



Doc. No. 78-4062-02

Release Notes for Cisco IOS Release 11.2 F

February 24, 1997

These release notes describe the features and caveats for Cisco Internetwork Operating System (Cisco IOS) Release 11.2 F, beginning with Release 11.2(3)F, up to and including Release 11.2(4)F.

Prior to Cisco IOS Release 11.2, maintenance releases of major Cisco IOS software releases were used to deliver additional new features. Beginning with Cisco IOS Release 11.2, Cisco Systems provides as many as three software release “trains” based on a single version of Cisco IOS software. Maintenance releases of the Major train software deliver fixes to software defects only, thus providing the most stable software for your network for the features you need. In addition to the Major train, there are up to two Early Deployment (ED) trains. One ED train—Release 11.2 P—delivers both fixes to software defects and support for new Cisco platforms. The other ED train—Release 11.2 F—delivers fixes to software defects, new platform support, and new cross-platform functionality.

Use Release 11.2 F when the features and functionality you need are provided only in this release.

Use this release note in conjunction with the *Release Notes for Cisco IOS Release 11.2* and *Release Notes for Cisco IOS Release 11.2 P* documents. The software caveats that apply to Release 11.2 and Release 11.2 P also apply to Release 11.2 F.

Introduction

These release notes discuss the following topics:

- Documentation, page 2
- Platform Support for Release 11.2 F, page 2
- New Features in Release 11.2(4)F, page 2
- New Features in Release 11.2(3)F, page 11

Corporate Headquarters

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

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

- Cisco IOS Packaging, page 13
- Memory Requirements for Release 11.2 F, page 24
- Microcode Software, page 25
- Important Notes, page 26
- Release 11.2(4)F Caveats, page 26
- Release 11.2(3)F Caveats/Release 11.2(4)F Modifications, page 26
- Cisco Connection Online, page 27
- Documentation CD-ROM, page 27

Documentation

For Cisco IOS Release 11.2 F, the Cisco IOS documentation consists of the *Feature Guide for Cisco IOS Release 11.2 P* and the *Feature Guide for Cisco IOS Release 11.2 F*. The feature guides supplement the Cisco IOS Release 11.2 configuration guide and command reference publications.

In the *Feature Guide for Cisco IOS Release 11.2 F*, each new feature is documented in its own section, which includes configuration tasks as well as new and changed command reference pages. Occasionally, new software features are documented in conjunction with the *Feature Guide for Cisco IOS Release 11.2 P*. The *Feature Guide for Cisco IOS Release 11.2 F* contains documentation for the new features described in these release notes.

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

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

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

Platform Support for Release 11.2 F

Cisco IOS Release 11.2 F supports the same router and access server platforms as Cisco IOS Release 11.2. For a list of additional platforms that might also be supported at each maintenance release, refer to the *Release Notes for Cisco IOS Release 11.2 P* document.

Release 11.2(4)F and later support the IPeXchange Internet Gateway platform.

New Features in Release 11.2(4)F

Maintenance releases of Cisco IOS Release 11.2 F deliver fixes to software defects, new platform support, and new cross-platform functionality.



Caution When determining whether to deploy software from the Major or Early Deployment release train, you should weigh the importance you place on maximizing product capability versus maximizing operational stability. Regardless of the train you choose, an early release of software should always be tried in a test network before being deployed in a production network.

The following software enhancements have been added to Release 11.2(4)F. These features are available only in Release 11.2 F. These features are documented in the *Feature Guide for Cisco IOS Release 11.2 F* publication. For additional platform support, refer to the *Release Notes for Cisco IOS Release 11.2 P*.

Note Some new features in Cisco IOS Release 11.2 F might not be supported on new platforms introduced in Cisco IOS Release 11.2 P.

Cisco 1003, Cisco 1004 IP/X31 Feature Set

A new feature set for the Cisco 1003 and Cisco 1004 ISDN routers is available in Cisco IOS Release 11.2(4)F and later releases. This feature set contains the same features as the Cisco 1003, Cisco 1004 IP set (see the *Release Notes for Cisco IOS Release 11.2*) and includes X.31 support. See Table 7 for a list of additional features available in this new feature set. Memory requirements for the IP/X31 feature set are shown in Table 10.

Double Authentication

Double Authentication provides additional authentication for Point-to-Point Protocol (PPP) sessions. Previously, PPP session authentication was limited to CHAP (or PAP). With Double Authentication, you essentially require remote users to pass a second stage of user authentication—after CHAP or PAP authentication—before they can gain network access.

If you configure your local host (NAS or router) for Double Authentication, remote users will be required to complete a second stage of authentication to gain their assigned user network privileges. This second (“double”) authentication requires a password that is known to the user but *not* stored on the user’s remote host. Therefore, the second authentication is specific to a user, not to a host. This feature provides an additional level of security that is be effective even if the remote host is stolen.

DRP Server Agent

The Director Response Protocol (DRP), a simple User Datagram Protocol (UDP)-based application developed by Cisco Systems, enables Cisco’s DistributedDirector product to query routers (DRP Server Agents) in the field for Border Gateway Protocol (BGP) and Interior Gateway Protocol (IGP) routing table metrics between distributed servers and clients. DistributedDirector, a separate standalone product, uses DRP to transparently redirect end-user service requests to the topologically closest responsive server. DRP enables DistributedDirector to provide dynamic, scalable, and “network intelligent” Internet traffic load distribution between multiple geographically dispersed servers.

DRP Server Agents are border routers (or peers to border routers) that support the geographically distributed servers for which DistributedDirector service distribution is desired. Note that, because DistributedDirector makes decisions based on BGP and IGP information, all DRP Server Agents must have access to full BGP and IGP routing tables.

Refer to the *Cisco DistributedDirector 2501 Installation and Configuration Guide* or the *Cisco DistributedDirector 4700-M Installation and Configuration Guide* for information on how to configure DistributedDirector.

Note Cisco IOS Release 11.2(4)F does not support the DRP Server Agent feature on the Cisco 3600 router.

IP Enhanced IGRP Route Authentication

This feature provides MD5 authentication of routing updates from the IP EIGRP routing protocol. The MD5 keyed digest in each IP Enhanced IGRP packet prevents the introduction of unauthorized or false routing messages from unapproved sources.

IPeXchange Internet Gateway

The IPeXchange Internet Gateway connects Novell NetWare or other IPX-based users to the Internet or other TCP/IP-based network services. IPeXchange allows workstations to use TCP/IP-based applications such as Telnet, FTP, and Netscape Navigator without requiring a TCP/IP protocol stack on each workstation. Instead, the IPeXchange Internet Gateway provides a TCP/IP gateway with a single IP address for the entire IPX network.

The IPeXchange Internet Gateway is a client/server product.

The server is a Cisco router that runs the Cisco IOS software as the IPeXchange server software. The server, which is sometimes referred to as a gateway, is connected to both an IPX network and a TCP/IP-based network, such as the Internet.

An IPeXchange client is a Windows 3.x- or Windows 95-based PC that runs the IPeXchange client software. The PC is connected to an IPX network.

The IPeXchange Internet Gateway offers the following benefits:

- A security firewall between the IPX network and the Internet using Cisco IOS software features.
- A fault-tolerant environment through the use of multiple IPeXchange gateways, multiple Internet connections, or both.

The following features sets for IPeXchange are available:

- Cisco 1003, Cisco 1004-based IPeXchange platforms:
 - IPeXchange 20 User 1003/1004 Set
 - IPeXchange 50 User 1003/1004 Set
- Cisco 1005-based IPeXchange platforms:
 - IPeXchange 20 User 1005 Sync Set
 - IPeXchange 50 User 1005 Sync Se
 - IPeXchange 1005 Async Set
- Cisco 2500-based IPeXchange platforms:
 - IP/IPX/AT/DEC IPeXchange Set
 - IP/IPX/AT/DEC IPeXchange Plus Set
 - IP/IPX/AT/DEC IPeXchange Plus 40 Set
 - IP/IPX/AT/DEC IPeXchange Plus 56 Set

IPX Named Access Lists

This feature allows you to identify IPX access lists with an alphanumeric string (a name) rather than a number. This feature allows you to configure an unlimited number of the following types of access lists:

- Standard
- Extended
- SAP
- NLSP route aggregating (also known as summary)

If you identify your access list with a name rather than a number, the mode and command syntax are slightly different. Currently, only packet and route filters can use a named list.

This feature allows you to maintain security by using a separate and easily identifiable access list for each user or interface. It also removes the limit of 100 lists per filter type.

Consider the following before configuring IPX named access lists:

- Access lists specified by name are not compatible with releases prior to 11.2(4)F.
- Access list names must be unique across all protocols.
- Numbered access lists are also available, as described in the Cisco IOS Release 11.2 *Network Protocols Configuration Guide, Part 2*.

IPX SAP-after-RIP

This feature links Service Advertising Protocol (SAP) updates to Routing Information Protocol (RIP) updates so that SAP broadcast and unicast updates automatically occur immediately after the completion of the corresponding RIP update. It ensures that no service information will be rejected by a remote router because it lacks a valid route to the service. As a result of this feature, periodic SAP updates are sent at the same frequency as RIP updates.

The default behavior of the router is to send RIP and SAP periodic updates with each using its own update interval, depending on the configuration. In addition, RIP and SAP periodic updates are jittered slightly, such that they tend to diverge from each other over time. This feature synchronizes SAP and RIP updates.

In addition, it is now possible to disable the sending of general RIP and/or SAP queries on a link when it first comes up.

Sending all SAP and RIP information in a single update reduces bandwidth demands and eliminates erroneous rejections of SAP broadcasts.

Linking SAP and RIP updates populates the service table at the remote router more quickly, because services will not be rejected due to the lack of a route to the service. This can be especially useful on WAN circuits where the update intervals have been greatly increased to reduce the overall level of periodic update traffic on the link.

RIP and SAP general queries are normally sent by remote routers when a circuit first comes up. On WAN circuits, two full updates of each kind are often sent across the link. The first update is a full broadcast update, triggered locally by the link-up event. The second update is a specific (unicast) reply triggered by the general query received from the remote router. By disabling the sending of general queries when the link first comes up, it is possible to reduce traffic to a single update, and save bandwidth.

NLSP Enhancements

This feature allows the router to interpret the maximum lifetime field in a Level 1 link-state packet (LSP) in hours or seconds. Previously, the field was interpreted in seconds only.

By being able to interpret the maximum lifetime field in hours, the router will be able to keep LSP packets for a much longer time which will reduce overhead on slower-speed serial links and keep ISDN links from becoming active unnecessarily.

PAD Enhancements

Cisco's implementation of packet assembler/disassembler (PAD) has been enhanced:

- PAD calls can now be made to destinations that are not reachable over physical X.25 interfaces, but over TCP tunnels. This enables a Cisco router with only an Ethernet interface to communicate with PAD protocols to an X.25 network using TCP based X.25 switching. To enable this function, use the **service pad to-xot** and **service pad from-xot** global configuration commands.
- The **/use-map** option is added to the **pad** command and to the **translate x25** command. This option allows all the X.25 map facilities to be applied to the outgoing PAD call or protocol translation call.
- The **idle minutes** argument is added to the **translate x25** command. This new incoming connection request option specifies the number of minutes the virtual circuit (VC) is idle. The option enables the protocol translator to clear a switched virtual circuit (SVC) after a set period of inactivity.

Per-User Configuration

The per-user configuration can tie together the following dialin features:

- Virtual interface templates, generic interface configuration and router-specific configuration information stored in the form of a virtual interface template that can be applied (*cloned*) to a virtual access interface each time any user dials in.
- AAA per-user security and interface configuration information stored on a separate AAA server and sent by the AAA server to the access server or router in response to authorization requests during the PPP authentication phase. The per-user configuration information can add to or override the generic configuration on a virtual interface.
- Virtual profiles, which can use either or both of the two sources of information above for virtual interface configuration. When a user dials in, virtual profiles can apply the generic interface configuration and then apply the per-user configuration to create a unique virtual access interface for that user.

A virtual access interface created dynamically for any user dialin session is deleted when the session ends. The resources used during the session are returned for other dialin uses.

With per-user configuration:

- Maintenance ease for service providers with a large number of access servers and a very large number of dial-in users. Service providers do not need to update all their routers and access servers when user-specific information changes; instead, they can update one AAA server.
- Scalability. By separating generic virtual interface configuration on the router from the configuration for each individual, Internet service providers and other enterprises with large numbers of dialin users can provide a uniquely configured interface for each individual user. In

addition, by separating the generic virtual interface configuration from the physical interfaces on the router, the number and types of physical interfaces on the router or access server are not intrinsic barriers to growth.

PPP over ATM

This feature enables a high-capacity central site router with an Asynchronous Transfer Mode (ATM) interface to terminate multiple Point-to-Point Protocol (PPP) connections. These PPP connections are typically received from remote branch offices that have PPP-compatible devices interconnecting directly to StrataCom ATM Switch Interface Shelf (AXIS) equipment through a leased-line connection.

A logical interface known as a virtual access interface associates each PPP connection to an ATM permanent virtual circuit (PVC). This configuration allows the PPP protocol to terminate at the router ATM interface as if received from a typical PPP serial interface. Each PPP connection is encapsulated in a separate ATM PVC, which acts as the physical medium over which PPP frames are transported.

The virtual access interface for each PVC obtains its configuration from a virtual template when the PVC is created. All PPP parameters are managed within the virtual template configuration. Multiple virtual access interfaces can spawn from a single virtual template, hence multiple PVCs can use a single virtual template.

The virtual access interface remains associated with a PVC as long as the PVC is configured. Once the PVC is deconfigured, the virtual access interface is marked as deleted. Shutting down the associated ATM interface also causes the virtual access interface to be marked as down (within 10 seconds), bringing the PPP connection down. If a keepalive timer of the virtual template is set on the interface, the virtual access interface uses the PPP echo mechanism to verify the existence of the remote peer. If an interface failure is detected and the PPP connection is brought down, the virtual access interface remains up.

This feature is ideally suited for enterprise customers or customers who use Cisco StrataCom ATM switches to access wide-area networks (WANs) or public ATM networks, such as organizations with many remote branch offices requiring access to high-density corporate headquarters.

TCP Intercept

The TCP intercept feature implements software to protect TCP servers from TCP SYN-flooding attacks, which are a type of denial-of-service attack.

A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a Web site, accessing e-mail, using FTP service, and so on.

The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP synchronization (SYN) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server and, if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection.

Virtual Interface Template Service

Beginning with Cisco IOS Release 11.2, virtual interfaces can be configured independently of any physical interface and applied dynamically, as needed, to create virtual access interfaces. When a user dials in, a predefined configuration template is used to configure a virtual access interface; when the user is done, the virtual access interface is torn down and the resources are freed for other dialin uses.

This feature provides a generic service that can be used to apply predefined configurations (virtual interface templates) in creating and freeing virtual access interfaces on the fly, as needed.

Virtual interface templates and virtual access interfaces are basically serial interfaces with no hardware associations; they are created and freed as needed.

The virtual interface template service provides the following benefits to customers with large numbers of dial-in users:

- For easier maintenance, allows customized configurations to be predefined and then applied dynamically when the specific need arises.
- For scalability, allows interface configuration to be separated from physical interfaces. Virtual interfaces can share characteristics, no matter what specific type of interface the user called on.
- For consistency and configuration ease, allows the same predefined template to be used for all users dialing in for a specific application.
- For efficient router operation, frees the virtual access interface memory for another dial-in use when the user's call ends.

Virtual Templates for Protocol Translation

Cisco IOS software Release 11.2 F enables you to simplify the process of configuring protocol translation to tunnel PPP or SLIP across X.25, TCP, and LAT networks. It does so by providing virtual template interfaces that you can configure independently and apply to any protocol translation configuration. You can configure virtual interface templates for one-step and two-step protocol translation.

Before virtual templates were implemented, you enabled asynchronous protocol functions on VTY lines by creating virtual *asynchronous* interfaces rather than virtual *access* interfaces. (For one-step translation, you did so by specifying **ppp** or **slip** as outgoing options in the **translate** command. For two-step translation, you did so by specifying the **vty-async** command.) The differences between virtual asynchronous interfaces and virtual access interfaces are as follows:

- Virtual asynchronous interfaces are allocated permanently, whereas virtual access interfaces are created dynamically when a user calls in, and are closed down when the connection drops.
- Virtual asynchronous interfaces were unconfigurable. That is, you could create a virtual asynchronous interface, though you could not configure it using interface configuration commands. However, virtual access interfaces are fully configurable via the virtual interface template. All attributes of the virtual interface template are cloned onto the virtual access interface when a call comes in.

Virtual access interfaces replace virtual asynchronous interfaces for both one-step and two-step translation.

Virtual Profiles

Virtual profiles is a unique PPP application that defines and applies per-user configuration information for users who dial in to a router. Virtual profiles allow user-specific configuration information to be applied irrespective of the media used for the dial-in call. The configuration information for virtual profiles can come from a virtual interface template, per-user configuration information stored on an AAA server, or both, depending on how the router and AAA server are configured.

Virtual profiles are intended to overcome current limitations on network scalability:

- AAA—Our current ability to change any configuration on a per-user basis is limited to the AV pairs that are allowed by the respective AAA implementation.
- Network protocols—Some protocols, such as IPX, expect each dialin user to come in from a different network; scalability improves when network numbers are applied dynamically for each user.
- Media—Each medium is limited to receiving calls from users statically defined; scalability improves when a user can dial in through any interface, which then has a user configuration dynamically bound to it.
- DDR—The dial-on-demand routing model is designed to learn routes when links come up but not to delete them when the link is torn down; scalability improves when routes are added dynamically when the need arises and deleted dynamically when the need is gone.
- Dialer profiles—Dialer profiles solve some of the limitations above, but cannot handle thousands of dialin remote nodes; scalability improves when virtual interfaces are not limited to the number of hardware interfaces in a router.

Virtual profiles overcome the limitations listed above by providing a *unique* interface for each user dialing in to a Cisco router/access server.

X.25 Enhancements

Cisco's X.25 offerings have been restructured to meet additional design goals that include greater modularity and consistent availability of X.25 services to the code that uses them. The following have been updated:

- Three classes X.25 services:
 - X.25
 - X.25 over TCP (XOT)
 - X.25 over Local-Area Networks (Connection Mode Network Service or CMNS)
- Four classes of X.25 service users:
 - Encapsulating routed traffic over X.25 (datagram encapsulation)
 - X.25 switching
 - Packet assembler/disassembler (PAD) support for asynchronous devices, including protocol translation between X.25 related protocols (X.28, X.29) and other protocol families (LAT, Telnet, PPP)
 - Qualified Logical Link Control (QLLC)
- Three underlying layers that can support an X.25 service:
 - Link Access Procedure, Balanced (LAPB)

- Link Access Procedure, D channel (LAPD)
- Logical Link Control, Type 2 (LLC2)

X.25 on ISDN

Basic Rate Interface (BRI) is an Integrated Systems Digital Network (ISDN) interface, and it consists of two B channels (B1 and B2) and one D channel. The B channels are used to transfer data, voice, and video. The D channel controls the B channels.

ISDN uses the D channel to carry signal information. ISDN can also use the D channel in a BRI to carry X.25 packets. The D channel has a capacity of 16 kbps, and the X.25 over D channel can utilize up to 9.6 kbps.

This feature allows you to set the parameters of the X.25-over-D-channel interface without disrupting the original ISDN interface configuration. In a normal ISDN BRI interface, the D and B channels are bundled together and represented as a single interface. The original BRI interface will continue to represent the D, B1, and B2 channels.

Because some end-user equipment uses static terminal endpoint identifiers (TEIs) to access this feature, static TEIs are supported. The dialer understands the X.25-over-D-channel calls and initiates them on a new interface.

X.25 traffic over the D channel can be used as a primary interface where low-volume, sporadic interactive traffic is the normal mode of operation.

Supported traffic includes IPX, AppleTalk, transparent bridging, XNS, DECnet, and IP.

X.28 Emulation

The Cisco IOS software provides an X.28 user emulation mode, which enables you to interact and control the PAD. During an exchange of control information, messages or commands sent from the terminal to the PAD are called PAD command signals. Messages sent from the PAD to the terminal are called PAD service signals. These signals and any transmitted data take the form of encoded character streams as defined by International Alphabet Number 5.

For asynchronous devices such as terminals or modems to access an X.25 network host, the device's packets must be assembled or disassembled by a PAD device. Using standard X.28 commands from the PAD, calls can be made into an X.25 network, X.3 PAD parameters can be set, or calls can be reset. There are 22 available X.3 PAD parameters to configure. These parameters can also be set by a remote X.25 host using X.29. Cisco's new X.28 PAD implementation enables users to access X.25 networks or set PAD parameters using the X.28 standard user interface. This standard interface is common in many European countries and adheres to the X.25 International Telecommunication Union Telecommunication (ITU-T) standards.

The new X.28 interface is designed for asynchronous devices that require X.25 transport to access a remote or native asynchronous or synchronous host application. Applications such as dial-up users accessing a remote X.25 host can use the X.28 interface. For example, banks implement Cisco routers to support back office applications, ATMs, point of sales authorization devices, and alarm systems. These alarm devices are connected asynchronously to the same Cisco router and report alarm conditions to a remote alarm host for the dispatch of police. Cisco's X.28 PAD calls can be transported over a public packet network, a private X.25 network, the Internet, a private IP based network, or a Frame Relay network. With this new service, Cisco now offers the flexibility to use either the X.28 interface directly or over a Cisco IOS application service such as protocol translation. The protocol translation VTY asynchronous application enables users to bidirectionally access an X.25 application with the PAD service or protocols such as Digital Equipment Corporation (DEC), local-area transport (LAT), and TCP.

New Features in Release 11.2(3)F

The following software enhancements have been added to Release 11.2(3)F. These features are available only in Release 11.2 F. These features are documented in the *Feature Guide for Cisco IOS Release 11.2 F*. For additional platform support, refer to the *Release Notes for Cisco IOS Release 11.2 P*.

AppleTalk Access List Enhancements

This feature adds functionality and improved performance when using AppleTalk access lists and filters.

The specific AppleTalk access list enhancements include the following:

- Access list fast switching
- Access lists for inbound interfaces

In previous releases of the Cisco IOS software, AppleTalk access lists, with the exception of NBP access lists, could be applied to outbound interfaces only. With this release, access lists can be applied to inbound and outbound interfaces.

- NBP access lists for outbound interfaces

In previous releases of Cisco IOS software, NBP access lists could be applied to inbound interfaces only. With this release, NBP access lists can be applied to inbound and outbound interfaces.

- NBP filter based on NBP packet type:
 - Broadcast Request
 - Forward Request
 - Lookup
 - Lookup Reply

Frame Relay MIB Extensions

The Cisco Frame Relay MIB adds proprietary extensions to the standard Frame Relay MIB (RFC 1315). It provides additional link-level and virtual circuit-level information and statistics that are mostly specific to Cisco Frame Relay implementation. This MIB provides SNMP network management access to most of the information covered by the **show frame-relay** commands, such as, **show frame-relay lmi**, **show frame-relay pvc**, **show frame-relay map**, and **show frame-relay svc**.

Kerberized Telnet

Kerberized Telnet enables a router to initiate or receive an encrypted Telnet session. Previously, all Telnet session traffic could only be transmitted as cleartext (readable) data.

You can use Kerberized Telnet when establishing a Telnet session to or from a router. When you use this feature, first you are authenticated by your Kerberos credentials, and then an encrypted Telnet session is established.

Cisco's Kerberized Telnet uses the following encryption standard: 56-bit Data Encryption Standard (DES) encryption with 64-bit Cipher Feedback (CFB).

This feature is available only if you have the 56-bit encryption image. 56-bit DES encryption is subject to U.S. government export control regulations.

Layer 2 Forwarding—Fast Switching

Cisco routers now fast switch Layer 2 Forwarding (L2F) traffic. In stack group environments in which some L2F traffic is offloaded to a powerful router, fast switching provides improved scalability.

Leased Line ISDN at 128 kbps

In Cisco IOS Release 11.2, leased-line service at 64 kbps via ISDN BRI is provided in Japan and Germany. In Cisco IOS Release 11.2(3)F, leased line service at 128 kbps via ISDN BRI is provided in Japan. This service combines two B channels into a single pipe.

Note Once an ISDN BRI interface is configured for access over leased lines, it is no longer a dialer interface, and signaling over the D channel no longer applies. Although the interface is called **interface bri n**, it is configured as a synchronous serial interface. However, the Cisco IOS commands that set the physical characteristics of a serial interface (such as the pulse time) do not apply to this interface.

TCP Enhancements

The following TCP functionality and performance enhancements have been added:

- Socket Interface for TCP

The TCP implementation prior to Cisco IOS software Release 11.2(3) did not have a socket API, and porting socket-based applications from other vendors to the Cisco IOS software was cumbersome. This feature implements some basic socket interface functions to reduce porting efforts. The new socket interface enables TCP applications to open and manage multiple connections asynchronously.

- TCP Selective Acknowledgment

The TCP selective acknowledgment feature improves performance in the event that multiple packets are lost from one TCP window of data.

Prior to this feature, with the limited information available from cumulative acknowledgments, a TCP sender could learn about only one lost packet per round-trip time. An aggressive sender could choose to retransmit packets early, but such retransmitted segments might have already been successfully received.

The TCP selective acknowledgment mechanism helps improve performance. The receiving TCP host returns selective acknowledgment packets to the sender, informing the sender of data that has been received. In other words, the receiver can acknowledge packets received out of order. The sender can then retransmit only the missing data segments (instead of everything since the first missing packet).

Prior to selective acknowledgment, if TCP lost packets 4 and 7 out of an 8-packet window, TCP would receive acknowledgment of only packets 1, 2, and 3. Packets 4 through 8 would have to be resent. With selective acknowledgment, TCP receives acknowledgment of packets 1, 2, 3, 5, 6, and 8. Only packets 4 and 7 have to be resent.

Refer to RFC 2018 for more detailed information on TCP selective acknowledgment.

- TCP Timestamp

The TCP timestamp option provides better TCP round-trip time measurements. Because the timestamps are always sent and echoed in both directions and the timestamp value in the header is always changing, TCP header compression will not compress the outgoing packet. To allow TCP header compression over a serial link, the TCP timestamp option is disabled.

Refer to RFC 1323 for more detailed information on TCP timestamp.

Tunneling of Asynchronous Security Protocols

Cisco's implementation of block serial tunneling (BSTUN) encapsulates Binary Synchronous Communications protocol (Bisync), Adplex, ADT Security Systems, Inc., Diebold, and asynchronous generic traffic for transfer over router links.

Cisco's tunneling of asynchronous security protocols feature (ASP) enables your Cisco 2500, 4000, or 4500 series router to support devices that use the following asynchronous security protocols:

- adplex
- adt-poll-select
- adt-vari-poll
- diebold
- async-generic

Note async-generic is not a protocol name. It is a keyword used to indicate generic support of other asynchronous security protocols that are not explicitly supported.

These protocols enable enterprises to transport polled asynchronous traffic over the same network that supports their Systems Network Architecture (SNA) and multiprotocol traffic, eliminating the need for separate facilities.

Cisco IOS Packaging

Not all features are available in all feature sets. The tables in this section indicate the platforms and feature sets that contain the new features in Release 11.2 F.

An explanation of the table entries follows:

- Basic. The basic feature set for the hardware platform.
- Plus. The basic feature set plus a variable set of additional features depending on the hardware platform selected.
- Encryption. The addition of 40-bit (Plus 40) or 56-bit (Plus 56) data encryption feature sets.

Cisco IOS images with strong encryption (including, but not limited to 56-bit DES) are subject to U.S. Government export controls, and have a limited distribution. Images to be installed outside the U.S. require an export license. Customer orders may be denied or subject to delay due to U.S. Government regulations. Contact your sales representative or distributor for more information, or send e-mail to export@cisco.com.

Note Release 11.2 introduces new feature-set image names for several feature sets available in earlier releases. For example, the prefix “igs-” has been replaced with “c2500-.” Image names have been changed to facilitate identifying the platform on which the image runs.

Feature Set Tables

The Cisco IOS software is available in different feature sets depending upon the platform. Table 1 lists the feature sets for the Cisco 7000 and Cisco 7500 series. Table 2 lists the feature sets for the Cisco 7200 series. Table 3 lists the feature sets for the Cisco 2500 series, Cisco 4000, Cisco 4500, and Cisco 4700. Table 4 lists platform-specific feature sets for the Cisco 2500 series and Cisco AS5100. Table 5 lists the feature sets for the Cisco AS5200. Table 6 lists the software for the Cisco 1003 and Cisco 1004 ISDN routers and the Cisco 1005 router. Table 7 lists the platform-specific software for the Cisco 1003 and Cisco 1004 ISDN routers. Table 8 lists platform-specific software for the Cisco 1005 router. Table 9 lists the feature sets for IPeXchange Internet Gateway.

Tables indicate new features in Release 11.2 F. For additional feature support, refer to the *Release Notes for Cisco IOS Release 11.2* publication.

The tables use the following conventions to identify features:

- D : the feature is offered in the basic feature set
- — : the feature is not offered in the feature set
- Plus: the feature is offered only in the Plus feature sets, not in the basic feature set
- Encrypt: for the Cisco 7500 series, the feature is offered only in the encryption feature sets (Encryption 40, Plus 40, Encryption 56, or Plus 56), not in the basic feature set

Note Encryption is not available on the Cisco AS5200, Cisco 7000 series, and Cisco 7200 series platforms.

Some Cisco platforms incorporate plus features into their basic feature sets.

Table 1 Cisco 7000 Series and Cisco 7500 Series Software Feature Sets

Features	Feature Set		
	IP Routing	Desktop/IBM ¹	Enterprise ¹
LAN Support			
AppleTalk Access List Enhancements	—	D	D
IPeXchange Internet Gateway	—	—	—
IPX Named Access Lists	—	D	D
IPX SAP-after-RIP	—	D	D
NLSP Enhancements	—	—	D
WAN Services			
Frame Relay MIB Extensions	D	D	D
Layer 2 Forwarding—Fast Switching	—	—	—
Leased Line ISDN at 128 kbps	—	—	—

Table 1 Cisco 7000 Series and Cisco 7500 Series Software Feature Sets (Continued)

Features	Feature Set		
	IP Routing	Desktop/IBM ¹	Enterprise ¹
PPP over ATM (Cisco 7500 only)	Ⓟ	Ⓟ	Ⓟ
X.25 Enhancements	Ⓟ	Ⓟ	Ⓟ
X.25 on ISDN	—	—	—
X.28 Emulation	—	—	Ⓟ
WAN Optimization			
PAD Enhancements	—	—	Ⓟ
IP Routing			
DRP Server Agent	Ⓟ	Ⓟ	Ⓟ
IP Enhanced IGRP Route Authentication	Ⓟ	Ⓟ	Ⓟ
TCP Enhancements	Ⓟ	Ⓟ	Ⓟ
TCP Intercept	—	—	Ⓟ
Security			
Double Authentication	Ⓟ	Ⓟ	Ⓟ
Kerberized Telnet (Cisco 7500 and RSP7000 only)	—	—	Encrypt 56
Per-User Configuration	Ⓟ	Ⓟ	Ⓟ
Virtual Profiles	Ⓟ	Ⓟ	Ⓟ
IBM Support			
Tunneling of Asynchronous Security Protocols	Ⓟ	Ⓟ	Ⓟ
Terminal Services			
Virtual Templates for Protocol Translation	—	—	Ⓟ

1. Desktop/IBM and Enterprise are available with APPN in a separate feature set. In Cisco IOS Release 11.2, APPN includes APPN Central Registration (CRR) and APPN over DLSw+.

Table 2 Cisco 7200 Series Software Feature Sets

Features	Feature Set			
	Network Layer 3 Switching	IP Routing	Desktop/IBM ¹	Enterprise ¹
LAN Support				
AppleTalk Access List Enhancements	—	—	Ⓟ	Ⓟ
IPeXchange Internet Gateway	—	—	—	—
IPX Named Access Lists	Ⓟ	—	Ⓟ	Ⓟ
IPX SAP-after-RIP	Ⓟ	—	Ⓟ	Ⓟ
NLSP Enhancements	—	—	—	Ⓟ

Table 2 Cisco 7200 Series Software Feature Sets (Continued)

Features	Feature Set			
	Network Layer 3 Switching	IP Routing	Desktop/IBM ¹	Enterprise ¹
WAN Services				
Frame Relay MIB Extensions	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Layer 2 Forwarding—Fast Switching	—	—	—	—
Leased Line ISDN at 128 kbps	—	—	—	—
PPP over ATM	—	—	—	—
X.25 Enhancements	Ⓜ	Ⓜ	Ⓜ	Ⓜ
X.25 on ISDN	—	—	—	—
X.28 Emulation	—	—	—	Ⓜ
WAN Optimization				
PAD Enhancements	—	—	—	Ⓜ
IP Routing				
DRP Server Agent	Ⓜ	Ⓜ	Ⓜ	Ⓜ
IP Enhanced IGRP Route Authentication	Ⓜ	Ⓜ	Ⓜ	Ⓜ
TCP Enhancements	Ⓜ	Ⓜ	Ⓜ	Ⓜ
TCP Intercept	—	—	—	Ⓜ
Security				
Double Authentication	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Kerberized Telnet	—	—	—	—
Per-User Configuration	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Virtual Profiles	Ⓜ	Ⓜ	Ⓜ	Ⓜ
IBM Support				
Tunneling of Asynchronous Security Protocols	Ⓜ	Ⓜ	Ⓜ	Ⓜ
Terminal Services				
Virtual Templates for Protocol Translation	Ⓜ	Ⓜ	Ⓜ	Ⓜ

1. Desktop/IBM and Enterprise are available with APPN in a separate feature set. Use the product numbers that specify APPN. APPN includes APPN Central Registration (CRR) and APPN over DLSw+.

Table 3 Cisco 2500 Series, Cisco 4000, Cisco 4500, and Cisco 4700 Software Feature Sets

Features	Feature Set				
	IP Routing	IP/IPX/ IBM/APPN ¹	Desktop (IP/IPX/ AppleTalk/DEC)	Desktop/ IPeXchange (IP/IPX/AppleTalk/ DEC/IPeXchange)	Enterprise ²
LAN Support					
AppleTalk Access List Enhancements	—	—	Ⓟ	Ⓟ	Ⓟ
IPeXchange Internet Gateway (Cisco 2500 only)	—	—	—	Ⓟ	—
IPX Named Access Lists	—	Ⓟ	Ⓟ	Ⓟ	Ⓟ
IPX SAP-after-RIP	—	Ⓟ	Ⓟ	Ⓟ	Ⓟ
NLSP Enhancements	—	—	—	—	Ⓟ
WAN Services					
Frame Relay MIB Extensions	Ⓟ	Ⓟ	Ⓟ	Ⓟ	Ⓟ
Layer 2 Forwarding—Fast Switching	—	—	Ⓟ	Ⓟ	Ⓟ
Leased Line ISDN at 128 kbps (Cisco 4000, Cisco 4500, and Cisco 4700 only)	Ⓟ	Ⓟ	Ⓟ	Ⓟ	Ⓟ
PPP over ATM	Ⓟ	Ⓟ	Ⓟ	Ⓟ	Ⓟ
X.25 Enhancements	Ⓟ	Ⓟ	Ⓟ	Ⓟ	Ⓟ
X.25 on ISDN	Ⓟ	Ⓟ	Ⓟ	Ⓟ	Ⓟ
X.28 Emulation	—	—	—	—	Ⓟ
WAN Optimization					
PAD Enhancements	—	—	—	—	Ⓟ
IP Routing					
DRP Server Agent	Ⓟ	Ⓟ	Ⓟ	Ⓟ	Ⓟ
IP Enhanced IGRP Route Authentication	Ⓟ	Ⓟ	Ⓟ	Ⓟ	Ⓟ
TCP Enhancements	Ⓟ	Ⓟ	Ⓟ	Ⓟ	Ⓟ
TCP Intercept	—	—	—	—	Ⓟ
Security					
Double Authentication	Ⓟ	Ⓟ	Ⓟ	Ⓟ	Ⓟ
Kerberized Telnet	—	—	—	—	Encrypt 56
Per-User Configuration (Cisco 4500 only)	Ⓟ	Ⓟ	Ⓟ	Ⓟ	Ⓟ
Virtual Profiles	Ⓟ	Ⓟ	Ⓟ	Ⓟ	Ⓟ
IBM Support					
Tunneling of Asynchronous Security Protocols	Ⓟ	Ⓟ	Ⓟ	Ⓟ	Ⓟ

Table 3 Cisco 2500 Series, Cisco 4000, Cisco 4500, and Cisco 4700 Software Feature Sets (Continued)

Features	Feature Set				
	IP Routing	IP/IPX/ IBM/APPN ¹	Desktop (IP/IPX/ AppleTalk/DEC)	Desktop/ IPeXchange (IP/IPX/AppleTalk/ DEC/IPeXchange)	Enterprise ²
Terminal Services					
Virtual Templates for Protocol Translation	—	—	—	—	Đ

1. This feature set has no additional options. It offers a low-end APPN solution for this set of hardware platforms.

2. Enterprise is available with APPN in a separate feature set. APPN includes APPN Central Registration (CRR) and APPN over DLSw+.

Table 4 Platform-Specific Cisco 2500 Series and AS5100 Access Server Software Feature Sets

Features	Feature Set			
	ISDN	CFRAD	LAN FRAD	Remote Access Server
LAN Support				
AppleTalk Access List Enhancements	—	—	—	—
IPeXchange Internet Gateway	—	—	—	—
IPX Named Access Lists	Đ	—	Đ	Đ
IPX SAP-after-RIP	Đ	—	Đ	Đ
NLSP Enhancements	—	—	—	—
WAN Services				
Frame Relay MIB Extensions	—	Đ	Đ	Đ
Layer 2 Forwarding—Fast Switching	—	—	—	Đ
Leased Line ISDN at 128 kbps	—	—	—	—
PPP over ATM	—	—	—	—
X.25 Enhancements	—	—	—	—
X.25 on ISDN	Đ	—	—	—
X.28 Emulation	—	—	—	—
WAN Optimization				
PAD Enhancements	—	Đ	—	—
IP Routing				
DRP Server Agent	—	—	—	—
IP Enhanced IGRP Route Authentication	Đ	Đ	Đ	Đ
TCP Enhancements	Đ	Đ	Đ	Đ
TCP Intercept	—	—	—	—
Security				
Double Authentication	Đ	Đ	Đ	Đ

Table 4 Platform-Specific Cisco 2500 Series and AS5100 Access Server Software Feature Sets (Continued)

Features	Feature Set			
	ISDN	CFRAD	LAN FRAD	Remote Access Server
Kerberized Telnet	—	—	—	—
Per-User Configuration	Ⓟ	Ⓟ	Ⓟ	Ⓟ
Virtual Profiles	Ⓟ	Ⓟ	Ⓟ	Ⓟ
IBM Support				
Tunneling of Asynchronous Security Protocols	—	Ⓟ	Ⓟ	—
Terminal Services				
Virtual Templates for Protocol Translation	—	Ⓟ	—	—

Table 5 Cisco AS5200 Access Server Software Feature Sets

Features	Feature Set		
	IP Routing	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise ¹
LAN Support			
AppleTalk Access List Enhancements	—	Ⓟ	Ⓟ
IPeXchange Internet Gateway	—	—	—
IPX Named Access Lists	—	Ⓟ	Ⓟ
IPX SAP-after-RIP	—	Ⓟ	Ⓟ
NLSP Enhancements	—	—	Ⓟ
WAN Services			
Frame Relay MIB Extensions	Ⓟ	Ⓟ	Ⓟ
Layer 2 Forwarding—Fast Switching	—	Ⓟ	Ⓟ
Leased Line ISDN at 128 kbps	—	—	—
PPP over ATM	—	—	—
X.25 Enhancements	Ⓟ	Ⓟ	Ⓟ
X.25 on ISDN	Ⓟ	Ⓟ	Ⓟ
X.28 Emulation	—	—	Ⓟ
WAN Optimization			
PAD Enhancements	—	—	Ⓟ
IP Routing			
DRP Server Agent	Ⓟ	Ⓟ	Ⓟ
IP Enhanced IGRP Route Authentication	Ⓟ	Ⓟ	Ⓟ
TCP Enhancements	Ⓟ	Ⓟ	Ⓟ
TCP Intercept	—	—	Ⓟ

Table 5 Cisco AS5200 Access Server Software Feature Sets (Continued)

Features	Feature Set		
	IP Routing	Desktop (IP/IPX/AppleTalk/DEC)	Enterprise ¹
Security			
Double Authentication	Ð	Ð	Ð
Kerberized Telnet	—	—	—
Per-User Configuration	Ð	Ð	Ð
Virtual Profiles	Ð	Ð	Ð
IBM Support			
Tunneling of Asynchronous Security Protocols	Ð	Ð	Ð
Terminal Services			
Virtual Templates for Protocol Translation	—	—	Ð

1. Enterprise is available with APPN in a separate feature set. APPN includes APPN Central Registration (CRR) and APPN over DLSw+.

Table 6 Cisco 1003, Cisco 1004, and Cisco 1005 Routers Software Feature Sets

Features	Feature Set ¹			
	IP Routing ²	IP/IPX Routing ²	IP/AppleTalk Routing ²	IP/IPX/AppleTalk Routing
LAN Support				
AppleTalk Access List Enhancements	—	—	—	Plus
IPeXchange Internet Gateway	—	—	—	—
IPX Named Access Lists	—	—	—	—
IPX SAP-after-RIP	—	Ð	—	Ð
NLSP Enhancements	—	—	—	Plus
WAN Services				
Frame Relay MIB Extensions (Cisco 1005 only)	Ð	Ð	Ð	Ð
Layer 2 Forwarding—Fast Switching	—	—	—	—
Leased Line ISDN at 128 kbps (Cisco 1003 and Cisco 1004 only)	Ð	Ð	Ð	Ð
PPP over ATM	—	—	—	—
X.25 Enhancements	Ð	Ð	Ð	Ð
X.25 on ISDN (Cisco 1003, Cisco 1004 only)	Ð	Ð	Ð	Ð
X.28 Emulation	—	—	—	—
WAN Optimization				
PAD Enhancements	—	—	—	—
IP Routing				
DRP Server Agent	—	—	—	—
IP Enhanced IGRP Route Authentication	Ð	Ð	Ð	Ð

Table 6 Cisco 1003, Cisco 1004, and Cisco 1005 Routers Software Feature Sets (Continued)

Features	Feature Set ¹			
	IP Routing ²	IP/IPX Routing ²	IP/AppleTalk Routing ²	IP/IPX/AppleTalk Routing
TCP Enhancements	Đ	Đ	Đ	Đ
TCP Intercept	—	—	—	—
Security				
Double Authentication	Đ	Đ	Đ	Đ
Kerberized Telnet	—	—	—	—
Per-User Configuration	Đ	Đ	Đ	Đ
Virtual Profiles	Đ	Đ	Đ	Đ
IBM Support				
Tunneling of Asynchronous Security Protocols	—	—	—	—
Terminal Services				
Virtual Templates for Protocol Translation	—	—	—	—

1. This table lists feature sets that are common to the Cisco 1003, Cisco 1004, and Cisco 1005. For Cisco 1005 platform-specific feature sets, see Table 8.

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.

Table 7 Cisco 1003, and Cisco 1004 Routers Platform-Specific Software Feature Set

Features	Feature Set
	IP/X31 Routing ¹
LAN Support	
AppleTalk Access List Enhancements	—
IPeXchange Internet Gateway	—
IPX Named Access Lists	—
IPX SAP-after-RIP	—
NLSP Enhancements	—
WAN Services	
Frame Relay MIB Extensions (Cisco 1005 only)	Đ
Layer 2 Forwarding—Fast Switching	—
Leased Line ISDN at 128 kbps (Cisco 1003 and Cisco 1004 only)	Đ
PPP over ATM	—
X.25 Enhancements	Đ
X.25 on ISDN (Cisco 1003, Cisco 1004 only)	Đ
X.28 Emulation	—
WAN Optimization	
PAD Enhancements	—

Table 7 Cisco 1003, and Cisco 1004 Routers Platform-Specific Software Feature Set (Continued)

Features	Feature Set
	IP/X31 Routing ¹
IP Routing	
DRP Server Agent	—
IP Enhanced IGRP Route Authentication	Đ
TCP Enhancements	Đ
TCP Intercept	—
Security	
Double Authentication	Đ
Kerberized Telnet	—
Per-User Configuration	Đ
Virtual Profiles	Đ
IBM Support	
Tunneling of Asynchronous Security Protocols	—
Terminal Services	
Virtual Templates for Protocol Translation	—

1. The IP/X31 feature set is not available with Plus, Plus 40, or Plus 56 feature set options in Cisco IOS Release 11.2.

Table 8 Cisco 1005 Platform-Specific Software Feature Sets

Features	Feature Set		
	IP/OSPF/PIM Routing ¹	IP/Async ¹	IP/IPX/Async ¹
LAN Support			
AppleTalk Access List Enhancements	—	—	—
IPeXchange Internet Gateway	—	—	—
IPX Named Access Lists	—	—	—
IPX SAP-after-RIP	—	—	Đ
NLSP Enhancements	—	—	—
WAN Services			
Frame Relay MIB Extensions	Đ	Đ	Đ
Layer 2 Forwarding—Fast Switching	—	—	—
Leased Line ISDN at 128 kbps	—	—	—
PPP over ATM	—	—	—
X.25 Enhancements	Đ	Đ	Đ
X.25 on ISDN	—	—	—
X.28 Emulation	—	—	—

Table 8 Cisco 1005 Platform-Specific Software Feature Sets (Continued)

Features	Feature Set		
	IP/OSPF/PIM Routing ¹	IP/Async ¹	IP/IPX/Async ¹
WAN Optimization			
PAD Enhancements	—	—	—
IP Routing			
DRP Server Agent	—	—	—
IP Enhanced IGRP Route Authentication	ⓓ	ⓓ	ⓓ
TCP Enhancements	ⓓ	ⓓ	ⓓ
TCP Intercept	—	—	—
Security			
Double Authentication	ⓓ	ⓓ	ⓓ
Kerberized Telnet	—	—	—
Per-User Configuration	ⓓ	ⓓ	ⓓ
Virtual Profiles	ⓓ	ⓓ	ⓓ
IBM Support			
Tunneling of Asynchronous Security Protocols	—	—	—
Terminal Services			
Virtual Templates for Protocol Translation	—	—	—

1. These feature sets are not available with the Plus, Plus 40, or Plus 56 feature set options in Cisco IOS Release 11.2.

Table 9 Cisco 1003/1004 and Cisco 1005 IPeXchange Internet Gateway Feature Sets

Features	Feature Set				
	20 User Cisco 1003/ 1004	50 User Cisco 1003/ 1004	20 User Cisco 1005 Sync	50 User Cisco 1005 Sync	Cisco 1005 Async
SNMP	—	ⓓ	—	ⓓ	ⓓ
ISDN	ⓓ	ⓓ	—	—	—
Frame Relay (RFC 1490)	—	—	ⓓ	ⓓ	—
PPP	ⓓ	ⓓ	ⓓ	ⓓ	ⓓ
HDLC	ⓓ	ⓓ	ⓓ	ⓓ	—
IP	ⓓ	ⓓ	ⓓ	ⓓ	ⓓ
IPX	ⓓ	ⓓ	ⓓ	ⓓ	ⓓ
IPXWAN 2.0	ⓓ	ⓓ	ⓓ	ⓓ	ⓓ
Telnet			ⓓ	ⓓ	ⓓ
AutoInstall			ⓓ	ⓓ	

Table 9 Cisco 1003/1004 and Cisco 1005 IPeXchange Internet Gateway Feature Sets (Continued)

Features	Feature Set				
	20 User Cisco 1003/ 1004	50 User Cisco 1003/ 1004	20 User Cisco 1005 Sync	50 User Cisco 1005 Sync	Cisco 1005 Async
ClickStart	ⓓ	ⓓ	ⓓ	ⓓ	ⓓ
Router monitoring	ⓓ	ⓓ	ⓓ	ⓓ	

Memory Requirements for Release 11.2 F

Unless otherwise noted, the memory requirement for feature sets in Release 11.2 F are the same as Release 11.2. Platforms not available in Release 11.2 or 11.2 P are shown in Table 10.

For new Cisco platforms, also refer to the *Release Notes for Cisco IOS Release 11.2 P*.

Note For the Cisco 7000 and Cisco 7010 routers to recognize Flash memory cards, 11.0 boot ROMs (or later) are required.

Table 10 Release 11.2 F Memory Requirements

Platform	Minimum Required Code Memory	Required Main Memory	Release 11.2 F Runs from
Cisco 1003, 1004 IPeXchange Internet Gateway			
IPeXchange 20 User 1003/1004 Set	2 MB Flash	8 MB RAM	RAM
IPeXchange 50 User 1003/1004 Set	4 MB Flash	8 MB RAM	RAM
Cisco 1005 IPeXchange Internet Gateway			
IPeXchange 20 User 1005 Set	2 MB Flash	8 MB RAM	RAM
IPeXchange 50 User 1005 Set	4 MB Flash	8 MB RAM	RAM
IPeXchange 1005 Async Set	2 MB Flash	8 MB RAM	RAM
Cisco 2500 IPeXchange Internet Gateway			
IP/IPX/AT/DEC IPeXchange Set	8 MB Flash	16 MB RAM	Flash
IP/IPX/AT/DEC IPeXchange Plus Set	8 MB Flash	16 MB RAM	Flash
IP/IPX/AT/DEC IPeXchange Plus 40 Set	8 MB Flash	16 MB RAM	Flash
IP/IPX/AT/DEC IPeXchange Plus 54 Set	8 MB Flash	16 MB RAM	Flash
Cisco 1003 and Cisco 1004 ISDN Routers			
IP/X31 Set	2 MB Flash	4 MB RAM	RAM

Microcode Software

Table 11 lists the current microcode versions for the Cisco 7000 series. Table 12 lists the current microcode versions for the Cisco 7500 series. Note that for the Cisco 7000 and Cisco 7500 series, microcode software images are bundled with the system software image—with the exception of the Channel Interface Processor (CIP) microcode (all system software images) and Versatile Interface Processor (VIP) microcode (certain system software images). Bundling eliminates the need to store separate microcode images. When the router starts, the system software unpacks the microcode software bundle and loads the proper software on all the interface processor boards. VIP and VIP2 microcode is bundled into all Cisco 7500 series feature sets listed in Table 1. VIP2C is bundled into Encryption feature sets.

Note For the Cisco 7000 series, all boards must use the Level 10 (or greater) microcode bundled (except CIP) with the system image.

Table 11 Bundled Microcode Versions, by Release, for the Cisco 7000 Series

Cisco IOS Release	Processor or Module ¹										
	AIP	EIP	FEIP	FIP	FSIP	HIP	MIP	SP	SSP	TRIP	VIP ²
Minimum Version Required	10.15	10.1	10.4	10.2	10.18	10.2	12.0	11.15	11.15	10.3	22.20
11.2(3)F	10.17	10.1	10.4	10.2	10.18	10.2	12.2	11.15	11.15	10.4	22.20
11.2(4)F	10.17	10.1	10.4	10.2	10.19	10.2	12.2	11.15	11.15	10.4	22.20

1. AIP (ATM Interface Processor), EIP (Ethernet Interface Processor), FEIP (Fast Ethernet Interface Processor), FIP (FDDI Interface Processor), FSIP (Fast Serial Interface Processor), HIP (HSSI Interface Processor), MIP (MultiChannel Interface Processor), SP (Switch Processor), SSP (Silicon Switch Processor), TRIP (Token Ring Interface Processor), VIP (Versatile Interface Processor).

2. VIP microcode resides within the Cisco IOS software; it is not “bundled” in.

Table 12 Bundled RSP Microcode Versions, by Release, for the Cisco 7000 Series

Cisco IOS Release	Processor or Module ¹												
	AIP	EIP	FEIP	FIP	FSIP	HIP	MIP	POSIP	RSP2 ²	TRIP	VIP ²	VIP2 ²	VIP2C ^{2,3}
Minimum Version Required	20.8	20.2	20.3	20.1	20.4	20.0	22.0	20.0	20.0	20.0	22.20	22.20	22.20
11.2(3)F	20.10	20.2	20.3	20.1	20.4	20.0	22.2	20.0	20.0	20.1	22.20	22.20	22.20
11.2(4)F	20.10	20.2	20.3	20.1	20.6	20.0	22.2	20.0	20.0	20.1	22.20	22.20	22.20

1. AIP (ATM Interface Processor), EIP (Ethernet Interface Processor), FEIP (Fast Ethernet Interface Processor), FIP (FDDI Interface Processor), FSIP (Fast Serial Interface Processor), HIP (HSSI Interface Processor), MIP (MultiChannel Interface Processor), POSIP (Packet over SONET OC-3 Interface Processor), RSP2 (Route Switch Processor), TRIP (Token Ring Interface Processor), VIP (Versatile Interface Processor), VIP2 (Second-Generation Versatile Interface Processor), VIP2C (Second-Generation Versatile Interface Processor—Encrypted).

2. RSP2, VIP, VIP2, and VIP2C microcode reside within the Cisco IOS software; they are not “bundled” in.

3. VIP2C was introduced in Release 11.2(2).

Channel Interface Processor (CIP) Microcode

Beginning with Cisco IOS Release 11.1, the CIP microcode is no longer bundled with the Cisco IOS software image. You must have Flash memory installed on the Route Processor (RP) card and 8 MB RAM installed on your CIP card to use the IBM channel attach features in Cisco IOS Release 11.1 and later. See the “Important Notes” section for more information about CIP microcode.

Important Notes

This section describes warnings and cautions about using the Cisco IOS Release 11.2 F software.

For additional information, refer to the *Release Notes for Cisco IOS Release 11.2* and the *Release Notes for Cisco IOS Release 11.2 P*.

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 installing Release 11.2 software on your router.

Release 11.2(4)F Caveats

This section describes possibly unexpected behavior by Release 11.2(4)F. Unless otherwise noted, this caveat applies to all 11.2 F releases, up to and including 11.2(4)F. The caveats listed here describe only the serious problems. For additional caveats against this release, refer to the *Release Notes for Cisco IOS Release 11.2* and the *Release Notes for Cisco IOS Release 11.2 P*. For additional caveats applicable to Release 11.2(4)F, use the Documentation CD-ROM or access CCO as described in the section “Cisco Connection Online” later in this document.

Wide-Area Networking

- A host route installed from PPP IP address negotiation might incorrectly contain the IP address from a previous negotiation. [CSCdi88836]

Release 11.2(3)F Caveats/Release 11.2(4)F Modifications

This section describes possibly unexpected behavior by Release 11.2(3)F. Unless otherwise noted, this caveat applies to all 11.2 F releases, up to and including 11.2(3)F. The caveats listed here describe only the serious problems. For additional caveats against this release, refer to the *Release Notes for Cisco IOS Release 11.2* and the *Release Notes for Cisco IOS Release 11.2 P*. For additional caveats applicable to Release 11.2(3)F, see the caveats sections for newer 11.2 F releases and use the Documentation CD-ROM or access CCO as described in the section “Cisco Connection Online” later in this document. The caveats for newer releases precede this section.

All caveats listed in this section are resolved in Release 11.2(4)F.

IBM Connectivity

- In a Cisco 4000 or Cisco 7000 series router, running RSRB with TCP Bridge Encapsulation (non-IP traffic such as IPX, XNS, VINES, or CLNS) over FDDI causes peer routers to crash. RSRB will work on these platforms when using any other medium such as serial. Cisco 4500 and Cisco 7500 series routers do not exhibit the problem. [CSCdi78066]

Cisco Connection Online

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

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

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

You can access CCO in the following ways:

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

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

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

Documentation CD-ROM

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

This document is to be used in conjunction with the *Release Notes for Cisco IOS Release 11.2*, *Release Notes for Cisco IOS Release 11.2 P*, *Feature Guide for Release 11.2 P*, *Feature Guide for Release 11.2 F*, and Release 11.2 configuration guides and command references.

AtmDirector, AutoConnect, AutoRoute, AXIS, BPX, Catalyst, CD-PAC, CiscoAdvantage, CiscoFusion, Cisco IOS, the Cisco IOS logo, *CiscoLink*, CiscoPro, the CiscoPro logo, CiscoRemote, the CiscoRemote logo, CiscoSecure, Cisco Systems, CiscoView, CiscoVision, CiscoWorks, ClickStart, ControlStream, EdgeConnect, EtherChannel, FairShare, FastCell, FastForward, FastManager, FastMate, FastPADImp, FastPADmicro, FastPADmp, FragmentFree, FrameClass, Fulcrum INS, IGX, Impact, Internet Junction, JumpStart, LAN²LAN Enterprise, LAN²LAN Remote Office, LightSwitch, MICA, NetBeyond, NetFlow, Newport Systems Solutions, *Packet*, PIX, Point and Click Internetworking, RouteStream, Secure/IP, SMARTnet, StrataSphere, StrataSphere BILLder, StrataSphere Connection Manager, StrataSphere Modeler, StrataSphere Optimizer, Stratm, StrataView Plus, StreamView, SwitchProbe, SwitchVision, SwitchWare, SynchroniCD, *The Cell*, The FastPacket Company, TokenSwitch, TrafficDirector, Virtual EtherSwitch, VirtualStream, VlanDirector, Web Clusters, WNIC, Workgroup Director, Workgroup Stack, and XCI are trademarks; Access by Cisco, Bringing the Power of Internetworking to Everyone, Enter the Net with MultiNet, and The Network Works. No Excuses. are service marks; and Cisco, the Cisco Systems logo, CollisionFree, Combinet, EtherSwitch, FastHub, FastLink, FastNIC, FastPacket, FastPAD, FastSwitch, ForeSight, Grand, Grand Junction, Grand Junction Networks, the Grand Junction Networks logo, HSSI, IGRP, IPX, Kalpana, the Kalpana logo, LightStream, MultiNet, MultiWare, OptiClass, Personal Ethernet, Phase/IP, RPS, StrataCom, TGV, the TGV logo, and UniverCD are registered trademarks of Cisco Systems, Inc. All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners.

Copyright © 1997, Cisco Systems, Inc.
All rights reserved. Printed in USA.
9611R