



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

April 16, 2001



Note

You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

These release notes for the Cisco 1000 series routers describe the enhancements provided in Cisco IOS Release 11.2 P. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 11.2 P, see *Caveats for Cisco IOS Release 11.2 P* that accompanies these release notes. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 11.2* on Cisco.com and the Documentation CD-ROM.



Note

Cisco IOS Release 11.2(26)P is the last scheduled maintenance release for Cisco IOS Release 11.2 P. TAC Support will continue to be available. These release notes will be the last release notes published for Cisco IOS Release 11.2 P.

Contents

These release notes describe the following topics:

- System Requirements, page 2
- New and Changed Information, page 10
- Important Notes, page 21
- Caveats, page 25
- Related Documentation, page 25



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

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

78-5212-15

- Obtaining Documentation, page 30
- Obtaining Technical Assistance, page 31

System Requirements

This section describes the system requirements for Cisco IOS Release 11.2 P:

- Memory Recommendations, page 2
- Hardware Supported, page 3
- Determining the Software Version, page 4
- Upgrading to a New Software Release, page 4
- Feature Set Tables, page 4

Memory Recommendations

Table 1 Memory Recommendations for the Cisco 1000 Series

Platforms	Image Name	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs from
Cisco 1003 and Cisco 1004	IP	c1000-y-mz	2/4 MB optional Flash	8 ¹ MB RAM	RAM
	IP Plus ²	c1000-bnsy-mz	2/4 MB optional Flash	8 MB RAM	RAM
	IP Plus 40	c1000-bnsy40-mz	2/4 MB optional Flash	8 MB RAM	RAM
	IP Plus 56	c1000-bnsy56-mz	2/4 MB optional Flash	8 MB RAM	RAM
	IP/IPX	c1000-ny-mz	2/4 MB optional Flash	8 MB RAM	RAM
	IP/AT	c1000-by-mz	2/4 MB optional Flash	8 MB RAM	RAM
	IP/IPX/AT	c1000-bny-mz	2/4 MB optional Flash	8 MB RAM	RAM
	IP/IPX/AT Plus	c1000-bnsy-mz	4 MB Flash ³	8 MB RAM	RAM
	IP/IPX/AT Plus 40	c1000-bnsy40-mz	4 MB Flash ³	8 MB RAM	RAM
	IP/IPX/AT Plus 56	c1000-bnsy56-mz	4 MB Flash ³	8 MB RAM	RAM

Table 1 Memory Recommendations for the Cisco 1000 Series (continued)

Platforms	Image Name	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs from
Cisco 1005	IP	c1005-y-mz	2/4 MB optional Flash	8 ¹ MB RAM	RAM
	IP Plus ⁴	c1005-bnsy-mz	4 MB Flash ³	8 MB RAM	RAM
	IP Plus 40	c1005-bnsy40-mz	4 MB Flash ³	8 MB RAM	RAM
	IP Plus 56	c1005-bnsy56-mz	4 MB Flash ³	8 MB RAM	RAM
	IP/IPX	c1005-ny-mz	2/4 MB optional Flash	8 MB RAM	RAM
	IP/AT	c1005-by-mz	2/4 MB optional Flash	8 ¹ MB RAM	RAM
	IP/IPX/AT	c1005-bny-mz	2/4 MB optional Flash	8 MB RAM	RAM
	IP/IPX/AT Plus	c1005-bnsy-mz	4 MB Flash ³	8 MB RAM	RAM
	IP/IPX/AT Plus 40	c1005-bnsy40-mz	4 MB Flash ³	8 MB RAM	RAM
	IP/IPX/AT Plus 56	c1005-bnsy56-mz	4 MB Flash ³	8 MB RAM	RAM
	IP/OSPF/PIM	c1005-y2-mz	2/4 MB optional Flash	8 MB RAM	RAM
	IP/Async	c1005-qy-mz	2/4 MB optional Flash	8 ¹ MB RAM	RAM
	IP/IPX/Async	c1005-nqy-mz	2/4 MB optional Flash	8 MB RAM	RAM

1. Only 4 MB DRAM is required for Releases 11.2(1) through 11.2(6).
2. Plus for the Cisco 1003 and Cisco 1004 includes OSPF, PIM, SMRP, NLSP, ATIP, AppleTalk AURP, RSVP, and NAT.
3. Only 2 MB of Flash memory is required for Releases 11.2(1) through 11.2(6).
4. Plus for the Cisco 1005 includes OSPF, PIM, NLSP, SMRP, AppleTalk IP, AppleTalk AURP, Frame Relay SVC, RSVP, and NAT.

Hardware Supported

Cisco IOS Release 11.2 P supports the Cisco 1000 series routers:

- Cisco 1003 and Cisco 1004 ISDN routers
- Cisco 1005 serial router

For detailed descriptions of the new hardware features, see “New and Changed Information” section on page 10.

Table 2 Supported Interfaces for the Cisco 1000 Series

Interface, Network Module, or Data Rate	Product Description	Platforms Supported
LAN Interfaces	Ethernet (10BaseT)	Cisco 1000 series
Data Rates	56/64/128 kbps	Cisco 1000 series
	1.544/2.048 Mbps	Cisco 1005 only
WAN Interfaces	EIA/TIA-232	Cisco 1005 only
	EIA/TIA-449	Cisco 1005 only
	EIA-530	Cisco 1005 only
	X.21	Cisco 1005 only
	V.35	Cisco 1005 only
	ISDN BRI	Cisco 1003 and Cisco 1004

Determining the Software Version

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

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 11.2 P Software (C1000-BNSY-MZ), Version 11.2(26)P, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *Upgrading the Cisco IOS Software Release in Cisco Routers and Modems* located at:

<http://www.cisco.com/warp/public/620/6.html>

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Cisco IOS Release 11.2 P supports the same feature sets as Cisco IOS Release 11.2, but Release 11.2 P can include new features supported by the Cisco 1000 series routers.



Caution

Cisco IOS images with strong encryption (including, but not limited to, 168-bit Triple Data Encryption Standard [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of United States government regulations. When applicable, purchaser and user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Table 3 and Table 4 list the features and feature sets supported by the Cisco 1000 series in Cisco IOS Release 11.2 P. Both use the following conventions:

- Basic—The feature is supported in the basic software image.
- Plus—The feature is supported in the Plus software image.
- – (en-dash)—The feature is not supported in the software image.

**Note**

This table might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard-copy documents were printed. If you have a Cisco.com login account, you can find image and release information regarding features prior to Cisco IOS Release 11.2(26)P by using the Feature Navigator tool at <http://www.cisco.com/go/fn>.

Table 3 Feature List by Feature Set for the Cisco 1000 Series, Part 1

Feature	Feature Set			
	IP Routing ¹	IP/IPX Routing ¹	IP/AppleTalk Routing ¹	IP/IPX/AppleTalk Routing
LAN Support				
AppleTalk 1 and 2 ²	–	–	Basic	Basic
GRE	Basic	Basic	Basic	Basic
Integrated routing and bridging (IRB) ³	Basic	Basic	Basic	Basic
IP	Basic	Basic	Basic	Basic
Novell IPX ⁴	–	Basic	–	Basic
Transparent and translational bridging ⁵	Basic	Basic	Basic	Basic
WAN Services⁶				
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
ISDN (Cisco 1003 and Cisco 1004) ⁷	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

Table 3 Feature List by Feature Set for the Cisco 1000 Series, Part 1 (continued)

Feature	Feature Set			
	IP Routing ¹	IP/IPX Routing ¹	IP/AppleTalk Routing ¹	IP/IPX/AppleTalk Routing
Dial backup	Basic	Basic	Basic	Basic
Dial-on-demand ⁸	Basic	Basic	Basic	Basic
Header ⁹ and link compression ¹⁰ (Cisco 1003 and Cisco 1004)	Basic	Basic	Basic	Basic
Payload compression (Cisco 1005 only)	Basic	Basic	Basic	Basic
Snapshot routing ¹¹	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
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

Table 3 Feature List by Feature Set for the Cisco 1000 Series, Part 1 (continued)

Feature	Feature Set			
	IP Routing ¹	IP/IPX Routing ¹	IP/AppleTalk Routing ¹	IP/IPX/AppleTalk Routing
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+ ¹²	Basic	Basic	Basic	Basic

1. 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.
2. This feature includes AppleTalk load balancing.
3. IRB supports IP, IPX, and AppleTalk; it is supported for transparent bridging, but not for SRB; it is supported on all media-type interfaces except X.25 and ISDN bridged interfaces; and IRB and concurrent routing and bridging (CRB) cannot operate at the same time.
4. The Novell IPX feature includes display SAP by name, IPX Access Control List violation logging, and plain-English IPX access lists.
5. Transparent and translational bridging is fast switched. This enhancement is on by default, but can be disabled.
6. 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 and IP/IPX features sets.
7. ISDN support includes calling line identification (CLI/ANI), ISDN subaddressing, and applicable WAN optimization features.
8. Dial-on-demand is available for the Cisco 1005 with “WAN Services” option only. See footnote 6.
9. IPX header compression (RFC 1553) is available in the feature sets that support IPX.
10. X.25 and Frame Relay payload compression. Payload compression is available for the Cisco 1005.
11. Snapshot routing is not included for the Cisco 1005.
12. TACACS+ Single Connection and TACACS+ SENDAUTH enhancements are supported.

Table 4 Feature List by Feature Set for the Cisco 1000 Series, 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
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	–	–

Table 4 Feature List by Feature Set for the Cisco 1000 Series, Part 2 (continued)

Feature	Feature Set		
	IP/OSPF/PIM Routing ¹	IP/Async ¹	IP/IPX/Async ¹
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
Security			
Access lists	Basic	Basic	Basic
Access security	Basic	Basic	Basic
Extended access lists	Basic	Basic	Basic
Kerberos V client support	–	–	–

Table 4 Feature List by Feature Set for the Cisco 1000 Series, Part 2 (continued)

Feature	Feature Set		
	IP/OSPF/PIM Routing ¹	IP/Async ¹	IP/IPX/Async ¹
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. This feature refers to 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.

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 1000 series routers for Release 11.2 P.

New Software Features in Cisco IOS Release 11.2(2)P and Later

There are no new software features supported by the Cisco 1000 series routers for Release 11.2(2)P and later.

New Software Features in Cisco IOS Release 11.2(1)P

The following new software features are supported by the Cisco 1000 series routers for Release 11.2(1)P and later. They are divided into the following categories:

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

Routing Protocols

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 recognize 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 permits 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: a limited memory and CPU, low-speed connections, and a default route configuration.

OSPF Not-So-Stubby-Areas (NSSA) defines a more flexible, hybrid method, whereby stub areas can import external OSPF routes in a limited fashion, so that OSPF can be extended across the stub to backbone connection.

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

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. 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 Benefits:

- NAT eliminates the need to readdress all hosts that require external access, saving time and money.
- 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.
- 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 ACL function similarly to their numbered counter-parts, 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 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 required quality of service of the application. The first RSVP-enabled router that receives the request informs the requesting host whether the requested resources are available or not. The request is forwarded to the next router, towards the sender of the traffic stream. If the reservations are successful, an end-to-end pipeline of resources is available for the application to obtain the required quality of service. RSVP enables applications with real-time traffic needs, such as multimedia applications, to coexist with bursty applications on the same network. RSVP works with both unicast and multicast applications.

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

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

RED is enabled on a per-interface basis. It “throttles back” lower-priority traffic first, allowing higher-priority traffic (as designated by an RSVP reservation or the IP precedence value) to continue unabated. RED works with RSVP to maintain end-to-end quality of service during peak traffic loads. Congestion is avoided by selectively dropping traffic during peak load periods. This is performed in a manner designed to damp out waves of sessions going through TCP slow start.

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

Exercise caution when enabling RED on interfaces that support multiprotocol traffic (in addition to TCP/IP), such as IPX or AppleTalk. RED is not designed for use with these protocols and could have deleterious affects. RED is a queuing technique; it cannot be used on the same interface as other queuing techniques, such as Standard Queuing, Custom Queuing, Priority Queuing, or Fair Queuing.

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

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 transmits 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 the suitability of Enhanced IGRP 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 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

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

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

Integrated routing and bridging provides:

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

Note that:

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

AppleTalk Features

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 becomes 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**—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 SAP table.
- **IPX Access Control List Violation Logging**—With this feature, routers can use existing router logging facilities to log IPX access control list (ACL) violations whenever a packet matches a particular access-list entry. The first packet to match an entry is logged immediately; updates are sent at approximately 5-minute intervals.

This feature allows logging of:

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

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

- **Plain English IPX access list**—Through the use of this feature, the most common protocol and socket numbers used in IPX extended ACLs can be specified by either name or number instead of only 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

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 *stack group*—a group of routers or access servers that operate as a group when receiving MLP calls. Any member of the stack group 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 stack group 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 stack group can be connected over many types of LAN or WAN media. stack group 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 dial-up pool at any time.
- The load for reassembly and resequencing can be shared across all devices in the stack group. 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) allows users from multiple disparate domains to gain secure access to their corporate home gateways via public networks or the Internet. This functionality is based on the Layer 2 Forwarding (L2F) specification that Cisco has proposed as an industry standard to the Internet Engineering Task Force (IETF).

Service providers who wish to offer private dial-up network services can use VPDN to provide a single telephone number for all their client organizations. A customer can use dial-up access to a local point of presence where the access server identifies the customer by PPP 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 independence of VPDN from 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 allow the user to separate the network layer, encapsulation, and dialer parameters portion of the configuration from that of the interface used to place or receive calls. Dialer profile extends the flexibility of current dial-up configurations. For example, on a single ISDN PRI or PRI rotary group, it is now possible to allocate separate profiles for different classes of user. These profiles 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—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 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 Combinet Packet Protocol (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). 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 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.

Security Features

New Features

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

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

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

exponentially with the number of routers. Router authentication requires the network administrator to compare the hashes produced by the routers once during initial configuration. This version of encryption is not IPSEC compliant.

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

TACACS+ Enhancements

The following features have been added to Cisco 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**—SENAUTH is a TACACS+ protocol change to increase security. SENDAUTH supersedes SENDPASS. SENDAUTH and SENDPASS are documented in Version 1.63 of the TACACS+ protocol specification, which is available from Cisco.com or via anonymous FTP from ftp-eng.cisco.com.

The network access server can support both SENDAUTH and SENDPASS simultaneously. It detects if the daemon is able to support SENDAUTH and, if not, uses 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 from the network access server.

Network Management

New Features

ClickStart—ClickStart is a powerful Web-based software solution for 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
- RTTMON Support
- Cisco IP Encryption MIB
- Cisco Modem Management MIB
- Cisco SYSLOG MIB
- Cisco TN3270 Server MIB

Important Notes

The following sections contain important notes about Cisco IOS Release 11.2 P that can apply to the Cisco 1000 series routers.

Traffic Shaping over Frame Relay

Traffic shaping over Frame Relay is available only in Release 11.2(8) and above. Refer to software caveat IDs CSCd60734 and CSCdi88662.

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.

Changes to LANE Commands

The commands **lane auto-config-atm-address**, **lane fixed-config-atm-address**, and **lane config-atm-address** have been changed. Previously, the effect of these commands depended on whether they were used on a major interface or on a subinterface. In Release 11.2(1) and later releases, the optional **config** keyword indicates that the command causes the configuration server to listen on the designated address. If the keyword is not used, the command causes the other LANE clients and servers on the interface to use the designated address to locate the configuration server. Refer to the *Wide-Area Networking Command Reference* publication for more information about these commands.

Enabling IPX Routing

The Token Ring interface is reset whenever IPX routing is enabled on that interface.

Using LAN Emulation (LANE)

Note the following information regarding the LAN Emulation (LANE) feature in Cisco IOS Release 11.2:

- LANE is available for use with Cisco 4500, 4700, 7000, and 7500 series routers connected to either an LS100 or LS1010 switch. LANE requires at least version 3.1(2) of the LS100 software, which requires a CPU upgrade if you are currently running software prior to version 2.5.
- The LS2020 cannot be used for LANE because it does not support UNI 3.0 and point-to-multipoint SVCs.
- Routing of IP, IPX, AppleTalk, DECnet, VINES, and XNS is supported.
- HSRP is supported.
- LANE does not support CLNS or LANE over PVCs.
- AppleTalk Phase 1 cannot be routed to AppleTalk Phase 2 via LANE.

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 the Apple Computer *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.

Some 40-Bit Encryption Images Are Unavailable

Cisco is conducting an internal review of the build and distribution processes associated with its 40-bit Cisco IOS cryptographic products. So that we can provide you with seamless access to Cisco IOS 40-bit encryption capability, Cisco provides access to the most current 40-bit encryption images, beginning with Releases 11.2 (12), 11.2(12)P, and 11.3(2). The following 40-bit encryption images are indefinitely unavailable: 11.2(1) - 11.2(11.2), 1.2(2)P - 11.2(11.1)P, 11.2(1)F - 11.2(4)F, 11.3(1).

This review is not related to any new or previously unreported bugs. The information gathered in the review is used to implement new automated development, and order processing applications.

Release 11.2(7a) Fixes Caveats CSCdj24132 and CSCdj21944

Cisco IOS Releases 11.2(7) and 11.2(7)P were deferred due to two severe defects. It was determined that these caveats were significant enough to merit a software rebuild. The rebuild includes the caveat fixes and is renumbered to 11.2(7a).

These defects are bugs CSCdj24132 and CSCdj21944 and are described as follows:

- A router crashes every time it receives an ISDN Q.931 DISCONNECT message. This problem only affects net3 switch types.

A router might also crash if the **clear interface bri** command is issued. This problem only affects net3, vn2/vn3, and ts013 switch types. [CSCdj24132]

- A memory allocation error occurs after a large number of modem calls are placed to an AS5200 configured for PRI ISDN. After the AS5200 starts to generate a number of these memory allocation error messages, calls cannot be answered.

The following are indicators that can be used to determine if the AS5200 is encountering this problem:

- When the Cisco AS5200 runs out of memory, MALLOC Failure messages similar to the one shown are displayed:

```
%SYS-2-MALLOCFAIL: Memory allocation of 1056 bytes failed from 0x2214E776, pool
Processor, alignment 0
-Process= "Net Periodic", ipl= 0, pid= 34
-Traceback= 2214D3E0 2214E542 2214E77E 2214BEC6 2214C12A 22159466 2215E86E 22140BDE
2213B688 2213B6E0
```

- If there is no ISDN process in the output from the **show process** command, and you start to see “%SYS-2-MALLOCFAIL” error messages, then the memory leak was caused by this bug.
- If there are more than 46 entries marked “Active” in the output from the **show isdn history** command, the memory leak was caused by this bug.

[CSCdj21944]

Release 11.2(7a) and all subsequent releases of Cisco IOS software include the fix for these caveats.

Release 11.2(10a) Fixes Caveats CSCdj58676 and CSCdj60533

Cisco IOS Releases 11.2(10) and 11.2(10)P were deferred due to two severe defects: CSCdj58676 and CSCdj60533. It was determined that these caveats were significant enough to merit a software rebuild. The rebuild includes the caveat fixes and is renumbered to 11.2(10a).

These defects are described as follows:

- With EIGRP routing configured, redistribution of the following type of routes into the EIGRP process do not work correctly:
 - A directly connected route
 - A static route with the next hop set to an interface
 - A static route with the next hop set to a dynamically learned route

The nature of the defect is that it only occurs after a dynamic event. If redistribution is manually configured, EIGRP initially reflects correct information in the topology table. However, after any sort of dynamic event, the topology table becomes invalid, and routing updates sent are inaccurate. [CSCdj58676]



Note The code changes committed by CSCdj58676 resolved some issues but created the symptoms reported in CSCdj65737. The code changes for CSCdj58676 were only committed to releases 11.2(10a), 11.2(10a)BC and 11.2(10a)P; therefore, they are the only ones affected by CSCdj65737. See the “Release 11.2(11) Reintroduces Caveat CSCdj28874” section on page 24 for more information related to CSCdj58676 and CSCdj65737.

- The ARP lookup routine might suspend, causing unexpected behaviors for IP protocols. For example, if the OSPF routing process is traversing a list of neighbors to send LSA packets and the ARP routine is called, the ARP routine suspension could cause a system reset. [CSCdj60533]

Release 11.2(11) Reintroduces Caveat CSCdj28874

CSCdj65737 was introduced by code changes associated with CSCdj58676. The issue is that routes are not being redistributed into EIGRP from other routing protocols if both protocols are routing for the same major network.

The code changes for CSCdj58676 were only applied to Releases 11.2(10a), 11.2(10a)BC and 11.2(10a)P; therefore, those releases are the only ones impacted by CSCdj65737. The fix to CSCdj65737 is to back out the code changes committed by CSCdj58676 and CSCdj28874. That change has the effect of reintroducing the behavior reported by CSCdj28874, which is described as follows:

- When a network is included in the EIGRP routing process because it is specified with the **network x.x.x.x** command and that same network is redistributed into EIGRP via the **redistribute connected** command, there are two entries for the network in the EIGRP topology table.

If the interface connecting that network goes down, only one of the two entries are removed from the topology table. The entry learned via redistribution remains in the topology table and is advertised, even though it is no longer valid. [CSCdj28874]

The code back-outs of CSCdj65737 and reintroduction of CSCdj28874 appears in the following releases:

- 11.2(11), 11.2(11)BC, 11.2(11)P
- 11.1(16), 11.1(16)AA, 11.1(16)CA, 11.1(16)IA

All defect resolution information pertaining to CSCdj58676 is superseded by the details relating to CSCdj65737.

The symptoms of CSCdj28874 can be avoided by not using the **redistributed connected** command and instead specifying the individual networks to be redistributed into Enhanced IGRP.

Release 11.2(15a) and 11.2(15a) P

After the release of Cisco IOS Release 11.2(15) and 11.2(15) P, a serious defect (caveat CSCdk33475) was identified that impacts Enhanced IGRP for Cisco IOS Releases 11.2(14.1) through 11.2(15.2) and Releases 11.2(14.1)P through 11.2(15.2)P. It was determined that this defect was significant enough to merit a software rebuild. The rebuild includes the caveat fix and is renumbered to Release 11.2(15a) and 11.2(15a)P.

Caveat CSCdk33475 causes a router to fail after the command **show ip eigrp events** is issued. While this **show** command is not required for normal operation, it is used often enough by TAC personnel and customers to cause major havoc to customers who are running images with this defect.

Release 11.2(15a) and 11.2(15a)P and all subsequent releases of Cisco IOS software, including Release 11.2(16) and 11.2(16)P, include the fix for this caveat.

Cisco IOS Release 11.2 Switches to Long-Cycle Maintenance Releases

Beginning with Cisco IOS Release 11.2(15) and 11.2(15)P, all subsequent 11.2 and 11.2 P releases switch to Long-Cycle Maintenance Releases. A new 11.2 and 11.2 P maintenance release is scheduled to be available every thirteen weeks during the Long-Cycle Maintenance Release period. Interim builds will be available approximately every three weeks.

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

For information on caveats in Cisco IOS Release 11.2 P, see *Caveats for Cisco IOS Release 11.2 P*.

All caveats in Cisco IOS Release 11.2 are also in Cisco IOS Release 11.2 P.

For information on caveats in Cisco IOS Release 11.2, see the caveats sections in *Cross-Platform Release Notes for Cisco IOS Release 11.2*, which list severity 1 and 2 caveats.



Note

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, go to Cisco.com and press **Login**. Then go to **Software Center: Cisco IOS Software: Cisco Bugtool Navigator II**. Another option is to go to <http://www.cisco.com/support/bugtools>.

Related Documentation

The following sections describe the documentation available for the Cisco 1000 series routers. These documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 25
- Platform-Specific Documents, page 26
- Feature Modules, page 27
- Cisco IOS Software Documentation Set, page 27

Release-Specific Documents

The following documents are specific to Cisco IOS Release 11.2 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 11.2*

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.2: Product Specific Release Notes for Cisco IOS Release 11.2: Cross-Platform Release Notes for Cisco IOS Release 11.2

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.2: Product Specific Release Notes for Cisco IOS Release 11.2: Cross-Platform Release Notes for Cisco IOS Release 11.2

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

Technical Documents

- Caveats for Cisco IOS Release 11.2 and 11.2 P

See the “Caveats” section in *Cross-Platform Release Notes for Cisco IOS Release 11.2* and the entire *Caveats for Cisco IOS Release 11.2 P* document, which contain caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 11.2 and Release 11.2 P.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.2: Product Specific Release Notes for Cisco IOS Release 11.2

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.2: Product Specific Release Notes for Cisco IOS Release 11.2



Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, go to Cisco.com and press **Login**. Then go to **Software Center: Cisco IOS Software: Cisco Bugtool Navigator II**. Another option is to go to <http://www.cisco.com/support/bugtools>.

Platform-Specific Documents

These individual and groups of documents are available for the Cisco 1000 series routers on Cisco.com and the Documentation CD-ROM:

- Cisco 1000 series hardware installation
- Cisco 1000 series configuration notes
- *Cisco 1003 and Cisco 1004 Public Network Certification*
- *Cisco 1003 and Cisco 1004 Series Router User Guide*
- *Cisco 1005 Public Network Certification*
- *Cisco 1005 User Guide*
- *Cisco 1020 Command Reference*
- *Cisco 1020 User Guide*
- *Cisco 1005 Public Network Certification*
- *Cisco 1003 and Cisco 1004 Public Network Certification*
- Release notes for Cisco 1000 series routers

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco Product Documentation: Access Servers and Routers: Fixed Configuration Access Routers: Cisco 1000 series

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Routers: Fixed Configuration Access Routers: Cisco 1000 series

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 11.2 P and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.2: Feature Guide for Cisco IOS Release 11.2 P

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.2: Feature Guide for Cisco IOS Release 11.2 P

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents that are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On Cisco.com and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.2: Cisco IOS Release 11.2 Configuration Guides/Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.2: Cisco IOS Release 11.2 Configuration Guides/Command References

Cisco IOS Release 11.2 Documentation Set

Table 5 describes the contents of the Cisco IOS Release 11.2 software documentation set, which is available in electronic form and in printed form ordered.



Note

You can find the most current Cisco IOS documentation on Cisco.com and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.2

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.2

Table 5 Cisco IOS Release 11.2 Documentation Set

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Configuration Fundamentals Configuration Guide</i> • <i>Configuration Fundamentals Command Reference</i> 	Access Server and Router Product Overview User Interface System Images and Configuration Files Using ClickStart, AutoInstall, and Setup Interfaces System Management
<ul style="list-style-type: none"> • <i>Security Configuration Guide</i> • <i>Security Command Reference</i> 	Network Access Security Terminal Access Security Accounting and Billing Traffic Filters Controlling Router Access Network Data Encryption with Router Authentication
<ul style="list-style-type: none"> • <i>Access Services Configuration Guide</i> • <i>Access Services Command Reference</i> 	Terminal Lines and Modem Support Network Connections AppleTalk Remote Access SLIP and PPP XRemote LAT Telnet TN3270 Protocol Translation Configuring Modem Support and Chat Scripts X.3 PAD Regular Expressions

Table 5 Cisco IOS Release 11.2 Documentation Set (continued)

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> 	

**Note**

Cisco Management Information Base (MIB) User Quick Reference is no longer published. If you have an account with Cisco.com, you can find the current list of MIBs supported by Cisco. To reach the *Cisco Network Management Toolkit*, go to Cisco.com, press **Login**, and click to **Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

The most current Cisco documentation is available on the World Wide Web at <http://www.cisco.com>. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

You can e-mail your comments to bug-doc@cisco.com.

For your convenience, many documents contain a response card behind the front cover for submitting your comments by mail. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

The following sections provide sources for obtaining technical assistance from Cisco Systems.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

Cisco.com registered users who cannot resolve a technical issue by using the TAC online resource can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section on page 25.

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

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

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