



Doc. No. 78-4828-01

Release Notes for the Cisco 3640 Routers for Cisco IOS Release 11.2(9)XA

October 6, 1997

These release notes describe the new features and significant software components for Cisco IOS Release 11.2(9)XA for Cisco 3640 routers.

Introduction

These release notes discuss the following topics:

- Cisco IOS Release 11.2 Paradigm, page 1
- Cisco IOS Documentation, page 4
- Software Features for the Cisco 3640 Release 11.2(9)XA, page 6
- Cisco IOS Feature Sets for Cisco 3640 Access Routers, page 22
- Upgrading to a New Software Release, page 28
- Memory Requirements, page 28
- Caveats for Release 11.2(9)XA, page 29
- Caveats for Release 11.2(9), page 29
- Cisco Connection Online, page 34
- Documentation CD-ROM, page 35

Cisco IOS Release 11.2 Paradigm

Before Cisco IOS Release 11.2, maintenance releases of major Cisco IOS software releases were used to deliver additional new features. Beginning with Cisco IOS Release 11.2, Cisco Systems provides two software release “trains” based on a single version of Cisco IOS software. Similar to a

Corporate Headquarters

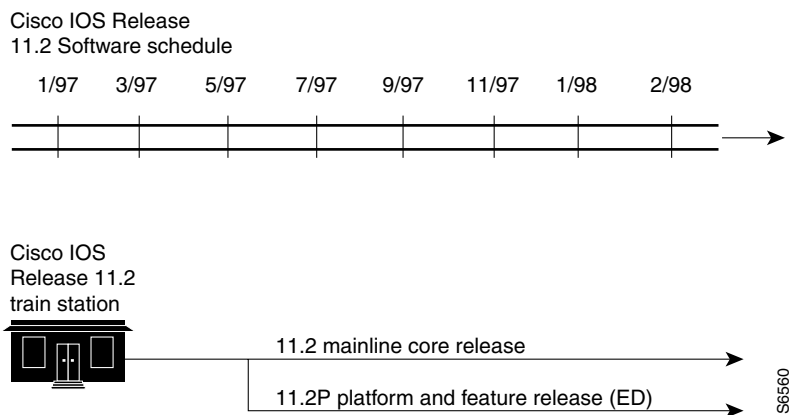
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

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

train rolling down the track and picking up passengers, after a release of Cisco IOS software is released to customers, it continues to pick up software fixes along the way and is rereleased as maintenance releases. Maintenance releases provide the most stable software for your network, for the features you need. In addition to the major train, there is typically an early deployment (ED) train. The ED train—Release 11.2 P—delivers both fixes to software defects and support for new Cisco platforms. Figure 1 shows the Cisco IOS 11.2 and the 11.2 P software releases.

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

Figure 1 Cisco IOS Release 11.2 Software Releases



To determine which Cisco IOS maintenance release is running on your 3640 router, log on to the router and enter the **show version** User EXEC command.

Cisco 3640 Router

As modular solutions, the Cisco 3640 enable corporations to increase dialup density and take advantage of current and emerging WAN technologies and networking capabilities. The Cisco 3640 is fully supported by the Cisco IOS software, which includes dialup connectivity, LAN-to-LAN routing, data and access security, WAN optimization, and multimedia features.

Table 1 lists the interface cards and network modules supported by the Cisco 3640 access routers.

Table 1 Supported WAN Interface Cards and Network Modules

Combination WAN/LAN Interface Cards
1 Ethernet and 2 WAN interface card
2 Ethernet and 2 WAN interface card
1 Ethernet, 1 Token Ring, and 2 WAN interface card
Standard WAN Interface Cards
1-port serial WAN interface card
1-port ISDN BRI WAN interface card

Table 1 Supported WAN Interface Cards and Network Modules (Continued)

1-port ISDN BRI with NT1 WAN interface card
1-port ISDN BRI with NT1 and U interface card slots
1-port switched 56K DSU WAN interface card
Channelized T1 and E1 ISDN PRI Network Modules
1-port channelized T1/ISDN PRI network module
1-port channelized T1/ISDN PRI with CSU network module
2-port channelized T1/ISDN PRI network module
2-port channelized T1/ISDN PRI with CSU network module
1-port channelized E1/ISDN PRI balanced network module
1-port channelized E1/ISDN PRI unbalanced network module
2-port channelized E1/ISDN PRI balanced network module
2-port channelized E1/ISDN PRI unbalanced network module
Blank network module panel
ISDN BRI Network Modules
4-port ISDN BRI network module with an S/T interface ¹
4-port ISDN BRI with NT1 network module ¹
8-port ISDN BRI network module with an S/T interface
8-port ISDN BRI with NT1 network module
Asynchronous/Synchronous Network Modules
4-port asynchronous/synchronous serial network module ¹
8-port asynchronous/synchronous serial network module
Additional Network Modules
1-port Ethernet network module
1-port Fast Ethernet
4-port Serial network module
4-port Ethernet
Hardware compression
16-port asynchronous
32-port asynchronous
Modem Network Modules
6-port digital modem network module
12-port digital modem network module
18-port digital modem network module
24-port digital modem network module
30-port digital modem network module
6-port digital modem SIMM

1. The 4-port module is not upgradable to the 8-port module.

Cisco IOS Documentation

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

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

The books and chapter topics are as follows:

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Configuration Fundamentals Configuration Guide</i> • <i>Configuration Fundamentals Command Reference</i> 	<ul style="list-style-type: none"> 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> 	<ul style="list-style-type: none"> 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> 	<ul style="list-style-type: none"> 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

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> 	ATM Dial-on-Demand Routing (DDR) Frame Relay ISDN LANE PPP for Wide-Area Networking SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 1</i> • <i>Network Protocols Command Reference, Part 1</i> 	IP IP Routing
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 2</i> • <i>Network Protocols Command Reference, Part 2</i> 	AppleTalk Novell IPX
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 3</i> • <i>Network Protocols Command Reference, Part 3</i> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Bridging and IBM Networking Configuration Guide</i> • <i>Bridging and IBM Networking Command Reference</i> 	Transparent Bridging Source-Route Bridging Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point Support SNA Frame Relay Access Support APPN NCIA Client/Server Topologies IBM Channel Attach
<ul style="list-style-type: none"> • <i>Cisco IOS Software Command Summary</i> • <i>Access Services Quick Configuration Guide</i> • <i>System Error Messages</i> • <i>Debug Command Reference</i> • <i>Cisco Management Information Base (MIB) User Quick Reference</i> 	

All the documents mentioned 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>.

Software Features for the Cisco 3640 Release 11.2(9)XA

This section is divided into the following subjects:

- Additional hardware features for software release 11.2(9)XA
- Routing Protocols
- Desktop Protocols
- Wide-Area Networking Features
- IBM Functionality
- Security Features
- Network Management

Additional Hardware Features for Software Release 11.2(9)XA

Digital modem network interfaces include the following:

- 60-modem
- 120-modem
- 180-modem
- 240-modem
- 300-modem

Note The digital modem network module is not supported on the Cisco 3620 router.

Note The digital modem network modules require the router to contain a PRI network module to accept modem calls over the ISDN channel. The PRI module (Cisco part numbers NM-CT1, NM-2CT1, NM-1CT1-CSU, NM-2CT1-CSU, NM-1CE1B, NM-1CE1U, NM-2CE1B, or NM-2CE1U) must be hardware revision 1.1 in order to accept modem calls over the ISDN channel.

Features Not Supported

The following features are not supported with the network in 11.2(9)XA release:

- Support for initiation or termination of calls through channelized T1/E1 interfaces
- Modem calls over BRI interfaces
- Concurrent support of ISDN PRI and BRI interfaces

- 56K modem support
- Fax

The following IOS CLI features/commands are not supported by the modem modules:

- Modem startup test
- Test modem back-to-back
- Modem hold reset
- Copy flash/tftp/rcp modem
- Modem at-mode-permit
- Modem at-mode
- Clear modem at-mode
- Modem poll time
- Modem status-poll
- Modem poll retry

Routing Protocols

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

IP Protocol and Feature Enhancements

The following new IP protocol software features are available:

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

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

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

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

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

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

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

Open Shortest Path First Enhancements

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

- **OSPF On-Demand Circuit**—OSPF On-Demand Circuit is an enhancement to the OSPF protocol, as described in RFC 1793, that allows efficient operation over demand circuits such as ISDN, X.25 Switched Virtual Circuits, and dialup lines. Previously, the periodic 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 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 to-backbone connection to become logically part of the same network.

Border Gateway Protocol version 4 (BGP4) Enhancements

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

- **BGP4 Soft Configuration**—BGP4 soft configuration allows BGP4 policies to be configured and activated without clearing the BGP session (without invalidating the forwarding cache). This enables policy reconfiguration without causing short-term interruptions to traffic being forwarded in the network.

- **BGP4 Multipath Support**— BGP4 Multipath Support provides BGP load balancing between multiple Exterior BGP (EBGP) sessions. If there are multiple EBGP sessions between the local autonomous system and the neighboring autonomous system, multipath support allows BGP to load balance among these sessions. Depending on the switching mode, per packet or per destination load balancing is performed. BGP4 Multipath Support can support up to six paths.
- **BGP4 Prefix Filtering with Inbound Route Maps**—This feature allows prefix-based matching support to the inbound neighbor route map. This feature allows an inbound route map to be used to enforce prefix-based policies.

Network Address Translation

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

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

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

NAT offers these advantages:

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

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

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

Named IP Access Control List

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

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

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

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

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

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

Multimedia and Quality of Service

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

- **Resource Reservation Protocol**—Resource Reservation Protocol (RSVP) enables applications to dynamically reserve necessary network resources from end-to-end for different classes of service. An application, which acts as a receiver for a traffic stream, initiates a request for reservation of resources (bandwidth) from the network, based on the application's required quality of service. The first RSVP-enabled router that receives the request informs the requesting host whether the requested resources are available or not. The request is forwarded to the next router, toward the sender of the traffic stream. If the reservations are successful, an end-to-end pipeline of resources is available for the application to obtain the required quality of service. RSVP enables applications with real-time traffic needs, such as multimedia applications, to coexist with bursty applications on the same network. RSVP works with both unicast and multicast applications.

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

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

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

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

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

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

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

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

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

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

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

Multiprotocol Routing

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

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

- IPX Service Advertisement Interleaving—Large IPX environments are typically characterized by many Service Advertisements, which can saturate lower-speed links at the expense of routing protocol messages. Enhanced IGRP now employs an interleaving technique to ensure that both traffic types receive sufficient bandwidth in large IPX networks.

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

Switching Features

Integrated Routing and Bridging has been added to Cisco's switching software:

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

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

Integrated routing and bridging provides:

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

Note that:

- IRB Currently supports three protocols: IP, IPX, and AppleTalk, in both fast switching and process switching modes.
- IRB is 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

AppleTalk Load Balancing has been added to Cisco's AppleTalk software:

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 Service Advertisement Protocol 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 intervals of approximately five minute.

This feature allows logging of:

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

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

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

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

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

Wide-Area Networking Features

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

ISDN/DDR Enhancements

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

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

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

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

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

With Multichassis Multilink PPP:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Frame Relay Enhancements

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

- **Frame Relay SVC Support (DTE)**—Access to Frame Relay networks is currently accomplished 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 on 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 virtual circuits 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

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-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 offers these advantages:

- 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.

ATM Enhancements

The following features have been added to Cisco's Asynchronous Transfer Mode (ATM) software:

- **Simple Server Redundancy Protocol for LAN Emulation**—The Simple Server Redundancy Protocol (SSRP) provides stand by redundancy for the following services used by clients in an ATM LAN Emulation (LANE) network: LAN Emulation Configuration Server (LECS), LAN Emulation Server (LES), and Broadcast-and-Unknown Server (BUS). As many as 16 LECSs can be defined for LightStream 1010 switches whereas LS100 switches support only four LECSs. Additionally, LECS addresses can be defined in ILMI on a per-port basis in the LightStream 1010.

LAN Emulation uses one LES/BUS per emulated LAN and one LECS per multiple emulated LANs. These service components represent single points of failure for each emulated LAN. SSRP removes these single points of failure, providing the redundancy that network managers need for campus ATM backbones with LAN Emulation without adding administrative overhead. A completely redundant, dual-homed ATM backbone can be built without any failure points when SSRP is combined with Hot Standby Router Protocol (HSRP), the dual-phy LANE card for the Catalyst 5000, and support for Spanning Tree on a per VLAN-basis.

- **Additional Protocol Routing Support for LAN Emulation**—This feature adds the ability to route DECnet, Banyan VINES, and XNS from a subinterface on an ATM router port running LAN Emulation client to any other subinterface on an ATM router port running LAN Emulation client or any other router port. Support for DECnet routing between VLANs for ATM LAN Emulation requires DECnet Phase IV.

When DECnet routing is configured, there is a one-time reset of the interface so that the MAC address of the interface can reflect the DECnet Phase IV MAC address conventions. If SSRP is also configured, there is a switchover to the secondary LECS and back as a result of configuring DECnet.

- **UNI 3.1 Signaling Support**—The full breadth of UNI signaling protocol support is available. The ATM Forum submitted the UNI 3.0 signaling specification to the ITU, which subsequently made changes to the SSCOP encapsulation used to make signaling reliable. UNI 3.1 was published later by the ATM Forum to align with the ITU, otherwise there is no difference in functionality between UNI 3.0, currently supported on all Cisco ATM platforms, and UNI 3.1.
- **Rate Queues for SVCs per subinterface**—In previous releases, SVCs which do not use static maps could not participate in traffic shaping—they were assigned to a rate queue at the interface line rate. In Release 11.2, all SVCs on an interface for which explicit traffic-shaping parameters have not been specified can be assigned a set of traffic-shaping parameters via a map-class tied to the interface. These parameters can, for example, be assigned to SVCs used to run RFC 1577 Classical IP over ATM.

Note The interface-level traffic shaping parameters are not applied to SVCs used for LAN Emulation (LANE). These SVCs continue to be unshaped.

- **AToM MIB Support**—This provides support for the AToM Management Information Base (MIB), described in IETF RFC 1695, which defines configuration information as well as error and cell-level counters. Release 11.2 provides a standard AToM MIB instrumentation for many of the counters already provided in the router's ATM interfaces.

AToM MIB instrumentation is used by network management applications, such as Cisco's AtmDirector, to perform topology auto-discovery and status checking.

IBM Functionality

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

New Features

The following new IBM software features are available:

- **Native Client Interface Architecture (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.
- **Response Time Reporter**—The Response Time Reporter (RTR) feature allows you to monitor network performance, network resources, and applications by measuring response times and availability. RTR statistics can be used to perform troubleshooting, problem notifications and pre-problem analysis. RTR offers enhanced functionality over a similar IBM product, NetView Performance Monitor.

RTR enables the following functions to be performed:

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

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

Advanced Peer-to-Peer Networking Enhancements

The following features have been added to Cisco's Advanced Peer-to-Peer Networking (APPN) software:

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

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

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

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

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

Data Link Switching+ Features and Enhancements

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

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

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

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

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

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

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

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

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

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

Security Features

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

New Features

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

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

All components of this feature are subject to 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.

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

TACACS+ Enhancements

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

- **TACACS+ Single Connection**—Single Connection is an enhancement to the network access server that increases the supported number of transactions per second 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(9)XA.

MIBs Supported

The following MIB support has been added:

- **APPN DLUR MIB**—See the “Advanced Peer-to-Peer Networking Enhancements” section for details.

- AToM MIB Support—See the “ATM Enhancements” section for details.
- 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

Important Notes

This section describes warnings and cautions about using the Cisco IOS Release 11.2(9)XA software. It discusses the following topics:

- Upgrading to a New Software Release
- Traffic shaping over Frame Relay in Release 11.2(1)
- LAN extension in Release 11.2(1)
- Changes to LANE Commands
- Channel Interface Processor (CIP) microcode
- Netbooting from VIP
- Source-route Bridging (SRB) over FDDI
- Enabling IPX routing
- Using AIP cards
- Using LAN Emulation (LANE)
- Forwarding of locally sourced AppleTalk packets

Cisco IOS Feature Sets for Cisco 3640 Access Routers

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

Table 2 and Table 3 use these feature set matrix symbols to identify features:

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

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

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

Table 2 list the standard feature sets supported in Release 11.2(9)XA

Table 2 Feature Set Matrix for Cisco 3640 Access Routers

Standard Feature Sets	Cisco 3640
IP	Ⓓ, Plus, Encrypt
Desktop (IP/IPX/AppleTalk/DEC)	Ⓓ, Plus, Encrypt
Enterprise	Ⓓ, Plus, Encrypt
Enterprise and APPN	Ⓓ, Plus, Encrypt
IP/IPX/IBM and APPN	Ⓓ ¹

1. IP/IPX/IBM/APPN has no additional options. It offers a low-end APPN solution for the Cisco 3640 routers.

Feature Set Tables

The Cisco IOS software is available in different feature sets depending on the platform. Table 3 lists the feature sets for the Cisco 3640 access routers.

Table 3 Cisco 3640 Feature Sets

Features Contained in Features Sets	Feature Sets			
	IP Routing	IP/IPX/IBM/APPN ¹	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise
LAN Support				
Apollo Domain	—	—	—	Ⓓ
AppleTalk 1 and 2	—	—	Ⓓ	Ⓓ
Banyan VINES	—	—	—	Ⓓ
Concurrent routing and bridging	Ⓓ	Ⓓ	Ⓓ	Ⓓ
DECnet IV	—	—	Ⓓ	Ⓓ
DECnet V	—	—	—	Ⓓ
GRE	Ⓓ	Ⓓ	Ⓓ	Ⓓ

Table 3 Cisco 3640 Feature Sets (Continued)

Features Contained in	Feature Sets			
	IP Routing	IP/IPX/IBM/APPN ¹	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise
Integrated routing and bridging (RB)	Ⓜ	Ⓜ	Ⓜ	Ⓜ
IP	Ⓜ	Ⓜ	Ⓜ	Ⓜ
LAN extension host	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Multiring	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Novell IPX	—	Ⓜ	Ⓜ	Ⓜ
OSI	—	—	—	Ⓜ
Source-route bridging	—	—	—	—
Transparent and translational bridging	Ⓜ	Ⓜ	Ⓜ	Ⓜ
XNS	—	—	—	Ⓜ
WAN Services				
Combinet packet protocol	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Dialer profiles	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Frame Relay	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Frame Relay SVC support (DTE)	—	—	—	Ⓜ
Frame Relay traffic shaping ²	—	—	—	—
Half bridge/half router for CPP and PPP	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Multichassis Multilink PPP (MMP)	Plus	—	Plus	Plus
Virtual Private dialup Network (VPDN)	Plus	—	Plus	Ⓜ
HDLC	Ⓜ	Ⓜ	Ⓜ	Ⓜ
IPXWAN 2.0	—	Ⓜ	Ⓜ	Ⓜ
ISDN ³	Ⓜ	Ⓜ	Ⓜ	Ⓜ
PPP ⁴	Ⓜ	Ⓜ	Ⓜ	Ⓜ
SMDS	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Switched 56	Ⓜ	Ⓜ	Ⓜ	Ⓜ
X.25 ⁵	Ⓜ	Ⓜ	Ⓜ	Ⓜ
WAN Optimization				
Bandwidth-on-demand	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Custom and priority queuing	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Dial backup	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Dial-on-demand	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Header ⁶ , link and payload compression ⁷	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Snapshot routing	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Weighted fair queuing	Ⓜ	Ⓜ	Ⓜ	Ⓜ
IP Routing				
BGP	Ⓜ	Ⓜ	Ⓜ	Ⓜ
BGP4	Ⓜ	Ⓜ	Ⓜ	Ⓜ

Table 3 Cisco 3640 Feature Sets (Continued)

Features Contained in Features Sets	Feature Sets			
	IP Routing	IP/IPX/IBM/APPN ¹	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise
EGP	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Enhanced IGRP	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Enhanced IGRP optimizations	Ⓜ	Ⓜ	Ⓜ	Ⓜ
ES-IS	—	—	—	Ⓜ
IGRP	Ⓜ	Ⓜ	Ⓜ	Ⓜ
IS-IS	—	—	—	Ⓜ
Named IP access control list	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Network Address Translation (NAT)	Plus	—	Plus	Plus
NHRP	Ⓜ	Ⓜ	Ⓜ	Ⓜ
OSPF	Ⓜ	Ⓜ	Ⓜ	Ⓜ
OSPF Not-So-Stubby-Areas (NSSA)	Ⓜ	Ⓜ	Ⓜ	Ⓜ
OSPF On Demand Circuit (RFC 1793)	Ⓜ	Ⓜ	Ⓜ	Ⓜ
PIM	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Policy-based routing	Ⓜ	Ⓜ	Ⓜ	Ⓜ
RIP	Ⓜ	Ⓜ	Ⓜ	Ⓜ
RIP Version 2	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Other Routing				
AURP	—	—	Ⓜ	Ⓜ
IPX RIP	—	Ⓜ	Ⓜ	Ⓜ
NLSP	—	Ⓜ	Ⓜ	Ⓜ
RTMP	—	—	Ⓜ	Ⓜ
SMRP	—	—	Ⓜ	Ⓜ
SRTP	—	—	—	Ⓜ
Multimedia and Quality of Service				
Generic traffic shaping	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Random Early Detection (RED)	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Resource Reservation Protocol (RSVP)	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Management				
AutoInstall	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Automatic modem configuration ⁸	Ⓜ	Ⓜ	Ⓜ	Ⓜ
HTTP server	Ⓜ	Ⓜ	Ⓜ	Ⓜ
RMON events and alarms ⁹	Ⓜ	Ⓜ	Ⓜ	Ⓜ
SNMP	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Telnet	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Security				
Access lists	Ⓜ	Ⓜ	Ⓜ	Ⓜ

Table 3 Cisco 3640 Feature Sets (Continued)

Features Contained in Features Sets	Feature Sets			
	IP Routing	IP/IPX/IBM/APPN ¹	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise
Access security	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Extended access lists	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Kerberized login	—	—	—	Ⓜ
Kerberos V client support	—	—	—	Ⓜ
Lock and key	—	—	—	Ⓜ
MAC security for hubs	Ⓜ	Ⓜ	Ⓜ	Ⓜ
MD5 routing authentication	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Network layer encryption (40-bit or export controlled 56-bit DES)	Encrypt	—	Encrypt	Encrypt
RADIUS	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Router authentication	Encrypt	—	Encrypt	Encrypt
TACACS+	Ⓜ	Ⓜ	Ⓜ	Ⓜ
IBM Support (Optional)¹⁰				
APPN	—	Ⓜ	—	Ⓜ
BAN for SNA Frame Relay support	Plus	Ⓜ	Ⓜ	Ⓜ
Bisync ¹¹	Plus	Ⓜ	Ⓜ	Ⓜ
Caching and filtering	Plus	Ⓜ	Ⓜ	Ⓜ
DLSw+	Plus	Ⓜ	Ⓜ	Ⓜ
Downstream PU concentration (DSPU)	Plus	Ⓜ	—	Ⓜ
Frame Relay SNA Support (RFC 1490)	Plus	Ⓜ	Ⓜ	Ⓜ
NetView Native Service Point	Plus	Ⓜ	Ⓜ	Ⓜ
QLLC ¹¹	Plus	Ⓜ	Ⓜ	Ⓜ
SDLC integration	Plus	Ⓜ	Ⓜ	Ⓜ
SDLC transport (STUN)	Plus	Ⓜ	Ⓜ	Ⓜ
SDLC-to-LAN conversion (SDLLC)	Plus	Ⓜ	Ⓜ	Ⓜ
SNA and NetBIOS WAN optimization via local acknowledgment	Plus	Ⓜ	Ⓜ	Ⓜ
SRB/RSRB	Plus	Ⓜ	Ⓜ	Ⓜ
SRT	Plus	Ⓜ	Ⓜ	Ⓜ
TG/COS	—	—	—	Ⓜ
Protocol Translation				
LAT	—	—	—	Ⓜ
Rlogin	—	—	—	Ⓜ
Remote Node				
ARAP 1.0/2.0	—	—	Ⓜ	Ⓜ
Asynchronous master interfaces	Ⓜ	Ⓜ	Ⓜ	Ⓜ

Table 3 Cisco 3640 Feature Sets (Continued)

Features Contained in Features Sets	Feature Sets			
	IP Routing	IP/IPX/IBM/APPN ¹	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise
ATCP	—	—	ⓓ	ⓓ
CPPP	ⓓ	ⓓ	ⓓ	ⓓ
CSLIP	ⓓ	ⓓ	ⓓ	ⓓ
DHCP	ⓓ	ⓓ	ⓓ	ⓓ
IP pooling	ⓓ	ⓓ	ⓓ	ⓓ
IPX and ARAP on virtual async interfaces	—	—	—	ⓓ
IPXCP	—	ⓓ	ⓓ	ⓓ
MacIP	—	—	ⓓ	ⓓ
NASI ¹²	—	ⓓ	ⓓ	ⓓ
NetBEUI over PPP	ⓓ	ⓓ	ⓓ	ⓓ
PPP	ⓓ	ⓓ	ⓓ	ⓓ
SLIP	ⓓ	ⓓ	ⓓ	ⓓ
Terminal Services				
LAT ¹³	—	—	—	ⓓ
Rlogin	ⓓ	ⓓ	ⓓ	ⓓ
Telnet	ⓓ	ⓓ	ⓓ	ⓓ
TN3270	—	—	—	ⓓ
X.25 PAD	ⓓ	ⓓ	ⓓ	ⓓ
Xremote	—	—	—	ⓓ

1. IP/IPX/IBM/APPN has no additional options. It offers a low-end APPN solution for the Cisco 3640 routers.

2. Frame Relay traffic shaping will be available in a future 11.2 P release.

3. ISDN support includes calling line identification (ANI), X.25 over the B channel, ISDN subaddressing, and applicable WAN optimization features.

4. PPP includes support for LAN protocols supported by the feature set, address negotiation, PAP and CHAP authentication, and PPP compression. Multilink PPP is available in Cisco IOS Release 11.0(4) and later releases.

5. Includes X.25 switching.

6. IPX header compression (RFC 1553) is available in the feature sets that support IPX in Cisco IOS Release 11.1(1) and later releases.

7. X.25 and Frame Relay payload compression are supported in Cisco IOS Release 11.0(4) and later releases.

8. Automatic modem configuration is available for all feature sets in Cisco IOS Release 11.1(2) and later releases. For the Enterprise feature set, automatic modem configuration is available in Cisco IOS 11.1(1) and later releases.

9. The RMON events and alarms groups are supported on all interfaces in Cisco IOS Release 11.1 and later releases. Enhanced RMON feature sets are also available.

10. "Optional" means a separate Cisco IOS feature set with the IBM base option: IP/IBM base, IP/IPX/IBM/APPN base, Desktop/IBM base, Enterprise/IBM base.

11. QLLC and Bisync are available in IP/IBM in Cisco IOS Release 11.0(3) and later releases, and in IP/IPX/IBM and Desktop/IBM base in Cisco IOS Release 11.0(2) and later releases.

12. NASI is supported in Cisco IOS Release 11.1(2) and later releases.

13. Use of LAT requires terminal license (FR-L8-10.X= for an 8-user license or FR-L16-10.X= for a 16-user license).

Upgrading 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, if you have a maintenance contract called SMARTnet, go to the following URL:

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

The Software Center window is displayed.

- Step 1** Click **Cisco IOS Software**. The Cisco IOS Software window is displayed.
- Step 2** Click **Cisco IOS 11.2**. The Cisco 11.2 Software Upgrade Planner window is displayed.
- Step 3** Click **Download Cisco IOS 11.2 Software**. The Software Checklist window is displayed.
- Step 4** Select the appropriate information in each section of the Software Checklist window.
 - Hardware
 - Release
 - Software and hardware release
- Step 5** Click **Execute**. The software release is downloaded to your desktop computer.
- Step 6** Transfer the software release to a local TFTP server on your network, 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 4 describes the memory requirements for Cisco 3640 access routers supported by Cisco IOS Release 11.2(9)XA.

Table 4 Cisco 3640 —Memory Requirements

Feature Set	Cisco 3640 Router	Required Flash Memory	Required DRAM Memory	Release 11.2(9)XA Runs from ¹
IP	Cisco 3640	4 MB Flash	16 MB DRAM	RAM
IP Plus	Cisco 3640	4 MB Flash	16 MB DRAM	RAM
IP Plus 40	Cisco 3640	4 MB Flash	16 MB DRAM	RAM
IP Plus 56	Cisco 3640	4 MB Flash	16 MB DRAM	RAM
Desktop	Cisco 3640	4 MB Flash	24 MB DRAM	RAM
Desktop Plus	Cisco 3640	4 MB Flash	24 MB DRAM	RAM
Desktop Plus 40	Cisco 3640	4 MB Flash	24 MB DRAM	RAM
Desktop Plus 56	Cisco 3640	4 MB Flash	24 MB DRAM	RAM

Table 4 Cisco 3640 —Memory Requirements (Continued)

Feature Set	Cisco 3640 Router	Required Flash Memory	Required DRAM Memory	Release 11.2(9)XA Runs from ¹
Enterprise	Cisco 3640	8 MB Flash	24 MB DRAM	RAM
Enterprise Plus	Cisco 3640	8 MB Flash	24 MB DRAM	RAM
Enterprise Plus 40	Cisco 3640	8 MB Flash	24 MB DRAM	RAM
Enterprise Plus 56	Cisco 3640	8 MB Flash	24 MB DRAM	RAM
Enterprise and APPN Plus	Cisco 3640	8 MB Flash	32 MB DRAM	RAM
Enterprise and APPN Plus 40	Cisco 3640	8 MB Flash	32 MB DRAM	RAM
Enterprise and APPN Plus 56	Cisco 3640	8 MB Flash	32 MB DRAM	RAM
IP/IPX/IBM/APPN	Cisco 3640	8 MB Flash	32 MB DRAM	RAM

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.

Caveats for Release 11.2(9)XA

This section describes possibly unexpected behavior by Cisco IOS Release 11.2(9)XA. Unless otherwise noted, these caveats apply to Cisco IOS Release 11.2 up to and including 11.2(9)XA. 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.

Note There are no caveats for the Cisco 3640 router for software Release 11.2(9)XA.

Caveats for Release 11.2(9)

This section describes possibly unexpected behavior by Cisco IOS Release 11.2(9). Unless otherwise noted, these caveats apply to Cisco IOS Release 11.2 up to and including 11.2(9). 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.

AppleTalk

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

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

- Remove autoselect and use ARAP dedicated.
- Use the ARAP 2.0.1 client instead.
- Turn on MNP10 on the ARAP 2.1 client.

- Modify the client CCL script to extend the pause to 3 seconds before exiting. [CSCdj09817]
- Mounting an AFP volume fails with the following error in ARAP 3.0:

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

Basic System Services

- The router might reload when trying to process the **show accounting** command. [CSCdi69364]
- The **show stacks** command fails to report the correct version of code running at the time of the last reload. This problem occurs when the Flash version of the Cisco IOS software does not match the running version of code. [CSCdi74380]
- Fast switching and optimum switching counters should be broken out separately in the output of the **show interface switching** command. [CSCdi87008]
- Traffic shaping is not currently supported over tunnels of any type or switching mode. The feature is currently under development. [CSCdi88997]
- When a router is configured with the command **ip identd** and with **aaa authentication login default tacacs+ enable** the router will reload itself under these conditions:
 - Router is resolving host names via an external DNS server
 - TACACS server is down
 - User gains access to the router via the backup “enable” method
 - User attempts to Telnet from the router to a host on the network

After the Telnet is initiated, the router will immediately reload.

The workaround for this problem is to not configure the **ip identd** command or to disable the **identd** process with the global command **no ip identd** (which is the default). [CSCdj19961]

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

IBM Connectivity

- The **dlsr remote-peer frame-relay interface serial** command does not work on a point-to-point subinterface. The workaround is to use multipoint and to do LLC mapping. [CSCdi55085]

- On a router running Cisco IOS Release 11.2, Enhanced IGRP fails to connect fully to other Enhanced IGRP routers across a single Token Ring interface, when source-route bridging is configured on the interface but source bridge spanning is not enabled. The workaround is to enable source bridge spanning on the Token Ring interface. [CSCdi70297]
- A bus error occurred at PC0x169a46. The stack trace indicates a problem in the LNX process. This problem occurs on X.25. [CSCdi73516]
- When the fast source-route translational bridging feature is configured, packets are corrupted. The workaround is to issue the **no source-bridge fastest ring-group fastest** command, which disables the fast source-route translational bridging feature. [CSCdi87612]
- A small window exists in which it is possible after a transmission group reinstallation that only one CP-CP session is established between the router and a neighboring node. In this case, the contention winner session from the perspective of the router is not activated. Once this occurs, the CP-CP contention winner session will only activate if the APPN subsystem is stopped and started. There is no known workaround. [CSCdj25859]
- An APPN router might display the following “Unanticipated CP_STATUS” message when the conloser CP-CP session goes down and comes back up without the conwinner session being deactivated:

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

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

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

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

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

- There may be intermittent failures when trying to link to bridges over the DLSw remote peers when running LNM over DLSw. The workaround is to reload the router that is directly attached to the LNM device. [CSCdj34112]
- When testing FRAS BAN for SDLC attached PU 2.1 and PU 2.0 and using RSRB backup over PSTN, the physical units 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 physical units, the **fras backup rsrb** statement had to be removed or the serial interfaces configuration had to be deleted and then readded. [CSCdj39306]

Interfaces and Bridging

- Connecting a Canary Fast Ethernet transceiver to the MII connector on VIP port adapters requires a microcode reload before the port will function properly. [CSCdi64606]

- On an RSP router, the “%CBUS-3-CTRUCHECK” error message is displayed and the Token Ring interface resets. To correct this problem, upgrade to RSP TRIP Microcode Version 20.1. [CSCdi74639]
- The error “%CBUS-3-CTRUCHECK: Unit 0, Microcode Check Error” occurs on Token Ring interfaces, causing the interface to reset. [CSCdj08654]
- An RSP2 router configured with a Fast Ethernet interface and a slow-speed serial interface may experience output packet drops on the serial interface, with incoming traffic on the Fast Ethernet interface. This problem occurs even with less traffic, such as during a regular ping.
To work around this problem, disable fast switching on the serial interface. [CSCdj17962]
- IBM RPL fails to load from a server with IPX routing enabled on a Cisco 3620 router. SMC RPL does not exhibit this behavior.
A LANalyzer trace indicates that the router is forwarding RPL requests out the same Token Ring interface port on which it received the packet. [CSCdj18835]
- The **pos specify-s1s0** and **pos specify-c2** POS interface specific configuration commands do not work correctly. [CSCdj25166]
- The dot5StatsTable does not return any value in IOS 11.2. [CSCdj32372]
- An NFS transmission problem and FDDI corruption occurred after installing 10.3(9)+ or 11.1(9)+ or 11.2(1)+. [CSCdj38715]

IP Routing Protocols

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

ISO CLNS

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

Novell IPX, XNS, and Apollo Domain

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

VINES

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

Wide-Area Networking

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

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

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

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

- The “%SYS-2-GETBUF” error message might appear. [CSCdi92482]
- A virtual access interface does not inherit the username from its parent interfaces when it hosts a PPP multilink session. Therefore, the **show user** command does not display the username associated with a virtual access interface, and SLIPON requests in Extended TACACS do not contain the username, resulting in possible authentication failures with Extended TACACS. [CSCdj04600]
- When using DLCI prioritization on a point-to-point Frame Relay subinterface and one of the DLCIs fails, the subinterface will either bounce once or continually bounce at every subsequent 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**.
Normally, the point-to-point subinterface should go down when the primary DLCI fails. If a secondary DLCI fails, the subinterface stays up but traffic destined only for that DLCI will fail. [CSCdj11056]
- A Cisco router running 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 might randomly and intermittently reload due to an MTU mismatch and generate system error messages similar to the following:

```
%SYS-3-OVERRUN: Block overrun at 4029DEA8 (redzone 743D3334)
[CSCdj19105]
```
- Although a router configured for HSRP on LANE replies correctly with the HSRP MAC address in an ARP reply, all packets issued by the router with a virtual IP address use the BIA MAC address as the source address. This makes it difficult for switches to know the forwarding port. [CSCdj28865]
- The BREAK sequence might not be received properly on platforms that use the Cirrus Logic asynchronous controllers. This includes the Cisco AS5100 and AS5200 routers. You might have to send the BREAK sequence multiple times before it is interpreted correctly. [CSCdj32121]
- When you configure dial-backup in a Legacy DDR environment, the primary link does not take over and does not clear the ISDN backup link whenever the kickout-load is reached on the primary interface. This works well in a dialer-profile or in a rotary-group environment. [CSCdj33786]
- When a dialer-profile is in standby mode, backing up a serial interface with the **backup interface dialer** command still allows incoming calls to this profile. Because the profile is in standby mode this should not be possible. [CSCdj34108]
- IP problems may be experienced when multiple PRIs are set up in a rotary and using a dialer interface. There may be a problem pinging the dial-in user because one PRI will be working and another PRI will not be working. There is no known workaround. [CSCdj34245]
- Configuration of a dialer interface for load backup (either with dialer profiles or legacy rotaries) could give rise to a flapping ISDN connection. This problem occurs especially when the bandwidth configured on the primary is less than the one on the dialer interface. [CSCdj39723]

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>.

This document is to be used in conjunction with the *Cisco IOS Release 11.2 configuration guides and command references*.

AccessPath, AtmDirector, Cache Director System, CD-PAC, Cisco IOS, the Cisco IOS logo, CiscoLink, the Cisco Powered Network logo, ClickStart, ControlStream, Fast Step, FragmentFree, IGX, JumpStart, LAN2LAN Enterprise, LAN2LAN Remote Office, MICA, NetBeyond, NetFlow, Netsys Technologies, Packet, PIX, Point and Click Internetworking, RouteStream, SMARTnet, Speed, 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 © 1997, Cisco Systems, Inc.
All rights reserved. Printed in USA.
978R

