



Text Part Number: 78-5057-11

Release Notes for the Cisco 2500 Series Routers for Cisco IOS Release 11.3 T

July 26, 1999

These release notes for Cisco 2500 series support Cisco IOS Release 11.3 T, up to and including Release 11.3(11)T. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of the software caveats that apply to Release 11.3(11)T, see the *Caveats for Cisco IOS Release 11.3 T* document that accompanies these release notes. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 11.3 T* document on CCO and the Documentation CD-ROM.

Contents

These release notes discuss the following topics:

- System Requirements, page 2
- New and Changed Information, page 16
- Installation Notes, page 48
- Important Notes, page 49
- Caveats, page 51
- Related Documentation, page 51
- Service and Support, page 55
- Cisco Connection Online, page 56
- Documentation CD-ROM, page 57

Corporate Headquarters

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

Copyright © 1999
Cisco Systems, Inc.
All rights reserved.

System Requirements

This section describes the system requirements for Release 11.3 T:

- Memory Requirements, page 2
- Hardware Supported, page 3
- Determining the Version of Your Software Release, page 4
- Upgrading to a New Software Release, page 4
- Feature Set Tables, page 5

Memory Requirements

Table 1 Memory Requirements for Cisco 2500 Series Routers

Platforms	Feature Sets ¹	Image Name	Software Image	Required Flash Memory	Required DRAM Memory	Runs from	In ²
Cisco 2500 Series	IP Feature Sets	IP	c2500-i-1	8 MB Flash	6 MB DRAM	Flash	
		IP/FW	c2500-io-1	8 MB Flash	4 MB DRAM	Flash	(3)
		IP Plus	c2500-is-1	8 MB Flash	4 MB DRAM	Flash	
		IP Plus 40	c2500-is40-1	8 MB Flash	4 MB DRAM	Flash	(3)
		IP Plus 56	c2500-is56-1	8 MB Flash	4 MB DRAM	Flash	(3)
		IP Plus IPsec 56	c2500-is56i-1	8 MB Flash	4 MB DRAM	Flash	(3)
		IP/IBM/APPN	c2500-ai3r4-1	8 MB Flash	8 MB DRAM	Flash	
		IP/IPX/AT/DEC	c2500-d-1	8 MB Flash	4 MB DRAM	Flash	
		IP/IPX/AT/DEC/FW Plus	c2500-dos-1	16 MB Flash	4 MB DRAM	Flash	(3)
		IP/IPX/AT/DEC Plus	c2500-ds-1	8 MB Flash	6 MB DRAM	Flash	
	Enterprise Feature Sets	Enterprise/APPN Plus	c2500-ajs-1	16 MB Flash	8 MB DRAM	Flash	
		Enterprise/APPN Plus 40	c2500-ajs40-1	16 MB Flash	8 MB DRAM	Flash	(3)
		Enterprise/APPN Plus 56	c2500-ajs56-1	16 MB Flash	8 MB DRAM	Flash	(3)
		Enterprise/APPN Plus IPsec 56	c2500-ajs56i-1	16 MB Flash	8 MB DRAM	Flash	(3)
		Enterprise/FW Plus	c2500-jos56-1	16 MB Flash	8 MB DRAM	Flash	(3)
		Enterprise/FW Plus IPsec 56	c2500-jos56i-1	16 MB Flash	8 MB DRAM	Flash	(3)
		Enterprise Plus	c2500-js-1	16 MB Flash	6 MB DRAM	Flash	
		Enterprise Plus 40	c2500-js40-1	16 MB Flash	8 MB DRAM	Flash	(3)
		Enterprise Plus 56	c2500-js56-1	16 MB Flash	8 MB DRAM	Flash	(3)
		Enterprise Plus IPsec 56	c2500-js56i-1	16 MB Flash	8 MB DRAM	Flash	(3)
	FRAD Feature Sets	FRAD	c2500-f-1	8 MB Flash	4 MB DRAM	Flash	
		LAN FRAD/OSPF	c2500-f2in-1	8 MB Flash	4 MB DRAM	Flash	
		LAN FRAD	c2500-fin-1	8 MB Flash	4 MB DRAM	Flash	
		Remote Access Server (RAS)	c2500-c-1	8 MB Flash	6 MB DRAM	Flash	
		ISDN	c2500-g-1	8 MB Flash	4 MB DRAM	Flash	

- 1 If you need to upgrade the main memory for your Cisco series router, be sure to order the upgrade specific to your router.
- 2 The number in the “In” column indicates the Cisco IOS release when the image was first introduced. For example, (4) means an image was introduced in Release 12.0(4)T. If a cell in this column is empty, the interface was included in the initial base release.

Hardware Supported

Cisco IOS Release 11.3 T supports the Cisco 2500 series:

- Single LAN: Cisco 2501, 2502, 2503, and 2504
- Dual LANs: Cisco 2513, 2514, and 2515
- Integrated HUBs: Cisco 2505, 2507, and 2516
- High Density Serial: Cisco 2520, 2521, 2522, and 2523
- Modular Routers: Cisco 2524 and 2525
- Access Servers:
 - Cisco AS2509 and 2509-ET
 - Cisco AS2509-RJ and AS2511-RJ
 - Cisco AS2511 and AS2512

For detailed descriptions of the new hardware features, see the “New and Changed Information” section on page 16

Table 2 Supported Interfaces for the Cisco 2500 Series

Interface, Network Module, or Data Rate	Platforms Supported
LAN Interfaces	
Ethernet (AUI)	Cisco 2501, 2503, 2509, 2511, 2513, 2514, 2520, 2522, and 2524 only
Ethernet (10BaseT)	Cisco 2505, 2507, 2516, and 2524 only
4-Mbps Token Ring	Cisco 2502, 2504, 2513, 2515, 2521, 2523, and 2525 only
16-Mbps Token Ring	Cisco 2502, 2504, 2513, 2515, 2521, 2523, and 2525 only
WAN Data Rates	
56/64 kbps up to 1.536 Mbps	Cisco 2500 series
128 kbps	Cisco 2500 series
WAN Interfaces	
EIA/TIA-232	Cisco 2500 series
EIA/TIA-449	Cisco 2500 series
EIA-530	Cisco 2500 series
X.21	Cisco 2500 series
V.35	Cisco 2500 series
Serial, synchronous	Cisco 2500 series
Serial, synchronous, and asynchronous	Cisco 2520, 2521, 2522, and 2523 only
ISDN BRI S/T	Cisco 2503, 2504, 2516, 2520, 2521, 2522, 2523, 2524, and 2525 only
ISDN BRI U	Cisco 2524 and 2525 only

Cisco AS2509-RJ and Cisco AS2511-RJ Access Servers

The Cisco AS2509-RJ and Cisco AS2511-RJ access servers connect asynchronous serial devices to LANs and WANs. The access servers combine the functions of a terminal server, protocol translator, and a router and perform both synchronous and asynchronous routing of supported protocols.

These access servers provide the following interfaces and ports:

- Eight (Cisco AS2509-RJ) or 16 (Cisco AS2511-RJ) asynchronous serial ports for connection to modems, terminals, or other asynchronous devices
- One Ethernet attachment unit interface (AUI) port for connection to a LAN
- One synchronous serial port for connection to a WAN
- One EIA/TIA-232 console port for connection to a console terminal
- One EIA/TIA-232 auxiliary port for connection to a terminal or modem

Generated SysObjectIDs

The Generated SysObjectIDs feature generates a unique sysObjectID for each Cisco 2500 series router and its derived partner product. For example, the sysObjectID values for a Cisco 2511, a partner 2511, and another partner 2511 are each different. The sysObjectID Simple Network Management Protocol (SNMP) MIB object is used to identify the device to be managed and make application-specific decisions. In some network management programs, this object determines which graphical element or name to display for a device.

Selective Packet Discard (SPD)

When in severe overload conditions, routers that cannot keep up with the incoming packet stream must drop packets. If no intelligence is applied to choosing which ones to discard, the stability of routing protocols is impacted. This feature applies some simple choices to selectively discard packets likely to be unimportant for routing and interface stability. SPD is enabled by default; there are no commands or configuration tasks required.

Determining the Version of Your Software Release

To determine the version of Cisco IOS software running on your Cisco 2500 series router, log in to the router, and enter the **show version** user EXEC command:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-io-1), Version 11.3(11)T, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For information about upgrading to a new software release, see the product bulletin *Cisco IOS Software Release 11.3 Upgrade Paths and Packaging Simplification* on CCO at:

Service & Support: Product Bulletins: Software

Under **Cisco IOS 11.3**, click **Cisco IOS Software Release 11.3 Upgrade Paths (#703: 12/97)**

This product bulletin does not contain information specific to Cisco IOS Release 11.3 T but provides generic upgrade information that may apply to Cisco IOS Release 11.3 T.

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.

Release 11.3 T supports the same feature sets as Release 11.3, but Release 11.3 T can include new features supported by the Cisco 2500 series.

Table 3 Feature Sets Supported by the Cisco 2500 Series

Feature Set Image Names	Feature Set Matrix Term	Software Image	Platforms	In ¹
IP	Basic ²	c2500-i-1	Cisco 2500 series	
IP/FW	Basic	c2500-io-1	Cisco 2500 series	(3)
IP Plus	Plus ³	c2500-is-1	Cisco 2500 series	
IP Plus 40	Plus 40 ⁴	c2500-is40-1	Cisco 2500 series	(3)
IP Plus 56	Plus 56 ⁵	c2500-is56-1	Cisco 2500 series	(3)
IP Plus IPSec 56	Plus, IPSec 56 ⁶	c2500-is56i-1	Cisco 2500 series	(3)
IP/IBM/APPN	Basic	c2500-ai3r4-1	Cisco 2500 series	
IP/IPX/AT/DEC	Basic	c2500-d-1	Cisco 2500 series	
IP/IPX/AT/DEC/FW Plus	Plus	c2500-dos-1	Cisco 2500 series	(3)
IP/IPX/AT/DEC Plus	Plus	c2500-ds-1	Cisco 2500 series	
Enterprise/APPN Plus	Plus	c2500-ajs-1	Cisco 2500 series	
Enterprise/APPN Plus 40	Plus 40	c2500-ajs40-1	Cisco 2500 series	(3)
Enterprise/APPN Plus 56	Plus 56	c2500-ajs56-1	Cisco 2500 series	(3)
Enterprise/APPN Plus IPSec 56	Plus, IPSec 56	c2500-ajs56i-1	Cisco 2500 series	(3)
Enterprise/FW Plus 56	Plus 56	c2500-jos56-1	Cisco 2500 series	(3)
Enterprise/FW Plus IPSec 56	Plus, IPSec 56	c2500-jos56i-1	Cisco 2500 series	(3)
Enterprise Plus	Plus	c2500-js-1	Cisco 2500 series	
Enterprise Plus 40	Plus 40	c2500-js40-1	Cisco 2500 series	(3)
Enterprise Plus 56	Plus 56	c2500-js56-1	Cisco 2500 series	(3)
Enterprise Plus IPSec 56	Plus, IPSec 56	c2500-js56i-1	Cisco 2500 series	(3)
FRAD	Basic	c2500-f-1	Cisco 2501, 2502, Cisco 2520–2523	
LAN FRAD/OSPF	Basic	c2500-f2in-1	Cisco 2501, 2502, Cisco 2520–2523	
LAN FRAD	Basic	c2500-fin-1	Cisco 2501, 2502, Cisco 2520–2523	
Remote Access Server (RAS)	Basic	c2500-c-1	Cisco 2500 series	
ISDN	Basic	c2500-g-1	Cisco 2500 series	

¹ The number in the “In” column indicates the Cisco IOS release when the image was first introduced. For example, (3) means an image was introduced in Release 11.3(3)T. If a cell in this column is empty, the interface was included in the initial base release.

² This feature set is offered in the basic feature set.

³ This feature set is offered in the Plus feature set.

System Requirements

- 4 This feature set is offered in the encryption feature sets, which consist of 40-bit (Plus 40) data encryption feature sets.
- 5 This feature set is offered in the encryption feature sets, which consist of 56-bit (Plus 56) data encryption feature sets.
- 6 This feature set is offered in the encryption feature sets, which consist of IPsec 56-bit (Plus IPsec 56) data encryption feature sets.



Caution Cisco IOS images with strong encryption (including, but not limited to, 56-bit data encryption feature sets) are subject to United States government export controls and limited distribution. Images to be installed outside the United States require an export license. Customer orders may be denied or subject to delay because of United States government regulations. Contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Table 4 and Table 5 list the features and feature sets supported by the Cisco 2500 series in Cisco IOS Release 11.3 T. Both use the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.

Note This feature set table only contains a selected list of features. This table is not cumulative—nor does it list all the features in each image.

Table 4 Feature List by Feature Set for the Cisco 2500 Series Routers, Part 1

Feature	Feature Set												
	IP	IP Plus	IP Plus 40 ¹	IP Plus 56 ¹	IP Plus IP-SEC 56 ²	ISDN	IP/IPX/ AT/ DEC	IP/IPX/ AT/ DEC Plus	IP/ IBM/ APPN	Enterprise Plus	Enterprise Plus 40 ¹	Enterprise Plus 56 ¹	Enterprise Plus IP-SEC 56 ²
IBM Support													
APPN High Performance Routing	No	No	No	No	No	No	No	No	Yes	No	No	No	No
APPN MIB Enhancements	No	No	No	No	No	No	No	No	Yes	No	No	No	No
APPN over Ethernet LAN Emulation	No	No	No	No	No	No	No	No	Yes	No	No	No	No
APPN Scalability Enhancements	No	No	No	No	No	No	No	No	Yes	No	No	No	No
Bisync Enhancements, includes: — Bisync 3780 Support — BSC Extended Addressing — Block Serial Tunneling (BSTUN) over Frame Relay	No	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes
Cisco MultiPath Channel (CMPC)	No	No	No	No	No	No	No	No	No	No	No	No	No

Table 4 Feature List by Feature Set for the Cisco 2500 Series Routers, Part 1 (continued)

Feature	Feature Set												
	IP	IP Plus	IP Plus 40 ¹	IP Plus 56 ¹	IP Plus IP-SEC 56 ²	ISDN	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus	IP/IBM/APPN	Enterprise Plus	Enterprise Plus 40 ¹	Enterprise Plus 56 ¹	Enterprise Plus IP-SEC 56 ²
DLSw+ Enhancements, <i>includes</i> : — Backup Peer Extensions for Encapsulation Types — DLSw+ Border Peer Caching — DLSw+ MIB Enhancements — DLSw+ SNA Type of Service — LLC2-to-SDLC Conversion Between PU4 Devices — NetBIOS Dial-on-Demand Routing — UDP Unicast Enhancement	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes
FRAS Enhancements, <i>includes</i> : — FRAS Boundary Network Node Enhancement — FRAS Dial Backup over DLSw+ — FRAS DLCI Backup — FRAS Host — FRAS MIB — SRB over Frame Relay	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes
RIF Passthru in DLSw+	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes
SRB over FDDI on Cisco 4000, 450, and 4700 Series Routers	No	No	No	No	No	No	No	No	No	No	No	No	No
TN3270 LU Nailing	No	No	No	No	No	No	No	No	No	No	No	No	No
TN3270 Server Enhancements	No	No	No	No	No	No	No	No	No	No	No	No	No
Token Ring LANE	No	No	No	No	No	No	No	No	No	No	No	No	No
Tunneling of Asynchronous Security Protocols	No	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes
Internet													
DRP Server Agent	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
DRP Server Agent Enhancements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
IP Routing													
Easy IP (Phase 1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hot Standby Router Protocol (HSRP) over ISL in Virtual LAN Configurations	No	No	No	No	No	No	No	No	No	No	No	No	No

System Requirements

Table 4 Feature List by Feature Set for the Cisco 2500 Series Routers, Part 1 (continued)

Feature	Feature Set												
	IP	IP Plus	IP Plus 40 ¹	IP Plus 56 ¹	IP Plus IP-SEC 56 ²	ISDN	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus	IP/IBM/APPN	Enterprise Plus	Enterprise Plus 40 ¹	Enterprise Plus 56 ¹	Enterprise Plus IP-SEC 56 ²
IP Enhanced IGRP Route Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Type of Service and Precedence for GRE Tunnels	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Network Address Translation (NAT)	No	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes
TCP Enhancements, includes: — TCP Selective Acknowledgment — TCP Timestamp	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN Support													
AppleTalk Access List Enhancements	No	No	No	No	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes
DECnet Accounting	No	No	No	No	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes
IPX Named Access Lists	No	No	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
IPX SAP-after-RIP	No	No	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
NLSP Enhancements	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes
NLSP Multicast Support	No	No	No	No	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes
Management													
Cisco Call History MIB Command Line Interface	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS Internationalization	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB, Phase 1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Inform Requests	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes
SNMPv2C	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Virtual Profiles	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPDN MIB and Syslog Facility	No	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes
Multimedia													
IP Multicast Load Splitting across Equal-Cost Paths	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Multicast over ATM Point-to-Multipoint Virtual Connections	No	No	No	No	No	No	No	No	No	No	No	No	No
IP Multicast over Token Ring LANs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 2500 Series Routers, Part 1 (continued)

Feature	Feature Set												
	IP	IP Plus	IP Plus 40 ¹	IP Plus 56 ¹	IP Plus IP-SEC 56 ²	ISDN	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus	IP/IBM/APPN	Enterprise Plus	Enterprise Plus 40 ¹	Enterprise Plus 56 ¹	Enterprise Plus IP-SEC 56 ²
PIM Version 2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stub IP Multicast Routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Quality of Service													
RTP Header Compression	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security													
Additional Vendor-Proprietary RADIUS Attributes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Automated Double Authentication	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes
Certificate Authority Interoperability	No	No	No	No	Yes	No	No	No	No	No	No	No	Yes
Cisco IOS Firewall: Context-Based Access Control	No	No	No	No	No	No	No	No	No	No	No	No	No
Double Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Encrypted Kerberized Telnet	No	No	No	No	No	No	No	No	No	No	No	Yes	Yes
HTTP Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Internet Key Exchange Security Protocol	No	No	Yes	Yes	Yes	No	No	No	No	No	Yes	Yes	Yes
IPSec Network Security	No	No	Yes	Yes	Yes	No	No	No	No	No	Yes	Yes	Yes
MS-CHAP Support	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes
Named Method Lists for AAA Authentication & Accounting	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Per-User Configuration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reflexive Access Lists	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes
TCP Intercept	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes
Vendor-Proprietary RADIUS Attributes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Switching													
AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs	No	No	No	No	No	No	No	No	No	No	No	No	No
CLNS and DECnet Fast Switching over PPP	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes

System Requirements

Table 4 Feature List by Feature Set for the Cisco 2500 Series Routers, Part 1 (continued)

Feature	Feature Set												
	IP	IP Plus	IP Plus 40 ¹	IP Plus 56 ¹	IP Plus IP-SEC 56 ²	ISDN	IP/IPX/AT/DEC	IP/IPX/AT/DEC Plus	IP/IBM/APPN	Enterprise Plus	Enterprise Plus 40 ¹	Enterprise Plus 56 ¹	Enterprise Plus IP-SEC 56 ²
DECnet/VINES/XNS over ISL, includes: — Banyan VINES Routing over ISL Virtual LANs — DECnet Routing over ISL Virtual LANs — XNS Routing over ISL Virtual LANs	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes
Fast-Switched Policy Routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX Routing over ISL Virtual LANs	No	No	No	No	No	No	No	No	No	No	No	No	No
VIP Distributed Switching Support for IP Encapsulated in ISL	No	No	No	No	No	No	No	No	No	No	No	No	No
Terminal Services													
Virtual Templates for Protocol Translation	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes
WAN Optimization													
ATM MIB Enhancements	No	No	No	No	No	No	No	No	No	No	No	No	No
PAD Enhancements	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes
PAD Subaddressing	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN Services													
Always On/Dynamic ISDN (AO/DI)	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes
Bandwidth Allocation Control Protocol	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes
Dialer Watch	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced Local Management Interface (ELMI)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Enhancements	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay MIB Extensions	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Router ForeSight	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Advice of Charge	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Caller ID Callback	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN NFAS	No	No	No	No	No	No	No	No	No	No	No	No	No
Layer 2 Forwarding—Fast Switching	No	Yes	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 2500 Series Routers, Part 1 (continued)

Feature	Feature Set												
	IP	IP Plus	IP Plus 40 ¹	IP Plus 56 ¹	IP Plus IP-SEC 56 ²	ISDN	IP/IPX/ AT/ DEC	IP/IPX/ AT/ DEC Plus	IP/ IBM/ APPN	Enterprise Plus	Enterprise Plus 40 ¹	Enterprise Plus 56 ¹	Enterprise Plus IP-SEC 56 ²
Leased Line ISDN at 128 kbps	No	No	No	No	No	No	No	No	No	No	No	No	No
Microsoft Point-to-Point Compression	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiple ISDN Switch Types	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
National ISDN Switch Types for BRI and PRI Interfaces	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP over ATM	No	No	No	No	No	No	No	No	No	No	No	No	No
Telnet Extensions for Dialout	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
X.25 Enhancements	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 on ISDN	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Switching between PVCs and SVCs	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.28 Emulation	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes

1 This image is not available in Releases 11.3(1)T and 11.3(2)T. It is available in Release 11.3(3)T and later 11.3 T releases.

2 This image is available in Release 11.3(3)T and later releases.

Table 5 Feature List by Feature Set for the Cisco 2500 Series Routers, Part 2

Feature	Feature Set												
	Enterprise/ APPN Plus	Enterprise/ APPN Plus 40 ¹	Enterprise/ APPN Plus 56 ¹	Enterprise/ APPN Plus IP-SEC 56 ²	RAS	IP/ FW ²	IP/ IPX/ AT/ DEC Plus ²	Enterprise/ FW Plus 56 ²	Enterprise/ IP-SEC 56 ²	FRAD	LAN FRAD	LAN OSPF	
IBM Support													
APPN High Performance Routing	Yes	Yes	Yes	Yes	No	No	No	No	No	Yes	Yes	Yes	
APPN MIB Enhancements	Yes	Yes	Yes	Yes	No	No	No	No	No	Yes	Yes	Yes	
APPN over Ethernet LAN Emulation	Yes	Yes	Yes	Yes	No	No	No	No	No	Yes	Yes	Yes	
APPN Scalability Enhancements	Yes	Yes	Yes	Yes	No	No	No	No	No	Yes	Yes	Yes	

System Requirements

Table 5 Feature List by Feature Set for the Cisco 2500 Series Routers, Part 2 (continued)

Feature	Feature Set											
	Enterprise/ APPN Plus	Enterprise/ APPN Plus 40 ¹	Enterprise/ APPN Plus 56 ¹	Enterprise/ APPN Plus IP- SEC 56 ²	RAS	IP/ FW ²	IP/ IPX/ AT/ DEC FW Plus ²	Enterprise/ FW Plus 56 ²	Enterprise/ FW Plus IP- SEC 56 ²	FRAD	LAN FRAD	LAN FRAD OSPF
Bisync Enhancements, includes: — Bisync 3780 Support — BSC Extended Addressing — Block Serial Tunneling (BSTUN) over Frame Relay	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Cisco MultiPath Channel (CMPC)	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
DLSw+ Enhancements, <i>includes:</i> — Backup Peer Extensions for Encapsulation Types — DLSw+ Border Peer Caching — DLSw+ MIB Enhancements — DLSw+ SNA Type of Service — LLC2-to-SDLC Conversion Between PU4 Devices — NetBIOS Dial-on-Demand Routing — UDP Unicast Enhancement	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes
FRAS Enhancements, includes: — FRAS Boundary Network Node Enhancement — FRAS Dial Backup over DLSw+ — FRAS DLCI Backup — FRAS Host — FRAS MIB — SRB over Frame Relay	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes
RIF Passthru in DLSw+	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes
SRB over FDDI on Cisco 4000, 4500, and 4700 Series Routers	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
TN3270 LU Nailing	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
TN3270 Server Enhancements	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
Token Ring LANE	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
Tunneling of Asynchronous Security Protocols	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 2500 Series Routers, Part 2 (continued)

Feature	Feature Set											
	En- ter- prise/ APPN Plus	En- ter- prise/ APPN Plus 40 ¹	En- ter- prise/ APPN Plus 56 ¹	En- ter- prise/ APPN Plus IP- SEC 56 ²	RAS	IP/ FW ²	IP/ IPX/ AT/ DEC FW Plus ²	En- ter- prise/ FW Plus 56 ²	En- ter- prise/ FW Plus 56 ²	FRAD	LAN FRAD	LAN FRAD OSPF
Internet												
DRP Server Agent	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DRP Server Agent Enhancements	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Routing												
Easy IP (Phase 1)	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hot Standby Router Protocol (HSRP) over ISL in Virtual LAN Configurations	No	No	No	No	No	No	No	No	No	No	No	No
IP Enhanced IGRP Route Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Type of Service and Precedence for GRE Tunnels	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Network Address Translation (NAT)	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No
TCP Enhancements, includes: — TCP Selective Acknowledgment — TCP Timestamp	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN Support												
AppleTalk Access List Enhancements	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No	No	No
DECnet Accounting	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No	No	No
IPX Named Access Lists	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No	No
IPX SAP-after-RIP	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No	No
NLSP Enhancements	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No	No
NLSP Multicast Support	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No	No	No
Management												
Cisco Call History MIB Command Line Interface	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS Internationalization	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB, Phase 1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMPv2C	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No	No	No
SNMP Inform Requests	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Profiles	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

System Requirements

Table 5 Feature List by Feature Set for the Cisco 2500 Series Routers, Part 2 (continued)

Feature	Feature Set											
	Enterprise/ APPN Plus	Enterprise/ APPN Plus 40 ¹	Enterprise/ APPN Plus 56 ¹	Enterprise/ APPN Plus IP- SEC 56 ²	RAS	IP/ FW ²	IP/ IPX/ AT/ DEC FW Plus ²	Enterprise/ FW Plus 56 ²	Enterprise/ FW Plus 56 ²	FRAD	LAN FRAD	LAN FRAD OSPF
VPDN MIB and Syslog Facility	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No	No
Multimedia												
IP Multicast Load Splitting across Equal-Cost Paths	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Multicast over ATM Point-to-Multipoint Virtual Connections	No	No	No	No	No	No	No	No	No	No	No	No
IP Multicast over Token Ring LANs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM Version 2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stub IP Multicast Routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Quality of Service												
RTP Header Compression	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security												
Additional Vendor-Proprietary RADIUS Attributes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Automated Double Authentication	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Certificate Authority Interoperability	No	No	No	Yes	No	No	No	No	Yes	No	No	No
Cisco IOS Firewall: Context-Based Access Control	No	No	No	No	No	Yes	Yes	Yes	Yes	No	No	No
Double Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Encrypted Kerberized Telnet	No	No	Yes	No	No	No	No	Yes	Yes	No	No	No
HTTP Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Internet Key Exchange Security Protocol	No	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No	No
IPSec Network Security	No	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No	No
MS-CHAP Support	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No	No
Named Method Lists for AAA Authentication & Accounting	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Per-User Configuration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reflexive Access Lists	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TCP Intercept	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No	No
Vendor-Proprietary RADIUS Attributes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 2500 Series Routers, Part 2 (continued)

Feature	Feature Set											
	En-ter-prise/ APPN Plus	En-ter-prise/ APPN Plus 40 ¹	En-ter-prise/ APPN Plus 56 ¹	En-ter-prise/ APPN Plus IP- SEC 56 ²	RAS	IP/ FW ²	IP/ IPX/ AT/ DEC FW Plus ²	En-ter-prise/ FW Plus 56 ²	En-ter-prise/ FW Plus 56 ²	FRAD	LAN FRAD	LAN FRAD OSPF
Switching												
AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs	No	No	No	No	No	No	No	No	No	No	No	No
CLNS and DECnet Fast Switching over PPP	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No	No
DECnet/Vines/XNS over ISL, includes: — Banyan VINES Routing over ISL Virtual LANs — DECnet Routing over ISL Virtual LANs — XNS Routing over ISL Virtual LANs	Yes	Yes	Yes	No	Yes	No	No	Yes	Yes	No	No	No
Fast-Switched Policy Routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX Routing over ISL Virtual LANs	No	No	No	No	No	No	No	No	No	No	No	No
VIP Distributed Switching Support for IP Encapsulated in ISL	No	No	No	No	No	No	No	No	No	No	No	No
Terminal Services												
Virtual Templates for Protocol Translation	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No	No	No
WAN Optimization												
ATM MIB Enhancements	No	No	No	No	No	No	No	No	No	No	No	No
PAD Enhancements	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No	No	No
PAD Subaddressing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN Services												
Always On/Dynamic ISDN (AO/DI)	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No	No
Bandwidth Allocation Control Protocol	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced Local Management Interface (ELMI)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Enhancements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay MIB Extensions	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Router ForeSight	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

New and Changed Information

Table 5 Feature List by Feature Set for the Cisco 2500 Series Routers, Part 2 (continued)

Feature	Feature Set											
	Enterprise/ APPN Plus	Enterprise/ APPN Plus 40 ¹	Enterprise/ APPN Plus 56 ¹	Enterprise/ APPN Plus IP- SEC 56 ²	RAS	IP/ FW ²	IP/ IPX/ AT/ DEC FW Plus ²	Enterprise/ FW Plus 56 ²	Enterprise/ FW Plus IP- SEC 56 ²	FRAD	LAN FRAD	LAN FRAD OSPF
ISDN Advice of Charge	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Caller ID Callback	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN NFAS	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
Layer 2 Forwarding—Fast Switching	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No	No
Leased Line ISDN at 128 kbps	No	No	No	No	No	No	No	No	No	No	No	No
Microsoft Point-to-Point Compression	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multiple ISDN Switch Types	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
National ISDN Switch Types for Basic Rate and Primary Rate Interfaces	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP over ATM	No	No	No	No	No	No	No	No	No	No	No	No
Telnet Extensions for Dialout	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Enhancements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 on ISDN	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Switching between PVCs and SVCs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.28 Emulation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

¹ This image is not available in Releases 11.3(1)T and 11.3(2)T. It is available in Release 11.3(3)T and later 11.3 T releases.

² This image is available in Release 11.3(3)T and later releases.

New and Changed Information

The following sections list the new features supported by the Cisco 2500 series routers for Cisco IOS Release 11.3 T.

No New Software Features in Release 11.3(5)T through 11.3(11)T

There are no new software features supported by the Cisco 2500 series in Cisco IOS Release 11.3(5)T through 11.3(11)T.

New Software Features in Release 11.3(4)T

The following new software feature is supported by the Cisco 2500 series in Release 11.3(4)T and later 11.3 T releases.

IP Type of Service and Precedence for GRE Tunnels

For more information about configuring the following new features, from CCO select **Service & Support**, go to **Documentation Home Page**, click **Cisco IOS Software Configuration**, click **Cisco IOS Release 11.3**, select **Cisco IOS 11.3 T New Features**, and then click **11.3(4)T New Features**. This information is also available on the Documentation CD-ROM.

Prior to the IP Type of Service and Precedence for GRE Tunnels feature, at generic route encapsulation-based tunnel endpoints, the Type of Service (TOS) bits (including precedence bits) were not copied to the tunnel or GRE IP header that encapsulates the inner packet. Instead, those bits were set to zero. This was not a problem unless the intermediate routers between two tunnel endpoints honored TOS or precedence bits, in which case those settings were ignored.

With the advent of virtual private network (VPN) and QoS applications, it is desirable to copy the TOS bits when the router encapsulates the packets using GRE. Thus, intermediate routers between tunnel endpoints can take advantage of the QoS features such as weighted fair queuing (WFQ) and weighted random early detection (WRED).

New Software Features in Release 11.3(3)T

The following new software features are supported by the Cisco 2500 series in Release 11.3(3)T and later 11.3 T releases.

Additional Vendor-Proprietary RADIUS Attributes

Remote Authentication Dial-In User Server (RADIUS) is an access server authentication, authorization, and accounting protocol originally developed by Livingston, Inc. Although an Internet Engineering Task Force (IETF) draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way.

In this release, Cisco IOS software introduces support for additional vendor-proprietary RADIUS attributes. For a complete list of supported IETF and vendor-proprietary RADIUS attributes, refer to the "RADIUS Attributes" appendix in the Cisco IOS Release 11.3 *Security Configuration Guide*.

Always On/Dynamic ISDN (AO/DI)

Always On/Dynamic ISDN (AO/DI) is an on-demand service that optimizes the use of an existing Integrated Services Digital Network (ISDN) signaling channel (D channel) to transport X.25 traffic. The X.25 D-channel call is placed from the subscriber to the packet data service provider. Multilink and TCP/IP protocols are encapsulated within the X.25 logical circuit carried by the D channel. The bearer channels (B channels) use the multilink protocol without the standard Q.922 and X.25 encapsulations and invoke additional bandwidth as needed. AO/DI takes full advantage of existing packet handlers at the central office by using an existing D channel to transport the X.25 traffic.

The link associated with the X.25 D-channel packet connection is used as the primary link of the multilink protocol. The D channel is a connectionless, packet-oriented link between the Customer Premise Equipment (CPE) and the central office. Because the D channel is always available, it is possible to offer "always available" services. On-demand functionality is achieved by using the B channels to temporarily boost data throughput and disconnecting them after use.

Automated Double Authentication

The automated double authentication feature enhances the existing double-authentication feature. With the existing double-authentication feature, a second level of user authentication is achieved for Telnet applications when the user enters a username and password. With automated double authentication, the user does not have to use Telnet but instead can respond to a dialog box that requests a username and password or PIN. (For information about the existing double authentication feature, refer to the “Configuring Authentication” chapter of the Cisco IOS Release *11.3 Security Configuration Guide*.)

Certificate Authority Interoperability

Certificate Authority (CA) interoperability is provided in support of the IP Security (IPSec) standard. CA interoperability permits Cisco IOS devices and CA devices to communicate so that your Cisco IOS device can obtain and use digital certificates from the CA. Although IPSec can be implemented in your network without the use of a CA, using a CA provides manageability and scalability for IPSec. For background and configuration information for IPSec, see the “IPSec Network Security” feature documentation.

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

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

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

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

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

The Cisco IOS Firewall feature set provides the following capabilities:

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

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

Internet Key Exchange Security Protocol

Internet Key Exchange Security Protocol (ISAKMP/Oakley) is a key management protocol, used in conjunction with the IPSec standard. IPSec is an IP security feature that provides robust authentication and encryption of IP packets. IPSec can be configured without ISAKMP/Oakley, but ISAKMP/Oakley enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. ISAKMP/Oakley is a hybrid protocol that implements the Oakley key exchange inside the ISAKMP framework.

IPSec Network Security

IPSec Network Security (IPSec) is a framework of open standards developed by the Internet Engineering Task Force (IETF). IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (“peers”) such as Cisco routers.

IPSec provides the following network security services:

- Privacy—IPSec can encrypt packets before transmitting them across a network.
- Integrity—IPSec authenticates packets at the destination peer to ensure that the data has not been altered during transmission.
- Authentication—Peers authenticate the source of all IPSec-protected packets.
- Anti-replay protection—Prevents capture and replay of packets; helps protect against denial-of-service attacks.

With IPSec, data can be transmitted across a public network without fear of observation, modification, or spoofing. This enables applications such as virtual private networks (VPNs), extranets, and remote user access.

IPSec services are similar to those provided by Cisco Encryption Technology, a proprietary security solution introduced in Release 11.2. (The IPSec standard was not yet available at Release 11.2.) However, IPSec provides a more robust security solution and is standards-based.

Microsoft Point-to-Point Compression

Microsoft Point-to-Point Compression (MPPC) compresses Point-to-Point Protocol (PPP) packets between Cisco and Microsoft client devices. The MPPC algorithm is designed to optimize processor and bandwidth utilization in order to support multiple simultaneous connections. The MPPC algorithm uses a Lempel-Ziv (LZ) based algorithm with a continuous history buffer called a dictionary.

MS-CHAP Support

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is the Microsoft version of CHAP and is an extension to RFC 1994. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; in this case, authentication occurs between a PC using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server (NAS).

MS-CHAP differs from the standard CHAP as follows:

- MS-CHAP is enabled by negotiating CHAP Algorithm 0x80 in LCP option 3, Authentication Protocol.
- The MS-CHAP Response packet is in a format designed to be compatible with Microsoft Windows NT 3.5 and 3.51, Microsoft Windows 95, and Microsoft LAN Manager 2.x. This format does not require the authenticator to store a clear or reversibly-encrypted password.
- MS-CHAP provides an authenticator-controlled authentication retry mechanism.
- MS-CHAP provides an authenticator-controlled change password mechanism.
- MS-CHAP defines a set a “reason-for failure” codes returned in the Failure packet message field.

Depending on the security protocols you have implemented, PPP authentication using MS-CHAP can be used with or without authentication, authorization, and accounting (AAA) security services. If you have enabled AAA, PPP authentication using MS-CHAP can be used in conjunction with both

TACACS+ and RADIUS. Two new vendor-specific RADIUS attributes (IETF Attribute 26) were added to enable RADIUS to support MS-CHAP. For a complete list of supported IETF and vendor-proprietary RADIUS attributes, refer to the “RADIUS Attributes” appendix in the Cisco IOS Release 11.3 *Security Configuration Guide*.

Multiple ISDN Switch Types

The **multiple ISDN switch types** feature means more than one ISDN switch type can be configured per router. You can apply an ISDN switch type on a per-interface basis, thus extending the existing global **isdn switch-type** command to the interface level. This allows Basic Rate Interfaces (BRI) and Primary Rate Interfaces (PRI) to run simultaneously on platforms that support both interface types.

The **isdn tei** command is also extended to the interface level. Terminal endpoint negotiation (TEI) determines when Layer 2 is activated (powerup or first-call).

Named Method Lists for AAA

In earlier Cisco IOS releases, only named authentication method lists were supported under Cisco authentication, authorization, and accounting (AAA) network security services. Release 11.3(3)T extends AAA to support both authorization and accounting named method lists. Named method lists for authorization and accounting function the same way as those for authentication; you can define different methods for authorization and accounting and apply those methods on a per-interface or per-line basis.

National ISDN Switch Types for Basic Rate and Primary Rate Interfaces

National ISDN switch types for basic rate and primary rate interfaces introduces changes to ISDN switch type commands:

- Adds a new switch type for PRI interfaces (**isdn switch-type primary-ni**).
- Changes the BRI basic-ni1 switch type to basic-ni (**isdn switch-type basic-ni**).
- Removes the ISDN vn2 switch type (**isdn switch-type vn2**) used in France. The existing vn3 switch type (**isdn switch-type vn3**) supports French vn2 switches.
- Removes the ISDN basic-nwnet3 switch type (**isdn switch-type basic-nwnet3**) used in Norway. The basic-net3 switch type (**isdn switch-type basic-net3**) supports Norway NET3 switches.
- Removes the ISDN basic-nznet3 switch type (**isdn switch-type basic-nznet3**) used by New Zealand NET3 switches. The ISDN basic-net3 switch type (**isdn switch-type basic-net3**) supports New Zealand NET3 switches.
- Adds the ability to configure outgoing PRI B channel selection for the T1 controller in ascending order (channel 1 to channel 23) or descending order (channel 23 to channel 1). Previously, the router selected a B channel for outgoing calls from the highest free channel in descending order. The E1 controller channel selection for ascending order is channel 1 to 31 and 31 to 1 for descending order.

Note The command parser still accepts the following switch types: basic-nwnet3, vn2, and basic-net3; however, when viewing the NVRAM configuration by using either the **show running configuration** or **write terminal** command, the basic-net3 or vn3 switch types are displayed, respectively.

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, providing the following 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.

NFAS with D Channel Backup

The DMS100 and NI2 switch types have been added to the existing Non-Facility Associated Signaling (NFAS) with D-channel backup feature. ISDN NFAS allows a single D channel to control multiple PRI interfaces. A backup D channel can be configured for use when the primary NFAS D channel fails. When the channelized T1 controllers are configured for ISDN PRI, only the NFAS primary D channel must be configured; its configuration is distributed to all the members of the associated NFAS group.

Use of a single D channel to control multiple PRI interfaces can free one B channel on each interface to carry other traffic. Any hard failure causes a switchover to the backup D channel, and currently connected calls remain connected.

RIF Passthru in DLSw+

By default, DLSw+ terminates the RIF for Token Ring, terminates the LLC for all media types, and forwards only data across a WAN with DLSw+ and TCP/IP headers. The RIF is a field in source-route bridged frames that indicates the SRB path the frame should take when traversing a Token Ring network. In the case of an explorer packet, the RIF is a field of the source-route bridged frame that indicates the SRB path that the SRB explorer has traversed so far. The RIF is limited to seven hop counts by the IBM standards. Because DLSw+ terminates the RIF at the virtual ring, the

network scalability increases because the hop count of the packet starts over, and the packet can traverse seven additional hops. RIF termination simplifies network design because ring numbers no longer have to be unique throughout an entire enterprise.

However, some environments do not function properly if the RIF is terminated. For that reason, DLSw+ now supports the RIF Passthru feature, in which the entire source-route bridged path appears in the RIF.

VPDN MIB and Syslog Facility

The Virtual Private Dialup Network (VPDN) Management Information Base (MIB) and syslog facility feature is intended to support all the tables and objects defined in the Cisco VPDN MIB for the user sessions of the VPDN features. There are a number of commands that provide information and statistics through the command-line interface (CLI); the Cisco VPDN MIB has been created to satisfy the need to provide information and statistics through SNMP.

New Software Features in Release 11.3(2)T

The following new software features are supported by the Cisco 2500 series in Release 11.3(2)T and later 11.3 T releases.

Cisco Database Connection

The Cisco Database Connection feature enables Cisco routers to implement IBM-distributed relational database architecture (DRDA) level 3 over TCP/IP. The Cisco router with Database Connection exists in the TCP/IP network, and clients use the Database Connection IP address and port on the router to connect to the IBM host system that exists in the SNA network.

When the Database Connection feature is configured on a router, client-based Open Database Connectivity (ODBC) applications can connect to the IBM family of IBM D2 relational databases, which include:

- DB2 for OS/390 (MVS)
- DB2 for Virtual Machine (VM)
- DB2 for Virtual Storage Extended (VSE) (SQL/DS)
- DB2 for OS/400
- DB2 Universal Server (AIX, HP-UX, UNIX, Solaris, Windows NT, Windows 95, OS/2, SCO OpenServer)

The router with Database Connection converts DRDA packets over TCP/IP to DRDA packets over APPC (LU 6.2) and then routes them to DB2 databases. Database Connection runs as a TCP/IP daemon on the router, accepting DRDA client connections over TCP/IP. When a client connects to the database on an IBM mainframe host, Database Connection allocates an APPC conversation over SNA to an IBM server and acts as a gateway between DRDA over TCP/IP and DRDA over APPC.

DRP Server Agent Enhancements

The DRP Server Agent enhancements are as follows:

- DistributedDirector can use BGP Multi-Exit Discriminators in traffic-redirection decisions.
- The DRP Server Agent can measure client-to-server link latency (round-trip time) for use in traffic-redirection decisions.

PIM Version 2

Protocol-Independent Multicast (PIM) Version 2 includes the following improvements over PIM Version 1:

- A single, active rendezvous point (RP) exists per multicast group, with multiple backup RPs. This compares to multiple active RPs for the same group in PIM Version 1.
- A bootstrap router (BSR) provides a fault-tolerant, automated RP discovery and distribution mechanism. Thus, routers dynamically learn the group-to-RP mappings.
- Sparse mode and dense mode are properties of a group, as opposed to an interface. The mode strongly recommended is sparse-dense mode, as opposed to sparse mode or dense mode only.
- PIM Join and Prune messages have more flexible encodings for multiple address families.
- A more flexible Hello packet format replaces the Query packet to encode current and future capability options.
- Register messages to an RP indicate whether they were sent by a border router or a designated router.
- PIM packets are no longer inside IGMP packets; they are standalone packets.

PIM Version 1, together with the Auto-RP feature, performs the same tasks as the PIM Version 2 BSR. However, Auto-RP is a standalone protocol, separate from PIM Version 1, and is a Cisco proprietary protocol. PIM Version 2 is a standards-track protocol in the Internet Engineering Task Force (IETF).

The Cisco PIM Version 2 implementation allows good interoperability and transition between Version 1 and Version 2. You can upgrade to PIM Version 2 incrementally. You can configure PIM Versions 1 and 2 on different routers within one network. Internally, all routers on a shared media network must run the same PIM version. Therefore, if a PIM Version 2 router detects a PIM Version 1 router, the Version 2 router downgrades itself to Version 1 until all Version 1 routers have been shut down or upgraded.

PIM uses the BSR to discover and announce RP-set information for each group prefix to all the routers in a PIM domain. This is the same function accomplished by Auto-RP, but the BSR is part of the PIM Version 2 specification. The BSR mechanism interoperates with Auto-RP.

To avoid a single point of failure, you can configure several candidate BSRs in a PIM domain. A BSR is automatically elected among the candidate BSRs; candidates use bootstrap messages to discover which BSR has the highest priority. This router then announces to all PIM routers in the PIM domain that it is the BSR.

Routers that are configured as candidate RPs then unicast to the BSR the group range for which they are responsible. The BSR includes this information in its bootstrap messages and disseminates it to all PIM routers in the domain. Based on this information, all routers are able to map multicast groups to specific RPs. As long as a router is receiving the bootstrap message, it has a current RP map.

Dialer Watch

Dialer Watch is a backup feature that integrates dial backup with routing capabilities. Prior dial backup implementations used the following conditions to trigger backup:

- Interesting packets were defined at central and remote routers using dial-on-demand routing (DDR).
- Connection loss occurred on a primary interface using a backup interface with floating static routes.
- Traffic thresholds were exceeded using a dialer load threshold.

Prior backup implementations might not have supplied optimum performance on some networks, such as those using Frame Relay multipoint subinterfaces or Frame Relay connections that do not support end-to-end LMI.

Dialer Watch provides reliable connectivity without relying solely on defining interesting traffic to trigger outgoing calls at the central router. Dialer Watch uses the convergence times and characteristics of dynamic routing protocols. Integrating backup and routing features enables Dialer Watch to monitor every deleted route. By configuring a set of watched routes that define the primary interface, you can monitor and track the status of the primary interface as watched routes are added and deleted. Watched routes are monitored in the following sequence:

- 1 Whenever a watched route is deleted, Dialer Watch checks to see if there is at least one valid route for any of the watched IP addresses defined.
- 2 If there is no valid route, the primary line is considered down and unusable.
- 3 If there is a valid route for at least one of the defined watched IP addresses, and if the route is pointing to an interface other than the backup interface configured for Dialer Watch, the primary link is considered up.
- 4 If the primary link goes down, Dialer Watch is immediately notified by the routing protocol, and the secondary link is brought up.
- 5 When the secondary link is up, the primary link is rechecked at the expiration of each idle timeout.
- 6 If the primary link remains down, the idle timer is indefinitely reset.
- 7 If the primary link is up, the secondary backup link is disconnected. Additionally, you can set a disable timer to create a delay for the secondary link to disconnect after the primary link is reestablished.

MS Callback

The MS Callback feature provides client-server callback services for Microsoft Windows 95 and Microsoft Windows NT clients. MS Callback supports the Microsoft Callback Control Protocol (MSCB). MSCB is a Microsoft proprietary protocol used by Windows 95 and Windows NT clients. MS Callback supports negotiated PPP Link Control Protocol (LCP) extensions initiated and agreed upon by the Microsoft client. MS Callback is added to existing PPP Callback functionality. Therefore, if you configure your Cisco access server to perform PPP Callback using Cisco IOS Release 11.3(2)T or later, MS Callback is automatically available.

MS Callback supports AAA security models using a local database or AAA server. MSCB uses LCP callback options with suboption type 6. The Cisco MS Callback feature supports clients with a user-specified callback number and server specified (preconfigured) callback number. MS Callback does not affect non-Microsoft machines that implement standard PPP LCP extensions as described in RFC 1570. In this scenario, MS Callback is transparent.

New Software Features in Release 11.3(1)T

The following new software features are supported by the Cisco 2500 series in Release 11.3(1)T and later 11.3 T releases.

IBM SUPPORT:

APPN High Performance Routing

High Performance Routing (HPR) is an enhancement to APPN that improves network performance and reliability. Considered the next step in the evolution of SNA networking, HPR replaces the APPN routing technique called intermediate session routing (ISR) and provides significant performance improvements over ISR.

HPR replaces ISR with two elements: Rapid Transport Protocol (RTP) and automatic network routing.

RTP is a transport protocol that provides functions including error recovery, packet resequencing, segmentation, selective retransmissions, flow control, and congestion control. It incorporates a new congestion avoidance algorithm, Adaptive Rate-Based (ARB) congestion control. ARB is a preventive rather than a reactive congestion-control mechanism and maximizes the usage of limited and costly bandwidth with consistent response time under heavy traffic.

Automatic network routing is a new type of connectionless source routing with priority. Automatic Network Routing provides a low-level routing mechanism that minimizes cycles and storage requirements for routing packets through intermediate nodes.

The Cisco HPR implementation is compliant with Version 6 of the HPR architecture of record. All functions are interoperable with the following IBM major platforms:

- ACF/VTAM 4.2
- AS/400
- PS/2 (running Communications Server Version 4.0 and above.)

APPN MIB Enhancements

The router APPN MIB implementation has been updated to support a new MIB definition recently approved by the APPN Implementors Workshop (AIW). The new MIB provides better manageability of APPN network nodes across implementations. It also adds objects for supporting connection networks.

In this release Cisco supports both the current and new MIBs to allow for migration of Cisco application customers from the current version, which supports RFC 1593, to a new version for this new MIB.

APPN over Ethernet LAN Emulation

APPN over Ethernet LAN Emulation (LANE) is an enhancement to the Cisco APPN intermediate session routing (ISR) implementation that allows an APPN router to participate in an emulated LAN. APPN over Ethernet LANE enables the APPN network node on the router to communicate with an end system on a switched LAN environment.

APPN Scalability Enhancements

Two new APPN scalability enhancement features, locate throttling and negative caching, are used to tune your APPN network to conserve network resources by queuing redundant searches and retaining unreachable searches.

The locate throttling feature prevents multiple broadcast locate searches that can occur when more than one resource requests sessions with the same destination LU.

The negative caching feature prevents excess searches to unreachable resources.

Backup Peer Extensions for Encapsulation Types

Three types of encapsulation are supported in DLSw+: direct, Fast-Sequenced Transport (FST), and TCP. Previously, DLSw+ supported only backup peers for FST and TCP peer types. This new Frame Relay/Direct Backup Peer feature extends the backup peer capability to all types of DLSw+ transportation types.

Bisync 3780 Support

The Cisco Bisync 3780 support feature has been enhanced to add a user-configurable address on contention interfaces.

BSC Extended Addressing

The Cisco Bisync support protocol stack (BSC) extended addressing feature can be used to configure a set of nonstandard Bisync addresses (for non-IBM Bisync devices that do not use the standard set of 3270 Control Unit addresses).

Block Serial Tunneling (BSTUN) over Frame Relay

The BSTUN over Frame Relay feature provides a tunnel mechanism for Bisync protocol without TCP/IP encapsulation.

Cisco Multipath Channel

Cisco MultiPath Channel (CMPC) is a Cisco Systems implementation of the IBM MultiPath Channel (MPC) feature. CMPC allows the virtual telecommunications access method (VTAM) to establish Advanced-Peer-to-Peer Networking (APPN) connections using both high performance routing (HPR) and intermediate session routing (ISR) through a channel-attached Cisco 7000 series router using the MPC protocols.

DLSw+ Border Peer Caching

With the border peer caching feature, border peers can build three caches (local, remote, and group) and check these caches before forwarding explorers for other routers.

DLSw+ MIB Enhancements

The Cisco DLSw+ Management Information Base (MIB) enhancement feature includes more information about the “plus” features. For example, the MIB describes the encapsulation type being used: direct, LLC2, FST, and TCP. Furthermore, for FST and direct, which use fast cache entries instead of circuits to establish sessions, the MIB includes FST and direct cache entries.

The MIB also describes configured defaults for promiscuous and on-demand peers. It provides information about border peers, dynamic peers, and backup peers. Previously, the MIB was not informed about the remote-peer IP address when using direct or LLC2 encapsulation. Now the remote-peer IP address is sent through the capabilities exchange and listed in the MIB. Finally, the new MIB includes traps for peer up or down and circuit up or down. This MIB provides SNMP network management access to most of the information in the **show dlsw capabilities** command.

DLSw+ SNA Type of Service

DLSw+ SNA type of service (TOS) sets the IP precedence bits in the IP header of DLSw+ packets. When APPN is running with DLSw+ and the priority option is specified on the **dlsw remote peer** command, SNA TOS maps APPN class of service (COS) to TCP TOS.

FRAS Boundary Network Node Enhancement

The Frame Relay Access Support (FRAS) Boundary Network Node (BNN) enhancement provides seamless processing at the router regardless of end-station changes. End stations can be added or deleted without reconfiguring the router. The FRAS BNN enhancement coexists with the original FRAS BNN feature.

FRAS Dial Backup over DLSw+

Frame Relay Access Support (FRAS) Dial Backup over DLSw+ is an enhancement to the Cisco FRAS implementation that you can use to configure a secondary path that is used when the Frame Relay network becomes unavailable. If preconfigured properly, when the primary link to the Frame Relay WAN fails, FRAS Dial Backup over DLSw+ automatically moves existing sessions to the alternate link. When the primary link is restored, existing sessions are kept on the backup connection so that they can be moved nondisruptively to the primary link at your discretion.

FRAS DLCI Backup

Frame Relay Access Support (FRAS) DLCI Backup is an enhancement to the Cisco FRAS implementation that you can use to configure a secondary serial or ISDN path to the host to be used when the Frame Relay network becomes unavailable. When the primary Frame Relay link to the Frame Relay WAN fails, the FRAS DLCI Backup feature causes the router to reroute all sessions from the main Frame Relay interface to the secondary interface. The secondary interface can be either serial or ISDN and must have a data link connection identifier (DLCI) configured.

FRAS Host

The FRAS (Frame Relay Access Support) Host feature provides connectivity from a Systems Network Architecture (SNA) Frame Relay Access Device (FRAD) to a Cisco router for SNA mainframe access. This feature also provides connectivity from remote SNA FRADs to LAN-attached front-end processors (FEFs) or to LAN-attached SNA minicomputers (such as AS/400s).

FRAS MIB

The FRAS Management Information Base (MIB) CISCO-DLCSW-MIB.MY is a collection of managed objects that can be accessed via a network management protocol such as SNMP. The objects in the MIB support LLC- and SDLC-attached devices for both BNN and BAN formats of RFC 1490. The FRAS MIB user interface is defined by the network manager SNMP application.

LLC2-to-SDLC Conversion Between PU4 Devices

Data-link switching plus (DLSw+) supports LLC2-to-Synchronous Data Link Control (SDLC) Protocol conversion between PU4 devices. The LLC2-SDLC for PU4 feature allows a SDLC-attached FEP to communicate over DLSw+ to a LAN-attached FEP.

NetBIOS Dial-on-Demand Routing

DLSw+ filters NetBIOS Session Alive packets from the WAN. You can transport NetBIOS in a dial-on-demand routing (DDR) environment by filtering NetBIOS Session Alive packets. NetBIOS periodically sends Session Alive packets as LLC2 I-frames. These packets do not require a response and are superfluous to the function of proper data flow. Furthermore, these packets keep DDR interfaces up, which causes unwanted per-packet charges in DDR networks.

SRB over Frame Relay

Cisco IOS encapsulates source-route bridging (SRB) traffic using RFC-1490 bridged IEEE 802.5 encapsulation to provide SRB over Frame Relay functionality. This functionality can be between Cisco routers or between a Cisco router and RFC-1490-compliant FRADs or routers.

TN3270 LU Nailing

Logical unit (LU) nailing allows a client IP address to be mapped, or “nailed,” to one or more LU local addresses on one or more physical units (PUs) by means of router configuration commands. You can control the relationship between the TN3270 client and the LU.

Clients from traditional TN3270 (non-TN3270E) devices can connect to specific LUs, which overcomes a limitation of TN3270 devices that cannot specify a “CONNECT LU.” LU nailing is useful for TN3270E clients because you can perform the configuration at the router, providing central control, rather than at the client.

TN3270 Server Enhancements

The enhancements for the TN3270 server include the following:

- RFC-1646 Printer Support
- Function Management Header (FMH) Support
- Unformatted System Services Table (USSTAB) Conversion
- IP Type of Service/Precedence Setting

RFC-1646 Printer Support

Cisco provides full RFC-1646 printer support in the TN3270 server. There are no configuration tasks or other options required in the CIP to take advantage of this support. Prior versions of the TN3270 server feature provided RFC-1647 support.

Function Management Header (FMH) Support

The Function Management Header (FMH) support is provided in the context of providing printer support for the kanji character set. There are no configuration tasks or other options required in the CIP to take advantage of this support.

When a client does not support FMH and the host sends an FMH, the client reports a bad datastream or prints random data. Prior to TN3270 server support of FMH, when a host sent an FMH, the session would be unbound. With suitable host and client software, you can print double-byte character set characters over an LU type 1 session.

Unformatted System Services Table (USSTAB) Conversion

The TN3270 server translates the host SNA character string (SCS) to 3270DS. In the initial release of TN3270 server, you were required to set up the host to provide either SCS or 3270DS data, depending on the needs of the client. That requirement no longer exists.

IP Type of Service/Precedence Setting

The TN3270 server supports IP type of service (TOS) precedence setting. TOS is used in router networks to make routing decisions for the generated IP packets. The TN3270 server generates packets that comply to IP TOS/precedence values. (Refer to RFC 1349 for a description of IP TOS/precedence.)

Token Ring LANE

The Token Ring LANE (TR-LANE) feature emulates an IEEE 802.5 Token Ring LAN using asynchronous transfer mode (ATM) technology. LANE provides a service interface for network layer protocols that is identical to existing MAC layers. No changes are required to existing upper layer protocols and applications. With TR-LANE, Token Ring packets are encapsulated in the appropriate ATM cells and sent across the ATM network. When the packets reach the other side of the ATM network, they are unencapsulated. LANE essentially bridges LAN traffic across ATM switches.

TR-LANE allows legacy Token Ring LAN users to take advantage of ATM benefits without modifying end-station hardware or software.

ATM uses connection-oriented service with point-to-point signaling or multicast signaling between source and destination devices. However, Token Ring LANs use connectionless service. Messages are broadcast to all devices on the network. With TR-LANE, routers and switches emulate the connectionless service of a Token Ring LAN for the endstations.

Tunneling of Asynchronous Security Protocols

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

The Cisco 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.

UDP Unicast Enhancement

Silicon Switch Processor (SSP) address resolution packets is be sent via User Datagram Protocol (UDP) unicast service rather than via TCP. SSP packets include `CANUREACH.EX`, `NETBIOS_NAME_QUERY_EX`, `NB_ADD_NAME.QUERY_EX`, and `DATAFRAME`.

UDP unicast enhances the scalability of TCP peer networks because it allows DLSw+ to better control address resolution packets and unnumbered information (UI) frames during periods of congestion. Previously, these frames were carried over TCP. TCP retransmits frames that get lost or delayed in transit and aggravate congestion. Because address resolution packets and UI frames are not sent on a reliable transport on the LAN, sending them reliably over the WAN is unnecessary. By using UDP for these frames, DLSw+ minimizes network congestion.

UDP unicast enhancement does not affect fast-sequenced transport (FST) or direct peer encapsulations.

INTERNET:

DRP Server Agent

The Director Response Protocol (DRP), a simple UDP-based application developed by Cisco Systems, enables the Cisco 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 2500 Series Installation and Configuration Guide* or the *Cisco DistributedDirector 4700 Installation and Configuration Guide* for information on how to configure DistributedDirector.

IP ROUTING:

Easy IP (Phase 1)

The Easy IP (Phase 1) feature combines Network Address Translation (NAT) and PPP/Internet Protocol Control Protocol (IPCP). This feature enables a Cisco router to automatically negotiate its own registered WAN interface Internet Protocol (IP) address from a central server and to enable all

remote hosts to access the global Internet using this single registered IP address. Because Easy IP uses existing port-level multiplexed NAT functionality within the Cisco IOS software, IP addresses on the remote LAN are invisible to the Internet.

Hot Standby Router Protocol over ISL in Virtual LAN Configurations

The Hot Standby Router Protocol (HSRP) provides a very high level of redundancy between hosts and gateway routers. HSRP also provides high network availability by enabling backup routes between hosts on Ethernet, Fast Ethernet, FDDI, and Token Ring networks. Cisco IOS devices that are running the HSRP send and receive multicast hello packets to detect router failure and to designate active and standby routers.

HSRP was first introduced with ATM LAN Emulation in Cisco IOS Release 11.0 and in Release 11.1 for virtual LAN (VLAN) configurations in IP networks using IEEE 802.10 encapsulations on FDDI media. Starting with Release 11.3, HSRP is also supported over Inter-Switch Links (ISLs) in VLAN configurations on Fast Ethernet. Now, HSRP functionality can be deployed with Cisco IOS VLANS using IEEE 802.10 on FDDI, ATM LAN Emulation, and ISL encapsulation on Fast Ethernet.

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.

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 re-sent. With selective acknowledgment, TCP receives acknowledgment of packets 1, 2, 3, 5, 6, and 8. Only packets 4 and 7 have to be re-sent. 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 does 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.

LAN SUPPORT:

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

DECnet Accounting

DECnet Accounting provides information about DECnet packets and the number of bytes that are switched through the Cisco IOS software. You collect accounting information based on the source and destination DECnet addresses. DECnet accounting tracks only DECnet traffic that is routed out an interface on which DECnet accounting is configured; it does not include traffic generated by or terminating at the router itself.

Digital-Subscriber-Line Bridge

The x digital-subscriber-line bridge support feature can be used to configure a router for intelligent bridge flooding for x digital subscriber line and other bridge applications.

IPX Named Access Lists

You can now identify IPX access lists with an alphanumeric string (a name) rather than a number. You can use this feature 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 provides enhanced security because you can use 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 that do not support this feature, such as Cisco IOS Release 11.2 or Release 11.2 P.
- Access list names must be unique across all protocols.
- Numbered access lists are also available as described in the Cisco IOS Release 11.3 *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 corresponding RIP update. The feature ensures that no service information is 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 as often as RIP updates.

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

In addition, you can disable the sending of general RIP 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 are not rejected for lack of a route to the service. This can be especially useful on WAN circuits where the update intervals are 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. Disabling the sending of general queries when the link first comes up reduces traffic to a single update and saves 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. The router keeps LSP packets for a much longer time, which reduces overhead on slower-speed serial links and keeps ISDN links from becoming active unnecessarily.

NLSP Multicast Support

The NLSP multicast support feature adds support for the use of NLSP multicast addressing for Ethernet, Token Ring, and FDDI router interfaces. This capability is only possible when the underlying Cisco hardware device or driver supports multicast addressing.

With this feature, the router defaults to using multicasts instead of broadcasts on Ethernet, Token Ring, and FDDI interfaces to address all NLSP routers on the network. If an adjacent device does not support NLSP multicasting, the router uses broadcasts on the affected interface. When routers running prior versions of Cisco IOS software are on the same network with routers running Cisco IOS Release 11.3, broadcasts are used on any segment shared by the two routers.

MANAGEMENT:

Cisco Call History MIB Command-Line Interface

A Cisco IOS command-line interface (CLI) is available for setting two Cisco Call History MIB parameters. These parameters are the number of entries to be retained by the MIB and the length of time to retain them, which correspond to the following MIB objects:

- `ciscoCallHistoryTableMaxLength`
- `ciscoCallHistoryRetainTimer`

When you save the router configuration before reloading the router, the parameter values are also saved. Before this release, SNMP was the only available means for setting the values of these parameters. However, when the parameters are set by SNMP, the old values are lost, and the parameters are reset to their default values whenever a router is reloaded. The Cisco Call History MIB CLI is enabled by default.

Cisco IOS Internationalization

The Cisco IOS internationalization feature makes available HTML server side includes (SSIs) to customize international or domestic HTML pages used for the Cisco web browser interface (such as ClickStart pages) and to store them in Flash memory on multiple Cisco IOS platforms. In addition, you can display 8-bit or multibyte international character sets (such as Japanese) and print the escape (ESC) character as a single character instead of as the caret and bracket symbols (^[]) on the Cisco Web browser and at the router command line.

Entity MIB, Phase 1

The Entity MIB (RFC 2037) describes the logical resources, physical resources, and logical-to-physical mappings of devices managed by a single SNMP agent. This feature implements the first phase of the Entity MIB, the logical entity table. The logical entity table describes the logical entities managed by a single agent. The Entity MIB also records the time of the last modification to any object in the Entity MIB and sends out a trap when any object is modified. The Entity MIB provides no managed objects with write access.

SNMP Inform Requests

The SNMP inform requests feature allows routers to send inform requests to SNMP managers. Agent routers can send SNMP notifications to SNMP managers when particular events occur.

For example, an agent router might send a message to a manager when the agent router experiences an error condition. SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again.

Thus, informs are more likely to reach their intended destinations. However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, but an inform can be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

SNMP Manager

The SNMP manager feature allows a router to serve as an SNMP manager. As an SNMP manager, the router can send SNMP requests to agents and receive SNMP responses and notifications from agents. When the SNMP manager process is enabled, the router can query other SNMP agents and process incoming SNMP traps.

SNMPv2C

The SNMPv2C feature replaces support for SNMPv2Classic with support for SNMPv2 and SNMPv2C. SNMPv2C replaces the party-based administrative and security framework of SNMPv2Classic with the community-based administrative framework while retaining 64-bit counters and get-bulk functionality. This feature implements RFCs 1901 through 1907, deprecating the implementation of RFCs 1441 through 1451.

Note Cisco IOS software continues to support SNMPv1.

The following commands are obsolete in Release 11.3:

- **snmp-server access-policy**
- **snmp-server context**
- **snmp-server party**

In addition, the **snmp-server trap-authentication** command has been replaced. Use the **snmp-server enable traps snmp authentication** command in its place. Existing configurations that use the **snmp-server trap-authentication** command are not affected; however, this command is not saved to the startup configuration.

Virtual Profiles

The Virtual Profiles feature is a unique PPP application that defines and applies per-user configuration information for users who dial in to a router. This feature allows 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 overcome current limitations on network scalability:

- **AAA**—The current ability for Cisco routers 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 dial-in 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 dial-in 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 or access server.

MULTIMEDIA:

IP Multicast Load Splitting Across Equal-Cost Paths

You can configure load splitting of IP multicast traffic across equal-cost paths. Previously, when there were equal-cost paths between routers, IP multicast packets traversed only one path. If a tunnel was configured, the same next hop was always used, and no load splitting occurred.

IP multicast load splitting is accomplished indirectly by consolidating the available bandwidth of all the physical links into a single tunnel interface. The underlying physical connections then use existing unicast load-splitting mechanisms for the tunnel (multicast) traffic. By configuring load splitting among equal-cost paths, you can use your links between routers more efficiently when sending IP multicast traffic.

Note This feature is load splitting the traffic, not load balancing the traffic.

IP Multicast over ATM Point-to-Multipoint Virtual Connections

The IP Multicast over ATM Point-to-Multipoint Virtual Connections feature dynamically creates ATM point-to-multipoint switched virtual connections (SVCs) to handle IP multicast traffic more efficiently. The feature can enhance router performance and link utilization because packets are not replicated and sent multiple times over the ATM interface.

IP Multicast over Token Ring LANs

Prior to this feature, IP multicast datagrams used the MAC-level broadcast address 0xFFFF.FFFF.FFFF, which placed an unnecessary burden on all devices that did not participate in IP multicast. The IP multicast over Token Ring LANs feature defines a way to map IP multicast addresses to a single Token Ring MAC address. This feature defines the Token Ring functional address (0xc000.0004.0000) that should be used over Token Ring. The Cisco Systems implementation complies with RFC 1469, *IP Multicast over Token-Ring Local Area Networks* (June 1993).

IP multicast transmissions over Token Ring interfaces are more efficient than they used to be. This feature reduces the load on other machines that do not participate in IP multicast because they do not receive these packets.

The following restrictions apply to this feature:

- This feature can be configured only on a Token Ring interface.
- Neighboring devices on the Token Ring on which this feature is used should also use the same functional address for IP multicast traffic.
- Because there are a limited number of Token Ring functional addresses, other protocols can be assigned to the Token Ring functional address 0xc000.0004.0000. Therefore, not every frame sent to the functional address is necessarily an IP multicast frame.

Stub IP Multicast Routing

When using PIM in a large network, there are often stub regions over which the administrator has limited control. To reduce the configuration and administration burden, you can configure a subset of PIM functionality that provides the stub region with connectivity but does not allow it to participate in or potentially complicate any routing decisions.

Stub IP multicast routing allows simple multicast connectivity and configuration at stub networks. It eliminates periodic flood-and-prune behavior across slow-speed links (ISDN and below) using dense mode. It does this by using forwarded IGMP reports as a type of Join message and selective PIM message filtering.

QUALITY OF SERVICE:

RTP Header Compression

Real-time Transport Protocol (RTP) carries packetized audio and video traffic over an IP network. RTP is described in RFC 1889. RTP is not intended for data traffic, which uses Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). RTP provides end-to-end network transport functions intended for applications transmitting real-time requirements, such as audio, video, or simulation data over multicast or unicast network services.

The minimal 12 bytes of the RTP header, combined with 20 bytes of IP header and 8 bytes of UDP header create a 40-byte RTP/IP/UDP header. The RTP packet has a payload of approximately 20 to 150 bytes for audio applications that use compressed payloads. It is very inefficient to transmit the RTP/IP/UDP header without compressing it.

The RTP header compression feature compresses the RTP/IP/UDP header in an RTP data packet from 40 bytes to approximately 2 to 5 bytes. It is a hop-by-hop compression scheme similar to RFC 1144 for TCP header compression. Using RTP header compression can benefit both telephony voice and multicast backbone (MBONE) applications running over slow links.

RTP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. It is also supported over ISDN interfaces.

Enabling compression on both ends of a low-bandwidth serial link can greatly reduce the network overhead if there is a lot of RTP traffic on that slow link. This compression is beneficial especially when the RTP payload size is small (as with compressed audio payloads of 20 to 50 bytes). Although the MBONE-style RTP traffic has higher payload sizes, compact encodings like Compressed Encoding for Linear Prediction (CELP) can also help considerably.

SECURITY:

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, remote users must 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 must 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 remote host of the user. Therefore, the second authentication is specific to a user, not to a host. This feature provides an additional level of security that is effective even if the remote host is stolen.

Encrypted Kerberized Telnet

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

You can use Encrypted 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.

The Cisco implementation of Encrypted 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. The 56-bit DES encryption image is subject to U.S. government export-control regulations.

HTTP Security

All Cisco routers and access servers running Cisco IOS Release 11.0(6) or later have an HTTP server, which is an embedded subcomponent of the Cisco IOS software. Users with a privilege level of 15 can use a web browser to issue Cisco IOS commands from a predefined home page. In Cisco IOS Release 11.3, the HTTP security feature enables users with a privilege level other than 15 to access the HTTP server.

In addition, a new command has been added to specify how HTTP server users are authenticated. The HTTP server in the Cisco IOS Release 11.2 software uses the enable password method to authenticate a user at privilege level 15. In Release 11.3, system administrators can specify enable; local; Terminal Access Controller Access Control System (TACACS); or authentication, authorization, and accounting (AAA) user authentication.

Using the HTTP Security feature, network administrators can provide HTTP-server access to users with a privilege level of less than 15. The Cisco Web browser interface then mirrors the functionality of the command-line interface (CLI).

Per-User Configuration

The Per-User Configuration can tie together the following dial-in features:

- Virtual interface templates, which are 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 that sends it 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 these two features 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 dial-in session is deleted when the session ends. The resources used during the session are returned for other dial-in 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 dial-in users can provide a uniquely configured interface for each 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.

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 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 never reach the server. The software continues to intercept and forward packets throughout the duration of the connection.

Vendor-Proprietary RADIUS Attributes

Remote Authentication Dial-In User Server (RADIUS) is an access server authentication and accounting protocol originally developed by Livingston, Inc. Although an Internet Engineering Task Force (IETF) draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software currently supports the IETF draft standard RADIUS. In this release, Cisco IOS software introduces support for the most common vendor-proprietary RADIUS attributes.

Some vendor-proprietary implementations of RADIUS let the administrator define static routes and IP pool definitions on the RADIUS server, instead of on each network access server. As each network access server starts up, it queries the RADIUS server for static route and IP pool information. In this release, a new command enables the Cisco router to obtain static routes and IP pool definition information from the RADIUS server at start-up time. This frees the user from having to configure such information on each network access server.

SWITCHING:

AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs

AppleTalk can now be routed over virtual LAN (VLAN) subinterfaces using ISL and IEEE 802.10 VLAN encapsulating protocols. The AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs feature provides full-feature Cisco IOS AppleTalk support on a per-VLAN basis, allowing standard AppleTalk capabilities to be configured on VLANs. This feature allows users to configure consolidated VLAN routing over a single VLAN trunking interface. Before this feature, AppleTalk could be routed only on the main interface on a LAN port. If AppleTalk routing was disabled on the

main interface or if the main interface was shut down, the entire physical interface would stop routing any AppleTalk packets. With this feature enabled, AppleTalk routing on subinterfaces are unaffected by changes in the main interface.

Banyan VINES Routing over ISL Virtual LANs

Banyan VINES can now be routed over virtual LAN (VLAN) subinterfaces using the ISL encapsulation protocol. The Banyan VINES Routing over ISL Virtual LANs feature provides full-feature Cisco IOS software Banyan VINES support on a per-VLAN basis, allowing standard Banyan VINES capabilities to be configured on VLANs.

CLNS and DECnet Fast Switching Support over PPP

Cisco now supports fast switching of incoming and outgoing DECnet and CLNS packets over PPP.

DECnet Routing over ISL Virtual LANs

DECnet can now be routed over virtual LAN (VLAN) subinterfaces using the ISL VLAN encapsulation protocols. The DECnet Routing over ISL Virtual LANs feature provides full-feature Cisco IOS software DECnet support on a per-VLAN basis, providing for standard DECnet capabilities to be configured on VLANs.

Fast-Switched Policy Routing

IP policy routing can now be fast-switched. Previously, policy routing could only be process-switched, which meant that on most platforms, the switching rate was approximately 1,000 to 10,000 packets per second. This was not fast enough for many applications. Users who need policy routing to occur at faster speeds can implement policy routing without slowing down the router.

IPX Routing over ISL Virtual LANs

The IPX Routing over ISL Virtual LANs (VLANs) feature extends Novell NetWare routing capabilities to include support for routing all standard IPX encapsulations for Ethernet frame types in VLAN configurations. Users with Novell NetWare environments can now configure any one of the four IPX Ethernet encapsulations to be routed using the Inter-Switch Link (ISL) encapsulation across VLAN boundaries. IPX encapsulation options now supported for VLAN traffic include:

- novell-ether (Novell Ethernet_802.3)
- sap (Novell Ethernet_802.2)
- arpa (Novell Ethernet_II)
- snap (Novell Ethernet_Snap)

VIP Distributed Switching Support for IP Encapsulated in ISL

With this feature, Inter-Switch Link (ISL) encapsulated IP packets can be switched on Versatile Interface Processor (VIP) controllers installed on Cisco 7500 series routers.

VIP distributed switching offloads switching of ISL VLAN IP traffic to the VIP card, removing involvement from the main CPU. Offloading ISL traffic to the VIP card significantly improves networking performance. Because you can install multiple VIP cards in a router, VLAN routing capacity is increased linearly according to the number of installed VIP cards.

XNS Routing over ISL Virtual LANs

XNS can now be routed over virtual LAN (VLAN) subinterfaces using the ISL VLAN encapsulation protocol. The XNS Routing over ISL Virtual LANs feature provides full-feature Cisco IOS software XNS support on a per-VLAN basis and provides for standard XNS capabilities to be configured on VLANs.

TERMINAL SERVICES:

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 configures a virtual access interface; when the user is done, the virtual access interface is torn down, and the resources are freed for other dial-in 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, 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, it allows customized configurations to be predefined and then applied dynamically when the specific need arises.
- For scalability, it allows interface configuration to be separated from physical interfaces. Virtual interfaces can share characteristics, regardless of the specific type of interface the user called on.
- For consistency and configuration ease, it allows the same predefined template to be used for all users dialing in for a specific application.
- For efficient router operation, it frees the virtual access interface memory for another dial-in use when a user call ends.

Virtual Templates for Protocol Translation

Using Cisco IOS Release 11.3, you can simplify the process of configuring protocol translation to tunnel PPP or SLIP across X.25, TCP, and LAT networks. Release 11.3 provides 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 ps.
- 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 with the virtual interface template. All attributes of the virtual interface template are cloned onto the virtual access interface when a call comes in.

WAN OPTIMIZATION:

ATM MIB Enhancements

The Cisco AAL5 MIB adds a proprietary extension to the standard ATM MIB (RFC 1695) to provide per-VC statistic counters that are currently displayed in response to the Cisco IOS command **show atm vc vcd** for ATM interfaces. This MIB extension allows SNMP network management system applications to query the same variables (SNMP objects) as those that can be gathered from the Cisco IOS command-line interface.

PAD Enhancements

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

- PAD calls can be made to destinations that are not reachable over physical X.25 interfaces, but that are reachable over TCP tunnels. A Cisco router with only an Ethernet interface can now 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.

PAD Subaddressing

You can use this feature to append a specified value to an X.121 calling address when that address is not sufficient to identify the source of a call. You can use PAD subaddressing to create unique X.121 calling addresses by including either a physical port number or a value specified for a line as a subaddress to the X.121 calling address.

PAD subaddressing enables an X.25 host application to uniquely identify the source of an X.121 call. For example, in some bank security-alarm applications, the central alarm host identifies the physical location of the alarm units from subaddressing information contained in the Call Request packet.

WAN SERVICES:

Bandwidth Allocation Control Protocol

The Bandwidth Allocation Control Protocol (BACP) described in RFC 2125 provides Multilink PPP peers with the ability to govern link utilization. After peers have successfully negotiated BACP, they can use the Bandwidth Allocation Protocol (BAP), a subset of BACP, to negotiate bandwidth allocation. BAP provides a set of rules governing dynamic bandwidth allocation through call control, a defined method for adding and removing links from a multilink bundle for Multilink PPP.

The addition of any link to an existing multilink bundle is controlled by a BAP call or callback request message, and the removal of a link can be controlled by a link drop message. BACP is designed to operate in both the virtual interface environment and the dialer interface environment. It can operate over any physical interface that is Multilink-PPP capable and has a dial capability; at initial release, BACP supports ISDN and asynchronous serial interfaces.

BACP provides the following benefits:

- Allows multilink implementations to interoperate by providing call control through the use of link types, speeds, and telephone numbers.
- Controls thrashing caused by links being brought up and removed in a short period of time.
- Ensures that both ends of the link are informed when links are added or removed from a multilink bundle.

Enhanced Local Management Interface

The Enhanced Local Management Interface feature provides an enhancement to the Frame Relay LMI protocol. Enhanced Local Management Interface enables automated exchange of Frame Relay Quality of Service (QoS) parameter information between the Cisco router and the Cisco wide-area switch. Routers can base congestion management and prioritization decisions on known QoS values, such as the Committed Information Rate (CIR), Committed Burst Size (Bc), and Excess Burst Size (Be). The router senses QoS values from the switch and can be configured to use those values in traffic shaping. This enhancement works between Cisco routers and Cisco wide-area switches (Cisco BPX and Cisco IGX platforms).

Frame Relay Enhancements

The Frame Relay enhancements introduced with this feature include:

- Standard-based FRF.9 Frame Relay compression for Cisco routers
- Hardware compression support for FRF.9 with the Compression Service Adapter (CSA)

Frame Relay compression can occur on the CSA board or on the main CPU of the router. FRF.9 is standard-based and therefore provides multivendor compatibility. FRF.9 compression uses higher compression ratios, allowing more data to be compressed for faster transmission.

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**.

Frame Relay Router ForeSight

The ForeSight application is the network traffic control software used in Cisco wide-area switches. The Cisco wide-area Frame Relay switch can extend ForeSight messages over a User-Network Interface (UNI), passing the backward congestion notification for virtual connections. The Router ForeSight feature allows Cisco Frame Relay routers to process and react to ForeSight messages and adjust virtual circuit level traffic shaping in a timely manner.

This feature must be explicitly configured on both the Cisco router and the Cisco wide-area switch. When enabled, the ForeSight application sends a message out at the configured time interval, which can range from 40 to 5000 milliseconds. The time interval between the ForeSight messages is set during configuration of the switch. Refer to the appropriate Cisco wide-area switch documentation for details for configuring this feature.

When a Cisco router receives a ForeSight message indicating that certain Data Link Connection Identifiers (DLCIs) are experiencing congestion, the Cisco router activates its traffic shaping function to slow down the output rate. The router reacts as it would if it detected the congestion by receiving a packet with the backward explicit congestion notification (BECN) bit set.

BECN requires a user packet to be sent in the direction of the congested DLCI to convey the signal, a process that is not predictable and therefore not reliable as a notification mechanism. Timed ForeSight messages guarantee that the router receives notification before congestion becomes a problem. Traffic can be slowed down in the direction of the congested DLCI.

The Frame Relay router ForeSight feature provides an improved mechanism for managing network traffic. It provides these benefits:

- The ability for Cisco routers to react to ForeSight backward congestion notification messages.
- Guaranteed notification of traffic congestion.

ISDN Advice of Charge

The ISDN Advice of Charge (AOC) feature is for ISDN PRI NET5 and ISDN BRI NET3 switch types only. Users can obtain charging information for all calls during the call (AOC-D), at the end of the call (AOC-E), or both to track call costs and to control and possibly reduce tariff charges through the use of the short-hold mode option.

The ISDN AOC feature also supports, for the AOC-D service, an optional, configurable short-hold mode that provides a dynamic idle timeout by measuring the call-charging period, based on the frequency of the AOC-D or the AOC-E message from the network. The short-hold mode idle time does the following:

- Disconnects a call just before the beginning of a new charging period if the call has been idle for at least the configured minimum idle time.
- Maintains the call to the end of the current charging period (past the configured idle timeout) if the time left in the charging period is longer.

Users must have subscribed through their local ISDN network for the ISDN services (AOC-D or AOC-E). No router configuration changes are required to retrieve this call charging information. Call accounting information for AOC-D and AOC-E messages is stored in SNMP MIB objects.

ISDN Caller ID Callback

The ISDN caller ID callback feature allows the initial incoming call from the client to the server to be rejected based on the caller ID message contained in the ISDN setup message and allows a callback to be initiated to the calling destination. This feature is independent of the encapsulation in effect and can be used with various encapsulations, such as PPP, HDLC, Frame Relay, and X.25.

In Cisco IOS Release 11.2, ISDN callback functionality required PPP or Combinet Packet Protocol (CPP) client authentication and client-server callback negotiation to proceed. If authentication and callback negotiations were successful, the callback server had to disconnect the call and then place a return call. Both the initial call and the return call were subject to tolls, and when service providers charge by the minute, even brief calls could be expensive.

Note ISDN caller ID callback conflicts with the dialer callback security feature for the dialer profiles feature for dial-on-demand routing (DDR). If dialer callback security is configured, it takes precedence; ISDN caller ID callback is ignored.

ISDN NFAS

ISDN Non-Facility Associated Signaling (NFAS) allows a single D channel to control multiple PRI interfaces. A backup D channel can also be configured for use when the primary NFAS D channel fails. Use of a single D channel to control multiple PRI interfaces can free the B channel on each interface to carry other traffic. After the controllers are configured, only the NFAS primary D channel must be configured; its configuration is distributed to all the members of the associated NFAS group.

LANE Per-subinterface Debug Messages

You can limit debug messages to those related to a particular subinterface. Some debug commands generate a large amount of output; by restricting output to information on a particular subinterface, you can reduce the number of debug messages generated.

Layer 2 Forwarding—Fast Switching

Cisco routers 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 11.3, leased-line service at 128 kbps via ISDN BRI is provided in Japan. This service combines two B channels into a single pipe.

Note After 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.

Multilink PPP Interleaving and Fair-Queuing Support

Interleaving on Multilink PPP allows large packets to be multilink encapsulated and fragmented into a small enough size to satisfy the delay requirements of real-time traffic; small real-time packets are not multilink encapsulated and are transmitted between fragments of the large packets. The interleaving feature also provides a special transmit queue for the smaller, delay-sensitive packets, enabling them to be transmitted earlier than other flows.

Weighted fair-queuing on Multilink PPP works at the packet level, not at the level of multilink fragments. Thus, if a small real-time packet gets queued behind a larger best-effort packet and no special queue has been reserved for real-time packets, the small packet is scheduled for transmission only after all the fragments of the larger packet are scheduled for transmission.

Weighted fair-queuing is supported on all interfaces that support Multilink PPP, including Multilink PPP virtual access interfaces and virtual interface templates. Weighted fair-queuing is enabled by default.

Fair-queuing on Multilink PPP overcomes a prior restriction. Previously, fair-queuing was not allowed on virtual access interfaces and virtual interface templates. Interleaving provides the delay bounds for delay-sensitive voice packets on a slow link that is used for other best-effort traffic.

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 Cisco wide-area network equipment through a leased-line connection.

A logical interface known as a virtual access interface associates each PPP connection to an ATM permanent virtual connection (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. After 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 wide-area ATM switches to access WANs or public ATM networks, such as organizations with many remote branch offices requiring access to high-density corporate headquarters.

Telnet Extensions for Dialout

The Telnet Extensions for Dialout feature is the network access server component of the Cisco DialOut Utility, used by local users to send faxes or connect to services outside the LAN by using modems attached (or internal) to a network access server. This feature extends the functionality of Telnet because users can control the activity of these modems from their desktop computers, using standard communications software. Because the Telnet Extensions for Dialout feature works with the client/desktop Cisco DialOut Utility, it is not a standalone feature. It enables the network access server to interface with the client/desktop component of the Cisco DialOut Utility. The client/desktop component of Cisco DialOut Utility must be installed on the client workstation before this feature can be used.

Telnet extensions allow the communications software running on the desktop computer of a client to control modem settings such as baud rate, parity, bit size, and stop bits. In addition, these extensions allow the network access server to return Carrier Detect signals to the communications software so that the software can determine when to start dialing a particular number.

The Telnet Extensions for Dialout feature uses reverse Telnet to access modems attached to the network access server. To enable this feature, you only need to configure the access server or router for reverse Telnet and configure the appropriate lines to both send and receive calls.

VPDN Tunnel Lookup Based on Dialed Number Information

The network service provider can select a specific VPDN tunnel for outgoing calls from a dial-in user by using the dialed number information service (DNIS) information provided on ISDN lines. The ability to select a tunnel based on DNIS provides additional flexibility to network service providers who offer VPDN services and to the corporations that use the services. Instead of having to use only the domain name for tunnel selection, tunnel selection can be based on the dialed number.

With this feature, a corporation that might have only one domain name can provide multiple, specific phone numbers for dialing into the network access server at the service provider point of presence. The service provider can select the tunnel to the appropriate services or portion of the corporate network based on the dialed number.

X.25 Enhancements

The Cisco X.25 implementation has 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 of X.25 services:
 - X.25
 - X.25 over TCP (XOT)
 - X.25 over LANs (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 supporting an X.25 service:
 - Link Access Procedure, Balanced (LAPB)
 - Link Access Procedure, D channel (LAPD)
 - Logical Link Control, Type 2 (LLC2)

X.25 Over 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 use up to 9.6 kbps.

You can 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 continues 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 recognizes 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.25 Switching Between PVCs and SVCs

This feature allows X.25 switching between permanent virtual connections (PVCs) and switched virtual connections (SVCs). Previously, X.25 switching was permitted only between circuits of the same type. Traffic that entered the router over a SVC could be forwarded only to another SVC. Likewise, traffic that entered the router over a PVC could be forwarded only to another PVC. This feature allows switching between the two circuit types.

X.28 Emulation

The Cisco IOS software provides an X.28 user emulation mode through which you can 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 packets of a device 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. The X.28 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. The Cisco X.28 PAD implementation 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 offers the flexibility to either use the X.28 interface directly or over a Cisco IOS application service such as protocol translation. The protocol translation vty asynchronous application provides bidirectional access to an X.25 application with the PAD service or protocols, such as Digital Equipment Corporation (DEC), local-area transport (LAT), and TCP.

Installation Notes

If you are upgrading to Cisco IOS Release 11.3 from an earlier Cisco IOS software release, you should save your current configuration file before configuring your access server with the Cisco IOS Release 11.3 T software. An unrecoverable error could occur during download or configuration.

Before downloading a software upgrade, read Product Bulletin #703, *Cisco IOS Software Release Upgrade Paths and Packaging Simplification*. The information in this bulletin supersedes all previous instructions. This bulletin is in the following location on CCO. Click **Service & Support**.

Near the bottom of the web page go to **Product Bulletins**, scroll down to the **Software** section, and then click **Cisco IOS Software Release 11.3 Upgrade Paths No. 703** under the heading **Cisco IOS 11.3**.

Important Notes

The following sections contain important notes about Cisco IOS Release 11.3 and can apply to the Cisco 2500 series.

Image Deferral, Cisco IOS Release 11.3(8)T

Cisco IOS Release 11.3(8)T was deferred to Release 11.3(8)T1 on all software images to incorporate corrections to the following caveats:

- CSCdk86294—The D channel is always in the shutdown state when non-facility associated signalling is configured.
- CSCdk80809—Enhanced Interior Gateway Routing Protocol (EIGRP) has difficulty converging on certain routes.

For more information on these caveats, refer to Bug Navigator II. Bug Navigator II is available at <http://www.cisco.com/support/bugtools>. On CCO, click this path:

Service & Support/ Online Technical Support/ Software Bug Toolkit/ Bug Navigator II

Enabling IPX Routing

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

Forwarding of Locally Sourced AppleTalk Packets

The Cisco 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 publication *Inside AppleTalk*. 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.

Using Source-Route Transparent Bridging and Source-Route Bridging on Cisco 2500 Routers

Certain products containing the Texas Instruments TMS380C26 Token Ring controller do not support Source-Route Transparent Bridging (SRT). SRT is the concurrent operation of Source-Route Bridging (SRB) and transparent bridging on the same interface.

The affected products, shipped between March 30, 1994, and January 16, 1995, are the Cisco 2502, Cisco 2504, Cisco 2510, Cisco 2512, Cisco 2513, and Cisco 2515. Units shipped before March 30, 1994, or after January 16, 1995, are not affected. They use the Texas Instruments TMS380C16 Token Ring controller, which supports SRT.

SRT support is necessary in two situations. In one, Token Ring networks are configured to SRB protocols such as SNA and NetBIOS, and they transparently bridge other protocols, such as IPX. In the other situation, SNA or NetBIOS uses SRB, and Windows NT is configured to use NetBIOS over IP. Certain other configuration alternatives do not require SRT (contact the Technical Assistance Center for more information).

As of Release 10.3(1), SRB in the following Cisco IOS feature sets is no longer supported: IP, IP/IPX, and Desktop. To use SRB, you need one of the following feature sets: IP/IBM base, IP/IPX/IBM base, IP/IPX/IBM/APPN, Desktop/IBM base, Enterprise, or Enterprise/APPN. In most non-IBM Token Ring environments, the multiring feature in IP, IP/IPX, and Desktop eliminates the need for IP/IBM base, IP/IPX/IBM base, IP/IPX/IBM/APPN, Desktop/IBM base, Enterprise, or Enterprise/APPN.

Removed Bridging Command

As of Release 11.3(2)T, the command **bridge group multicast-source** is no longer available. This command was removed to comply with the source-route-transparent (SRT) bridging implementation.

Missing Source-Route Bridging Commands

Due to a production problem, many source-route bridging commands were omitted from the printed version of the *Cisco IOS Software Command Summary* (78-4746-01). For complete documentation of all source-route bridging commands, refer to the *Bridging and IBM Networking Command Reference* (78-4743-01). You can also obtain the most current documentation on the Documentation CD-ROM or Cisco Connection Online (CCO).

New TACACS+ Attribute-Value (AV) Pair

A new authorization feature was added in Release 11.3(1) that allows for separate configuration and authorization of Multilink PPP. This can cause MLP authorization to fail in TACACS+ servers that do not include the relevant authorization permissions in the configuration. For TACACS+, the following attribute-value (AV) pair should be added for all users who are allowed to negotiate Multilink PPP:

```
service = ppp protocol = multilink {
```

Configuring VPDN

For information about configuring VPDN and to access the VPDN command reference, see the Cisco Documentation CD-ROM. Using a web browser, go to: http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/dial_c/dcp9/dcvpdn.htm.

This URL is subject to change without notice. If it changes, point your web browser to **Service & Support/ Documentation Home Page/ Cisco IOS Software Configuration/ Cisco IOS Release 11.3/ Configuration Guides, Command References/ Dial Solutions Configuration Guide/ Virtual Private Dialup Networks/ Configuring Virtual Private Dialup Networks**.

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 11.3 T, see *Caveats for Cisco IOS Release 11.3 T* on CCO and the Documentation CD-ROM.

All caveats in Release 11.3 are also in Release 11.3 T.

For information on caveats in Cisco IOS Release 11.3, see the “Important Notes and Caveats for Release 11.3” section in *Cross-Platform Release Notes for Cisco IOS Release 11.3* on CCO and the Documentation CD-ROM. These release notes list severity 1 and 2 caveats affecting all maintenance releases.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Service & Support: Online Technical Support: Software Bug Toolkit**, or at <http://www.cisco.com/support/bugtools>.

Related Documentation

The following sections describe the documentation available for the Cisco 2500 series. 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 CCO and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 51
- Platform-Specific Documents, page 52
- Feature Modules, page 53
- Cisco IOS Software Documentation Set, page 53

Release-Specific Documents

The following documents are specific to Release 11.3 and are located on CCO and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 11.3*

On CCO at:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3

- Product bulletins, field notices, and other release-specific documents on CCO at:

Service & Support: Technical Documents

- *Caveats for Cisco IOS Release 11.3 T*

As a supplement to the caveats listed in the “Caveats” section on page 51, see *Caveats for Cisco IOS Release 11.3 T*, which contains caveats applicable to all platforms for all maintenance releases of Release 11.3 T.

On CCO at:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Product Specific Release Notes for Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Product Specific Release Notes for Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Service & Support: Online Technical Support: Software Bug Toolkit**, or at <http://www.cisco.com/support/bugtools>.

Platform-Specific Documents

These documents are available for the Cisco 2500 series on CCO and the Documentation CD-ROM:

- *Cisco 2524 and Cisco 2525 Public Network Certification*
- *Installing WAN Modules in the Cisco 2524 and Cisco 2525 Routers*
- *Cisco 2524 and Cisco 2525 Router User Guide*
- Release Notes for Cisco 2500 Series Routers
- *Redundant Power Systems*
- *Regulatory and Safety Information for the Cisco 2500 Series*
- Supporting Documentation for the Cisco 2500 Series

On CCO at:

Service & Support: Documentation Home Page: Access Servers and Access Routers: Modular Access Routers or Fixed Configuration Access Routers: Cisco 2500 Series Routers

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers or Fixed Configuration Access Routers: Cisco 2500 Series Routers

Feature Modules

Feature modules describe new features supported by Release 11.3 T 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 CCO at:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3 [AA, NA, T, XA] New Features

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3 [AA, NA, T, XA] New Features

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

You can reach these documents on CCO at:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS Release 11.3 Configuration Guides, Command References: Configuration Guide Master Index or Command Reference Master Index

Release 11.3 Documentation Set

Table 1 describes the contents of the Cisco IOS Release 11.3 software documentation set, which is available in electronic form and also in printed form upon request.

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

You can reach the Cisco IOS documentation set from CCO at:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3

Related Documentation

You can reach the Cisco IOS documentation set on the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3

Table 1 Cisco IOS Software Release 11.3 Documentation Set

Books	Chapter Topics
<ul style="list-style-type: none">• <i>Configuration Fundamentals Configuration Guide</i>• <i>Configuration Fundamentals Command Reference</i>	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management Interface Configuration System Management
<ul style="list-style-type: none">• <i>Network Protocols Configuration Guide, Part 1</i>• <i>Network Protocols Command Reference, Part 1</i>	IP Addressing IP Services IP Routing Protocols
<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>Wide-Area Networking Configuration Guide</i>• <i>Wide-Area Networking Command Reference</i>	Wide-Area Networking Overview ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none">• <i>Security Configuration Guide</i>• <i>Security Command Reference</i>	AAA Security Services Security Server Protocols Traffic Filtering Network Data Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options
<ul style="list-style-type: none">• <i>Dial Solutions Configuration Guide</i>• <i>Dial Solutions Command Reference</i>	Business Applications and Scenarios Dial-In Port Setup Dial-In Terminal Services and Remote Note Configuration Dial Authentication Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Dial-Related Addressing Services (NAT/Easy IP) Cost-Control Solutions Network Traffic over ISDN Channels X.25 over ISDN Virtual Private Dialup Networks
<ul style="list-style-type: none">• <i>Cisco IOS Switching Services Configuration Guide</i>• <i>Cisco IOS Switching Services Command Reference</i>	Switching Paths for IP Networks NetFlow Switching Virtual LAN (VLAN) Routing LAN Emulation

Table 1 Cisco IOS Software Release 11.3 Documentation Set (continued)

Books	Chapter Topics
<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>Configuration Guide Master Index</i> • <i>Command Reference Master Index</i> 	

Note The *Cisco Management Information Base (MIB) User Quick Reference* publication is no longer being published. For the latest list of MIBs supported by Cisco, see the Cisco Network Management Toolkit on Cisco Connection Online. On CCO, go to **Service & Support**, select **Software Center**, and click **Network Management Products**. Next, select **Cisco Network Management Toolkit**, and click **Cisco MIBs**.

Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in “Service and Support” of *Cisco Information Packet* shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems’ primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a CCO login account, you can access the following URL, which contains links and tips on configuring your Cisco products:

http://www.cisco.com/kobayashi/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path: **Products & Technologies: Products: Technical Tips.**

The following sections are provided from the Technical Tips page:

- Configuration Cookbooks—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Describes the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Provides technical tips related to specific hardware platforms.
- Hot Tips—Describes popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.
- Internetworking Features—Lists tips on using and deploying Cisco IOS software features and services.
- Sample Configurations—Provides actual configuration examples that are complete with topology and annotations.
- Software Products—Contains Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Applications and Software, Network Management, Network Protection Software Tips, and WAN Switching Products and Software.
- Special Collections—Lists other helpful documents, including Case Studies, References & Request for Comments (RFCs), and Security Advisories.

Cisco Connection Online

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

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

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

You can access CCO in the following ways:

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

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

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

Documentation CD-ROM

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, the Cisco Certified Internetwork Expert logo, CiscoLink, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Technologies logo, ConnectWay, ControlStream, Fast Step, FireRunner, GigaStack, IGX, JumpStart, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, Packet, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, ServiceWay, SlideCast, SMARTnet, StreamView, The Cell, TrafficDirector, TransPath, ViewRunner, VirtualStream, VisionWay, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks™; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks(SM); and Asist, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks® of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. (9905R)

Copyright © 1999, Cisco Systems, Inc.
All rights reserved.

