VC basis and the transmission rate is adjusted based on the number of BECN-tagged packets received.
- Defines queuing at the VC or subinterface level. Custom Queuing with the Per VC Queuing and Rate Enforcement capabilities enable Frame Relay VCs to be configured to carry multiple traffic types (such as IP, SNA and IPX), with bandwidth guaranteed for each traffic type.

The three capabilities of the Traffic Shaping for Frame Relay feature require the router to buffer packets to control traffic flow and compute data rate tables. Because of this router memory and CPU utilization, these features must be used judiciously to regulate critical traffic flows while not degrading overall Frame Relay performance.

IBM Functionality

This section describes the IBM network software features and support that are new in the Cisco IOS Release 11.2(8) P.

New Features

The following new IBM software features are available:

- Native Client Interface Architecture (NCIA) 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.

Note that each client is a full SNA PU with one or more LUs. As such, each device requires one LLC connection at the central site router.

- 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 a 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 Release 11.2.

Data Link Switching+ (DLSw+) Features and Enhancements

The following features have been added to Cisco's 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 (LNM) 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 (NSP) 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 PU 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.

- Down Stream Physical Unit (DSPU) over DLSw+—Down Stream 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 PU 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.

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 International Traffic in Arms Regulations (ITAR) export restrictions. 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. This version of encryption is not IPSEC compliant.

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 number of transactions per second supported. 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**—SENDAUTH 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 CCO 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.

SENDAUTH 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:

- AToM MIB Support
- RTTMON Support

See the "New Features" subsection in the "IBM Functionality" section for details.

- Cisco IP Encryption MIB
- Cisco Modem Management MIB
- Cisco SYSLOG MIB
- Cisco TN3270 Server MIB

Cisco IOS Feature Sets for Cisco 1600 Series Routers

This section lists Cisco IOS software feature sets available in Cisco IOS Release 11.2 P. 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 U.S. require an export license. Customer orders may be denied or subject to delay because of United States 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 P.

Table 1 Feature Set Matrix for Cisco 1600 Series Routers

Standard Feature Sets	Options
IP	Basic, Plus, Encrypt
IP/IPX	Basic, Plus, Encrypt
IP/AppleTalk	Basic, Plus, Encrypt
IP/IPX/AppleTalk	Basic, Plus, Encrypt
IP/IPX/IBM	Basic, Plus, Encrypt
Firewall ¹	Basic
IP/Firewall ¹	Basic
IP/IPX/Firewall Plus ¹	Plus
IP/IPX/AT/IBM/Firewall Plus 56 ¹	Encrypt

1. Available only in Release 11.2(11)P and later releases.

Feature Set Tables

The Cisco IOS software is available in different feature sets depending on the platform. Table 2 lists the feature sets for the Cisco 1600 series routers.

Table 2 Cisco 1600 Series Routers Feature Sets

Features Contained in Feature Sets	Feature Sets					
	IP	IP/IPX	IP/AppleTalk	IP/IPX/AppleTalk	IP/IPX/IBM	Firewall ¹
LAN Support						—
AppleTalk 1 and 2 ²	—	—	Basic	Basic	—	—
Integrated routing and bridging (IRB) ³	Basic	Basic	Basic	Basic	Basic	—
IP	Basic	Basic	Basic	Basic	Basic	—
Novell IPX ⁴	—	Basic	—	Basic	Basic	—
Transparent bridging	Basic	Basic	Basic	Basic	Basic	—
WAN Services						—
Asynchronous	Basic	Basic	Basic	Basic	Basic	—
Frame Relay	Basic	Basic	Basic	Basic	Basic	—
Frame Relay SVC support (DTE)	Plus	Plus	Plus	Plus	Plus	—
Frame Relay traffic shaping	Basic	Basic	Basic	Basic	Basic	—
HDLC	Basic	Basic	Basic	Basic	Basic	—
ISDN ⁵	Basic	Basic	Basic	Basic	Basic	—
PPP ⁶	Basic	Basic	Basic	Basic	Basic	—
SMDS	Basic	Basic	Basic	Basic	Basic	—
Switched 56	Basic	Basic	Basic	Basic	Basic	—
X.25	Basic	Basic	Basic	Basic	Basic	—
SLIP asynchronous only	Basic	Basic	Basic	Basic	Basic	—
WAN Optimization						—
Bandwidth-on-demand ⁷	Basic	Basic	Basic	Basic	Basic	—
Custom and priority queuing	Basic	Basic	Basic	Basic	Basic	—
Dial backup	Basic	Basic	Basic	Basic	Basic	—
Dial-on-demand	Basic	Basic	Basic	Basic	Basic	—
Header, link, and payload compression	Basic	Basic	Basic	Basic	Basic	—
Header and link compression	Basic	Basic	Basic	Basic	Basic	—
Snapshot routing	Basic	Basic	Basic	Basic	Basic	—
Weighted fair queuing	Basic	Basic	Basic	Basic	Basic	—
IPX and SPX spoofing	—	Basic	—	Basic	Basic	—
IP Routing						—
AppleTalk SMRP Multicast	—	—	Plus	Plus	—	—
Enhanced IGRP	Basic	Basic	Basic	Basic	Basic	—
IGRP	Basic	Basic	Basic	Basic	Basic	—
IP Multicast (PIM)	Plus	Plus	Plus	Plus	Plus	—

Table 2 Cisco 1600 Series Routers Feature Sets (Continued)

Features Contained in Feature Sets	Feature Sets					
	IP	IP/IPX	IP/AppleTalk	IP/IPX/AppleTalk	IP/IPX/IBM	Firewall ¹
Network Address Translation (NAT)	Plus	Plus	Plus	Plus	Plus	—
On Demand Routing (ODR)	Basic	Basic	Basic	Basic	Basic	—
OSPF	Plus	Plus	Plus	Plus	Plus	—
OSPF On Demand Circuit (RFC 1793)	Plus	Plus	Plus	Plus	Plus	—
PIM	Plus	Plus	Plus	Plus	Plus	—
RIP	Basic	Basic	Basic	Basic	Basic	—
RIP Version 2	Basic	Basic	Basic	Basic	Basic	—
Other Routing						—
IPX RIP	—	Basic	—	Basic	Basic	—
RTMP	—	—	Basic	Basic	—	—
NLSP	—	Plus	—	Plus	Plus	—
Multimedia and Quality of Service						—
Generic traffic shaping	Plus	Plus	Plus	Plus	Plus	—
Random Early Detection (RED)	Plus	Plus	Plus	Plus	Plus	—
Resource Reservation Protocol (RSVP)	Plus	Plus	Plus	Plus	Plus	—
Management						—
SNMP	Basic	Basic	Basic	Basic	Basic	—
Telnet	Basic	Basic	Basic	Basic	Basic	—
Console port	Basic	Basic	Basic	Basic	Basic	—
Networking Timing Protocol (NTP)	Plus	Plus	Plus	Plus	Plus	—
Simple Networking Timing Protocol (SNTTP)	Basic	Basic	Basic	Basic	Basic	—
Security						—
Access lists	Basic	Basic	Basic	Basic	Basic	—
Cisco IOS Firewall: Context-Based Access Control	—	—	—	—	—	Encrypt
Extended access lists	Basic	Basic	Basic	Basic	Basic	—
TACACS Plus	Basic	Basic	Basic	Basic	Basic	—
RADIUS	Plus	Plus	Plus	Plus	Plus	—
GRE tunneling	Basic	Basic	Basic	Basic	Basic	—
Lock and key	Basic	Basic	Basic	Basic	Basic	—
Network layer encryption, 40-bit (Plus 40) and 56-bit (Plus 56)	Encrypt	Encrypt	Encrypt	Encrypt	Encrypt	—
Virtual Private Dialup Network	Plus	Plus	Plus	Plus	Plus	—

1. Includes Firewall, IP/Firewall, IP/IPX/Firewall Plus, and IP/IPX/AT/IBM/Firewall Plus 56 feature sets. Available only in Cisco IOS Release 11.2(11)P and later releases.

2. AppleTalk load balancing is available in Cisco IOS Release 11.2.

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. In Cisco IOS Release 11.2, 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 (CLI/ANI), ISDN subaddressing, and applicable WAN optimization features.
6. PPP includes support for LAN protocols supported by the feature set, address negotiation, PAP and CHAP authentication, and PPP compression. Multilink PPP is included with Cisco IOS Release 11.0(4) and later releases.
7. Bandwidth-on-demand means two B-channel calls to the same destination.

Upgrading to a New Software Release

If you are upgrading to Cisco IOS Release 11.2 from an earlier Cisco IOS software release, you should save your current configuration file before configuring your access server with the Cisco IOS Release 11.2 software. An unrecoverable error could occur during download or configuration.

Cisco IOS Upgrade Procedure

For instructions on downloading a current Cisco IOS release from the CCO Trivial File Transfer Protocol (TFTP) server, go to the following URL. This URL is subject to change without notice.

<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, using a terminal emulation application, such as TCP Connect.
- Step 7 Log on to your router. Copy the software release from your TFTP server to your router, using the **copy tftp** command.

Memory Requirements

Table 3 describes the memory requirements for the Cisco 1600 series platform's feature set supported by Cisco IOS Release 11.2 P.

Table 3 Cisco 1600 Series—Memory Requirements

Cisco IOS Rel 11.2(10) P Feature Set	Required Memory for Cisco 1601—1604 (Run From Flash)		Required Memory for Cisco 1605-R (Run From RAM)	
	Flash ¹	DRAM	Flash ¹	DRAM
IP Only	4 MB ²	2 MB ²	2 MB ²	8 MB ²
IP Plus	6 MB	4 MB	4 MB	8 MB
IP Plus 40	6 MB	4 MB	4 MB	8 MB
IP Plus 56	6 MB	4 MB	4 MB	8 MB
IP/IPX	4 MB	2 MB	2 MB	8 MB
IP/IPX Plus	6 MB	4 MB	4 MB	8 MB
IP/IPX Plus 40	6 MB	4 MB	4 MB	10 MB
IP/IPX Plus 56	6 MB	4 MB	4 MB	10 MB
IP/Appletalk	4 MB	2 MB	2 MB	8 MB
IP/Appletalk Plus	6 MB	4 MB	4 MB	8 MB
IP/Appletalk Plus 40	6 MB	4 MB	4 MB	10 MB
IP/Appletalk Plus 56	6 MB	4 MB	4 MB	10 MB
IP/IPX/Appletalk	6 MB	4 MB	4 MB	8 MB
IP/IPX/Appletalk Plus	6 MB	4 MB	4 MB	10 MB
IP/IPX/Appletalk Plus 40	6 MB	4 MB	4 MB	10 MB
IP/IPX/Appletalk Plus 56	6 MB	4 MB	4 MB	10 MB
IP/IPX/IBM	6 MB	4 MB	4 MB	10 MB
IP/IPX IBM Plus	8 MB	4 MB	4 MB	12 MB
IP/IPX IBM Plus 40	8 MB	4 MB	4 MB	12 MB
IP/IPX IBM Plus 56	8 MB	4 MB	4 MB	12 MB

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

Caveats for Release 11.2(1) Through 11.2(11) P

This section describes possibly unexpected behavior by Release 11.2(11) P. Unless otherwise noted, these caveats apply to Release 11.2 up to and including 11.2(11) P. The caveats listed here describe only the serious problems. For the complete list of caveats against Release 11.2, use the Documentation CD-ROM or access CCO as described in the section “Cisco Connection Online” later in this document.

Access Server

- Under rare circumstances, a Cisco AS5200 may crash after displaying either a “%SYS-2-BLOCK” or “%SYS-2-BLOCKHUNG” message. [CSCdj30206]
- Under unknown circumstances, an AS5200 PRI D channel may get stuck in the state “TEL_ASSIGNED” rather than “MULTIPLE FRAME ESTABLISHED” which is the normal operating condition. This state is shown by the **show isdn status** command.

The workaround at this time is to reload the router. Issuing the **shut** and **no shut** commands on the affected interface does not help. [CSCdj41613]

- Running Cirrus’ microcode version less than 0x1F will cause high CPU utilization on the Cisco AS5200, which can cause existing calls to drop. [CSCdj68729]

AppleTalk

- The system may unexpectedly stop sending AARP request packets. Turning on AARP gleaning may help alleviate the problem. [CSCdi41414]
- 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.
- Turn on MNP10 on the ARAP 2.1 client.
- Modify the client CCL script to extend the pause to 3 seconds before exiting. [CSCdj09817]
- The Catalyst 5000 RSM with only 16 MB of RAM may experience a system reload at initialization if running the -jsv image. The workaround is to add more memory. [CSCdj63501]

Basic System Services

- On RSP interfaces, optimum switching is supposed to be the default. However, depending on the link order of the image, it can default to off. [CSCdi54567]
- If you see the message “%RSP-3-RESTART: interface Serial x/y, output stuck” on an RSP-based platform, you might have problems with the output interfaces. This problem can occur when bursty traffic is optimum-switched to an output interface on which either **fair queue** or **transmit-buffers backing-store** is enabled. A possible workaround is to disable optimum switching. [CSCdi56782]
- The router might reload when trying to process the **show accounting** command. [CSCdi69364]
- In certain cases, the number of packets shown in the IP flow cache packet size distribution does not match the number shown in the cache statistics. [CSCdi71766]

- 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]
- Adding an RSRB peer with direct encapsulation on a Cisco 7000 router configured with CSNA causes a “%RSP-3-RESTART: cbus complex restart” message and takes down the CIP interface. [CSCdi82836]
- Fast switching and optimum switching counters should be broken out separately in the output of the **show interface switching** command. [CSCdi87008]
- Enabling custom queuing on a Cisco 7200 router may result in an excessive increase in CPU use. [CSCdj05099]
- A timing window within `ccp_up` could cause the router to crash if a packet gets sent to the hardware or distributed compressor while CCP is coming up. [CSCdj12504]
- Under heavy interrupt load, driver instrumentation gets hit repeatedly while processes are accessing the instrumentation variables (for example, last output time). This causes a number of problems, including stuck output and incorrect user displays. There is no known workaround. [CSCdj15583]
- A router configured with the **ip identd** and with **aaa authentication login default tacacs+ enable** commands reloads 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 immediately reloads.

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]
- A recovery mechanism for misaligned 64-bit accesses has been added. This new functionality is similar to the current misaligned handler for shorter misaligned accesses. [CSCdj20738]
- Currently, Cisco 7200 series routers do not produce a core dump for the I/O memory region in any Cisco IOS release. Sometimes it is necessary to get this information if memory corruption is suspected. [CSCdj25189]
- On a Cisco RSP7000 or 7500, optimum switching appears to negatively interfere with Frame Relay switching. An IP route cache is created and connectivity between sites is lost. The behavior appears to be sporadic. [CSCdj26122]
- The **tacacs-server directed-request restricted** command applies only 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 nonrestricted servers as well. This inconsistency can cause authentication to pass while authorization fails for a given user. [CSCdj37496]
- In rare cases, an error may occur in Cisco routers. It may be seen as an error message describing an inconsistent state in allocating or deallocating blocks of memory.

An error was introduced by CSCdj42505 in Release 11.2 P and CSCdj22736 in Release 11.1CC. It does not exist in other IOS releases. [CSCdj44667]

- A Cisco router reloads with a bus error after adding three to four segments on a Cisco 7206 running Release 11.2(8)P. [CSCdj57506]
- An SNMP trap process can cause high CPU utilization. The workaround is to remove SNMP. [CSCdj63629]
- The patch added in CSCdi37706 and incorporated into Cisco IOS Releases 11.2(8.1), 11.2(8.1)P, 11.3(0.2) and 11.2(8.1)BC was intended to correct a cosmetic problem with command authorization.

Instead it exposed a bug in older implementations of the developers kit TACACS+ daemon (freeware) and will cause certain command authorizations to fail.

All freeware daemon versions prior to version 3.0.13 are subject to this problem including the ACE Safeword Security Server daemon. CiscoSecure daemons are not affected. [CSCdj66657]

- When a user dials into an AS5200/AS5300 using ISDN, the cpmActiveUserID object in the CISCO-POP-MGMT.mib is not updated and is left blank. [CSCdj66942]
- ARAP (ARA 2.1 & 3.0 client) with single line password using TACACS+ does not work.

To use the single line option, specify `username*password` in the username field and the word "arap" (lower case) in the password field.

The ARA 2.1 client returns the error "The connection attempt has failed. The server you called is not a valid Remote Access."

The ARA 3.0 client returns the error "User authentication failed. Check your user name and password and try again." [CSCdj68015]

EXEC and Configuration Parser

- When the encapsulation is changed on an interface from one that supports weighted fair queuing to one that does not, and the change is made from the console or auxiliary port, there may be an 8-Kb memory loss each time the encapsulation is changed. To identify this problem, examine the output of the **show memory allocating-process** command, which shows that the number of memory blocks allocated by the EXEC increases each time you change the encapsulation. If you do not change the encapsulation on an interface often, this problem should not have a significant impact on system performance. [CSCdi89723]
- If the line speed on an AS5300 is configured for tty lines that span a Microcom modem followed by a Moca modem, the output of the **show running-config** and **copy running-config startup-config** commands is wrong for the **speed** commands on those lines. [CSCdj41555]

IBM Connectivity

- Low-end platforms cache invalid RIF entries when using any form of the **multiring** command. This problem can also be seen in the DLSw reachability cache and with possible loops with LNM. [CSCdi50344]
- RSRB does not declare the peer dead until the keepalive times out. In order for RSRB to detect the dead peer so that the ring list can be cleaned up properly, set the keepalive value as small as possible. [CSCdi50513]
- Removing a DLSw configuration by configuring **no dlsw local-peer** and adding the DLSw configuration back can cause a memory leak in the middle buffer. [CSCdi51479]

- In some mixed-vendor bridge environments, Automatic Spanning Tree (AST) may not become active if the Cisco platform is the root bridge. The **message-age-increment** option is now available as part of the **source-bridge spanning** command to assist with the message-age count manipulation. This hidden command may be needed when the existing MAXAGE value is insufficient for network diameter and the maximum age is not configurable by the vendor bridges. [CSCdi53651]
- The LAN Network Manager (LNM) fails to link to the router's source bridge after the Token Ring interface is shut down on the remote router. The **show lnm bridge** command continues to display "Active Link" to the LNM. This problem does not occur when bridges are linked locally to the LNM. The workaround is to remove the **source-bridge** command from the Token Ring interface and configure it back in. [CSCdi53954]
- When the router is configured to use the DSPU feature, it may crash during deactivation of multiple downstream physical units (PUs). [CSCdi54114]
- A router may crash when DSPU debugging is enabled on a Cisco 4500 or Cisco 7500 router. [CSCdi54277]
- The BADLINESTATE message indicates that a frame was received while the router was transmitting. This points to a misconfiguration somewhere in the system as the bisync protocol is supposed to ensure half-duplex operation.
 - If the connecting device is configured FULL-DUPLEX or CONSTANT RTS, configure the interface `bsc fdx`.
 - The poll-timeout of the connecting HOST may be too short. To recover, issue the **shut** command on the interface. [CSCdi54541]
- Some NetBIOS applications that require a UI frame in response to Add Name Query cannot connect using a DLSw peer on demand if the NetBIOS circuit is the initial circuit that triggers the peer-on-demand to connect. [CSCdi54796]
- A sniffer trace shows duplicate ring numbers in the RIF when proxy explorers are in use. New SNA sessions fail to connect to the FEP. The workaround is to issue the **clear rif** command. [CSCdi55032]
- It is not possible to configure more than one DLSw remote peer using direct encapsulation for the same Frame Relay interface. The following error message is produced when the second peer is defined:

```
%Must remove the remote-peer to change the lf
```

The workaround is to use TCP encapsulation. [CSCdi55075]
- 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]
- A connection to a DLU (DSPU or APPN) across RSRB may fail if the remote SAP address is not enabled at the destination router. The workaround is to enable the remote SAP address. [CSCdi56660]
- DLSw FST encapsulation does not work over WAN, Token Ring, or FDDI interfaces. [CSCdi57207]
- An APPN router may unbind an LU6.2 session after receiving an unsolicited IPM with a nonzero next-window size. [CSCdi57730]

- A FRAS BNN-to-SDLC link does not restart when a Frame Relay interface is power-cycled. After the CSU is powered off, the “fras backup rsrb” kicks to put the SDLLC traffic across the RSRB peers. When the CSU is powered back on and the Frame Relay DLCI comes back up, the FRAS BNN connection to the SDLC nodes does not reactivate, although connections to Token Ring nodes do restart. [CSCdi61156]

- When an AS400 is configured as a network management focal point, it will initiate the MDS transaction program. The router does not handle it properly and corrupts memory.

The workaround is to turn off the focal point feature in the AS400. See the network attribute configuration panel in the AS/400. [CSCdi67820]

- 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 fastswitch ring-group fastswitch** command, which disables the fast source-route translational bridging feature. [CSCdi87612]
- A Cisco 7204 router running Cisco IOS Release 11.2(4) and the rsr-bridging feature is intermittently reloaded by itself with a software-forced crash resulting from memory corruption. [CSCdj13017]

- A router configured for DLSw has a buffer leak in the middle and big buffers. Eventually, the router runs out of I/O memory.

The problem is related to the way DLSw backup peers are configured. This problem occurs only if the local router is configured with backup peer commands and the remote router also has a configured peer and is not promiscuous.

The workaround is to remove the DLSw backup peer configuration. [CSCdj21664]

- The backup is not invoked until the interface transitions to the down state. [CSCdj22613]
- 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 must be removed or the serial interfaces configuration deleted and then readded. [CSCdj39306]

- When using APPN ISR over an RSRB port over FDDI, a Cisco 7200 series router may start sending frames with the non-bitswapped address of the target device.

To work around this problem, configure a MAC address on the target device that is always the same whether it is canonical or non-canonical (for example, 4242.6666.ffff). [CSCdj48606]

- An APPN router may fail the ACT_ROUTE if using parallel transmission groups (TGs). This problem may occur when an APPN router has two parallel links defined with the adjacent node. If the adjacent node activated a link to the network node (NN) requesting a TG number that had previously been used for a different defined link activation, the NN may fail the ACTIVATE_ROUTE. The APPN router sometimes tries to incorrectly activate the route using the other inactive link that has the same TG number. [CSCdj49814]

- Under certain circumstances, APPN may crash with the following stack trace.

```
> System was restarted by bus error at PC 0x6C75DC[_Mfree(0x6c75b6)+0x26], address
0xFFFFFFFF8[_etext(0x73ab50)+0xff8c54a8]
> Image text-base: 0x00012000[___start(0x12000)+0x0], data-base:
0x0073AB50[___etext(0x73ab50)+0x0]
> FP: 0x872C74[_etext(0x73ab50)+0x138124], RA:
0x6588BC[_session_failure_clean_up(0x658502)+0x3ba]
```

```
> FP: 0x872EB8[_etext(0x73ab50)+0x138368], RA:
0x65C6E6[_process_cp_status_sig(0x65c2da)+0x40c]
> FP: 0x8730F0[_etext(0x73ab50)+0x1385a0], RA:
0x64D820[_xxxms00(0x64d64e)+0x1d2]
> FP: 0x873210[_etext(0x73ab50)+0x1386c0], RA:
0xB720C[_process_hari_kari(0xb720c)+0x0]
```

[CSCdj51051]

- Frames may get corrupted while moving from an Ethernet segment to a FRAS-BAN interface. This is because of a problem in transparent bridging with Frame Relay. This caveat is the same as CSCdj47881. [CSCdj58692]
- A Cisco 2500 series router can crash when configuring the **x25 map qlc ntn** command in a DSPU PU over X25 configuration. There is no known workaround. [CSCdj61675]
- When source-route translational bridging is used, LLC sessions initiated from the transparent domain results in the source route's largest frame being incorrectly set to 4472 bytes instead of 1500 bytes. The result is that SNA and NetBIOS sessions may fail if the source-route station sends a frame with a payload that exceeds the maximum allowable size of 1500 bytes for Ethernet media.

The problem typically occurs when NetBIOS is utilized to allow workstations to communicate between Ethernet and Token Ring. It also occurs when SNA is used.

The workaround is to disable fast-switching by using the **no source-bridge transparent fastswitch** command or configuring the end stations to use frames with a payload of less than or equal to 1500 bytes. [CSCdj62385]

- The APPN router may have an excessive amount of processor memory allocated to APPN after experiencing several spikes in APPN processing. The APPN memory manager was optimized to release groups of unused pools back to the operating system. [CSCdj62502]
- A Cisco 4500 router running Release 11.2(9.1) crashed when configured for bisync (BSC) [CSCdj65763]
- The router may send a FRMR when the role is primary. The default behavior is changed so that it can only send FRMR as a secondary. If this presents a problem, use the **frmr-disable** interface configuration option to prevent a FRMR from being sent as a primary or secondary. [CSCdj66967]
- Any DLUR installation with over 800 to 1000 downstream PUs may experience a reload with the following backtrace:

```
[abort(0x601f2c3c)+0x8]
[crashdump(0x601f0b20)+0x94]
[process_handle_watchdog(0x601c2f08)+0xb4]
[signal_receive(0x601b7d58)+0xa8]
[process_forced_here(0x60169424)+0x68]
[locate_node_index(0x607dbcc0)+0x64]
[etext(0x60849e00)+0xcbee04]
```

[CSCdj67966]

- DSPU over RSRB with FST encapsulation reloads with a bus error similar to the following, when an upstream or downstream connection is initializing:

```
System was restarted by bus error at PC 0xCC6B8, address 0xFC4AFC82 4000 Software
(C4000-JS-M), Version 11.2(10.3), MAINTENANCE INTERIM SOFTWARE Compiled Mon
01-Dec-97 19:45 by ckralik (current version) Image text-base: 0x00012000,
data-base: 0x0076AE64
```

The workaround is to use TCP encapsulation for RSRB or to switch to DLSw. [CSCdj68261]

Interfaces and Bridging

- The serial interface on a Cisco 2500 series router enters a looped state if it is configured as a backup DTE interface and if the cable is disconnected and reconnected a few times. To fix the problem, enter the **clear interface** command. [CSCdi32528]
- Running SRB over FDDI on Cisco 4000 series routers may not perform as well as expected. However, this behavior should not seriously impact network functionality. [CSCdi69101]
- 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 FDDI interface driver can interact poorly with OSPF during OIR, causing SPF recalculations. This occurs only when OSPF is running on a FDDI interface that is not being inserted or removed. This fix eliminates the spurious indication from the driver that the SPF recalculation needs to take place. [CSCdi81407]
- Running high traffic on a Cisco 3620 that is running Cisco IOS Release 11.1 AA images on a two Ethernet in/two Ethernet out testbed shows that the sustained performance for fast-switching drops dramatically at near-line rate. The problem disappears once traffic is reduced. This problem does not occur with Release 11.2 P images. [CSCdi83922]
- OIR removal of a FIP from one slot into another will cause the FDDI to permanently remain in DOWN/DOWN. A reload is needed to get it up. OIR removal and putting it back into the same slot works fine. [CSCdi87221]
- A TRIP interface configured for transparent bridging but not configured for source-route bridging may silently drop some incoming frames. Specifically, if the interface receives a frame with a length less than 120 bytes and the RII bit is set (indicating a source-route bridging frame) it may drop the next frame received. This can cause the interface’s keepalive processing to fail and can lead to sporadic resets on the interface. [CSCdi88756]
- A Cisco 7500 series router might resign its active HSRP status when configured on an FEIP, if no other router is on the segment. The workaround is to turn off HSRP. [CSCdi93012]
- The error “%CBUS-3-CTRUCHECK: Unit 0, Microcode Check Error” occurs on Token Ring interfaces, causing the interface to reset. [CSCdj08654]
- The POS interface specific configuration commands **pos specify-s1s0** and **pos specify-c2** do not work correctly. [CSCdj09646]
- A Cisco AS5200 crashes with a bus error if it is powered on without any modem modules plugged into it. [CSCdj20225]
- Under certain circumstances, rebooting a Cisco 2524 may cause the router to pause indefinitely with a T1 connected to a Fractional T1 module. The workaround is to unplug the T1 prior to the reload. [CSCdj22485]
- The V.110 modules in an AS5200 fails the first time the **autoselect ppp** command is used after power up or when the **modem hold-reset** command is used on all 12 ports simultaneously. A workaround for this problem is to execute the **clear line** command on all V.110 lines after the following events:
 - Power up initialization.
 - Using the **modem hold-reset** command on all 12 ports.
 [CSCdj23972]

- Setting **encapsulation fddi** without bridging enabled on a VIP2/FDDI and FIP in RSP causes the interface to bridge transparently. The **encapsulation fddi** command should only be used with bridging enabled. As a workaround, use the **no bridge-group 1** command to disable bridging. [CSCdj24479]
- The **pos specify-sls0** and **pos specify-c2** POS-interface-specific configuration commands do not work correctly. [CSCdj25166]
- When a Token Ring interface is configured with a small MTU size, it could crash when it receives a frame larger than the MTU size. [CSCdj27678]
- The router does not respond to ARPs correctly when bridging IP on a channelized T1 interface. Therefore, Telnets to and from the router will fail. [CSCdj31285]
- A Cisco 2520 low-speed port may sometimes ignore group polls. This problem occurs on average once per minute and appears to occur only when the router is configured for half duplex and is using a DTE cable.

This problem has minimal impact on the performance of the multidrop line because a FEP usually resorts to individual polling. [CSCdj33392]

- IOS does not correctly return values for Token Ring soft error counters via SNMP. This may cause some SNMP management applications that query the Token Ring MIB to report errors. [CSCdj35713]
- Data corruption has been experienced at high bidirectional traffic rates. Corruption can also occur at high bidirectional traffic rates (when interface is throttling) when issuing the **shut** command. Data corruption is possible if you are using Rev2 Mueslix and an release earlier than Release 11.2(9)P. [CSCdj43672]
- An AS5300 system with Microcom and Mica modems can crash if fast ring is disabled. The problem occurs because the code does not check for a Microcom or Mica carrier card before accessing registers on the board. The current code assumes a Microcom card. Mixed Microcom/Mica configurations cannot be supported with this bug present. A similar crash with the same stack trace was also seen with only Microcom modems, but this is much harder to reproduce. [CSCdj44456]
- TTY lines on access servers may hang when control characters are sent in dumb terminal mode (no PPP or SLIP). A show line shows the TTY line in a ready state, but no response or prompt is seen from the access server when the activation character is sent (default is a return). Doing a clear line # does allow for the line to recover and respond to the activation character. [CSCdj46760]
- A “System restarted by bus error at PC 0x4262AA, address 0xFFFFF0FC” message may be received when the **frame-relay payload-compression packet-by-packet** command is entered under the subinterface. [CSCdj49344]
- On the Cisco AS5200 platform, a group of four ports may stop processing PPP packets on the interface. You can identify this problem by looking for a group of four contiguous ports that have a much higher volume of calls than the other ports on the AS5200. Currently, the only workaround is to reload the router. The port modems should be busied out until the router can be reloaded. [CSCdj51974]
- In rare cases, a Cisco 7200 series router with a Token Ring port adapter may crash if one of its Token Ring ports attempts to insert into the ring and fails due to a ring error. [CSCdj59796]
- With BVI used to route 802.2, the input queue counters might increment to the limit and then the BVI interface wedges until the router is reset. One possible workaround is to set the values high enough that the router stays up until it can be reset. [CSCdj68273]

- When IRB is enabled, the BVI interface may not overwrite the real incoming interface in the ARP response, so an incomplete ARP entry is installed and “wrong cable” is listed in the **debug arp** output. [CSCdj68785]
- The “%LINK-3-TOOBIG: Interface Lex1, Output packet size of= 1520 bytes too big” error occurred on a Cisco 4500 router after upgrading to Cisco IOS Release 11.2(9). [CSCdj69018]
- On a Cisco AS5100, the “%CIRRUS-3-SETCHAN: Serial3: setchan called in CD2430 interrupt context” error continuously appeared on the console. Users were still able to call into and connect with the router but performance was significantly impacted. [CSCdj69387]

IP Routing Protocols

- A spurious memory access can occur when switching from flow switching to process switching using the **no ip route-cache** command and then back to flow switching using the **ip route-cache flow** command. [CSCdj08350]
- 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]
- A crash occurred because of a memory leak. Output from the **show memory** command shows “IP Input” and “Pool Manager” holding onto memory. [CSCdj23080]
- Currently all packets denied by an access list are sent to the process level to generate an ICMP administratively prohibited message. Some of these packets are dropped because Cisco routers limit ICMP generation to two packets per second. This behavior results in excessive CPU load. [CSCdj35407]
- In some instances, a configured BGP router ID is not used after the router reloads. Instead, the router uses the highest IP interface address as its router ID, until the **clear ip bgp** command is executed.

A workaround is to configure a loopback on the interface whose address is greater than any other address on the router. [CSCdj37962]

- 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 attempting to set the ipNetToMediaType value with SNMP, the following error is returned and the value is not set:

```
snmpset: The value given has incorrect type or length. [CSCdj43710]
```

- In the presence of a large number of subnets, a CPUHOG message similar to the following may be generated:

```
%SYS-3-CPUHOG: Task ran for 2608 msec (73/65), Process = BGP scanner, PC = 176388
```

[CSCdj45966]

- Manual summarization with EIGRP does not work correctly. A summary route does not get advertised but one or more of the more specific routes do. [CSCdj46525]
- A router is crashing in GRE fast-switching routines without any changes in topology or configuration. [CSCdj50361]
- RIP might cause a “SYS-3-CPUHOG” message. [CSCdj51693]

- Remote routers connected to a Cisco 7513 used as hub Frame Relay router cannot see the IPX servers local to the Cisco 7513. The Cisco 7513 reloaded afterwards. [CSCdj54367]
- A Cisco 7000 series running Cisco IOS Release 11.2(9) crashes in dual_rtupdate. [CSCdj54728]
- Under certain conditions, an LS type 5 is not generated by the ABR in response to a received LS type 7. [CSCdj55301]
- A router may crash when configured with a very large IP accounting threshold. A workaround is to configure a small threshold or to leave it at the default. [CSCdj55512]
- With certain **route-map** configurations or a soft-reconfiguration, the LOCAL_PREF for a path may be set to zero, resulting in the wrong path being selected. [CSCdj55839]
- A problem occurs when a third EIP6 is added to a Cisco 7000 series already running EIGRP on two EIP6s, a TRIP4 and an FIP in an EIGRP topology. In the EIGRP topology, some of the networks that connect to the existing Ethernet interfaces may be lost. The IP routing table still shows the routes but not all connected networks are advertised in EIGRP. A workaround is to issue the **redistribute connected** command. [CSCdj57362]
- Under rare circumstances, a BGP router sends BGP updates with a duplicate community attribute, which triggers the neighbor reset. [CSCdj64103]
- EIGRP topology entries from the redistribution of connected routes where EIGRP is already running natively may not clear when the interface goes down. [CSCdj68388]
- When an interface is configured to send RIP V1 packets while running RIP V2, the router sends out corrupt packets. V2 packets are not effected. There is no known workaround. [CSCdj69026]

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 is 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]
- A dynamically discovered CLNS route does not overwrite a static CLNS route pointing to a down interface. As a workaround, remove the static route definition from the configuration and issue the **clear clns route** command. [CSCdj31228]

LAT

- LAT services are not available on the router when IRB is enabled. [CSCdj52841]

LLC Type 2

- A Cisco 4700 router may report intermittent “SYS-2-LINKED” error messages even though there is no memory shortage. [CSCdi52327]
- When running DLSw+ over Ethernet, the router transmits corrupted frames on retransmission. The retransmission occurs on receipt of a REJ frame from the end station or if an acknowledgement of the frame is not received within the LLC2 T1 timeout. [CSCdi52934]
- Timers are not cleaned up properly in LLC2. This may result in crashes when RSRB local acknowledgment is used under a high load. [CSCdj42474]

Miscellaneous

- Netview Service Point acquires but does not free VTY lines. The only way to recover the VTY lines is by using the **clear line** command. [CSCdi51685]
- A memory leak can occur that is related to the traffic rate and the TCP process. This leak is difficult to reproduce, but can be identified by an input queue wedge on a router configured for RSRB with TCP encapsulation. The output of a **show buffer** command indicates memory errors. Other symptoms include small buffers being created but not trimmed, and explorers being received with a wrong SNAP type value. [CSCdi54739]
- Only the Cisco 7500 family running encryption over VIP interfaces is affected by this problem. RSP software based encryption does not work when encrypted traffic is flowing over any Cisco 7500 VIP interface. Customers with VIP2-40 or higher interfaces need to run VIP distributed encryption. There is no workaround for other VIP2 models other than using an older non-VIP interface. [CSCdi74884]
- Packets may become stuck in the input queue of the destination interface if traffic sent over a GRE tunnel is encrypted. The packets become stuck in the input queue when the encrypted session between the peer routers is not established. The not established condition exists when traffic to be encrypted first begins flowing and also when the encrypted session time duration expires. The impact of this caveat can be lessened by configuring the encrypted session timeout to be substantially longer than the 30 minute default with the **crypto key-timeout minutes** command. [CSCdi90177]
- When a **no shut** command is issued on the ISDN interface, and **logging** and **logging trap** is configured, the router crashes. [CSCdj05365]
- If a CIP TN3270 PU is configured to connect from the host to the CIP via NCP, the link may fail. The workaround is to configure the CIP TN3270 PUs as connecting at the host. [CSCdj07152]
- Configuring both ISL and Multilink Multichassis PPP can cause a memory consistency check failure. The failure may lead to a software forced crash after a few calls have been received. [CSCdj22189]
- Under rare circumstances, the Cisco AS5200 may issue the “%SYS-3-BADMAGIC: Corrupt block at 20000000 (magic xxxxxxxx)” message and crash with a software forced crash. There is no workaround at this time. [CSCdj22429]
- HSRP can raise the CPU while the peer HSRP router is reloaded. The problem occurs when there is more than one HSRP group and the two peer routers have many HSRP peers. This caveat addresses HSRP scalability. The workaround is to reduce the HSPP groups, and/or increase the HSRP hello and hold time. Another symptom is that the interface resets go up until HSRP is stabilized. [CSCdj29595]
- Both HSRP routers on a FDDI ring go active and stay active on a Cisco 7000 series FDDI port adapter. Network instability can cause a FDDI ring to partition or be disrupted in a manner that causes HSRP peers to not receive hellos from their neighbors and therefore become active.
 HSRP routers send hello packets from a virtual MAC address, which is a function of the standby group number. When the ring heals, both routers are active and sourcing hellos from the same (virtual) MAC address.

FDDI devices must strip their frames off the ring. One method of doing this is to recognize frames by source MAC address. When the problem occurs, the FDDI PAs will mistakenly strip the other router's packets from the FDDI ring without processing them. This causes both routers to remain active since they do not hear hellos from their neighbors.

This problem can also occur when FDDI PAs are used in conjunction with other FDDI interfaces, such as the FIP or Cisco 4000 series FDDI module.

If only one standby group is in use, the **standby use-bia** command can be used on both routers to cause hellos to be sourced from the burned in address instead of the virtual MAC address. This will prevent the problem.

If the problem occurs, performing an interface reset by issuing the **shut** and **no shut** commands returns the routers to a normal state.

Increasing the HSRP hello intervals causes the problem to occur less often since the routers will be able to tolerate a longer period of instability before missing enough hellos to go active. [CSCdj30049]

- An AppleTalk packet traveling through RSM from one VLAN to another receives an improper 802.3 packet length. This affects other network devices that use this field. [CSCdj36862]
- A router running encryption may show “%ALIGN-3-SPURIOUS: Spurious memory access made at 0x60825E” messages. This means that the router had to access from memory twice in order to execute an instruction. It does not affect the connectivity operation of the router. At this time, the CPU overhead has been minimal. [CSCdj43491]
- A Cisco 7513 running Cisco IOS Release 11.2(9)P with a channelized E1 card and **channel-group** configured has a problem when a 40-bit crypto session is configured. When the crypto session from the Cisco 7513 side is started, the session is set up fine. However, the interface link protocol will go up and down. The only way to recover is to remove the **channel-group** and add it back on without crypto configuration [CSCdj50970]
- A Cisco 3620 router restarts after a software-forced crash at PC 0x60198F78. The decoded stack indicates memory corruption. [CSCdj51896]
- BOOTP/DHCP fails when attempted over an encryption session between routers if the BOOTP/DHCP traffic will be encrypted by matching the access list. This failure also affects any packets that are forwarded by the **ip helper address** command, such as Windows 95 Netbios over TCP/IP. The workaround is to adjust the access list so that these packets are not encrypted. [CSCdj54355]
- A router crashed after adding a new crypto link. [CSCdj60818]
- RBE from RSP2 to Cisco 4000 over Frame Relay subinterfaces fails. Other combinations do not fail. [CSCdj65337]

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]
- When using IPX-EIGRP over ISDN with floating static routes, there may be a short delay (about 10 seconds) before the application is able to get through. [CSCdj38031]
- Before a floating static route is installed, a waiting period is observed when the network is down and unreachable. If IPX watchdogs or SPX keepalives arrive during this time, they will be dropped, leading to session timeouts. [CSCdj50629]
- A problem occurs when using a floating static route across an ISDN link and IPX EIGRP is the primary dynamic routing protocol. When the link goes down, the EIGRP route is installed but after the floating static is configured and the line goes down and then back up there is no route to that network. The EIGRP route is received but never fully installed because of what seems to be incomplete removal of the floating static route. [CSCdj52947]

TCP/IP Host-Mode Services

- Under rare circumstances, a router reload may occur while running TCP to X.25 protocol translation. [CSCdj23230]

Wide-Area Networking

- When using a VIP controller in a Cisco 7000 series router with a Silicon Switch Processor (SSP), the SSP cannot access the second port adapter when the VIP is installed in slot 4. As a workaround, install the VIP in slots 0 through 3. [CSCdi41639]
- When a Cisco 4000 with a Basic Rate Interface (BRI) has the **isdn tei powerup** configuration flag set, the watchdog timeout will crash the router. A workaround is to configure the router with the **isdn tei first-call** command. [CSCdi45360]
- 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.

See associated caveat CSCdi52882. [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]

- On a Cisco 4500 or Cisco 4700, a packet may be registered in both the input and output hold queues when going from ATM to other network links. This may affect the values of the input and output queue length fields in the output of the **show interface** command. On a Cisco 4500 or Cisco 4700 configured with ATM, another fast network link, and a slow network link, this behavior may have some impact on the overall throughput of the traffic from ATM to another fast network link when the slow link is flooded with too many packets from ATM. However, we are unaware of any environments in which network functionality could be seriously impaired by this. The correct router behavior would be to drop packets over the slow link without affecting the traffic from ATM to another fast link. [CSCdi69441]
- ARP replies are not sent over a PPP multilink interface. As a workaround, you can configure a static ARP on the remote device or disable PPP multilink. [CSCdi88185]
- The transmitter on an ATM interface on a Cisco 4000 series router could hang if PVCs or SVCs are cleared (torn down/ removed using command line interface) when the OUTPUT queue is wedged. [CSCdi90150]
- ISDN leased-line does not come up after a reload on a Cisco 3600 series router. [CSCdj03228]

- A problem has been observed on a Cisco 3640 router running Cisco IOS 11.1(8) with an 8-port MultiBRI with built-in NT-1 module. Upon power up, the user is unable to use the BRI interfaces. These interfaces report not receiving TEI or EID information from the local switch. The local switch is an AT&T 5ESS emulating NI-1.

A workaround is to disconnect and reconnect every BRI interface once the router is fully operational.

This problem seems to be related to CSCdj04241. [CSCdj04625]

- Configuring STUN peers on a DLSw network causes the DLSw peers to disconnect. The debug on DLSw shows a “DLSw: keepalive failure for peer on interface Serial” message. The STUN process looks like it is intercepting the DLSw keepalives. [CSCdj08875]
- When using DLCI prioritization on a point-to-point Frame Relay subinterface and one of the DLCIs fails, the subinterface may bounce once or continually 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 for that DLCI only will fail. [CSCdj11056]

- Dynamic DLCI mappings may inadvertently remain mapped after switched virtual circuit teardown, as can be seen using the command **show frame-relay map**. [CSCdj11851]
- In some circumstances, the system may reload when using the dialer hold queue.

As a workaround, configure the **no dialer hold-queue** command. [CSCdj12397]

- Intermittent ping failure may occur when pinging over a DDR interface using LAPD encapsulation. There is no workaround [CSCdj20072]
- Frame Relay SVC calls may give the following Traceback message:

```
%SYS-2-LINKED: Bad enqueue of 8F3288 in queue 9570C8
-Process= "LAPF Input", ipl= 6, pid= 36
-Traceback= EBE30 EAA88 4A73B4 4A8E10
```

[CSCdj29721]

- Back-to-back branch instructions can cause unpredictable things to happen with the MIPS processor. When one was found in the no_throttling() function, a nop was inserted to avoid possible problems. [CSCdj29854]
- In the ISDN Layer2, Layer3, and management entity tasks, memory pointers become invalid. The problem results from a race condition between tasks when memory is freed in one task and then another task attempts to access this now invalid pointer. This scenario has been seen only on ISDN BRI platforms in which a number of the BRI interfaces experience persistent deactivation causing the management entity to be shut down. Add validmem_complete() checks before accessing or freeing pkt, pkg or primitive pointers. [CSCdj40403]
- When ATM traffic-shaping is enabled on an ATM interface along with priority-queueing, priority queueing does not work as desired.

To work around this problem, turn off ATM traffic-shaping over that interface. Another workaround is to use Cisco IOS Release 11.2(2) or earlier, including Release 11.1.

[CSCdj45778]

- A problem occurs when memory is low and someone executes a **show isdn history** command. [CSCdj46541]

- When the **ip tcp header-compression** and **ppp multilink** commands are configured together on the same interface, the router may crash.

The workaround is to remove the **ip tcp header-compression** or **ppp multilink** commands. [CSCdj53093]

- Multilink will only bring one link when used as backup on a DDR interface even though dialer-load threshold is configured. To work around this problem, configure the **no ppp multilink** command. [CSCdj56109]
- A problem has been identified with traffic shaping on the Cisco 4500 ATM NIMs. [CSCdj56673]
- Under rare conditions, an RSP4 may reload when an FSIP with active HDLC encapsulation interfaces is in use. [CSCdj57591]
- A Cisco 7500 series router with an AIP running Cisco IOS Release 11.2(6) might give out the following error messages:

```
atm_parse_packet (ATM2/0) :Invalid VC(0) received, type=A2D2
atm_parse_packet (ATM2/0) :Invalid VC(0) received, type=A2D2
atm_parse_packet (ATM2/0) :Invalid VC(0) received, type=A2D2
```

In addition, the input errors displayed by the **show interface atm** command increase.

This problem seems to occur only with Release 11.2(6). The workaround is to downgrade to Release 11.2(4) [CSCdj57704]

- When configuring **map-class frame-relay BC committed-burst-size**, the system may encounter a CPU exception with reason = EXEC_ADERR(1200) and restart.

There is no workaround, for this intermittent problem. [CSCdj62139]

- When using Frame Relay SVCs, Cisco IOS appears to not include the magnitude parameters for Be and Bc on the SVC CONNECT message. It only includes them in the SETUP message. The SVC circuits are on S4/0 for both routers. Without the magnitude parameters, the biggest value Bc and Be can be is approximately 130 Kb. There is no known workaround. [CSCdj63173]
- Some Windows 95 dial sessions that use script files do not connect to an asynchronous interface on Cisco access servers. [CSCdj63311]
- A Frame Relay interface configured for ANSI LMI will acknowledge a Cisco LMI update when the router should ignore it. [CSCdj64207]
- A Cisco LS1010 may not be able to establish an SVC when acting as an RFC1577 ARP client. Debugs reveal "Quality of Service Unavailable." [CSCdj64327]
- The **map-class** commands **frame-relay bc out** and **frame-relay be out** are accepted by the Enterprise image. These parameters are relevant for SVC setup. However, the traffic shaping code does not use them. As a result, the values appear to be unset. This behavior can be avoided by using the commands **frame-relay bc number** and **frame-relay be number** [CSCdj65624]
- When running LAPB over a DDR interface with **dialer hold-queue** configured, a traceback error message is generated when dialing out and the call connects. The traceback is not catastrophic but indicates a 20-byte memory leak on every dial attempt. As a workaround, configure the **no dialer hold-queue** command on the DDR interface. [CSCdj65756]
- The router may reload when booting up an image from a saved X.25 routing configuration. This problem was introduced in Release 11.2(10.1). [CSCdj67115]
- When the system is reducing its rate in response to the receipt of BEcNS, the reduction may not be predictable. Rate adjustments are made once per interval if any number of BEcNs were received during that interval. [CSCdj67297]

- Configuring a PVC via the **frame-relay interface-dlci** command on multipoint subinterfaces causes a system reload if the PVC was previously learned via inverse ARP. [CSCdj67510]
- A BRI interface may lose a TEI after it is reset. The router fails to request a second TEI after the reset. If the BRI is reset a second time, the router regains both of the TEIs. [CSCdj69824]

Caveats for Release 11.2(1) Through 11.2(10)

This section describes possibly unexpected behavior by Release 11.2(10) P. Unless otherwise noted, these caveats apply to Release 11.2 up to and including 11.2(10) P. The caveats listed here describe only the serious problems. For the complete list of caveats against Release 11.2, use the Documentation CD-ROM or access CCO as described in the section “Cisco Connection Online” later in this document.

Access Server

- When Frame Relay over ISDN is configured on a LES-typed driver based platform (such as a Cisco 7500, 5200, or 7200 series router), and the input packets are fast-switched (for example, the output interface has fast switch mode enabled), the BRI/PRI interface has an input queue wedge problem. The symptom was that the input queue count was incremented up to the maximum queue length and then began to drop input packets. [CSCdj45631]

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]
- IPTALK is completely broken in Release 11.2 because the llap header is missing in all IPTALK packets. There is no workaround. [CSCdj50179]
- An IPTALK interface will not come up after a reboot if the order of tunnel interface precedes its physical interface (for example, Ethernet or serial). The symptom is that the **iptalk** command from tunnel interface disappears after reboot. There is no workaround. [CSCdj58363]

Basic System Services

- Sometimes a memory leak that consumes I/O memory can be triggered in the pool manager. [CSCdi90521]
- Under extremely heavy CPU interrupt states, a router with FSIP, CT3 or any serial interface may experience the following “output stuck” error message:

```
%RSP-3-RESTART: interface Serial12/0/0:28, output stuck
```

The problem occurs on Cisco routers in the 7000 family using the CT3 or 4/8 port FSIP cards or any serial interface under Cisco IOS Release 11.1(10)CA, 11.1(11), and 11.2. It has been observed only under oversubscribed traffic load.

As a workaround, configure the interface for FIFO queueing via the **no fair-queue** command.

The command **transmit-buffers backing-store** is on by default when an interface is configured for weighted fair-queueing. If the **no fair-queue** interface command is used, which changes the queueing strategy to FIFO, then **transmit-buffers backing-store** is off by default.

This caveat has been resolved in the following Cisco IOS releases: 11.2(6.2)P 11.1(11.4) 11.1(11)CA 11.1(11.4)IA [CSCdj12815]

- If a **map-list** is configured, the **show running** command may cause the router to crash if the “Last configuration change at...” informational string exceeds a total length of 80 characters. [CSCdj13986]
- An EXEC prompt does not appear until the TCP connection for accounting EXEC is sent and acknowledged. Accounting EXEC acts like wait-start, even though start-stop is configured. [CSCdj27123]
- Performing a Telnet from the router with TACACS configured might cause a router to reload with a bus error. The exact cause is still under investigation.

This problem has been seen only with Cisco IOS Release 11.2 or later. [CSCdj36356]

- A Cisco 7200 or 3600 series router may crash with a bus error when doing protocol translation between X.25 and PPP. The workaround for the problem is to turn on **header-compression passive** in the translate statement. [CSCdj37556]
- When traffic shaping on the Cisco 7500 series routers, enough traffic may not be switched to achieve the specified traffic level. [CSCdj50861]
- The Cisco 7500 series routers may not correctly allocate the right number of packet memory (memd) buffers to some network interfaces. The problem requires a large number of interfaces whose collective bandwidth is high, but their MTU is smaller than another buffer pool.

For example, a problem was found with a Cisco 7500 using a large number of Fast Ethernet and/or Ethernet interfaces and one or more FDDI interfaces. The pool of packet memory should have allocated 80 percent of the memory to the Ethernet and Fast Ethernet interfaces, which use an MTU of 1536. Instead it received 20 percent of the memory, and the lone FDDI interface with MTU 4512 got 80 percent of the packet memory.

The problem occurred with 55 Ethernet, 6 Fast Ethernet, and 1 FDDI network interfaces. The problem did not occur with fewer interfaces, specifically 36 Ethernet, 5 Fast Ethernet, and 1 FDDI interfaces.

The problem may show up as a high number of input drops on some router interfaces. [CSCdj55428]

- At times, a Cisco 1000 series router sends SNMP queries to the next hop on the route instead of to the address configured in the SNMP server statement in the configuration. [CSCdj56216]
- The input queue may be wedged with IP packets if the **exception dump** command is configured.

The following are known workarounds:

- Increase the input queue to 175. ([75]Original Queue amount+[100] per **exception dump x.x.x.x** command)

- Remove the **exception dump x.x.x.x** command.

[CSCdj58035]

- When Frame Relay traffic shaping is enabled on a serial interface, disabling and reenabling weighted fair queuing will cause a system restart. [CSCdj58431]
- When a router is highly loaded and traffic-shaping is active on the outgoing interface, it might be possible that LMI control messages get queued in traffic-shaping queues, causing LMI protocol to go down. [CSCdj64221]
- When **frame-relay traffic-shaping** is enabled and the **clear counters** command is issued, the system may restart.

The workaround is to remove and then reenable **frame-relay traffic-shaping** to clear its counters. [CSCdj65742]

IBM Connectivity

- The APPN router may crash during an SNMP access to the APPN MIB. This problem occurs only after an unused APPN node is garbage-collected. The crash has the following backtrace:

```
System was restarted by bus error at PC 0x8B5902, address 0x4AFC4AFC PC:
process_snmp_trs_tg_inc

0x8B5CAC: _process_ms_data_req_trs(0x8b5aaa)+0x202
0x87E5FE: _xxxtos00(0x87d6b0)+0xf4e 0x180E5C: _process_hari_kari(0x180e5c)+0x0
```

[CSCdj36824]

- On RSP-based routers, the pseudo-MAC address assigned to a bridge port on a source-route bridge virtual ring group is incorrectly formatted to Ethernet format during Cisco IOS startup. This MAC address is used to establish a bridge link from IBM LAN Network Manager and can be shown by using the **show lnm config EXEC** command. [CSCdj38360]
- A downstream LU is unable to get the logo screen from the host even though other LUs on the downstream PU can. The router shows the DSPU state of that LU to be Reset or dsLUStart, while the host shows the state as Active. The LU is recovered by deactivating, then reactivating the LU at the host.

This state may occur if the downstream LU has previously failed to reply to ACTLU, or if the host has failed to respond to a NOTIFY (available or not available) from DSPU within a timeout period of 20 seconds.

Recovery requires the host operator to recycle the LU at the host. [CSCdj45783]

- When RSRB with TCP encapsulation is configured with priority peers and some of the priority peers are closed or dead, an explorer packet may continuously try to open the closed or dead priority peer. After several tries, the router may crash with memory corruption. [CSCdj47493]
- Executing a **show source** command may cause the router to restart unexpectedly if a virtual ring group or remote peer is deconfigured when the **source-bridge** command output is waiting at the **-- more --** prompt.

The workaround is to not reconfigure virtual rings or remote peers while executing a **show source** command. [CSCdj49973]

- Normal nonextended unbind (0x3201) was extended with corrupted information, which caused rejection by the host. As far as the host is concerned, the session is still active. A user cannot clean up this session without bringing down the link. [CSCdj50581]
- RIF may be modified incorrectly when multiring and SRB proxy explorer are configured on an interface but the SRB triplet is not configured, as shown in the following example:

```
interface TokenRing0/0
ip address <ip-address>
multiring ip
source-bridge proxy-explorer
```

Note the absence of the **source-bridge locRn bn remRn** command.

The **source-bridge proxy-explorer** statement does not show up in the configuration unless the SRB triplet is configured.

A workaround for this problem is to configure the **no source-bridge proxy-explorer** command. [CSCdj51631]

- When running proxy explorer and NetBIOS name caching on a Token Ring interface of a Cisco 7200, alignment errors occur. [CSCdj52522]
- A router may reload when removing configuration of X.25 PVCs for QLLC. [CSCdj57872]
- When an actpu is followed by a dactpu from VTAM and there is no response from the downstream device to either flow, after a disconnect is received from the downstream device, DLUR will send a -rsp(actpu) upstream instead of the proper flow, a +rsp(dactpu). This can cause the PU from the DLUS perspective to hang in the PDACP state. [CSCdj61872]
- It is rare, but possible, for DLUS to send a -rsp(REQDACTPU). When this happens, it indicates that VTAM has already cleaned up the PU in question. When receiving this response, DLUR must clean up the PU in order to keep the PU from being stuck in the “stopping” state. [CSCdj61879]
- When using APPN/DLUR with a large number of LUs (over 1000), a memory spike can occur during the processing of a downstream PU outage. In extreme cases, this memory spike can be large enough to exhaust memory in the APPN/DLUR router, which can cause a reload. [CSCdj61908]
- Session attempts fail with DLUR generating a sense 08060000 in a rare case where the LU name list gets corrupted. This problem is easily identified by the VTAM LU showing active state, while the **show appn dlur-lu name** display does not show the LU. [CSCdj62172]

Interfaces and Bridging

- When **ip route-cache cbus** is configured on an interface, intermittent router crashes could occur because of an incoherent cache entry data structure.

If this incoherency occurs and does not cause a router crash, it may instead cause cbus switching to be automatically disabled, and the interface resorts to fast switching (or SSE switching if SSE switching were also configured). [CSCdi43526]

- When adding to or removing a subinterface from a Frame Relay interface, all DLCIs are brought down until the Frame Relay switch sends the PVC information again. The whole interface resets when a user tries to add the **ip address** command. A workaround for part of the problem is to turn off CDP globally or on individual interfaces. In this case, turn off CDP on the serial interface before adding or removing subinterfaces. CSCdj02488 (integrated into Cisco IOS Release 11.1(11) and 11.2(5.1)) fixed the rest of the problem.[CSCdj07291]
- Under certain conditions, packets may stay on the input queue. The condition that caused packets to stay on the input queue has been removed. [CSCdj30087]
- When transparent bridging to a Token Ring interface, the interface can read in a frame it has forwarded onto the Token Ring interface. This will cause the bridge table to be incorrect. This problem affects only the mid-range and low-end platforms. [CSCdj41666]
- A Catalyst 5000 RSM populated with an ATM Port Adapter with LANE client(s) configured can get its ATM interface stuck in a down state if a user creates new VLAN interfaces.

Symptoms include the following message being displayed to the console:

```
%CBUS-3-CATMREJCMD: ATM0/0 Teardown VC command failed (error code 0x0008)
```

Saving the RSM configuration and reloading its image will clear the error condition.

[CSCdj41802]

- Compression for HDLC encapsulated bridging only payload compresses Spanning Protocol packets. Actual bridged packets are forwarded with their payloads uncompressed. Prior to this release, bridged packets may have had their MAC addresses corrupted if STAC compression was enabled with HDLC encapsulation. [CSCdj50894]
- In Cisco 7500 series routers, **sh dialer** is not working. The workaround is to use **sh dialer int serial x/y** . [CSCdj51612]
- A Cisco Catalyst 5000 cannot change packet format from SNAP to ARPA. [CSCdj53698]
- With IRB configured on the router, IPX clients cannot log into services on a bridged interface. Removing the IPX routing from the BVI fixes the bridged interface but you lose the routing. At this time, this feature is not supported. [CSCdj54050]
- If you are doing IRB with RFC1483 PVCs, you may see certain IP anomalies, such as ARP resolution not working or ARP resolutions taking place but you cannot ping the neighboring device. [CSCdj54558]
- AppleTalk might fail when packets are bridged through PPP transit. [CSCdj61857]

IP Routing Protocols

- A router may crash with a “System restarted by bus error at PC 0x60394488, address 0xD0D0D0D” message when running Cisco IOS 11.1(9) RSP with a heavy load of EIGRP and CSNA traffic. [CSCdj29447]
- If OSPF external routes are summarized using the **summary-address** command, and the number of external routes being covered by this summary address drops to zero, the external summary will be flushed, but the router originating the summary will not install any matching external or nssa routes that may be present in its database.

The router can be forced to install the matching route by using the **clear ip route *** command. [CSCdj32471]
- BOOTP requests being sent to 0.0.0.0 get forwarded to the gateway of last resort when there is one. [CSCdj33809]
- 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]
- A Cisco 7513 router running EIGRP reloads with the following message:

```
"System restarted by error - an arithmetic exception, PC 0x60286234"
```

The program counter value points to an EIGRP IOS routine. [CSCdj38361]
- Under some circumstances, the router will crash when removing a static IP route. [CSCdj45152]
- Multicast forwarding stops if fast-switching is turned on on an incoming ATM LANE subinterface. A workaround is to disable fast-switching on that interface by issuing the **no ip mroute-cache** command. [CSCdj45777]
- If the OSPF summary host route is overwritten by a route from another routing process which has lower administrative distance, it is possible that the OSPF summary host route will not be reinstalled after the latter route is removed. In particular, it only happens if the host route address is also the router ID of some ASBR. [CSCdj49161]
- Entering the **no ipx routing** command then enabling EIGRP can crash the router. This is a regression of CSCdj54141. [CSCdj53541]

- When one of the routers on a broadcast network has been partitioned in which at least one partition has only one router, OSPF will generate a stub advertisement for this network in the isolated router's router LSA. This stub route will overwrite the normal network route calculated using the network LSA, regardless of the path cost.

This problem exists in all releases starting with Release 10.3. This will be fixed in 11.1 and newer releases. [CSCdj53804]

- The Proteon router's internal address is advertised as a host route instead of a network in the router's LSA. A host route is represented as a Type 3 link (Stub Network) whose link ID is the host's IP address and whose link data is the mask of all ones (0xffffffff). This host route is advertised into all OSPF areas. [CSCdj56079]
- If you are doing IRB with RFC1483 PVCs, you may see certain IP anomalies such as ARP resolution not working or ARP resolutions taking place but you cannot ping the neighboring device. [CSCdj58194]
- Customer moved the IP multicast tunnels (DVMRP, GRE) from a serial interface to an ATM interface on a Cisco 4700 router. The packets are now process-switched instead of fast-switched, which causes a lot of CPU (IP INPUT).

When the serial interface is used for incoming packets and the ATM interface for outgoing packets, there is no problem. Incoming packets on the ATM interface and outgoing packets on the serial interface also experience this problem.

We used several Cisco IOS releases, with always the same effect. It seems that incoming packets are not fast switched. [CSCdj59076]

- SYS-3-CPUHOG error messages occurred after the software was upgraded from Release 11.0 to Release 11.2(8) or 11.2(9). The error messages may occur because the OSPF database refreshes every 30 minutes. This problem occurs with large IP OSPF networks with multiple areas. There is no known workaround. [CSCdj60461]
- The ARP lookup routine may suspend, causing unexpected behaviors for IP protocols. For example; if the OSPF routing process is traversing a list of neighbors to send LSA packets and the ARP routine is called, the ARP routine suspension could cause a system reset. The problem was resolved in Release 11.2(10a). [CSCdj60533]
- OSPF ABR does not generate a summary for some connected networks. This problem occurs when an unnumbered interface is used with OSPF. A summary for a connected network that is put in the same area as the unnumbered interface might not be generated to other areas.
The workaround is to redistribute the connected network into OSPF to retain connectivity to those networks. [CSCdj60959]
- Dynamic redistribution into EIGRP from another routing protocol fails if the routes being redistributed fall within the same major network as EIGRP. A temporary workaround is to remove the redistribution statement from the EIGRP configuration, then reinsert the redistribution statement. [CSCdj65737]

ISO CLNS

- Under certain circumstances, a Cisco 7505 router running Release 11.1(13a)CA1 reloads if the netID is changed under the IS-IS routing process. [CSCdj49485]

LLC Type 2

- If an RSRB session is disconnected by the local LAN side at exactly the same time as a data message is received from a remote host, a situation can occur which will lead to a crash in `llc_get_queue_status()`.

There is no workaround. [CSCdj62026]

Miscellaneous

- 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]

Novell IPX, XNS, and Apollo Domain

- Using any of the **xns flooding** commands may cause the router to reload and issue alignment, bad pool, or buffer warnings. [CSCdj23479]
- With LAPB/Frame Relay encapsulation, you might see “%SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level” messages on the console. It is possible (rarely) that an XNS connected route for this interface doesn’t get installed in the route table.

As a workaround, try one of the following:

- Issue the **shut** and **no shut** commands on the affected interface.
- Reconfigure the IPX network using the **no ipx network** command, followed by **ipx network**. [CSCdj53721]
- There are two problems associated with this caveat:
 - Sometimes a connected network does not appear in the routing table just after reload. Issuing the **shut** and **no shut** commands should correct the behavior.
 - If **ipx routing** is disabled (using the **no ipx routing** command), you could see something like a steady memory leak, unexpected router behavior, or a router crash. The only known resolution is to power cycle the router every time you issue the **no ipx routing** command. [CSCdj54141]
- If some interfaces change state when you disable and re-enable IPX/XNS routing, there is a possibility of losing the IPX/XNS background process.

Symptoms could be loss of network connectivity or a slow memory leak until the router cannot allocate any more memory. You need to reload the router to correct this situation. [CSCdj57257]

Wide-Area Networking

- With a router running NetBIOS Frames Protocol (NBF) over Token Ring, a device connected via async or ISDN with PPP encapsulation appears to connect successfully but is unable to see other NetBIOS devices in a domain. [CSCdi72429]
- VIP requires but does not have a mechanism to determine the health or status of a VIP card. Specifically, there needs to be a way to show tech-support, alignment, and logging information. The **show controllers** command should be extended to provide this information: **show controllers vip *x command*** where *x* is the VIP slot number and *command* is either tech-support, alignment, or logging. [CSCdj17006]

- A Cisco router running 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 stop making Frame Relay SVC calls after a long time. [CSCdj29722]
- 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. Because the profile is in standby mode, this behavior should not be possible. [CSCdj34108]
- Routers configured for Frame Relay switching will lose a **frame-relay route** command in the running configuration when the corresponding DLCI has been deleted. To restore the original configuration, execute the **copy start run** or **config memory** command or reload the router. [CSCdj43340]
- SSCOP sequence number is a 3-byte field. Because the SSCOP code in Cisco IOS Releases 11.0, 11.1, and 11.2 code does not handle the wraparound elegantly, in some conditions when the sequence number wraparound after exceeding the maximum of 16777215, a large number of buffers are queued and eventually cause the memory leak/starvation on the router. [CSCdj45157]
- Direct broadcast with the physical-broadcast destination MAC address is not forwarded to the helper address over ATM/LANE interface. [CSCdj51378]
- A router crashed with a bus error while running the output for **show dialer map**. [CSCdj52360]
- When a configuration of two systems has Frame Relay LMI timeouts set differently on DTE and DCE systems, the PVCs could remain active but no data is transferred because one system declared the connection inactive while the other system still thought it was active.
The workaround is to set the timeout values the same using the **lmi-t392dce** parameter. [CSCdj53354]
- If LES/BUS is configured on the Catalyst 5000, pulling down one client in the ELAN can affect other clients. This problem happens very rarely. The workaround is to restart the LES/BUS on the Catalyst 5000. [CSCdj54587]
- When a **static map** is deleted, calls associated with that map are not disconnected. For point-to-point calls, this does not cause any problems. However, for point-to-multipoint ATM calls, the leaf on the multipoint VC will be left in place. If the map to that same NSAP is replaced, a new call is attempted instead of reusing the existing leaf on the existing VC. The result is that an add-party message is delivered to the remote router and is subsequently rejected. The end result is no broadcast connectivity. The workaround is to clear the existing calls when changing the map configuration with a **clear int atm interface** command. [CSCdj57309]
- Cisco IOS Releases 11.2(1) through 11.2(10) are technically not in compliance with RFC 1990. The RFC requires that the first multilink fragment that is transmitted after adding a second link to a bundle which previously only had one link must be transmitted over the first link in the bundle. Instead, the first fragment is being transmitted over the newly added link. This can result in the peer receiving packets out of sequence.
There is no known workaround. [CSCdj57498]
- A Cisco 4000 Router reloads when **frame-relay traffic-shaping** is unconfigured. The only workaround is to destroy the configuration on the router, reload it, and restore the configuration. [CSCdj61097]
- Frame Relay is broken. Most of the protocols on Frame Relay may not work and packets may get dropped or misbehave because parsing of packets is not properly done in some cases. [CSCdj67384]

Caveats for Release 11.2(1) Through 11.2(9)

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

Basic System Services

- The following commands are not present:

— `copy bootflash {rcp | tftp}`

— `copy flash {rcp | tftp}`

The workaround for copying from flash to TFTP or RCP is to use the following command instead of a flash keyword:

`copy flash:<IOS filename {rcp | tftp}`

This does not work with bootflash however. [CSCdj38964]

- In extremely unusual situations the router displays the following error message on a frequent basis:

```
%SYS-6-STACKLOW: Stack for level CxBus Interfaces running low, 0/1000
```

The router might halt after displaying this message. [CSCdi54119]

- A timing conflict between the HTTP server and TACACS+ code can cause the HTTP process to hang when configured to use TACACS+ for authentication. Since the HTTP server uses a tty to handle I/O for the request, these hung processes can tie up all available ttys. [CSCdi84657]
- When custom or priority queuing is turned off on an interface that does not support fair queuing, the queuing data structures associated with the interface are left in an inconsistent state. In particular, the enqueue and the dequeue routines are not reset and this causes the system to crash when the routines are invoked the next time. Once the system is rebooted the inconsistency is cleared. [CSCdj29439]
- RMON alarms do not work properly on a number of MIBs that use internal MIB caching to speed up MIB object value retrieval. The only workaround is to set up an SNMP get poll on these objects to force an update to the MIB cache, with a poll period within the alarmInterval time. The following MIBs have this problem:

```
APPN-DLUR-MIB
IBM-6611-APPN-MIB
CISCO-CIPCSNA-MIB
CISCO-CIPLAN-MIB
CISCO-CIPTCPIP-MIB
CISCO-SNA-LLC-MIB
SNA-NAU-MIB
CISCO-TN3270SERVER-MIB
OLD-CISCO-IP-MIB
BGP4-MIB
LAN-EMULATION-CLIENT-MIB
RFC1406-MIB
RMON-MIB
IF-MIB
RFC1398-MIB
```

OLD-CISCO-INTERFACES-MIB
 CISCO-PING-MIB
 CISCO-QLLC01-MIB [CSCdj34766]

- A memory leak exists in the Flash file system. Using SNMP to poll the ciscoFlashMIB objects, or using the **show flash** command line interface (CLI) commands can result in non-trivial amounts of memory being allocated and never freed. Repeating these polls or CLI commands eventually results in the system using up all available memory. The ciscoFlashMIB can be disabled (SNMP is prevented from polling this MIB) using SNMP views. For example, the SNMP configuration **snmp-server community public ro** can be changed to the following:

```
snmp-server view no-flash internet included
snmp-server view no-flash ciscoFlashMIB excluded
snmp-server community public view no-flash ro
```

The result is the SNMP polls using the **public community** string can access objects in the entire MIB space (internet) except for those objects in the ciscoFlashMIB space. This affects any NMS applications that rely on the ciscoFlashMIB objects. [CSCdj35443]

- 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]
- An SNMP Get of an individual instance from the ipNetToMediaTable might fail, even though an SNMP Get-next successfully retrieves the instance. This might occur on table entries referring to software interfaces (for example, subinterfaces, loopbacks, or tunnels) or hardware interfaces that have been hot-swapped. There is no workaround. [CSCdj43639]
- A crash occurred in the Frame Relay packet classifier function called by the WFQ routine. A workaround for this problem is to disable WFQ on the interface with Frame Relay encapsulation. [CSCdj45516]

IBM Connectivity

- A small window exists in which it is possible after a transmission group reinitialization 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 only activates if the APPN subsystem is stopped and started. There is no workaround. [CSCdj25859]
- An APPN router might display the following “Unanticipated CP_STATUS” message when the contention loser CP-CP session goes down and comes back up without the contention winner 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 contention loser is stopped. To clear this problem, stop and restart the APPN subsystem. If the CP-CP sessions are between the router and the host, you can also clear this problem by terminating either CP-CP session on the host. [CSCdj33718]

- There might 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]
- An APPN DLUR router might reload with SegV exception in ndr_sndtp_encap_mu in a timing window where the DLUR supported device disconnects before a request_actpu is sent to the DLUS for that device. [CSCdj37172]
- A DSPU router with an SDLC attached 3174 leaves a terminal hung after a terminal power-reset. Vtam inact/act of LU fixes. A workaround is to remove the DWSPU and connect the 3174 via DLSw. [CSCdj37185]
- APPN enforces the maximum size of a CV10 (product set identifier) on XID to not exceed 60 bytes. Some products include a CV10 that is larger than the 60 byte value. These products fail XID negotiation with APPN. [CSCdj40144]
- In the event that APPN/DLUR has processed and sent a bind request to a downstream device and that device has not responded to the bind, issuing a **vary,inact** command on the host for the LU name for which that bind is destined does not completely clean up the session as it should. [CSCdj40147]
- When a connection is attempted over a port defined with the len-connection operand, APPN can loose 128 bytes of memory for each connection attempt. [CSCdj40190]
- DLSw FST might corrupt the frame header if the riflen is different on both sides. [CSCdj40582]
- Memory leaks occur when APPN TPsend_search is sending locate search requests to adjacent nodes when a link failure occurs. [CSCdj40915]
- When RSRB with TCP encapsulation is configured and remwait or dead peers exist, an explorer packet might continuously try to open the remwait or dead peer. After several tries, the router might crash with memory corruption. A workaround is to remove any remwait or dead peer statements. [CSCdj42427]
- An APPN router might crash with a bus error if a race condition is experienced during cleanup processing. The stacktrace shows the crash occurred in Qfind_front while executing a psp00 function. An example stacktrace for this problem is shown below.

```
System was restarted by bus error at PC 0x3784864, address 0xF0110208 PC
0x3784864[_Qfind_front(0x3040a04+0x743e44)+0x1c] RA:
0x36C1F2E[_queue_find_front(0x3040a04+0x68151c)+0xe] RA:
0x36CC554[_psbfrm(0x3040a04+0x68bb30)+0x20] RA:
0x36CDAF6[_psp00(0x3040a04+0x68cfd4)+0x11e] RA:
0x314BD78[_process_hari_kari(0x3040a04+0x10b374)+0x0] [CSCdj44198]
```

- APPN crashed when it received a CV35 without the Termination Procedure Origin Name (TPON) field. [CSCdj44661]
- Configuration of SRB on a second interface yields the following traceback information from LNM:

```
%LNM3-3-BADCLSIRET: bogus Invalid ret code (0x7007) init_clsi_op_proc, bogus
-Traceback= 60791120 6078FE48 6078FDC4 607890E0 6078ED48 60226648 60226634
[CSCdj45268]
```

- DLUR bind processing might cause stack corruption, resulting in a reload with PC 0x0. This problem is caused by attempting to parse the user data subfields beyond the location where the subfields exist. The reload only occurs if the byte that is two bytes beyond the end of the user data area is 0x3 or 0x4. This is a very rare occurrence. [CSCdj45676]
- In large APPN network environments over 200 NNs, numerous broadcast searches could happen during initial start up or intermediate links recovery. The memory usage surge might bring down the entire network. [CSCdj45705]
- The message “%APPN-0-APPNEMERG: Mfreeing bad storage, addr = 60BB7188, header = 60BB6B20, 00000218 -Process= “ndrmain”, ipl= 0, pid= 62” might be issued when a DLUR served PU disconnects. [CSCdj46783]
- A router does not pass SRB directed frames if the SRB proxy-explorer feature is configured. The SRB proxy-explorer is used with NetBIOS name caching. [CSCdj47797]
- Some 68K-based routers might crash while running APPN. This memory corruption might occur after a rare combination of APPN detail displays, followed by a **show appn stat** display. [CSCdj47941]
- When enabling source bridge translational bridging feature, the router runs out of I/O memory caused by a buffer leak in the small and the middle buffers. The workaround is to disable sr/tlb. [CSCdj49533]

Interfaces and Bridging

- In certain cases, a router might bring Layer 1 down without an apparent reason. Hereafter, a new TEI is negotiated with the switch. The latter still keeps all call references belonging to the previous TEI, since no DISCONNECT is seen on L3. [CSCdj11840]
- An SNMP agent might return erroneous values, and under some conditions the ifInUcastPkts counter returns decreasing values, which is incorrect. [CSCdj23790]
- The Internal Clock of ATM-lite is not initialized properly. This causes loopback ping to fail because there is no clock. [CSCdj24890]
- PPP compression and custom queuing are incompatible features and might cause the router to crash. To work around this problem, turn off all fancy queuing. [CSCdj25503]
- In X.25 packet-by-packet compression, error checking code is fixed after malloc for decompression history buffer. [CSCdj29139]
- dot5StatsTable does not return any value in Cisco IOS Release 11.2 software. [CSCdj32372]
- NFS transmission problems and FDDI excessive claims occur after installing Releases 10.3(9) through 10.3(18), 11.1(9) through 11.1(14), or 11.2(1) through 11.2(9). This problem is specific to the CX-FIP interface board. [CSCdj38715]
- An NT client/server sending out multiple ARP requests to the BVI interface of the router causes a loss of connection. The workaround is to enable ARP SNAP **arp timeout 120**. [CSCdj46855]
- The PA-4R might incorrectly adjust the datagram size of an incoming packet to include extra padding at the end of the packet. This problem only occurs under moderate or heavy traffic load where multiple PA-4R interfaces are consuming many particle buffers. The problem also only occurs for packets with a packet length that is a multiple of 512 bytes, 513 bytes, 514 bytes or 515 bytes. The only workaround is to reduce the token ring interface’s MTU to 508 bytes or less. [CSCdj48183]
- The ATM lite port adapter on the VIP2 platform does not function. The interface repeatedly goes up and down and does not have any output. [CSCdj51923]

- When connecting a Canary Fast Ethernet transceiver to the MII connector on VIP port adapters, reload the microcode so that the port functions properly. [CSCdi64606]
- The auto-enable feature for packet-by-packet Frame Relay compression is removed and this form of compression is allowed to be manually enabled. [CSCdi85183]

IP Routing Protocols

- A routing node is removed from the IP cache Radix tree and the buffer is set free, but it can still be traversed from the treetop and cause a crash (it can still be accessed after it is set free). [CSCdj17314]
- IP cache is not invalidated for destinations that use the default routes even after the next hop is down. The workaround is to issue the **clear ip cache** command. [CSCdj26446]
- After the **ip default-network** statement is issued, the default network route is not propagated to other routers in the network. There is no workaround for this problem. [CSCdj28362]
- EIGRP topology entries from the redistribution of connected routes where EIGRP is already running natively might not clear when an interface goes down. [CSCdj28874]
- A router crashes after receiving multicast packets with the illegal source address 0.0.0.0. The workaround is to configure the access list to filter out packets with a source IP address of 0.0.0.0. [CSCdj32995]
- When the OSPF interface command **ip ospf authentication-key** *key* is configured with a key length longer than 19 characters including any trailing space, OSPF internal data is corrupted. The **write terminal** command might reload the router. The workaround is to not enter a key longer than 19 characters, regardless of whether or not it is encrypted. The same problem occurs with the **ip ospf message-digest** *key-id* **md5** *key* command. In this case, the key length should not be longer than 36 characters. [CSCdj37583]
- After the **aggregate-address summary-only** command is configured, issuing the same command without **summary-only** does not unsuppress the more specifics of the aggregate. A workaround is to negate the whole **aggregate-address** command first. [CSCdj42066]
- ICMP that cannot be reached are incorrectly sent out for multicast packets. [CSCdj43447]
- During a ping, each packet takes more than two seconds to be output. With ATM static maps, the wait is not necessary for IP over ATM. [CSCdj47856]
- Entering the no **ip gdb rip** command twice might crash the router. [CSCdj48291]

LAT

- The following message might be erroneously displayed:

```
%LAT-3-BADDATA: Tty124, Data pointer does not correspond to current packet
```

When many LAT sessions are active, and a received data slot starts in the last 14 bytes of a full Ethernet frame, data for that slot is discarded. [CSCdi82343]

Novell IPX, XNS, and Apollo Domain

- A route might become stuck in a “deletion pending” state after an **ipx down** command. This could occur if you issue the commands **ipx down** and **no ipx network** in the same or reverse order, with very little time between them. The workaround is to disable and reenab IPX routing on the router. [CSCdi91755]

- XNS routes might get deleted on serial interfaces at boot time. The workaround is to issue the **shut** and **no shut** commands on the affected interface. [CSCdj25806]
- IPX does not advertise static or floating static routes if they are created before the interface that the routes connected to is up. The workaround is to issue the **shut** and **no shut** commands on the interface to which the static or floating static routes are connected. [CSCdj41584]
- Running IPX EIGRP with a maximum path set greater than one, the router might not remove the SAP after the interface is down if it is learned via more than one path. [CSCdj45364]
- If a route goes away via aging (180 seconds) and the default route is known, a cache entry might be installed for the network using the default route path. If the network comes back within the next 60 seconds, a new cache entry pointing to the now valid path might not be installed and the cache still points to the default route path for the network. A workaround is to issue the **clear ipx route** and **clear ipx cache** commands, or run without using the default route. [CSCdj47705]

TCP/IP Host-Mode Services

- A router might restart with a bus error at address 0xD0D0D5D in module tcpdriver_del. [CSCdj26703]

VINES

- A router might unexpectedly reload when VINES SRTP routing is configured. The workaround is to remove the **vines srtp-enabled** command. [CSCdj37888]

Wide-Area Networking

- Under certain conditions, a router might reload during an ISDN call setup with the SPC bit set. This problem only occurs with 1TR6 ISDN switch types. [CSCdj20841]
- While using Distributed Fast Switching, buffer headers can be stranded in the outgoing VIPs transmit queue when that interface has been taken down. This is more likely to occur when a faster interface is switching to a slower one. Ignores and drops might increase on the input interface as it fails to obtain a needed buffer header to switch the packet. The rxcurr on the input interface also remains above rxlow even when traffic is not arriving on the interface. The VIP continues to drain the transmit queue of the interface even when it is administratively down. This allows the buffer headers to be returned to the originating local free queue. This might cause the number of drops on outbound interface to increase significantly when the interface is taken down. However, this behavior is normal as the downed interface drops any packets sent to it when it is not up. [CSCdj21693]
- The Frame Relay LMI Enquiry and Status messages stop being exchanged after a short time of successful communication. The statistics incorrectly report timeouts and message activity. [CSCdj31567]
- If a BRI port attached to an NI-1 ISDN switch using two SPIDs gets a Layer 1 deactivation and reactivation (typically due to adverse line conditions or temporary disconnection of the cable), that port might not be able to reestablish Layer 2 connectivity on the second TEI and, therefore, not be able to use the second B channel. Issuing the **show isdn status** command reports TEI_ASSIGNED on one of the TEIs instead of MULTIPLE_FRAME_ESTABLISHED on both. A workaround is to have your service provider configure a single SPID that can control two B channels. [CSCdj41311]

- Using NetBIOS over PPP might result in traceback messages complaining about invalid memory action at interrupt with traceback information appended:

```
%SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level
```


[CSCdj42341]
- This patch prevents the use of an invalid pak-info_start pointer when doing payload compression on RSP platforms, thus avoiding a crash. [CSCdj43332]
- The router configured with “isdn incoming-voice data 56” might wrongfully treat an incoming voice call as 64 kbps. [CSCdj43717]
- When ATM-lite is the third of three fast PAs on a NPE-150, its rx pool is be forced to operate out of DRAM. When ATM-lite is running in a NPE-100, where it is designed to operate out of DRAM. Sometimes packets that are to be handled at the process level appear in the wrong queues. For example, a routing packet might end up in a SSCOP queue or a LANE queue, causing the SSCOP or LANE to operate abnormally or result in interface flapping. [CSCdj46634]
- An ATM Lite connected to a Newbridge causes the laser to shut down after 8 seconds for 2 seconds. The workaround is to replace the ATM Lite with AIP. [CSCdj46914]
- A remote DLSw peering router might send a DM response just after the LLC2 connection is established if the router is very busy and the PC station responds immediately to the UA with a RR. The client needs to reestablish the connection. [CSCdj47782]
- A boot image without a subsystem containing IPCP restarts a router. [CSCdj48085]
- When using the **frame-relay map class** or **frame-relay traffic-rate** commands, and when the rate is being reduced in response to BECN, the default lower limit is zero, while the expected default is CIR/2. The workaround for this behavior is to define the rate using the CIR/BC/BE parameters. [CSCdj49145]
- The router might unexpectedly restart when configuring an X.25 PVC that is locally switched. [CSCdj49828]

The **show x25 vc** command will cause the router to unexpectedly restart if there is a combination of locally switched virtual circuits and other virtual circuits. [CSCdj50405]

Caveats for Release 11.2(1) Through 11.2(8)

This section describes possibly unexpected behavior by Release 11.2(8). Unless otherwise noted, these caveats apply to Release 11.2 up to and including 11.2(8). The caveats listed here describe only the serious problems. For the complete list of caveats against Release 11.2, use the Documentation CD-ROM or access CCO as described in the section “Cisco Connection Online” later in this document.

Access Server

- A reload might occur if the command **show modem slot/modem-port** is issued when the associated modem is in the autoconfigure mode. Autoconfigure mode is normally a short interval during which the modem is reset and reinitialized by the **modem autoconfigure** command. [CSCdj17224]

AppleTalk

- ATCP might cause AppleTalk to corrupt memory and reload the router. There is no workaround. [CSCdj23355]

Basic System Services

- Connected routes stay in the routing table when a card is disabled and in an analyzed wedged state. [CSCdj08355]
- The error “System restarted by bus error at invalid address” is caused by intermittent Telnet sessions on a Cisco AS500 platform running Cisco IOS Release 11.1(10)AA. This problem occurs because of a race condition when doing DNS name query, and DNS name cache is removed in the middle of the process.

There is no workaround on the router side. On the DNS server side, configuring DNS TTL to be one minute or longer might work around this problem. However, this workaround might not be acceptable for some applications. [CSCdj16824]

- This bug might be user specific; the following error message occurs when a user’s script executes the **show start** command:

```
% Non-volatile configuration memory has not been set up
```

The user’s script is used to change passwords. Current testing indicates that it might be a software checksum error. [CSCdj18107]

- During a boot Flash format, systems with earlier release images will not recognize Intel boot Flash SIMMs 28F004S5 (device code A7), 28F008S5 (device code A6), and 28F016S5 (device code 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. [CSCdj20681]

- On RSP-based platforms, the following error might occur, indicating a problem with a hardware enqueue:

```
%RSP-2-QAERROR: reused or zero link error, write at addr 00C0 (QA) log 2600C040, data 00070000 00000000
```

This message might be followed by the following error and a crash:

```
Unexpected exception, CPU signal 10, PC = 0x601C4658
```

This message is caused by a memory access problem in the diagnostic code handling the original QA error. [CSCdj29751]

- The object `cmInitialLineConnections` in the `CISCO-MODEM-MGMT-MIB` is supposed to return only non-zero values. The current implementation returns all counter values, including zeroes. This problem is not serious if only single-valued SNMP retrievals (`getone...`) of **cmInitialLineConnections** are performed. In actuality, SNMP retrievals of multiple values (`getmany...`) are often used. The problem is much more pronounced in the second case. [CSCdj30171]

- A memory leak exists in the Flash filesystem. Using SNMP to poll the `ciscoFlashMIB` objects, or using the **show flash** command line interface (CLI) commands can result in non-trivial amounts of memory being allocated and never freed. Repeating these polls or CLI commands eventually results in the system using up all available memory.

The `ciscoFlashMIB` can essentially be disabled (SNMP is prevented from polling this MIB) via use of SNMP views. For example, the SNMP configuration **snmp-server community public ro** can be changed to the following:

```
snmp-server view no-flash internet included
snmp-server view no-flash ciscoFlashMIB excluded
snmp-server community public view no-flash ro
```

The result is the SNMP polls using the **public community** string can access objects in the entire MIB space (internet) except for those objects in the ciscoFlashMIB space. This affects any NMS applications that rely on the ciscoFlashMIB objects. [CSCdj35443]

- When inbound PAP authentication is configured to use TACACS+ with a down-rev daemon (for example, Freeware 2.1) the system leaks one TACACS+ packet for every PAP authentication it performs. Upgrading to a daemon that understands the latest version of the TACACS+ protocol (version 193) is an effective workaround. [CSCdj36449]

EXEC and Configuration Parser

- Entering the **privilege route-map level *x* set as-path prepend *x*** command in configure mode might cause the router to reload, even though the number after **prepend** is not necessary. To work around this problem, do not enter a number after **prepend**. [CSCdj37035]

IBM Connectivity

- QLLC/RSRB forwards IEEE XID frames like other XID frames to VTAM. Some devices use IEEE XID frames (format 8, type 1) instead of test frames. [CSCdi86682]
- Issuing the **show lnm station** command might cause the routers to reload, especially when the stations are getting in and out of the ring. [CSCdj09905]
- When SRB and transparent bridging are both configured on two interfaces, Sr frames with an Ethernet type of 0x600 or 0x800 are not forwarded and do not show up as source errors. This problem first appeared in Cisco IOS Release 11.1(12). [CSCdj18483]
- Continuously issuing the **appn ping** command causes the router to hang indefinitely. [CSCdj19525]
- The router might reload unexpectedly with a stack trace pointing to llc2_timer. [CSCdj21370]
- When RSRB with TCP encapsulation is configured and there are dead peers, an explorer packet might continuously try to open the dead peer. After several tries, the router might crash with memory corruption. The workaround is to remove any dead peer statements. [CSCdj24658]
- When using promiscuous or peer-on-demand peers and there are more than 100 circuits connected, a memory corruption crash might result when the promiscuous or peer-on-demand peers disconnect. The corruption occurs when circuit cleanup is delayed due to end station delay, LAN network delay, or high router CPU usage. [CSCdj26284]

An APPN image might restart because of a CPU HOG problem when processing a link failure event by the Directory Service APPN process (xxxdns00). This might occur when a lot of locate requests are pending. There is no known workaround. The router is forced to restart by the system watchdog process (software-forced reload event). [CSCdj26423]

- DLSw local-switching from VDLC to LLC media does not work correctly. [CSCdj28900]
- The timer that controls the daily cleanup of APPN topology and the 5-day rebroadcast of topology resources owned by this APPN node can fail after 45 days. At this time, other nodes where the timer is still functioning properly might age out the topology of the node with the failed timer after 15 days. Thus, after a total of 60 days, APPN routing failures and failed CP-CP sessions might result between APPN network nodes.

Because other network events (link outages, and so forth) can trigger a node to send a TDU, this problem might not appear after a 60-day uptime—it might occur much later or not at all. However, any APPN router running in the network for over 60 days is at risk of experiencing this problem.

Stopping and restarting APPN is a workaround for this problem until the next timer wrap, which can be up to 45 days, but might be less depending on the current value of the timer. Reloading the router will reset the timer and avoid the problem for an additional 60 days. [CSCdj29014]

- A router configured for RSRB might crash with a watchdog timeout during low memory conditions and/or continual peer state changes. [CSCdj30381]
- A DLUR router might reject unbind requests from the host if it has not received a bind response from the downstream LU.

If the downstream device never responds to the outstanding bind, the DLUR router will wait indefinitely and not free the local-form session ID (lfsid). This might cause a situation in which the host tries to reuse an lfsid after it has sent an unbind request, but the DLUR rejects the new bind request because it believes that this lfsid is in use. If the host continuously tries to use the lfsid that the DLUR believes is in use, no new sessions can be established. This problem occurs only when the downstream device does not respond to a bind request. [CSCdj30386]

- Sometimes linkstations might get stuck in a XIDSENT state when an APPN linkstation fails and recovery is attempted. Caveat CSCdi77040 provides a fix for this problem on the system side. This caveat provides the corresponding fix for APPN. [CSCdj30552]
- When using APPN/DLUR with the **prefer-active-dlus** configuration command specified on the APPN control point, DLUR might not properly connect to a backup DLUS in cases where the primary DLUS is available in the network but has the served PUs varied inactive. [CSCdj31261]
- When using the **len-connection** configuration command on the APPN port and there are at least 30 XID3 devices connecting in through that port, a rare sequence of events of devices connecting and reconnecting can cause a reload. [CSCdj31264]
- Any device connecting to APPN/DLUR that does not carry a cv0E with a CPname specified on XID (any PU2.0 and some older PU2.1 implementations) causes APPN to fail to release 536 bytes of memory each time the device disconnects and reconnects. Any device connecting on a port with LEN-connection defined also exhibits this behavior. When memory is exhausted, the APPN subsystem might stop or the router might reload. [CSCdj33429]
- An APPN router might display the following “Unanticipated CP_STATUS” message when the contention loser CP-CP session goes down and comes back up without the contention winner 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 contention loser 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]

- When an LLC2 connection is configured to work over ATM LANE for DLSW, the connection succeeds until a retransmission is required, at which time it fails. [CSCdj34873]

- A user is unable to enter an XID option on an interface configured for QLLC and DLSW. [CSCdj35448]
- If the DLUR router received fixed session-level pacing values on the primary stage, it might modify these pacing values before forwarding the bind to the secondary stage. [CSCdj36195]
- The router might reload when reverse-QLLC connections disconnect using QLLC/DLSw+. [CSCdj36613]
- A problem occurs when an LU node specific node attempts to start a session with a set of invalid bind parameters. This results in a locate-find (with the bind in the CDINIT) being sent through the Cisco APPN network to the end VTAM CP. The end VTAM CP rejects the locate-find with a 0835003A sense and sends this back with a control vector CV35 of minimum length of 8 bytes to the originator via the Cisco APPN NN. The APPN NN then rejects the frame with a 08953500 sense and drops the CP-CP session between the Cisco router and VTAM CPs. [CSCdj37479]

Interfaces and Bridging

- Issuing the **no channel-group** command on a MultiChannel Interface Processor (MIP) causes the router to reload if OSPF is configured. [CSCdi79844]
- Bridging from a serial interface to a Fast Ethernet interface with ISL encapsulation fails because the serial input queue is not cleaned up. [CSCdj01443]
- When bridging IP and routing AppleTalk, assigning the bridge-group to the LEX interface causes AARP entries to disappear and become no longer resolved. [CSCdj22825]
- In X.25 packet by packet compression, error checking code is fixed after malloc for the decompression history buffer. [CSCdj29139]

IP Routing Protocols

- Under unusual circumstances, EIGRP might reinitialize multiple peers when a stuck-in-active condition occurs, instead of just the peer through which the route was stuck. [CSCdi83660]
- Under certain circumstances, if a Cisco router receives a route with a lower rip2 metric, the router might go into a hold-down state with an infinite metric. [CSCdj15295]
- Under certain circumstances, a Cisco router interprets an IP packet broadcast at the link-layer as an IP-directed broadcast. When the router determines that the original packet was a directed broadcast, it forwards the packet to any other interfaces that belong to the directed broadcast address because Cisco routers forward directed broadcasts by default. Though the destination IP address of the original packet appears to be that of a directed broadcast, the router should not forward the packet, since it is actually a link-layer broadcast. [CSCdj16052]
- A router might crash after the fifth EIGRP process is configured. CSCdi36031 is a related caveat. [CSCdj17508]
- An IP cache is not invalidated for destinations that use the default routes even after the next hop is down. The workaround is to use the **clear ip cache** command. [CSCdj26446]
- Major net summarization is incorrectly done if there are two equal cost direct connect interfaces. To work around this problem, use the **clear ip route *** command. [CSCdj30971]
- Dense mode interfaces are not always populated in the outgoing interfaces of a multicast route. This problem was introduced by CSCdi25373. [CSCdj32187]
- When doing a trace route from a router to a broadcast network address, NO ICMP TTL Exceeded is sent back by the next hop Cisco router. [CSCdj33761]

- An old incoming interface is not populated in the OIF during RPF transitions. [CSCdj34457]

ISO CLNS

- CLNS fast switching is not working between PVCs defined on ATM subinterfaces. [CSCdj23817]

LAT

- When performing protocol translation from X.25 to LAT, spurious memory accesses might be seen in console messages as well as in the output from the **show alignment EXEC** command. [CSCdj18470]

Novell IPX, XNS, and Apollo Domain

- IPX fast switching might fail over a PRI interface, resulting in IPX client connections not being established over the PRI even though the IPX servers are visible. The workaround is to configure **no ipx route-cache** on the PRI interface. [CSCdj29133]
- XNS does not learn the new non-canonical format of Token Ring MAC addresses. It retains the old canonical format address for its node address. This would cause routing failure. The workaround is to disable and reenables XNS network on all the Token Ring interfaces. This affects only RSP platforms and when you upgrade an XNS configured router from a version that has the bug CSCdi48110 to a version that has this bug fixed. [CSCdj29916]
- The **ipx nlsr** command *tag* option is not being displayed as an option, making routing between NLSP areas impossible. [CSCdj33746]

TCP/IP Host-Mode Services

- An interface might become wedged with input queue 76/75. This is caused by both syslog and SNMP traps. The workaround is to disable both syslog and SNMP traps using the commands **no snmp-server host ip-address** and **no logging ip-address**. [CSCdj27567]
- New TCP connections might become stuck in SYNSENT state when router is low on memory. [CSCdj30008]

TN3270

- International (8-bit) characters do not echo when using TN3270. [CSCdj22231]

VINES

- Issuing the **write memory** command might cause the system to reload while writing the VINES access list to memory. Issuing the **write terminal** or **show vines access** commands might also halt the system. The workaround is to delete the configuration file and reconfigure the system. [CSCdi49737]

Wide-Area Networking

- CMNS connections might suffer spurious X.25 resets under traffic load. [CSCdi40875]

- There is a problem that only affects the PPP reliable protocol. No other protocols are affected, such as HDLC. [CSCdi70242]
- A BRI interface with Frame Relay encapsulation configured does not function correctly. A call stays up for a few seconds, LMI messages are exchanged, and as soon as the DLCI goes from INACTIVE to DELETED, the BRI is physically reset. Therefore, it is impossible to use Frame Relay over ISDN. [CSCdj09661]
- When a router receives a valid Frame Relay Setup message while the local SVC's map-class is not yet properly configured, the router crashes. The crash point and the stack trace might be like one of the following:

```
Current PC: 0x90F61C[bcopy(0x90f56c)+0xb0] FP:
0xCC65C4[_etext(0x96f3ec)+0x3571d8] RA:
0x5E1EF2[_fr_svc_send_msg_to_nli(0x5e1eca)+0x28] FP:
0xCC65E8[_etext(0x96f3ec)+0x3571fc] RA: 0x5DD98C[_FRU0_Setup(0x5dd8e2)+0xaa] FP:
0xCC6620[_etext(0x96f3ec)+0x357234] RA:
0x5DD894[_svc_process_l3_event(0x5dd786)+0x10e] FP:
0xCC6664[_etext(0x96f3ec)+0x357278] RA: 0x5DA17A[_l3_ie_parse(0x5d9d32)+0x448]
FP: 0xCC66A4[_etext(0x96f3ec)+0x3572b8] RA:
0x5D9B84[_l3_ie_parse_process(0x5d9b14)+0x70] FP:
0xCC66C0[_etext(0x96f3ec)+0x3572d4] RA:
0x1CC372[_process_hari_kari(0x1cc372)+0x0]
```

```
Current PC: 0x5E1D8E[_fr_svc_call_id_to_nli(0x5e1cf0)+0x9e] FP:
0xCC5CCC[_etext(0x970900)+0x3553cc] RA:
0x5E2176[_fr_svc_send_msg_to_nli(0x5e214e)+0x28] FP:
0xCC5CF0[_etext(0x970900)+0x3553f0] RA: 0x5DDC10[_FRU0_Setup(0x5ddb66)+0xaa] FP:
0xCC5D28[_etext(0x970900)+0x355428] RA:
0x5DDB18[_svc_process_l3_event(0x5dda0a)+0x10e] FP:
0xCC5D6C[_etext(0x970900)+0x35546c] RA: 0x5DA3FE[_l3_ie_parse(0x5d9fb6)+0x448]
FP: 0xCC5DAC[_etext(0x970900)+0x3554ac] RA:
0x5D9E08[_l3_ie_parse_process(0x5d9d98)+0x70] FP:
0xCC5DC8[_etext(0x970900)+0x3554c8] RA:
0x1CC3BA[_process_hari_kari(0x1cc3ba)+0x0] [CSCdj13019]
```

- Packets that are exactly the size of the MAC encapsulation size are not bridged. This means that TEST and XID frames are not be bridged. Instead, they are passed up to the process level, which responds to them. [CSCdj14748]
- The MAC address of an ATM interface in a router, instead of the actual MAC address of an end station connected to a LANE client, is entered in the ARP cache. This problem occurs after several hours. A temporary workaround is to clear the ARP cache of the router. Other workarounds include removing bridging from LANE subinterfaces, disabling proxy ARP or correctly configuring the subnet mask of end stations in a LANE environment. [CSCdj19293]
- The output of the **show dialer** command shows that the “dialer state is call pending” and the dialer could not be used after it received a call from the destination. This caveat could be related to CSCdi80876. [CSCdj19790]

Upon bootup, OIR, microcode reload, and cbus complex restarts, the router shows CCBTIMEOUT error messages on VIPs that result in a disabled wedged status. This problem occurs with bad PAs and PAs in a “not-ready” state. The cause of the problem is when PCI access is tried and the PA does not respond, thus resulting in CCBTIMEOUTS. [CSCdj21639]

- When per VC custom or priority queuing is configured prior to the initialization of the VC, the functionality is not correctly initialized and is not activated. [CSCdj28240]
- Use of IPX with very large packet sizes might result in a memory leak when transmitting packets via PPP multilink. [CSCdj29387]

- ATCP negotiation fails when an ARAP 3.0f1c4 client attempts to connect to a Cisco access server. This was found during Beta testing of the ARAP 3.0 software. The actual ARAP protocol works fine; it is only ATCP that fails. [CSCdj31323]

Caveats for Release 11.2(1) Through 11.2(4)

This section describes possibly unexpected behavior by Release 11.2(4). Unless otherwise noted, these caveats apply to Release 11.2 up to and including 11.2(4). The caveats listed here describe only the serious problems. For the complete list of caveats against Release 11.2, use the Documentation CD-ROM or access CCO as described in the section “Cisco Connection Online” later in this document.

Basic System Services

- On RSP systems, the router reloads with a SegV error when trying to free a misqueued buffer or a buffer that is an invalid size. The buffer might contain a bad packet passed to it from another router. [CSCdi74039]
- Ethernet interfaces might experience XBUFHDR and INVRTN errors. [CSCdi75404]
- On RSP systems with HIP, TRIP, or FIP interfaces, when the MTU is larger than 4096 bytes on TRIP or FIP interfaces or larger than 8192 on HIP interfaces, there is a rare chance that a system error might occur. When this happens, the message “CYBus error 8” or “CYBus error 10” is displayed. [CSCdi75522]
- The router might reload inadvertently if you respond improperly to extended ping dialog prompts. [CSCdi88443]
- A memory leak occurs whenever TACACS+ is enabled. Memory is released to the EXEC process as seen via the **show memory** command. The leak appears to have originated in Release 11.0(10) and affects Cisco IOS software released thereafter. [CSCdi89479]
- Under some circumstances, processing an SNMP Get request might result in a message similar to the following being displayed on the console:


```
%SNMP-3-CPUHOG: Processing Get of lifEntry.75.34
```

 [CSCdi93084]
- SNMP traps process can consume memory if presented with a large number of traps to deliver. [CSCdj02181]
- Under unknown circumstances, the router might restart due to a Bus Error. [CSCdj02493]

Interfaces and Bridging

- The **show** diagnostic command does not display Fast Ethernet Interface Processor port adapter information. [CSCdi33967]
- A problem occurs when performing a *getnext* operation on the *dot1dTpFdbTable* in the Bridge MIB. A *getnext* will not retrieve a request of index + 1 and will instead return the lexicographically next index. An example of this behavior follows:

If the table has the entries with indices of:

```
0000.0000.0001 0000.0000.0002 0000.0000.0003 0000.0000.0005
```

a *getnext* of 0000.0000.0002 returns the index 0000.0000.0005 because 0000.0000.0003 is the index requested + 1

a *getnext* of 0000.0000.0003 returns the index 0000.0000.0005 because 0000.0000.0005 is greater than the requested index + 1. [CSCdi84559]

- A problem occurs when the router is configured for Integrated Routing and Bridging (IRB). The problem affects all platforms. A bad decision in the forwarding of packets whose destination is not in the bridge table could cause the router to reload. [CSCdi92194]

IP Routing Protocols

- IGMP and PIM should support multicast addresses (for example, c000.0004.0000) as configurable options on Token Ring interfaces instead of requiring broadcast address (for example, ffff.ffff.ffff). [CSCdi83845]
- Configuring OSPF NSSA (Not So Stubby Areas) can affect the way routes are redistributed into OSPF. This defect was first observed in Release 11.2(3). [CSCdi88321]
- A prefix that has the “no-export” community string set from an inbound route map is incorrectly advertised to EBGp peers. A workaround is to configure a route map to set “no-export” community on the outbound side of the peering router instead. [CSCdj01351]
- It is possible for memory corruption and memory leaks to occur when PIM packets are sent. [CSCdj02092]
- Under certain timing-related circumstances, the use of per-user routes might cause a router to reload when the interface that caused the routes to be installed goes down. This is because both the IP background process and the per-user code attempt to remove this route. [CSCdj02347]

ISO CLNS

- If minimum-sized (or sweeping-sized) CLNS pings are performed and the CLNS source and destination addresses are very long, the system may fail. The workaround is to raise the minimum ping size to at least 63 bytes. [CSCdi91040]

Novell IPX, XNS, and Apollo Domain

- When a device running LANE is configured as a LEC, it does not acknowledge any secondary IPX networks with frame types different from the primary. The **debug ipx packet** command displays these received packets as “bad pkt.” Only packets that arrive with the same IPX frame type as the primary IPX network on the ATM interface of the router are properly accepted. [CSCdi85215]
- In a redundant IPX Enhanced IGRP network running IPX incremental SAP, the router’s SAP table may contain out of date information, such as the socket number if the socket number was changed from its initial advertisement. [CSCdi85953]
- SPX keepalive spoofing will cease to spoof after a router has been up for 24 days or longer. The **debug ipx spx-spoof** command shows packets being skipped at the time when they should be spoofed. The only workaround is to reload the router once every three weeks. [CSCdi86079]
- XNS RIP requests for all networks cause normal periodic RIP updates to be delayed or skipped. [CSCdi90419]
- When IPX incremental SAP is running, the router’s SAP table might not contain all the SAPs in the network if one of its interfaces goes down and comes back up later. [CSCdi90899]
- When running IPX incremental SAP, the router might not remove all the SAPs that are no longer reachable via this router. [CSCdi90907]

TCP/IP Host-Mode Services

- A Telnet session with a nonzero number of unread input bytes cannot be cleared. [CSCdi88267]
- IP packets with valid TTLs (of varying values) received on a VIP2 serial port adapter or FSIP (both on RSP2 platform) with TCP header compression are intermittently dropped. The router sends an ICMP Time Exceeded message to the source.
- The **show ip traffic** command indicates that the ICMP Time Exceeded counter increments.
A workaround is to turn off TCP header compression. [CSCdj01681]

Wide-Area Networking

- In certain environments, I/O and processor memory are being consumed by processes in the router, primarily the Critical Background process, and the router runs out of memory after 29 hours of operation. [CSCdi80450]
- When using a 4ESS PRI to place an international call (011), the call might be rejected with the error “cause i = 0x839C - invalid number format.” [CSCdi81069]
- Using the command **no pri-group** while traffic is being passed can result in a bus error. The command may be used safely when no traffic is being passed. [CSCdi82055]
- The **dialer hold-queue** command does not queue packets when it is used with dialer profiles. As a workaround, use the legacy DDR configuration instead of dialer profiles. [CSCdi84272]
- Random restarts because of bus errors occur at least two to three times per day. The problem might be in the DDR software. [CSCdi86765]
- When TEST/XID packets are received by a LANE client, the router might crash. There is no workaround for this problem. [CSCdi90868]
- Under heavy call volume, the router might not return memory to the free pool when it is no longer needed. This will eventually result in a low-memory or no-memory condition, which might manifest itself in several different error messages. [CSCdj02481]

EXEC and Configuration Parser

- When you change the encapsulation on an interface from one that supports weighted fair queueing to one that does not and you make the change from the console or aux port, there can be a memory loss of 8 KB each time you change the encapsulation. You can identify this problem by examining the output of the **show memory allocating-process** command, which shows that the number of memory blocks allocated by the exec increases each time you change the encapsulation. If you do not change the encapsulation on an interface often, this problem should not have a significant impact on system performance. [CSCdi89723]

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 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 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>.

Depending on which release of software is running on your router, use this document in conjunction with the Cisco IOS Release 11.2 configuration guides and command references.

AccessPath, AtmDirector, Cache Director System, the CCIE logo, CD-PAC, Centri, Centri Bronze, Centri Gold, Centri Security Manager, Centri Silver, the Cisco Capital logo, Cisco IOS, the Cisco IOS logo, *CiscoLink*, the Cisco Powered Network logo, the Cisco Press logo, ClickStart, ControlStream, Fast Step, FragmentFree, IGX, JumpStart, Kernel Proxy, LAN²LAN Enterprise, LAN²LAN Remote Office, MICA, Natural Network Viewer, NetBeyond, Netsys Technologies, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RouteStream, Secure Script, SMARTnet, StrataSphere, StrataSphere BILLder, StrataSphere Connection Manager, StrataSphere Modeler, StrataSphere Optimizer, Stratum, StreamView, SwitchProbe, *The Cell*, TokenSwitch, TrafficDirector, VirtualStream, VlanDirector, Workgroup Director, Workgroup Stack, and XCI are trademarks; The Network Works. No Excuses. is a service mark; and BPX, Catalyst, Cisco, Cisco Systems, the Cisco Systems logo, EtherChannel, FastHub, FastPacket, ForeSight, IPX, LightStream, OptiClass, Phase/IP, StrataCom, and StrataView Plus 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.
9711R