



Doc. No. 78-4612-05

Release Notes for the Cisco 1000 Series Routers for Cisco IOS Release 11.2

March 2, 1998

These release notes describe the new features and significant software components for Cisco IOS Release 11.2, up to and including Release 11.2(12) for Cisco 1000 series routers.

Introduction

These release notes discuss the following topics:

- Determining Your Cisco IOS Release, page 2
- Cisco 1000 Series Routers and Platforms Supported, page 2
- Documentation, page 3
- Online Navigation, page 5
- New Features in Release 11.2(1), page 6
- Cisco IOS Feature Sets for Cisco 1000 Series Routers, page 21
- Upgrading to a New Software Release, page 26
- Memory Requirements, page 27
- Important Notes, page 28
- Caveats for Release 11.2(1) Through 11.2(12), page 29
- Caveats for Release 11.2(1) Through 11.2(11), page 29
- Caveats for Release 11.2(1) Through 11.2(10), page 30
- Caveats for Release 11.2(1) Through 11.2(9), page 30
- Caveats for Release 11.2(1) Through 11.2(8), page 31
- Caveats for Release 11.2(1) Through 11.2(7), page 32
- Caveats for Release 11.2(1) Through 11.2(6), page 32

Corporate Headquarters

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

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

- Caveats for Release 11.2(1) Through 11.2(5), page 33
- Caveats for Release 11.2(1) Through 11.2(4), page 33
- Caveats for Release 11.2(1) Through 11.2(3), page 34
- Caveats for Release 11.2(1) Through 11.2(2), page 35
- Caveats for Release 11.2(1), page 35
- Caveats for Release 11.2(1), page 35
- Documentation CD-ROM, page 37

Determining Your Cisco IOS Release

To view the version of Cisco IOS software that is running on your Cisco 1000 series router, log in to the router, and enter the **show version** user EXEC command:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 1005 Software (C1005-Y-M), Version 11.2(7a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Tue 01-Jul-97 14:22 by kuong
Image text-base: 0x02004000, data-base: 0x022665E0

ROM: System Bootstrap, Version 5.3(17727) [enf 129], INTERIM SOFTWARE
BOOTFLASH: 1000 Bootstrap Software (C1000-RBOOT-R), Experimental Version
10.3(17727) [enf 100]

althame uptime is 1 minute
System restarted by reload
System image file is "master/c1005-y-mz.112-7a", booted via tftp from
223.255.254.254

cisco 1000 (68360) processor (revision @) with 3584K/512K bytes of memory.
Processor board ID 01329973
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
8K bytes of non-volatile configuration memory.
2048K bytes of processor board PCMCIA flash (Read/Write)
```

Cisco 1000 Series Routers and Platforms Supported

The following routers are supported by Cisco IOS Release 11.2:

- Cisco 1003 and Cisco 1004 ISDN routers
- Cisco 1005 router
- Cisco 1000 LAN Extender

Table 1 and Table 1 summarize the LAN and WAN interfaces supported on each Cisco 1000 series router. “Yes” means that a particular interface is supported. “No” means it is not supported.

Table 1 LAN Interfaces Supported

Interface	Cisco 1003/1004	Cisco 1005	Cisco 1000 LAN Extender
Ethernet (AUI)	No	No	Yes
Ethernet (10BaseT)	Yes	Yes	Yes

Table 2 WAN Interfaces Supported

Interface	Cisco 1003/1004	Cisco 1005	Cisco 1000 LAN Extender
EIA/TIA-232	No	Yes	No
X.21	No	Yes	Yes
V.35	No	Yes	Yes
EIA/TIA-449	No	Yes	No
EIA-530	No	Yes	No
ISDN BRI	Yes	Yes	No

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 is 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

Books	Chapter Topics
<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
<ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> 	<ul style="list-style-type: none"> 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> 	IP
<ul style="list-style-type: none"> • <i>Network Protocols Command Reference, Part 1</i> 	IP Routing
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 2</i> 	AppleTalk
<ul style="list-style-type: none"> • <i>Network Protocols Command Reference, Part 2</i> 	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> 	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> 	

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>.

Online Navigation

The Cisco IOS software documentation set is available as printed manuals or electronic documents. You can access the electronic documents either on the Cisco Documentation CD-ROM or at Cisco Connection Online (CCO) on the World Wide Web:

- On the Documentation CD-ROM, go to *Cisco Product Documentation*, select *Cisco IOS Software Configuration*, and then select *Cisco IOS Release 11.2*.
- On CCO, go to *Software and Support* and select *Documentation*. Next, select *Documentation*, click *Cisco IOS Software Configuration*, and then click *Cisco IOS Release 11.2*.

New online navigation enhancements for Release 11.2 include:

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

On the Documentation CD-ROM or CCO, go to *Cisco IOS Release 11.2*, and select *Cisco IOS Release 11.2 Configuration Guides, Command References*. Then select *Configuration Guide Master Index* or *Command Reference Master Index*. To access documentation related to an index entry, click the page number following the entry.

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

On the Documentation CD-ROM or CCO, go to *Cisco IOS Release 11.2*, and select *Cisco IOS Release 11.2 Configuration Guides, Command References*. Next, select *Cisco IOS 11.2 New Features*.

To access configuration documentation for a feature, do one of the following:

- Click the page number following the feature name.
- Using your browser Search function, search on one or more keywords from the feature name.

For additional information about the Documentation CD-ROM and CCO, refer to the sections “Caveats for Release 11.2(1)” and “Documentation CD-ROM” at the end of these release notes.

New Features in Release 11.2(1)

The following software enhancements added to Release 11.2 are divided into the following subjects:

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

Routing Protocols

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

IP Protocol and Feature Enhancements

The following new IP protocol software features are available:

- On Demand Routing—On Demand Routing (ODR) is a mechanism that provides minimum-overhead Internet Protocol (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 ceases.
- 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 do 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 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 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 area to backbone area connection to become logically part of the same network.

Border Gateway Protocol version 4 (BGP4) Enhancements

The following features have been added to Cisco BGP4 software:

- **BGP4 Soft Configuration**—BGP4 soft configuration allows BGP4 policies to be configured and activated without clearing the BGP session, hence 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 (AS) and the neighboring AS, 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.

- 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 might 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 similarly to their numbered counter-parts.

This feature also includes a new configuration mode, that 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 re-creating the entire list.

Currently, only packet and route filters can use Named IP ACL. 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 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 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 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.

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 that 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 (Frame Relay, SMDS, Ethernet, and so on.)

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 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 queuing algorithm, resulting in improved memory utilization. The combination of these factors further increases Enhanced IGRP suitability for deployment, particularly on low-end routers.
- **Implicit Protocol Acknowledgments:** Enhanced IGRP running within a router maintains state and reachability information about neighboring routers. This mechanism has been modified so that it no longer requires explicit notifications to be exchanged, but rather accepts 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 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: You can extend the bridge domain across the router interfaces to provide temporary solutions 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.
- Currently, IRB 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

The following feature has been added to Cisco 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 Novell software:

- **Display SAP by Name**—Network managers can 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 SAP table.
- **IPX Access Control List Violation Logging**—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—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.

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 ISDN and DDR software:

- Multichassis Multilink PPP (MMP)—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 a MLP bundle across multiple, independent platforms. The primary application for MMP is the ISDN dial-up 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 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.

- New devices can be added to the dial-up 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 Dial-up Network— Virtual Private Dial-up Network (VPDN) provides users from multiple disparate domains with secure access to their corporate home gateways via public networks or the Internet. This functionality is based on the Layer 2 Forwarding (L2F) specification that Cisco has proposed to the Internet Engineering Task Force (IETF) as an industry standard.

Service providers who wish to offer private dial-up network services can use VPDN to provide a single telephone number for all their client organizations. A customer can use dial-up access to a local point of presence where the access server identifies the customer by PPP username. The

PPP username is also used to establish a home gateway destination. When the home gateway is identified, the access server builds a secure tunnel across the service provider backbone to the customer 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 the VPDN independence of WAN technology. Because 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 are used 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 might 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 Link Access Procedure Balance (LAPB) encapsulation on DDR links or Snapshot Routing capabilities.

- **Combinet Packet Protocol (CPP) Support**—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 could not 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 software-based internetworks.

CPP does not provide many of the functions available in the Cisco 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 Combinet Packet Protocol (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 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 Systems Network Architecture (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 initial release of Cisco IOS Release 11.2.

New Features

The following new IBM software features are available:

- Native Client Interface Architecture Server—The native client interface architecture (NCIA) server, introduced by Cisco Systems for access of IBM SNA applications over routed internetworks, is 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 unencapsulates the TCP/IP packet and sends the LLC data to the host processor via remote source-route bridging (RSRB) or Data Data link switching plus (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 on RSRB peer connections.

Note that each client is a full SNA physical unit (PU) with one or more logical unit (LU)s. As such, each device requires one LLC connection at the central site router. The Cisco 4700 currently supports 3000 to 4000 LLC connections.

- TN3270 Server—The TN3270 Server is a new feature of the Channel Interface Processor (CIP) for the Cisco 7000 family of routers. The TN3270 Server allows TN3270 and TN3270E clients access to IBM and IBM-compatible mainframes without the limitations of existing alternatives. It off-loads 100 percent of the TCP/IP and TN3270 cycles from the mainframe and offers a robust, scalable, and dynamic implementation that meets the stringent requirements of the data center.

The TN3270 Server on the CIP supports up to 8000 concurrent sessions on a CIP and up to 16,000 concurrent sessions on a CIP2 card. The TN3270 Server offers the following advanced capabilities:

- Load Balancing and Redundancy: Provides effective utilization of CIP resources and more consistent response times.
- End-to-End Session Visibility: Provides enhanced management of resources.
- SNA Session Switching: The SNA Session Switch enables cross-domain traffic to bypass the owning virtual telecommunications access method (VTAM).
- TN3270E Support: In combination with a TN3270E client, provides advanced SNA management and SNA functionality, including printer support.
- Dynamic Definition of Dependent LUs: Provides simplified configuration and network definition at the router and in VTAM.
- Dynamic Allocation of LUs: Removes the need to pool LU resources while supporting multiple SNA model types.

TN3270 Server requires 32 MB of CIP DRAM to support up to 4000 sessions, 64 MB to support 8000 sessions, and 128 MB to support 16000 sessions. TN3270 Server can run concurrently with any of the other CIP applications (IP Datagram, TCP/IP Off-load, or CSNA), but operation of any of these features affects the total number of sessions supported due to contention for CIP processor cycles.

- Fast Switched Source-Route Translational Bridging —With software Release 11.2, Switched Source-Route Translational Bridging (SR/TLB) is fast switched. No queuing is done, and resource utilization is low. This enhancement is on by default, but can be disabled. It is supported across all router platforms.

Fast Switched SR/TLB improves performance on all platforms by a factor of at least two. It is ideal for IBM environments (for example, where low-cost Ethernet adapters are being installed on campus, but Token Ring connectivity to a front-end processor

(FEP) is still required) and for campus environments with a mix of Token Ring and Ethernet LANs or switches that rely on the Cisco IOS software for translational bridging.

- 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 Simple Network Management Protocol (SNMP) traps 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.

APPN Enhancements

The following features have been added to Cisco 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 (NN) to register the resources of end nodes (ENs) to the Central Directory Service (CDS) on advanced communication facility/virtual telecommunication Access Method (ACF/VTAM). A Cisco IOS NN now registers resource names with a VTAM CDS as soon as it establishes connectivity with it. Prior to this enhancement, the router acting as a NN could not register EN resources. ACF/VTAM could, however, query the router to find these resources.

The CDS reduces broadcast traffic in the network. Without an active CDS on ACF/VTAM, the NN must send a broadcast message to the network to locate nonlocal resources required for a session. With an active CDS, the NN 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, ENs should register the resources with the NN. Depending on the EN implementation, registration might occur automatically, might require configuration on the EN, or might not be a function of the EN.

- **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 NN and the DLUs attached to it for more complete network management information.

Data Link Switching+ (DLSw+) Features and Enhancements

The following features have been added to Cisco 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 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 the Cisco 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 the Cisco 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.

- Advanced Peer-to-Peer Networking (APPN) over DLSw+—Advanced Peer-to-Peer Networking (APPN) over DLSw+ allows the Cisco 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 (NNs).

- Source-Route Bridging (SRB) over FDDI to DLSw+—This feature allows access to DLSw+ over source-route bridged Fiber Distributed Data Interface (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 is useful either in environments with Token Ring switches that use FDDI as a campus backbone or in environments with Cisco 7000 and Cisco 7500 series routers providing SRB over an FDDI backbone.

This feature allows SRB over FDDI to provide the highest speed access between campus resources, while concurrently allowing DLSw+ for access to remote resources.

Currently, SRB over FDDI is supported by the Cisco 7000 and Cisco 7500 series platforms only.

Security Features

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

New Features

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

This feature can be used to build multiprotocol Virtual Private Networks (VPNs), using encrypted Generic Routing Encapsulation (GRE) tunnels. It can also be used to deploy secure telecommuting services, intranet privacy, and virtual collaborative or community-of-interest networks.

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

- **Kerberos V Client Support**—This feature provides full support of Kerberos V client authentication, including credential forwarding.

Systems with existing Kerberos V infrastructures can use their Key Distribution Centers (KDCs) to authenticate end users for network or router access.

This is a client implementation, not a Kerberos KDC. Kerberos is generally considered a legacy security service and is most beneficial in networks already using Kerberos.

TACACS+ Enhancements

The following features have been added to the Cisco Terminal Access Controller Access Control System (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 yields 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 generates 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 can 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.

New Features

ClickStart—ClickStart is a Web-based software solution for installing and configuring a Cisco router in minutes. ClickStart enables Cisco 1000 series ISDN access routers to be accessed by any Web browser on any desktop platform including MS Windows, Windows 95, Windows NT, UNIX, and MacOS. The easy-to-use Web-based interface guides users through the router installation process. By completing an initial setup form, a user can easily configure the router and bring up the ISDN network connection. The router is then manageable from a central location so that fine-tuning and upgrades can be performed remotely.

MIBs Supported

The following MIB support has been added:

- APPN DLUR MIB
See the “APPN 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

Cisco IOS Feature Sets for Cisco 1000 Series Routers

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

Table 3 through Table 5 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 might 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 might 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 5 provides a matrix of the new feature set organization and shows which feature sets are available on the various hardware platforms. These feature sets only apply to Cisco IOS Release 11.2.

Table 3 Cisco IOS Release 11.2 Feature Sets for Cisco 1000 Series Routers

Standard Feature Sets	Matrix Symbol
IP	Basic
IP/IPX	Basic
IP/AppleTalk	Basic
IP/IPX/AppleTalk	Basic, Plus, and Encrypt
IP/OSPF/PIM	Basic
IP/Async	Basic
IP/IPX/Async	Basic

Feature Set Tables

The Cisco IOS software is available in different feature sets depending upon the platform. Table 4 and Table 5 list the available feature sets for the Cisco series routers.

Table 4 Cisco 1003, Cisco 1004, and Cisco 1005 Routers Software Feature Sets , Part 1

Feature	Feature Set ¹			
	IP Routing ²	IP/IPX Routing ²	IP/AppleTalk Routing ²	IP/IPX/AppleTalk Routing
LAN Support				
AppleTalk 1 and 2 ³	—	—	Basic	Basic
GRE	Basic	Basic	Basic	Basic
Integrated routing and bridging (IRB) ⁴	Basic	Basic	Basic	Basic
IP	Basic	Basic	Basic	Basic
Novell IPX ⁵	—	Basic	—	Basic
Transparent and translational bridging ⁶	Basic	Basic	Basic	Basic
WAN Services⁷				
Dialer profiles	Basic	Basic	Basic	Basic
Frame Relay (Cisco 1005 only)	Basic	Basic	Basic	Basic
Frame Relay SVC Support (DTE) (Cisco 1005 only)	Plus	Plus	Plus	Plus
Frame Relay traffic shaping (Cisco 1005 only)	Basic	Basic	Basic	Basic
HDLC	Basic	Basic	Basic	Basic

Table 4 Cisco 1003, Cisco 1004, and Cisco 1005 Routers Software Feature Sets (Continued), Part 1

Feature	Feature Set ¹			
	IP Routing ²	IP/IPX Routing ²	IP/AppleTalk Routing ²	IP/IPX/AppleTalk Routing
ISDN (Cisco 1003 and Cisco 1004) ⁸	Basic	Basic	Basic	Basic
PPP	Basic	Basic	Basic	Basic
SMDS (Cisco 1005 only)	Basic	Basic	Basic	Basic
Switched 56 (Cisco 1005 only)	Basic	Basic	Basic	Basic
X.25	Basic	Basic	Basic	Basic
SLIP (Cisco 1005 only)	Basic	Basic	—	—
WAN Optimization				
Bandwidth-on-demand (Cisco 1003 and Cisco 1004)	Basic	Basic	Basic	Basic
Custom and priority queuing	Basic	Basic	Basic	Basic
Dial backup	Basic	Basic	Basic	Basic
Dial-on-demand ⁹	Basic	Basic	Basic	Basic
Header ¹⁰ and link compression ¹¹ (Cisco 1003 and Cisco 1004)	Basic	Basic	Basic	Basic
Payload compression (Cisco 1005 only)	Basic	Basic	Basic	Basic
Snapshot routing ¹²	Basic	Basic	Basic	Basic
Weighted fair queuing	Basic	Basic	Basic	Basic
IP Routing				
Enhanced IGRP	Basic	Basic	Basic	Basic
Enhanced IGRP Optimizations	Basic	Basic	Basic	Basic
IGRP	Basic	Basic	Basic	Basic
Network Address Translation Table (NAT)	Plus	Plus	Plus	Plus
On Demand Routing (ODR)	Basic	Basic	Basic	Basic
OSPF	Plus	Plus	Plus	Plus
OSPF Not-So-Stubby-Areas (NSSA)	Plus	Plus	Plus	Plus
OSPF On Demand Circuit (RFC 1793)	Plus	Plus	Plus	Plus
PIM	Plus	Plus	Plus	Plus
RIP	Basic	Basic	Basic	Basic
RIP Version 2	Basic	Basic	Basic	Basic
Other Routing				
AURP	—	—	Plus	Plus
IPX RIP	—	Basic	—	Basic
NLSP	Plus	Plus	Plus	Plus
SMRP	Plus	Plus	Plus	Plus
RTMP	—	—	Basic	Basic
Multimedia and Quality of Service				
Random Early Detection (RED)	Plus	Plus	Plus	Plus

Table 4 Cisco 1003, Cisco 1004, and Cisco 1005 Routers Software Feature Sets (Continued), Part 1

Feature	Feature Set ¹			
	IP Routing ²	IP/IPX Routing ²	IP/AppleTalk Routing ²	IP/IPX/AppleTalk Routing
Resource Reservation Protocol (RSVP)	Plus	Plus	Plus	Plus
Management				
ClickStart	Basic	Basic	Basic	Basic
HTTP Server	Basic	Basic	Basic	Basic
SNMP	Basic	Basic	Basic	Basic
Telnet	Basic	Basic	Basic	Basic
Security				
Access lists	Basic	Basic	Basic	Basic
Access security	Basic	Basic	Basic	Basic
Extended access lists	Basic	Basic	Basic	Basic
Lock and key	Basic	Basic	Basic	Basic
Router authentication and network layer encryption (40-bit or export-controlled 56-bit DES)	Encrypt	Encrypt	Encrypt	Encrypt
TACACS+ ¹³	Basic	Basic	Basic	Basic

1. This table lists feature sets that are common to the Cisco 1003, 1004, and 1005. For Cisco 1005 platform-specific feature sets, see Table 5.
2. The IP, IP/IPX, and IP/AppleTalk feature sets are not available with Plus, Plus 40, or Plus 56 feature-set options in Cisco IOS Release 11.2.
3. Includes AppleTalk load balancing.
4. 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.
5. The Novell IPX feature includes display SAP by name, IPX Access Control List violation logging, and plain-English IPX access lists.
6. Transparent and translational bridging is fast switched. This enhancement is on by default, but can be disabled.
7. Cisco 1005 "WAN Services" offers three feature set options: Option 1 includes HDLC, PPP, SDMS, and Frame Relay, but not X.25, and is available on all feature sets; Option 2 includes X.25 only and is available with the IP/IPX, IP/AppleTalk, and IP/IPX/AppleTalk feature sets; and Option 3 includes Async, PPP, and SLIP and is available with the IP, IP/IPX feature sets.
8. ISDN support includes calling line identification (CLI/ANI), ISDN subaddressing, and applicable WAN optimization features.
9. Dial-on-demand is available for the Cisco 1005 with "WAN Services" option only. See footnote 7, above.
10. IPX header compression (RFC 1553) is available in the feature sets that support IPX.
11. X.25 and Frame Relay payload compression. Payload compression is available for the Cisco 1005.
12. Snapshot routing is not included for the Cisco 1005.
13. TACACS+ Single Connection and TACACS+ SENDAUTH enhancements are supported.

Table 5 Cisco 1005 Platform-Specific Software Feature Sets, Part 2

Feature	Feature Set		
	IP/OSPF/PIM Routing ¹	IP/Async ¹	IP/IPX/Async ¹
LAN Support			
AppleTalk 1 and 2	—	—	—
GRE	Basic	Basic	Basic
Integrated routing and bridging (IRB) ²	Basic	Basic	Basic
IP	Basic	Basic	Basic
Novell IPX ³	—	—	Basic

Table 5 Cisco 1005 Platform-Specific Software Feature Sets, Part 2 (Continued)

Feature	Feature Set		
	IP/OSPF/PIM Routing ¹	IP/Async ¹	IP/IPX/Async ¹
Transparent and translational bridging ⁴	Basic	Basic	Basic
WAN Services⁵			
Async	—	Basic	Basic
Dialer profiles	Basic	Basic	Basic
Frame Relay	Basic	—	—
Frame Relay traffic shaping	Basic	—	—
HDLC	Basic	—	—
PPP ⁶	Basic	Basic	Basic
SMDS	Basic	—	—
Switched 56	Basic	—	—
X.25 ⁷	Basic	—	—
SLIP	—	Basic	Basic
WAN Optimization			
Custom and priority queuing	Basic	Basic	Basic
Dial-on-demand ⁸	Basic	Basic	Basic
Header ⁹ , link and payload compression ¹⁰	Basic	Basic	Basic
Snapshot routing ¹¹	Basic	Basic	Basic
Weighted fair queuing	Basic	Basic	Basic
IP Routing			
Enhanced IGRP	Basic	Basic	Basic
Enhanced IGRP Optimizations	Basic	Basic	Basic
IGRP	Basic	Basic	Basic
On Demand Routing (ODR)	Basic	Basic	Basic
OSPF	Basic	—	—
OSPF Not-So-Stubby-Areas (NSSA)	Basic	—	—
OSPF On Demand Circuit (RFC 1793)	Basic	—	—
PIM	Basic	—	—
RIP	Basic	Basic	Basic
RIP Version 2	Basic	Basic	Basic
Other Routing			
IPX RIP	—	—	Basic
Management			
ClickStart	Basic	Basic	Basic
HTTP Server	Basic	Basic	Basic
SNMP	Basic	Basic	Basic
Telnet	Basic	Basic	Basic

Table 5 Cisco 1005 Platform-Specific Software Feature Sets, Part 2 (Continued)

Feature	Feature Set		
	IP/OSPF/PIM Routing ¹	IP/Async ¹	IP/IPX/Async ¹
Security			
Access lists	Basic	Basic	Basic
Access security	Basic	Basic	Basic
Extended access lists	Basic	Basic	Basic
Kerberos V client support	—	—	—
Lock and key	Basic	Basic	Basic
TACACS+ ¹²	Basic	Basic	Basic

1. These feature sets are not available with the Plus, Plus 40, or Plus 56 feature set options in Cisco IOS Release 11.2.
2. 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.
3. The Novell IPX feature includes display SAP by name, IPX Access Control List violation logging, and plain-English IPX access lists.
4. Transparent and translational bridging is fast switched. This enhancement is on by default, but can be disabled.
5. Cisco 1005 “WAN Services” offers three feature-set options: Option 1 includes HDLC, PPP, SDMS, and Frame Relay, but not X.25, and is available on all feature sets; Option 2 includes X.25 only and is available with the IP/IPX, IP/AppleTalk, and IP/IPX/AppleTalk feature sets; and Option 3 includes async, PPP, and SLIP and is available with the IP, IP/IPX features sets.
6. PPP includes support for LAN protocols supported by the feature set, address negotiation, PAP and CHAP authentication, Multilink PPP, and PPP compression.
7. X.25 is available for the Cisco 1005 only and is available by itself in “WAN Services” Option 2 for the following feature sets: IP/IPX, IP/AppleTalk, and IP/IPX/AppleTalk.
8. Dial-on-demand is available for the Cisco 1005 with “WAN Services” option only. See footnote 5. above.
9. IPX header compression (RFC 1553) is available in the feature sets that support IPX.
10. X.25 and Frame Relay payload compression.
11. Snapshot routing is not included for the Cisco 1005.
12. TACACS+ Single Connection and TACACS+ SENDAUTH enhancements are supported.

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 software 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

Beginning with Cisco IOS Release 10.3, some software image sizes exceed 4 MB and, when compressed, exceed 2 MB. Also, some systems now require more than 1 MB of main system memory for data structure tables.

For Cisco routers to take advantage of the Release 11.2 features, you must upgrade the code or main system memory. Some platforms have specific chip or architecture requirements that affect what can be upgraded and in what increments.

Table 6 and Table 7 describe the memory requirements for each Cisco 1000 series router feature set supported by Cisco IOS Release 11.2.

Table 6 Cisco 1003 and Cisco 1004 Memory Requirements

Feature Set ¹	Required Flash Memory	Required Main Memory	Release 11.2 Runs from ²
IP	2/4 MB optional	8 ³ MB	RAM
IP Plus ⁴	2/4 MB optional	8 MB	RAM
IP Plus 40	2/4 MB optional	8 MB	RAM
IP Plus 56	2/4 MB optional	8 MB	RAM
IP/IPX	2/4 MB optional	8 MB	RAM
IP/AT	2/4 MB optional	8 MB	RAM
IP/IPX/AT	2/4 MB optional	8 MB	RAM
IP/IPX/AT Plus	4 MB ⁵	8 MB	RAM
IP/IPX/AT Plus 40	4 MB ⁵	8 MB	RAM
IP/IPX/AT Plus 56	4 MB ⁵	8 MB	RAM

1. If you need to upgrade the main memory for your Cisco 1003, Cisco 1004, or Cisco 1005 router, be sure to order the upgrade specific to your router.
2. When a system is running from Flash memory, you cannot update the system while it is running. You must use the Flash load helper.
3. Only 4 MB DRAM is required for releases 11.2(1) through 11.2(6).
4. Plus for the Cisco 1003 and Cisco 1004 includes OSPF, PIM, SMRP, NLSP, ATIP, AppleTalk AURP, RSVP, and NAT.
5. Only 2 MB of Flash memory is required for releases 11.2(1) through 11.2(6).

Table 7 Cisco 1005 Memory Requirements

Feature Set ¹	Required Flash Memory	Required Main Memory	Release 11.2 Runs from ²
IP	2/4 MB optional	8 ³ MB	RAM
IP Plus ³	4 MB ⁵	8 MB	RAM
IP Plus 40	4 MB ⁵	8 MB	RAM
IP Plus 56	4 MB ⁵	8 MB	RAM
IP/IPX	2/4 MB optional	8 MB	RAM
IP/AT	2/4 MB optional	8 ³ MB	RAM
IP/IPX/AT	2/4 MB optional	8 MB	RAM
IP/IPX/AT Plus	4 MB ⁵	8 MB	RAM
IP/IPX/AT Plus 40	4 MB ⁵	8 MB	RAM
IP/IPX/AT Plus 56	4 MB ⁵	8 MB	RAM
IP/OSPF/PIM	2/4 MB optional	8 MB	RAM
IP/Async	2/4 MB optional	8 ³ MB	RAM
IP/IPX/Async	2/4 MB optional	8 MB	RAM

1. If you need to upgrade the main memory for your Cisco 1003, Cisco 1004, or Cisco 1005 router, be sure to order the upgrade specific to your router.
2. When a system is running from Flash memory, you cannot update the system while it is running. You must use the Flash load helper.
3. Plus for the Cisco 1005 includes OSPF, PIM, NLSP, SMRP, AppleTalk IP, AppleTalk AURP, Frame Relay SVC, RSVP, and NAT.

Important Notes

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

- Traffic Shaping over Frame Relay
- LAN Extension
- Forwarding of Locally Sourced AppleTalk Packets

Traffic Shaping over Frame Relay

Traffic shaping over Frame Relay is available only in Release 11.2(8) and above. Refer to software defect IDs CSCdi60734 and CSCdi 88662.

LAN Extension

The LAN extension interface does not function correctly in Release 11.2(1). The behavior is that the LAN extension NCP negotiates and sets the LAN extension interface state to “up” and the **show controller lex number** command displays the message “No inventory message received from LAN Extender.” Turning on the LAN extension RCMD debugging shows that every remote command is being rejected with the message “LEX-RCMD: encapsulation failure.” There is no workaround. Refer to software defect ID CSCdi66478. This defect is fixed in software Release 11.2(2) and above.

Forwarding of Locally Sourced AppleTalk Packets

Our implementation of AppleTalk does not forward packets with local-source and destination network addresses. This behavior does not conform to the definition of AppleTalk in Apple Computer's *Inside AppleTalk* publication. However, this behavior is designed to prevent any possible corruption of the AppleTalk Address Resolution Protocol (AARP) table in any AppleTalk node that is performing MAC-address gleaning.

Caveats for Release 11.2(1) Through 11.2(12)

Possibly unexpected behavior in Cisco IOS Release 11.2 exists in the following areas:

- Access Server
- AppleTalk
- Basic System Services
- IBM Connectivity
- Interfaces and Bridging
- IP Routing Protocols
- ISO CLNS
- Novell IPX, XNS, and Apollo Domain
- TCP/IP Host-Mode Services
- Wide-Area Networking

A complete list of the caveats, including descriptions and possible workarounds, is available on the Documentation CD-ROM and on CCO:

- On the Documentation CD-ROM, go to *Cisco Product Documentation*, select *Cisco IOS Software Configuration*, click on *Cisco IOS Release 11.2*, then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, select *Important Notes and Caveats for Release 11.2*.
- On CCO, go to *Software and Support* and select *Documentation*. Next, go to *Cisco Documentation*, click on *Cisco IOS Software Configuration*, select *Cisco IOS Release 11.2*, and then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, click on *Important Notes and Caveats for Release 11.2*.

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

Possibly unexpected behavior in Cisco IOS Release 11.2 exists in the following areas:

- Access Server
- AppleTalk
- Basic System Services
- EXEC and Configuration Parser
- IBM Connectivity
- Interfaces and Bridging
- IP Routing Protocols
- LAT

- LLC Type 2
- Novell IPX, XNS, and Apollo Domain
- TCP/IP Host-Mode Services
- Wide-Area Networking

A complete list of the caveats, including descriptions and possible workarounds, is available on the Documentation CD-ROM and on CCO:

- On the Documentation CD-ROM, go to *Cisco Product Documentation*, select *Cisco IOS Software Configuration*, click on *Cisco IOS Release 11.2*, then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, select *Important Notes and Caveats for Release 11.2*.
- On CCO, go to *Software and Support* and select *Documentation*. Next, go to *Cisco Documentation*, click on *Cisco IOS Software Configuration*, select *Cisco IOS Release 11.2*, and then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, click on *Important Notes and Caveats for Release 11.2*.

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

Possibly unexpected behavior in Cisco IOS Release 11.2 exists in the following areas:

- Access Server
- AppleTalk
- Basic System Services
- IBM Connectivity
- Interfaces and Bridging
- IP Routing Protocols
- ISO CLNS
- LLC Type 2
- Novell IPX, XNS, and Apollo Domain
- Wide-Area Networking

A complete list of the caveats, including descriptions and possible workarounds, is available on the Documentation CD-ROM and on CCO:

- On the Documentation CD-ROM, go to *Cisco Product Documentation*, select *Cisco IOS Software Configuration*, click on *Cisco IOS Release 11.2*, then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, select *Important Notes and Caveats for Release 11.2*.
- On CCO, go to *Software and Support* and select *Documentation*. Next, go to *Cisco Documentation*, click on *Cisco IOS Software Configuration*, select *Cisco IOS Release 11.2*, and then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, click on *Important Notes and Caveats for Release 11.2*.

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

Possibly unexpected behavior in Cisco IOS Release 11.2 exists in the following areas:

- Basic System Services
- IBM Connectivity

- Interfaces and Bridging
- IP Routing Protocols
- LAT
- Novell IPX, XNS, and Apollo Domain
- Protocol Translation
- TCP/IP Host-Mode Services
- VINES
- Wide-Area Networking

A complete list of the caveats, including descriptions and possible workarounds, is available on the Documentation CD-ROM and on CCO:

- On the Documentation CD-ROM, go to *Cisco Product Documentation*, select *Cisco IOS Software Configuration*, click on *Cisco IOS Release 11.2*, then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, select *Important Notes and Caveats for Release 11.2*.
- On CCO, go to *Software and Support* and select *Documentation*. Next, go to *Cisco Documentation*, click on *Cisco IOS Software Configuration*, select *Cisco IOS Release 11.2*, and then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, click on *Important Notes and Caveats for Release 11.2*.

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

Possibly unexpected behavior in Cisco IOS Release 11.2 exists in the following areas:

- Access Server
- AppleTalk
- Basic System Services
- DECnet
- EXEC and Configuration Parser
- IBM Connectivity
- Interfaces and Bridging
- IP Routing Protocols
- ISO CLNS
- LAT
- Novell IPX, XNS, and Apollo Domain
- TCP/IP Host-Mode Services
- TN3270
- VINES
- Wide-Area Networking

A complete list of the caveats, including descriptions and possible workarounds, is available on the Documentation CD-ROM and on CCO:

- On the Documentation CD-ROM, go to *Cisco Product Documentation*, select *Cisco IOS Software Configuration*, click on *Cisco IOS Release 11.2*, then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, select *Important Notes and Caveats for Release 11.2*.
- On CCO, go to *Software and Support* and select *Documentation*. Next, go to *Cisco Documentation*, click on *Cisco IOS Software Configuration*, select *Cisco IOS Release 11.2*, and then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, click on *Important Notes and Caveats for Release 11.2*.

Caveats for Release 11.2(1) Through 11.2(7)

Possibly unexpected behavior in Cisco IOS Release 11.2 exists in the following areas:

- Access Server
- AppleTalk
- Basic System Services
- IBM Connectivity
- Interfaces and Bridging
- ISO CLNS
- Novell IPX, XNS, and Apollo Domain
- Wide-Area Networking

A complete list of the caveats, including descriptions and possible workarounds, is available on the Documentation CD-ROM and on CCO:

- On the Documentation CD-ROM, go to *Cisco Product Documentation*, select *Cisco IOS Software Configuration*, click on *Cisco IOS Release 11.2*, then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, select *Important Notes and Caveats for Release 11.2*.
- On CCO, go to *Software and Support* and select *Documentation*. Next, go to *Cisco Documentation*, click on *Cisco IOS Software Configuration*, select *Cisco IOS Release 11.2*, and then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, click on *Important Notes and Caveats for Release 11.2*.

Caveats for Release 11.2(1) Through 11.2(6)

Possibly unexpected behavior in Cisco IOS Release 11.2 exists in the following areas:

- AppleTalk
- Basic System Services
- IBM Connectivity
- Interfaces and Bridging
- IP Routing Protocols
- ISO CLNS
- TCP/IP Host-Mode Services
- Wide-Area Networking

A complete list of the caveats, including descriptions and possible workarounds, is available on the Documentation CD-ROM and on CCO:

- On the Documentation CD-ROM, go to *Cisco Product Documentation*, select *Cisco IOS Software Configuration*, click on *Cisco IOS Release 11.2*, then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, select *Important Notes and Caveats for Release 11.2*.
- On CCO, go to *Software and Support* and select *Documentation*. Next, go to *Cisco Documentation*, click on *Cisco IOS Software Configuration*, select *Cisco IOS Release 11.2*, and then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, click on *Important Notes and Caveats for Release 11.2*.

Caveats for Release 11.2(1) Through 11.2(5)

Possibly unexpected behavior in Cisco IOS Release 11.2 exists in the following areas:

- Basic System Services
- EXEC and Configuration Parser
- IBM Connectivity
- Interfaces and Bridging
- IP Routing Protocols
- Novell IPX, XNS, and Apollo Domain
- TCP/IP Host-Mode Services
- Wide-Area Networking

A complete list of the caveats, including descriptions and possible workarounds, is available on the Documentation CD-ROM and on CCO:

- On the Documentation CD-ROM, go to *Cisco Product Documentation*, select *Cisco IOS Software Configuration*, click on *Cisco IOS Release 11.2*, then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, select *Important Notes and Caveats for Release 11.2*.
- On CCO, go to *Software and Support* and select *Documentation*. Next, go to *Cisco Documentation*, click on *Cisco IOS Software Configuration*, select *Cisco IOS Release 11.2*, and then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, click on *Important Notes and Caveats for Release 11.2*.

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

Possibly unexpected behavior in Cisco IOS Release 11.2 exists in the following areas:

- Basic System Services
- IBM Connectivity
- Interfaces and Bridging
- IP Routing Protocols
- ISO CLNS
- Novell IPX, XNS, and Apollo Domain
- REXEC and Configuration Parser
- TCP/IP Host-Mode Services

- VINES
- Wide-Area Networking

A complete list of the caveats, including descriptions and possible workarounds, is available on the Documentation CD-ROM and on CCO:

- On the Documentation CD-ROM, go to *Cisco Product Documentation*, select *Cisco IOS Software Configuration*, click on *Cisco IOS Release 11.2*, then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, select *Important Notes and Caveats for Release 11.2*.
- On CCO, go to *Software and Support* and select *Documentation*. Next, go to *Cisco Documentation*, click on *Cisco IOS Software Configuration*, select *Cisco IOS Release 11.2*, and then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, click on *Important Notes and Caveats for Release 11.2*.

Caveats for Release 11.2(1) Through 11.2(3)

Possibly unexpected behavior in Cisco IOS Release 11.2 exists in the following areas:

- AppleTalk
- Basic System Services
- IBM Connectivity
- Interfaces and Bridging
- IP Routing Protocols
- ISO CLNS
- Novell IPX, XNS, and Apollo Domain
- Protocol Translation
- TCP/IP Host-Mode Services
- VINES
- Wide-Area Networking
- Interfaces and Bridging

A complete list of the caveats, including descriptions and possible workarounds, is available on the Documentation CD-ROM and on CCO:

- On the Documentation CD-ROM, go to *Cisco Product Documentation*, select *Cisco IOS Software Configuration*, click on *Cisco IOS Release 11.2*, then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, select *Important Notes and Caveats for Release 11.2*.
- On CCO, go to *Software and Support* and select *Documentation*. Next, go to *Cisco Documentation*, click on *Cisco IOS Software Configuration*, select *Cisco IOS Release 11.2*, and then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, click on *Important Notes and Caveats for Release 11.2*.

Caveats for Release 11.2(1) Through 11.2(2)

Possibly unexpected behavior in Cisco IOS Release 11.2 exists in the following areas:

- AppleTalk
- Basic System Services
- IBM Connectivity
- Interfaces and Bridging
- IP Routing Protocols
- ISO CLNS
- Novell IPX, XNS, and Apollo Domain
- Protocol Translation
- TCP/IP Host-Mode Services
- VINES
- Wide-Area Networking
- Interfaces and Bridging

A complete list of the caveats, including descriptions and possible workarounds, is available on the Documentation CD-ROM and on CCO:

- On the Documentation CD-ROM, go to *Cisco Product Documentation*, select *Cisco IOS Software Configuration*, click on *Cisco IOS Release 11.2*, then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, select *Important Notes and Caveats for Release 11.2*.
- On CCO, go to *Software and Support* and select *Documentation*. Next, go to *Cisco Documentation*, click on *Cisco IOS Software Configuration*, select *Cisco IOS Release 11.2*, and then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, click on *Important Notes and Caveats for Release 11.2*.

Caveats for Release 11.2(1)

Possibly unexpected behavior in Cisco IOS Release 11.2 exists in the following areas:

- AppleTalk
- Basic System Services
- IBM Connectivity
- Interfaces and Bridging
- IP Routing Protocols
- ISO CLNS
- Novell IPX, XNS, and Apollo Domain
- Protocol Translation
- TCP/IP Host-Mode Services
- VINES
- Wide-Area Networking
- Interfaces and Bridging

A complete list of the caveats, including descriptions and possible workarounds, is available on the Documentation CD-ROM and on CCO:

- On the Documentation CD-ROM, go to *Cisco Product Documentation*, select *Cisco IOS Software Configuration*, click on *Cisco IOS Release 11.2*, then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, select *Important Notes and Caveats for Release 11.2*.
- On CCO, go to *Software and Support* and select *Documentation*. Next, go to *Cisco Documentation*, click on *Cisco IOS Software Configuration*, select *Cisco IOS Release 11.2*, and then select *Release Notes for Cisco IOS Release 11.2*. From the bulleted list, click on *Important Notes and Caveats for Release 11.2*.

Cisco Connection Online

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

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

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

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, 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 NetWorks logo, 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, Stratm, StreamView, SwitchProbe, *The Cell*, TrafficDirector, VirtualStream, VlanDirector, Workgroup Director, Workgroup Stack, and XCI are trademarks; Empowering the Internet Generation and The Network Works. No Excuses. are service marks; 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.
9802R

