

Cisco IOS Software Release 11.3

New Features

This product bulletin describes new features introduced in Cisco IOS™ Software Release 11.3.

Release 11.3 Overview

Cisco IOS software Release 11.3 is a major release with a limited life.

Included in this release are the following:

- All Release 11.2 functionality (refer to *Cisco IOS software Release 11.2 New Features* product bulletin #487 at the following URL: http://www.cisco.com/warp/customer/cc/cisco/mkt/ios/rel/112/prodlit/487_pp.htm)
- All platform support introduced on the 11.2P early deployment release
- All features planned for the 11.2F early deployment release are outlined in this document.

Cisco IOS software Release 11.3 will receive regular maintenance like all other major releases. However, Release 11.3 will be a limited life release, with at least one year of regular maintenance. Since it is a limited life release, it will not be taken to the general deployment (GD) milestone. Cisco IOS software Release 11.3 is recommended for specific environments where its unique capabilities are required. Moreover, because Release 11.3 will not be supported for a full two years, it should only be used in environments in which it is acceptable to move to a newer major release for maintenance updates.

There are two FCS dates for Cisco IOS software Release 11.3(1):

- Electronic transfer availability from CCO—12/22/97
- Media-based shipments—12/29/97

Cisco IOS Release 11.3(1) software product orderability begins on 12/22/97.

Cisco strongly recommends that customers select and deploy “general deployment” release versions of software for fundamental network infrastructures. A software release reaches the “general deployment” milestone when Cisco feels that it is suitable for general deployment anywhere in a customer’s network that the features and functionality of the release are required. Compared with FCS releases, these releases contain fewer unknowns and are more time-proven versions of software that can be deployed broadly across a production network. Software at FCS is focused on delivery of new features and has greater unknowns. As such, it should only be used for initial “point” use of new features. Any early release software should always be used in a test network before being fully deployed in a production network.

Please refer to product bulletin #704, *Cisco IOS Software Release 11.3(1) Ordering Procedures and Platform Hardware Support* for an overview of the release offerings, including summaries of platforms and feature sets supported. *Cisco IOS Software Release 11.3 Ordering Procedures and Hardware Platform Support* product bulletin #704 will be available upon CCO FCS of the Cisco IOS 11.3 software Release scheduled for 12/22/97.

For upgrade paths, refer to product bulletin #703, *Cisco IOS Software Release 11.3 Upgrade Paths and Packaging Simplification*.

Additional Sources

For additional information on Cisco IOS software Release 11.3, please refer to the following sources:

- *Cisco IOS Software Release 11.3 Upgrade Paths and Packaging Simplification*
- *RFCs and Other Standards Supported in Cisco IOS Software Release 11.3(1)*
- *Cisco IOS Software Feature Matrices, Releases 10.3 through 11.3*
- *Cisco IOS Software Release 11.3(1) Ordering Procedures and Platform Hardware Support*
- *Cisco IOS Software Release 11.3 Release Notes*

Security

Reflexive Access Lists

Description: Reflexive access lists allow the packet filter to “remember” what it has seen, and then allow only the corresponding response packets back in through the filtering mechanism. To be counted as a response, the incoming packet must be from the host and port to which the outbound packet was sent, and must be directed to the host and port that sent the outbound packet. The router essentially modifies the filtering rules on the fly to accommodate these returning packets.

Benefits: Reflexive access lists can be included in a router-based firewall defense, as they provide greater control over which packets enter your network.

Considerations/Platforms: Reflexive access lists can be defined with extended named IP access lists only. Reflexive access lists cannot be used with numbered or standard named IP access lists or with other protocol access lists. This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco 5200 series, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Jocelyne Okrent

Vendor-Proprietary RADIUS Attributes

Description: 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.

Benefits: Some vendor-proprietary implementations of RADIUS let the administrator define static routes and IP pool definitions on the RADIUS server, instead of on each individual 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 startup time, freeing up the user from having to configure such information on each individual network access server.

Considerations/Platforms: The following platforms support vendor-proprietary attributes for RADIUS: Cisco 1003/4, Cisco 1005 series, Cisco 2500, Cisco 25FX, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Roger Farnsworth

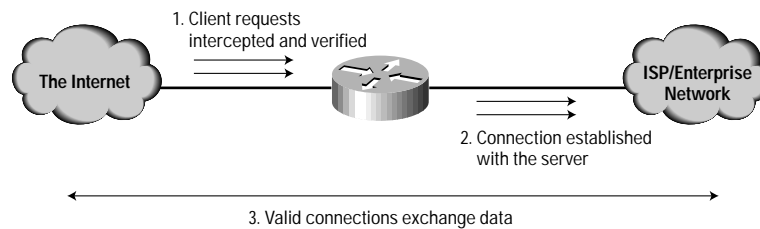
TCP Intercept

Description: Cisco IOS TCP Intercept capability is designed to combat the denial-of-service (DoS) attack known as synchronization (SYN) Flooding. System hackers who carry out this type of network attack can potentially prevent legitimate users from connecting to a Web site, accessing e-mail or using FTP services.

This DoS attack essentially involves flooding a server with a barrage of hand-crafted requests for connection. However, since these messages have invalid return addresses, the connections can never be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests. While this scheme does not represent a networking

security compromise in itself, it can paralyze on-line services. This mechanism exploits the connection-oriented TCP protocol (which is used to carry the vast majority of Internet applications) and because the attack is an abuse of the defined standard for TCP, this vulnerability exists to some degree in all implementations. TCP Intercept is designed to prevent a SYN Flooding DoS attack by tracking, optionally intercepting and validating TCP connection requests.

Figure 1 TCP Intercept



Integrated within the Cisco IOS software, it need only be deployed at the key points that connect to external networks and once a TCP connection has been fully established, the session is Fast Switched.

Benefits: This feature is an effective response to the SYN Flooding denial-of-service type attack and represents Cisco's on-going commitment to secure internetworking.

Platforms/Considerations: This functionality is available in Enterprise and Service Provider IOS images. It is supported on these platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Manager: Jocelyne Okrent

Encrypted Kerberized Telnet

Description: Encrypted Kerberized Telnet enables a router to initiate or receive an encrypted Telnet session. Previously, all Telnet session traffic could be transmitted only 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.

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

Benefits: This feature allows network managers to securely manage remote devices. Without this feature, all Telnet sessions with the router are in cleartext and subject to eavesdropping. This feature also allows integration of Cisco IOS software into an existing Kerberos system for authentication purposes.

Considerations/Platforms: This feature is available only if you have a 56-bit encryption image. 56-bit DES encryption is subject to U.S. government export control regulations.

Requires a customer-supplied Kerberos Key Distribution Center (KDC) and the use of a kerberized version of Telnet. This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, and the Cisco 7500 series.

Product Marketing Contact: Terry Bernstein

Tunneling of Asynchronous Security Protocols

Description: Cisco's implementation of the BSTUN feature encapsulates Binary Synchronous Communications protocol (Bisync), Adplex, ADT Security Systems, Inc., Diebold, and asynchronous generic traffic for transfer over router links. Cisco's tunneling of the asynchronous security protocols feature (ASP) enables your Cisco 2500, Cisco 4000, or Cisco 4500, 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.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 1600, Cisco 2500, Cisco 25FX, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, and the Cisco 7500 series.

Product Marketing Contact: Roger Farnsworth, Paul Sikorski

HTTP Security

Description: All Cisco routers and access servers running Cisco IOS Release 11.0(6) or later have a Hypertext Transfer Protocol (HTTP) server, which is an embedded subcomponent of the Cisco IOS software. The HTTP server allows users with a privilege level of 15 to issue Cisco IOS commands from a predefined home page using a Web browser. In previous releases, Cisco IOS software allowed only users with a privilege level of 15 to access the Cisco Web browser interface. With release 11.3, the HTTP security feature enables users with a privilege level below 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 11.3 software uses the enable password method to authenticate a user at privilege level 15. In this release, system administrators can now specify enable; local; Terminal Access Controller Access Control System (TACACS); or AAA user authentication. Because the HTTP Security feature enables network administrators to provide HTTP server access to users with a privilege level of less than 15, the Cisco Web browser interface can mirror the functionality of the CLI.

Benefits: Simplifies Web-based and remote configuration and control of Cisco IOS features.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 1003/4, Cisco 1005 series, Cisco 1600, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Tom Tinor

IPX SAP-after-RIP

Description: This feature links Service Advertising Protocol (SAP) updates to Routing Information Protocol (RIP) updates so that SAP broadcast and unicast updates automatically occur immediately after the completion of the corresponding RIP update. It ensures that no service information 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 at the same frequency as RIP updates.


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

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

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

Benefits:

- 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 because there is no route to the service. This can be especially useful on WAN circuits where the update intervals have been greatly increased to reduce the overall level of periodic update traffic on the link.



Considerations/Platforms: This feature is supported on the following platforms: Cisco 1000, Cisco 1005, Cisco 1600, Cisco 2500, Cisco 25FX, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Roger Farnsworth

AppleTalk Access List Enhancements

Description: AppleTalk access list enhancements add 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 Name Binding Protocol (NBP) access lists, could be applied to outbound interfaces only. With release 11.3, 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 release 11.3, 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

Benefits: AppleTalk access list enhancements offer many specific benefits. First, Access list fast switching improves the performance of AppleTalk traffic when access lists are defined on an interface. Also, Access lists for inbound interfaces provide greater flexibility in isolating network traffic. For example, using inbound access lists makes it very easy to implement firewalls by filtering all traffic coming in to the network from remote nodes. Furthermore, NBP access lists for outbound interfaces provide greater flexibility in creating access lists and designing a routed network. Finally, NBP filtering based on packet type broadens the choices in creating access lists for AppleTalk networks using NBP.

Product Marketing Contact: Peter Long

EIGRP Route Authentication

Description: This IOS 11.3 feature adds a keyed MD5 digest to all EIGRP routing protocol packets thus providing route authentication. Timed Key-chains are used in order to provide smooth transition during key rollover.

Benefits: Deploying route authentication enhances security and ensure the integrity of the information exchanged between topological peers.

Platforms/Considerations: This configurable feature is available across all IOS 11.3 images supporting the EIGRP protocol. This feature is supported on the following platforms: Cisco 1003/4, Cisco 1005, Cisco 1600, Cisco 2500, Cisco 25FX, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Manager: Martin McNealis

DECnet Accounting

Description: DECnet accounting allows you to collect 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.

Benefits: Enhanced management using existing networking hardware in tandem with Cisco IOS software.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Roger Farnsworth

Double Authentication

Description: Double authentication provides additional authentication for PPP sessions. Previously, PPP session authentication was limited to CHAP (or PAP). With double authentication, you essentially require remote users to pass a second stage of user authentication—after CHAP or PAP authentication—before they can gain network access. If you configure your local host (NAS or router) for double authentication, remote users are required to complete a second stage of authentication to gain their assigned user network privileges. This second (“double”) authentication requires a password that is known to the user but not stored on the user’s remote host. Therefore, the second authentication is specific to a user, not to a host.

Benefits: Provides an additional level of security that is effective even if the remote host is stolen.

Considerations/Platforms: This feature is supported on the following Cisco platforms: Cisco 1003/4, Cisco 1005, Cisco 1600, Cisco 2500, Cisco 25FX, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Roger Farnsworth

Switching

Fast Switched Policy Routing

Description: In today’s high performance networks, organizations need the freedom to implement packet forwarding and routing according to their own defined policies in a way that goes beyond traditional routing protocol concerns. Where administrative issues, quality-of-service (QoS) requirements or virtual private network (VPN) topologies dictate that traffic should be routed through specific paths, policy routing, introduced in Cisco IOS Software Release 11.0, can provide the solution. By using policy routing, customers can implement policies that selectively cause packets to take different paths.

Policy routing also provides a mechanism to mark packets so that certain kinds of traffic receive differentiated, preferential service when used in combination with queuing and congestion management techniques enabled through the Cisco IOS software. These techniques provide an extremely powerful, simple, and flexible tool enabling network managers to implement policy within their networks. Policy routing allows the Cisco IOS to classify traffic based on extended access lists. Customers are able to implement traffic policies based on source and/or destination IP addresses, TCP port numbers, and/or packet lengths. Cisco IOS release 11.3 enhances Policy Routing support by adding Fast Switching support.

Benefits: The benefits that can be achieved by implementing policy-based routing in the networks include:

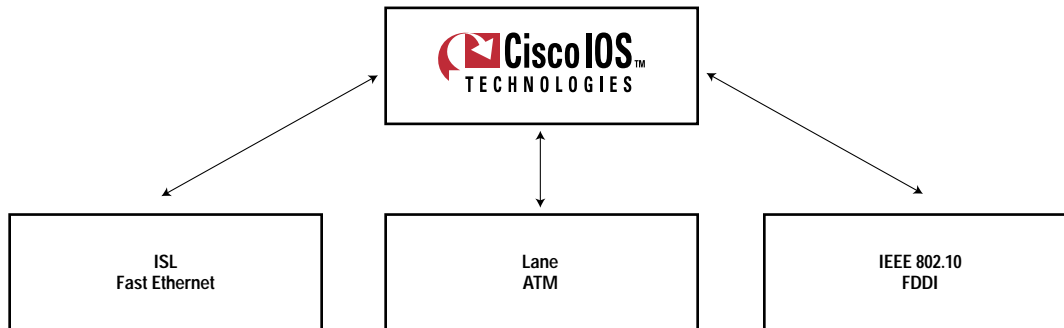
- *Source-Based Transit Provider Selection:* Internet Service Providers (ISPs) and other organizations can use policy-based routing to route traffic originating from different sets of users through different Internet connections across the policy routers.
- *Quality of Service (QoS):* Organizations can provide QoS to differentiated traffic by setting the precedence or type of service (TOS) values in the IP packet headers at the periphery of the network and leveraging queuing mechanisms to prioritize traffic in the core or backbone of the network.
- *Cost Savings:* Organizations can achieve cost savings by distributing interactive and batch traffic among low-bandwidth, low-cost permanent paths and high-bandwidth, high-cost, switched paths.
- *Load Sharing:* In addition to the dynamic load-sharing capabilities offered by destination-based routing that the Cisco IOS software has always supported, network managers can now implement policies to distribute traffic among multiple paths based on the traffic characteristics. Customers can specify routing policies and implement these policies in their networks.
- *Platforms/Considerations:* This functionality is available on the following platforms: Cisco 1600 series, Cisco 2500, Cisco 3600, Cisco 4x00, Cisco AS5x00, C5x00 with RSM, Cisco 7200, and the Cisco 7500 series.

Product Marketing Manager: Martin McNealis

vLAN Routing

Description: By definition vLANs perform network partitioning and traffic separation at Layer 2. Cisco Systems offers the industry's most comprehensive vLAN capabilities across its strategic product family and supports multiple vLAN protocols optimized for different media - Cisco's Inter Switch Link (ISL) for 100BaseT Fast Ethernet (Gigabit Ethernet planned), the IEEE 802.10 Standard for FDDI backbones and via LAN Emulation over ATM:

Figure 2 vLAN Routing



Additionally once the IEEE's 802.1Q Virtual LANs Standard is ratified, the Cisco IOS will offer full support of this Standard.

Communications between different virtual LANs requires a Layer 3 routing or a Layer 2 translation function. The Cisco IOS introduced vLAN routing for IP and Novell IPX as well as translation between vLAN trunking and non-vLAN interfaces in software release 11.1. Release 11.3 extends vLAN support to include full inter-vLAN routing for Appletalk, DECnet, Vines and XNS over ISL, Appletalk over IEEE 802.10 vLANs, and configurable IPX encapsulation support. A switched vLAN domain corresponds to a routed subnet/network number and is represented in the Cisco IOS via a vLAN subinterface. Standard routing attributes such as network advertisements, secondary addresses, helper addresses etc. are applicable and vLAN routing/translation is Fast Switched.

Benefits: As switched networks evolve to distributed virtual LANs, the feature-rich Cisco IOS is able to provide key inter-vLAN communications for the widest range of protocols and therefore allow the network infrastructure to scale.

Considerations/Platforms: Virtual LAN Routing functionality is available across any IOS platform capable of supporting Fast Ethernet, ATM or FDDI trunking media. On C36xx and C4xxx routers this functionality is contained within the IOS "Plus" images.

Product Marketing Manager: Martin McNealis

Source-Route Bridging (SRB) over FDDI on Cisco 4000-M, 4500-M, and 4700-M Routers

Description: This feature extends support for SRB on an FDDI interface to the Cisco 4000-M, Cisco 4500-M, and Cisco 4700-M routers.

Benefits: Improves performance and simplifies network design by allowing DLSw+ end stations to connect to a DLSw+ router over an FDDI backbone ring.

Considerations/Platforms: This feature is supported on the following platforms: The Cisco 4000-M, Cisco 4500-M, and Cisco 4700-M routers equipped with FDDI interfaces.

Product Marketing Contact: Paul Sikorski

SRB over Frame Relay

Description: Cisco IOS software encapsulates SRB traffic using RFC 1490 Bridged 802.5 encapsulation to provide SRB-over-Frame-Relay functionality. This functionality can be used between Cisco routers or between a Cisco router and RFC 1490-compliant FRADs or routers.

Benefits: Improves scalability in environments that have installed FRADs but lack a scalable central-site solution.

Product Marketing Contact: Paul Sikorski

VIP Distributed Switching Support for IP Encapsulated in ISL

Description: 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.

Benefits: VIP distributed switching offloads switching of ISL virtual LAN (VLAN) IP traffic to the VIP card, easing the burden on the main CPU. As a result, offloading ISL traffic to the VIP card significantly improves networking performance. Because you can install multiple VIP cards in a router, VLAN routing capacity increases linearly according to the number of installed VIP cards.

Considerations/Platforms: This feature is supported on the Cisco 7500 series platform

Product Marketing Contact: Tom Russell

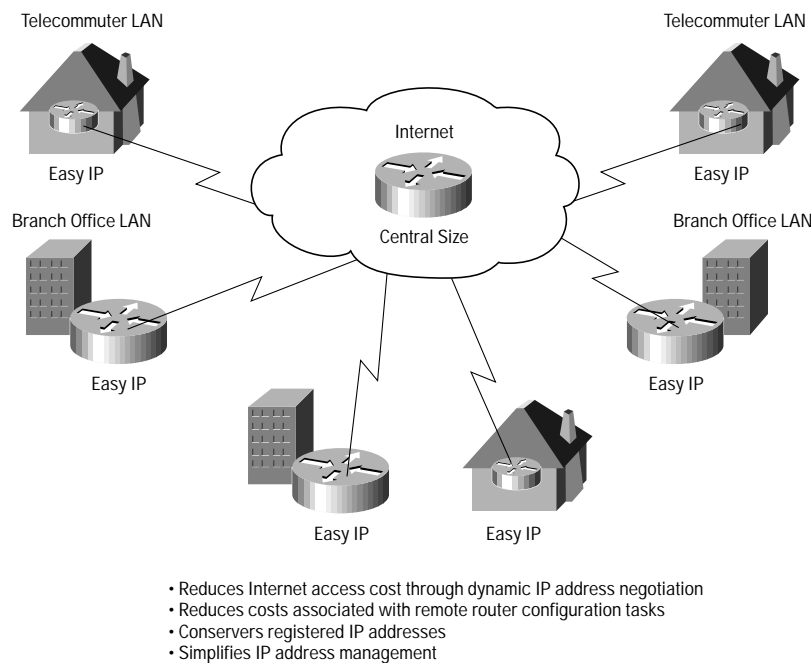
Connectivity

Easy IP (Phase 1)

Description: A combination of Network Address Translation ([NAT]-described in RFC 1631) and PPP/IP Control Protocol (IPCP) (defined in RFC 1332), Cisco IOS Easy IP enables a Cisco router to automatically negotiate its own registered IP address from a central server via the PPP/IPCP, and enables all remote hosts to access the global Internet using a single registered IP address. Within the context of Cisco IOS Easy IP, port and address translation (PAT) is used to translate all internal private addresses to a single outside registered IP address.

Cisco IOS Easy IP enables network administrators to allocate a single registered IP address to each remote LAN such that any host on the LAN can access public network infrastructure.

Figure 3 Cisco IOS Easy IP



Benefits: Cisco IOS Easy IP dramatically lowers Internet access costs for remote networks, eases IP address management, simplifies remote small office/home office (SOHO) access to the Internet, and provides remote network privacy. Using dynamic IP address negotiation (PPP/IPCP) at each remote site substantially reduces Internet access costs. Because Cisco IOS Easy IP utilizes existing port-level NAT functionality within Cisco IOS software, IP addresses on the remote LAN are invisible to the Internet, making it inherently more secure. As seen by the external network, the source IP address of all traffic from the remote LAN is the single registered IP address of the Easy IP router's WAN interface.



Cisco IOS Easy IP enables ISPs to maximize their customer bases while minimizing the required number of registered IP addresses. This feature simplifies and reduces costs associated with global IP address management tasks for ISPs and their customers. Because only a single registered IP address is required to support all users on an entire remote LAN, customers and ISPs can use their registered IP addresses more efficiently.

Considerations/Platforms: Cisco IOS Easy IP is supported on all platforms that support Cisco IOS NAT. Specifically, it is supported on the following platforms: Cisco 1003/4, Cisco 1005, Cisco 1600, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series. Cisco IOS Easy IP Phase 1, which includes NAT and PPP/PCP negotiation capabilities, assumes that all remote LAN hosts have statically configured IP addresses. Cisco IOS Easy IP Phase 2, which adds Dynamic Host Configuration Protocol ([DHCP]-RFC 1541) server capabilities, enables the Cisco IOS Easy IP router to dynamically allocate IP addresses to the remote LAN hosts via DHCP. Cisco IOS Easy IP Phase 2 will be available in Q2 CY, 98.

Product Marketing Contact: Kevin Delgadillo

Leased Line ISDN at 128 kbps

Description: In Cisco IOS Release 11.3, leased-line service at 64 kbps via ISDN BRI is provided in Japan and Germany. Configuration of this feature is described in the Wide-Area Networking Configuration Guide for Cisco IOS Release 11.2.

With Leased Line ISDN at 128 kbps, 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.

Benefits: You can now leverage economical ISDN service for fast, digital connections to remote sites.

Considerations/Platforms: This feature is supported on these platforms: Cisco 1003/4, Cisco 1600, Cisco 3600, Cisco 4000, and the Cisco 4500 series.

The Cisco 2500 series does not support this feature because its BRI hardware does not support channel aggregation.

This feature requires the following:

- One or more ISDN BRI hardware interfaces that support channel aggregation.
- Service provider support for ISDN channel aggregation at 128 kbps; currently offered in Japan.

Product Marketing Contact: Anita Freeman

Per-User Configuration

Description:

- The per-user configuration can tie together the following dial-in features:
 - Virtual interface templates, generic interface configuration, and router-specific configuration information stored in the form of a virtual interface template that can be applied (cloned) to a virtual access interface each time any user dials in.
 - AAA per-user security and interface configuration information stored on a separate AAA server and sent by the AAA server to the access server or router in response to authorization requests during the PPP authentication phase; the per-user configuration information can add to or override the generic configuration on a virtual interface.
 - Virtual profiles, which can use either or both of these two sources of information 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.

Benefits:

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

Considerations/Platforms: This feature is supported on all platforms that support Multilink PPP: Cisco 1003/4, Cisco 1005, Cisco 1600 series, Cisco 2500, Cisco 25FX, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Roger Farnsworth



Telnet Extensions for Dialout

Description: The Telnet extensions for dialout feature is the network access server component of the Cisco dialout utility, which enables 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 by enabling users to control the activity of these modems from their desktop computers using standard communications software. Because the Telnet extensions for dialout feature works in conjunction 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 client's desktop computer 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.

Benefits:

- Network access server modem control from a desktop computer
- Significantly reduced equipment and maintenance costs because modem equipment and dialout maintenance are confined to the network access server
- Outbound faxing (requires Class 2 modem)
- Access to bulletin boards and Internet service providers (ISPs) using standard desktop applications
- Works with standard applications such as WinFax Pro, America Online, ProComm, and PCAnywhere
- Compatible with existing operating systems such as Windows 3.1x, Windows 95, and Windows NT 4.0

Considerations/Platforms: This feature is supported on the following platforms: Cisco 2500 Series (2509, 2510, 2512, 2516) and the Cisco AS5200.

Before you enable this feature on your router or access server, you must complete initial router or access server configuration so that the device successfully operates within your Ethernet-based network. In addition, to ensure network security, it is strongly suggested that you implement some sort of security solution, whether local or remote. For information about configuring security, refer to the Cisco IOS Release 11.2 Security Configuration Guide.

Before clients can use this feature, they must install and configure the following components on their desktop computers:

- Cisco dialout utility
- Communication software application, such as WinFax Pro

For information about initial router or access server configuration, refer to the Cisco IOS Release 11.2 Access Services Quick Configuration Guide. For information about Cisco dialout utility configuration, refer to the Cisco DialOut Utility User Guide or the Cisco dialout Utility quick reference cards.

Product Marketing Contact: Anita Freeman

ISDN Advice of Charge

Description: The Integrated Service Digital Network (ISDN) Advice of Charge (AOC) feature is for ISDN Primary Rate Interface (PRI) Network Entity Title 5 (NET5) and ISDN Basic Rate Interface (BRI) NET3 switch types only. This feature allows users to obtain charging information for all calls during the call (AOC-D) or at the end of the call (AOC-E) or both. However, AOC information at call setup is not supported. Users must have subscribed through their local ISDN network to receive the AOC information from the switch. No router configuration changes are required to retrieve this call-charging information.

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 will do the following:

- Disconnect a call just prior to the beginning of a new charging period if the call has been idle for at least the configured minimum idle time

- Maintain 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. Incoming calls are disconnected using the static dialer idle timeout value.

The AOC-D and AOC-E messages are part of the Facility Information Element (FIE) message. Its contents can be verified with the debug q931 command.

Call accounting information from AOC-D and AOC-E messages is stored in Simple Network Management Protocol (SNMP) Management Information Base (MIB) objects.

Benefits: This feature allows users to track call costs and to control and possibly reduce tariff charges through the use of the short-hold mode.

Considerations/Platforms: This feature is supported on all platforms that include ISDN BRI or ISDN PRI: Cisco 1003/4 series, Cisco 1005, Cisco 1600 series, Cisco 2500, Cisco 4000, (Cisco 4000, 4000, 4500, 4500, 4700), Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Users must subscribe to the ISDN AOC service with their local ISDN network.

List of Terms:

- *AOC-D message*—ISDN Advice of Charge information sent during a call. The message is sent periodically by the network to subscribers of AOC during-call services.
- *AOC-E message*—ISDN Advice of Charge information sent at the end of a call. The message is sent periodically by the network to subscribers of AOC end-of-call services.
- *Short-hold mode*—Configurable option for outgoing calls that causes the dialer idle timeout to be at the end of the current charging period, after a specified minimum idle time has elapsed. If the link has been idle less than the specified minimum time, the call remains connected into another charging period.

Product Marketing Contact: Anita Freeman

ISDN Caller ID Callback

Description: 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.

Before Cisco IOS Release 11.3, ISDN callback functionality required Point-to-Point (PPP) or Combinet Packet Protocol (CPP) client authentication and client-server callback negotiation to proceed. If authentication and callback negotiation 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.

This feature is independent of the encapsulation in effect and can be used with various encapsulations, such as PPP, High-Level Data Link Control (HDLC), Frame Relay, and X.25.

Note: The ISDN caller ID callback feature 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.

Benefits: The ISDN caller ID callback feature allows users to control costs because charges do not apply to the initial, rejected call.

Considerations/Platforms: This feature is supported for both ISDN BRI and ISDN PRI on these platforms: Cisco 1003/4, Cisco 1005, Cisco 1600 series, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Caller ID screening requires a local switch that is capable of delivering the caller ID to the router or access server. If you enable caller ID screening but do not have such a switch, no calls will be allowed in.

ISDN caller ID callback requires DDR to be configured and bidirectional dialing to be working between the calling and callback routers. Detailed DDR prerequisites depend on whether you have configured legacy DDR or dialer profiles.

For a legacy DDR configuration, ISDN caller ID callback has the following prerequisite:

- A dialer map command is configured for the dial string that is used in the incoming call setup message. The dial string is used in the callback.
- For a dialer profiles configuration, ISDN caller ID callback has the following prerequisites:

- A dialer caller command is configured to screen for the dial-in number.
- A dialer string command is configured with the number to use in the callback.

Product Marketing Contact: Anita Freeman

ISDN NFAS

Description: ISDN Nonfacility 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.

Benefits: Use of a single D channel to control multiple PRI interfaces can free one 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.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 1003/4, Cisco 1005, Cisco 1600, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

The router must connect to an AT&T 4ESS ISDN PRI switch. It must also have a channelized T1 controller and, as a result, be ISDN PRI capable.

In addition, the router's channelized T1 controllers must be configured for ISDN PRI, as described in the "Configuring ISDN" chapter of the Wide-Area Networking Configuration Guide for Cisco IOS Release 11.2.

List of Terms:

- *24-B channel interface*—PRI channel group configured to have no NFAS D channel; all its channels are B channels.
- *NFAS group*—PRI channel group (the group of interfaces) under control of a single D channel. The channel group can include all the ISDN channels on multiple T1 controllers.
- *NFAS member*—PRI interface in an NFAS group. For example, an NFAS group might include serial interfaces 1/0:23, 1/1:23, and 2/0:23 if T1 controllers 1/0, 1/1, and 2/0 are configured for NFAS.

Product Marketing Contact: Anita Freeman

Virtual Interface Template Service

Description: Beginning with Cisco IOS Release 11.3, virtual interface templates can be configured independently of any physical interface and applied dynamically, as needed, to create virtual access interfaces. When a user dials in, a predefined configuration template is used to configure a virtual access interface; when the user is done, the virtual access interface goes down and the resources are freed for other dial-in uses.

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

Virtual interface templates are serial interface configurations with no hardware associations, and virtual access interfaces are virtual interfaces that are created, configured dynamically, and freed as needed. The following limitations apply:

- Although a system can have as many as ten virtual interface templates, four is a more realistic limit.
- When in use, each virtual access interface cloned from a template requires the same amount of memory as a serial interface. Cisco routers support a maximum of 300 virtual interfaces per system.
- Virtual access interfaces are not directly configurable by users, except by configuring a virtual interface template or including a user's configuration information on an Authentication, Authorization, and Accounting (AAA) server. However, information about an in-use virtual access interface can be displayed and the virtual access interface can be cleared.
- Virtual interface templates provide no direct value to users; they must be applied to or associated with a feature by use of a command with the virtual-template keyword.
- For example, the interface virtual-template command can be used to create the virtual interface template and the multilink virtual-template command can be used to apply the virtual template to a multilink stack group. The virtual-profile virtual-template command is used to specify that a virtual interface template will be used as a source of configuration information for virtual profiles.

Features that Apply Virtual Interface Templates

This is a partial list of features that apply virtual interface templates to create virtual access interfaces dynamically:

- Virtual Profiles
- Virtual Private Dialup Networks
- Multichassis Multilink PPP (MMP)
- Virtual Templates for Protocol Translation
- PPP over ATM

Benefits: The virtual interface template service provides the following benefits to customers with numerous dial-in users:

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

All prerequisites depend on the feature that is applying a virtual interface template to create a virtual access interface. Virtual interface templates themselves have no other prerequisites.

The order in which you create virtual interface templates and virtual profiles, and configure the features that use the templates and profiles, is not important. They must exist, however, before someone calling in can use them.

List of Terms:

- *Cloning*—Creating and configuring a virtual access interface by applying a specific virtual template. The virtual template is the source of the generic user information and router-dependent information. The result of cloning is a virtual access interface configured with all the commands in the template.
- *Virtual access interface*—Instance of a unique virtual interface that is created dynamically and exists temporarily. Virtual access interfaces can be created and configured differently by different applications, such as virtual profiles and virtual private dialup networks (VPDNs).
- *Virtual interface template*—Generic configuration of an interface for a certain purpose or configuration common to certain users, plus router-dependent information. This takes the form of a list of Cisco IOS interface commands to be applied to the virtual interface as needed. Several applications can apply virtual interface templates, but generally each application uses a single template. Each virtual interface template is identified by number.
- *Virtual profile*—Unique virtual access interface created dynamically for a specific user when the user calls in and torn down dynamically when the call disconnects. The sources of configuration information for the virtual profile can be a virtual interface template (general configuration and router-specific information stored on the local router) -- for a group of users.
- *Per-user configuration (stored on an AAA server)*—for the specific user who dials in. Configuration of a virtual access interface begins with a virtual interface template (if any), followed by application of per-user configuration for the particular user's dial-in session (if any).

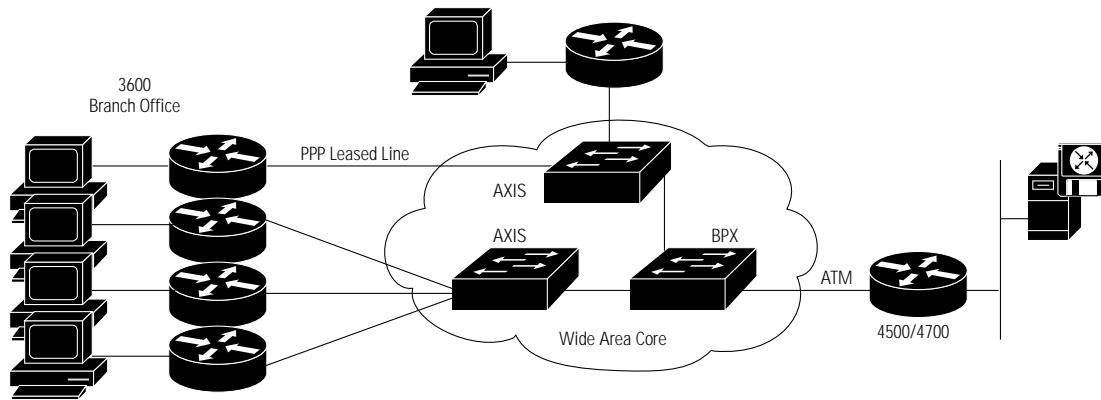
Product Marketing Contact: April Chou

PPP over ATM

Description: Enables a high-capacity central site router with an ATM interface to terminate multiple PPP connections. These PPP connections are typically received from remote branch offices that have PPP-compatible devices interconnecting directly to Cisco-StrataCom ATM Switch Interface Shelf (AXIS) equipment through a leased-line connection.

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

Figure 4 PPP Over ATM



Benefits: The PPP-over-ATM feature is ideally suited for enterprise customers or customers who use Cisco-StrataCom ATM switches to access WANs or public ATM networks, such as organizations with many remote branch offices requiring access to high-density corporate headquarters. Figure 18(?) shows a typical scenario for using PPP over ATM.

Dedicated lower-speed connections can be aggregated across a wide area and concentrated into high-capacity ATM core routers. This solution realizes the following benefits:

- Provides a more complete solution for branch office interconnection to ATM-equipped centers
- Permits economical use of ATM across a wide area and reduces long-distance circuit costs
- Uses a single ATM connection to aggregate all connections at the central location, saving the expense of multiple lines.

Platforms/Considerations: Cisco IOS software supports up to 150 PPP over ATM VC's, but numbers may vary depending on router capacities. This feature is supported on the platforms: Cisco 4500, Cisco 7500 series.

Product Marketing Contact: Keith Travis

X.25 Enhancements

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

- There are three classes of X.25 services:
 - X.25
 - X.25 over TCP (XOT)
 - X.25 over Local-Area Networks (Connection-Mode Network Service, or CMNS)
- Four classes of X.25 service users:
 - Encapsulating routed traffic over X.25 (datagram encapsulation)
 - X.25 switching
 - Packet assembler/disassembler (PAD) support for asynchronous devices, including protocol translation between X.25-related protocols (X.28, X.29) and other protocol families (LAT, Telnet, PPP)
 - Qualified Logical Link Control (QLLC)
- Three underlying layers that can support an X.25 service:
 - Link Access Procedure, Balanced (LAPB)
 - Link Access Procedure, D channel (LAPD)
 - Logical Link Control, Type 2 (LLC2)

In addition to ensuring compliance with the standard X.25 specifications, Cisco has enhanced its X.25 functionality with several additional features:

- *Called address suppression*—Gives the network implementer the ability to configure a router to remove or suppress the X.121 called (destination) address in the call request packet.
- *Calling address suppression or replacement*—Gives the network implementer the ability to configure a router to remove/suppress and force or change the X.121 calling (source) address in the call request packet; X.25 networks normally route on the destination or called address, so this feature does not affect network routing.
- *Substitution of source or destination X.121 addresses*—When interconnecting two separate X.25 networks, you must sometimes provide for address translation for local routes; the X.25 switch software supports translation of X.25 source and destination addresses for local switching; this feature is now supported for X.25 transport over IP, XOT.

Detailed configuration information on these features can be found in the Cisco Wide-Area Networking Configuration Guide.

Benefits: The modularization of the X.25 protocol engine has enabled Cisco to take advantage of common internal pathways as well as new Cisco IOS software operating system enhancements. This revision has given Cisco more flexibility in adding new features to the code and access to Cisco IOS software features such as “fancy queuing” techniques.

Considerations/Platforms: This feature is available in the IP image for all of the following platforms: Cisco 2500 series, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

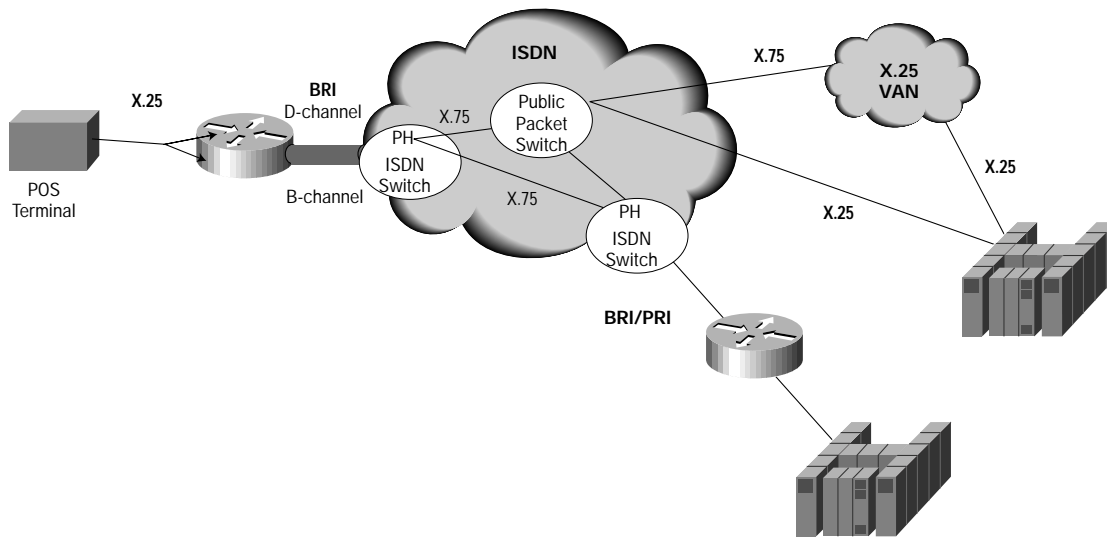
Product Marketing Contact: Ruben Rios

X.25 on ISDN

Description: In addition to Cisco's support of X.25 transport over the ISDN B-channel, Cisco now allows the use of the D-channel in a BRI to carry X.25 packets. The D-channel has a capacity of 16 kbps, and the X.25 over D channel can utilize up to 9.6 kbps.

Benefits: This feature allows you to set the parameters of the X.25-over-D-channel interface without disrupting the original ISDN interface configuration. 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, such as point-of-sale terminals doing transaction authorization.

Figure 5 X.25 Transport Over ISDN



Considerations/Platforms: Supported traffic includes IPX, AppleTalk, transparent bridging, XNS, DECnet, and IP. Because some end-user equipment uses static terminal endpoint identifiers (TEIs) to access this feature, static TEIs are supported. The dialer understands the X.25-over-D-channel calls and initiates them on a new interface. This feature is available on Cisco 1003/4, Cisco 1005, Cisco 1600, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series platforms.

Product Marketing Contact: Ruben Rios

X.25 Switching between PVCs and SVCs

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

Benefits: Some older equipment with X.25 interfaces support only PVCs which are not as easily manageable as SVC provisioning. This feature allows the network implementer to convert the PVC to an SVC, making the network more efficient.

Considerations/Platforms: Available in the IP image for the following platforms: Cisco 1003/4, Cisco 1005, Cisco 1600, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200 series, Cisco 7200, and the Cisco 7500 series platforms.

Product Marketing Contact: Ruben Rios

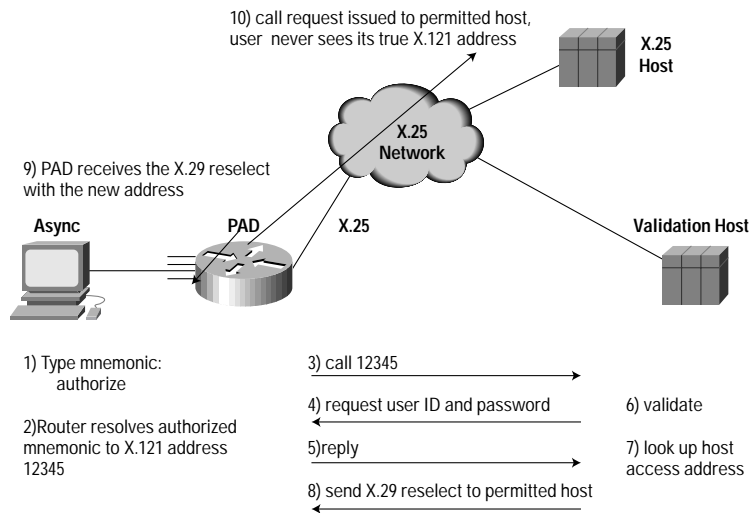
X.28 Emulation

Description: The Cisco IOS software provides an X.28 user emulation mode, which enables you to interact and control the PAD. During an exchange of control information, messages or commands sent from the terminal to the PAD are called PAD command signals. Messages sent from the PAD to the terminal are called PAD service signals.

The new X.28 emulation mode supports most of the 22 X.3 PAD parameters, all the X.29 commands, including reselect, all the X.28 PAD commands, and mnemonics. This standard interface is common in many European countries and adheres to the X.25 International Telecommunication Union Telecommunication (ITU-T) standards.

Benefits: This new feature provides a classic X.28 user interface, which enables you to interact and control the PAD. Applications such as dialup users accessing a remote X.25 host can use the new X.28 interface. Cisco's X.28 PAD calls can be transported over a public packet network, a private X.25 network, the Internet, a private IP-based network, or a Frame Relay network. X.29 reselect feature usually works with an external validation host for security checking and DNS-like X.25 naming/selection of destination within a public/private network. The following drawing illustrates one possible use of X.29 reselect in a host validation application.

Figure 6 X.28 Emulation



Considerations/Platforms: This feature is available in the IP image for all of the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, and the Cisco AS5200 series platforms. Available in the Enterprise image for the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Ruben Rios

PAD Subaddressing

Description:

- This feature allows you to append a specified value to an X.121 calling address, if the X.121 calling address is not sufficient to identify the source of a call. PAD subaddressing allows you 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.

Benefits: 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.

Considerations/Platforms: This feature is available in the IP image for all of the following platforms: Cisco 1003/4, Cisco 1005, Cisco 1600, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, and the Cisco AS5200, Cisco 7200, and the Cisco 7500 series platforms.

Product Marketing Contact: Ruben Rios

Benefits: An application for this new feature is bank alarms. The alarm unit makes a call to the alarm host only when an alarm condition exists. Bidirectionally, the alarm host needs to access the alarm unit several times per day to check the status of the unit when no alarm condition is present.

Product Marketing Contact: Ruben Rios

PAD Enhancements

Description:

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

Benefits: These enhancements enable the user to new features to manage and transport PAD calls over both traditional X.25 circuits as well as TCP interfaces.

Considerations/Platforms: This feature is available in the IP image for all of the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series platforms.

Product Marketing Contact: Ruben Rios

Multilink PPP Interleaving and Fair Queuing Support

Description: 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 on 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 will be scheduled for transmission only after all the fragments of the larger packet are scheduled for transmission. Weighted fair-queuing is now 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.

Benefits: 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.

Considerations/Platforms: This feature is supported on all platforms on which Multilink PPP is supported, which include these platforms: Cisco 1003/4, Cisco 1005 series, Cisco 2500, Cisco 4000, Cisco AS5200, Cisco 7200, and the Cisco 7500 series

Product Marketing Contact: April Chou

Scalability

VPDN Enhancements

Layer 2 Forwarding—Fast Switching

Description: Layer 2 Forwarding (L2F) is now fast switched, as well as process switched. In stack group environments in which some L2F traffic is offloaded to a powerful router, fast switching provides improved scalability and improves performance.

Benefits: L2F—Fast switching improves performance of features based on L2F, such as VPDN and MMP.

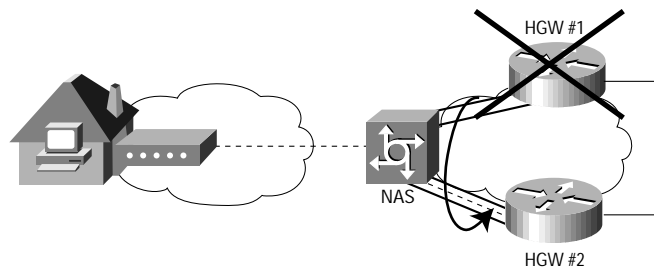
Considerations/Platforms: This feature is supported on the following platforms: Cisco 1600, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, and the Cisco 7500 series.

Product Marketing Contact: April Chou

L2F Backup

Description: With L2F Backup, multiple home gateway peers can be configured. Only if the connection to primary home gateways is unreachable, will the NAS will establish a connection with one of the backup home gateways.

Figure 7 Layer 2 Forwarding—Backup



- Allows configuration of multiple Home Gateway peers
- If connection to primary Home Gateways is lost, NAS establishes connection with backups
- Improves reliability, minimizes costly downtime

Benefits: L2F backup can be used to improve reliability.

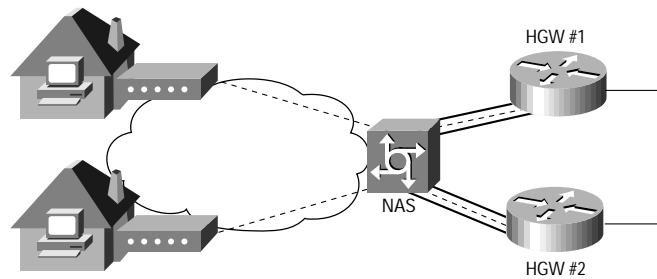
Considerations/Platforms: Multilink PPP is not yet supported with L2F backup in Release 11.3. It is anticipated that Multilink support will be available in Release 11.3T. The configuration must be done at the AAA server.

Product Marketing Contact: April Chou

L2F Load Sharing

Description: This feature provides the ability to have multiple tunnel connections between one NAS and multiple home gateways. Random sessions load sharing is done across the multiple home gateways.

Figure 8 Layer 2 Forwarding—Load Sharing



- Allows multiple tunnel connections between one NAS and multiple Home Gateways
- Improves number of sessions Home Corporations can support
- Improves reliability—If one Home Gateway fails, data can be transmitted via remaining Home Gateways

Benefits: The L2F load sharing improves the number of sessions home corporations can support. It also improves reliability; if one of the home gateway fails, data can be transmitted via one of the remaining Home Gateways.

Considerations/Platforms: This feature is not yet supported with Multilink PPP. The configuration must be done at the AAA server.

Product Marketing Contact: April Chou

L2F DNS Name Support

Description: Home gateway names can be used for Domain Name Support (DNS) lookup instead of configuring the home gateway IP addresses. If the name is detected in the IP address AV pair, the NAS will perform the local name cache lookup. If there is no cache entry, DNS query will be done.

Benefits: The NAS is no longer required to update the IP address changes done on the Home Gateways.

Considerations/Platforms: The configuration must be done at the AAA server.

Product Marketing Contact: April Chou

L2F Domain Name Flexibility

Description: The domain name flexibility feature allows the customer to use the domain name other than the @<domain>.<tld> command. The domain name itself can be before or after the delimiters. For example, username!<domain>.<tld> as well as domain>.<tld>%username are both possible with the proper configuration. The configuration also allows username to be before or after the domain name delimiter.

Benefits: This feature is designed to improve the flexibility of domain name usage.

Considerations/Platforms: The supported domain name delimiters are @ /% - \ #.


Product Marketing Contact: April Chou

FRF.9 Payload Compression for Frame Relay

Description: This feature permits payload compression of data within Frame Relay packets. The compression is performed on a stream basis, yielding a compression ratio of approximately 1.5:1 to 2:1, depending on packet/data characteristics. This compression is based on the Frame Relay Forum Implementation Agreement FRF.9 for Data Compression over Frame Relay. FRF.9 provides for a negotiation process for compression.

Benefits:

- This feature decreases costs associated with Frame Relay links by allowing more data to pass over a given speed line.
- 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.
- FRF.9 compression provides the ability to maintain multiple decompression/compression histories on a per-DLCI basis.



Considerations/Platforms: This feature is supported on all serial ports on Cisco routers that support Frame Relay. It offers hardware compression support for FRF.9 is provided with the compression service adapter (CSA). This feature is supported on the following platforms: Cisco 1005, Cisco 1600, Cisco 2500, Cisco 25FX, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, and the Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Sanjay Bhardwaj

Bandwidth Allocation Control Protocol

Description: The PPP Bandwidth Allocation Control Protocol (BACP) provides Multilink PPP (MLP) peers with the ability to govern link utilization. After peers have successfully negotiated BACP, they can use the Bandwidth Allocation Protocol (BAP), which is 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 MLP is used.

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 is controlled by a link drop message.

This feature is designed to operate in both the virtual interface environment and the dialer interface environment. It can operate over any physical interface that is PPP multilink capable and has a dial capability; at initial release, BACP supports ISDN and asynchronous serial interfaces.

Benefits: Bandwidth Allocation Control Protocol allows multilink implementations to interoperate by providing call control through the use of link types, speeds, and telephone numbers. BACP also controls thrashing caused by links being brought up and removed in a short period of time. Finally, this feature ensures that both ends of the link are informed when links are added or removed from a multilink bundle.

Considerations/Platforms: In this initial release, support of PPP BACP on virtual interfaces in an Multichassis Multilink PPP (MMP) environment is restricted to incoming calls on the multilink group. Support of PPP BACP for outgoing calls is provided by dialer interface configuration only. In Release 11.3, dialer support is provided only for legacy DDR dialer configurations; BACP cannot be used in conjunction with the dialer profiles DDR feature.

This feature is supported on these platforms: Cisco 1003/4, Cisco 1600, Cisco 1005 series, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series

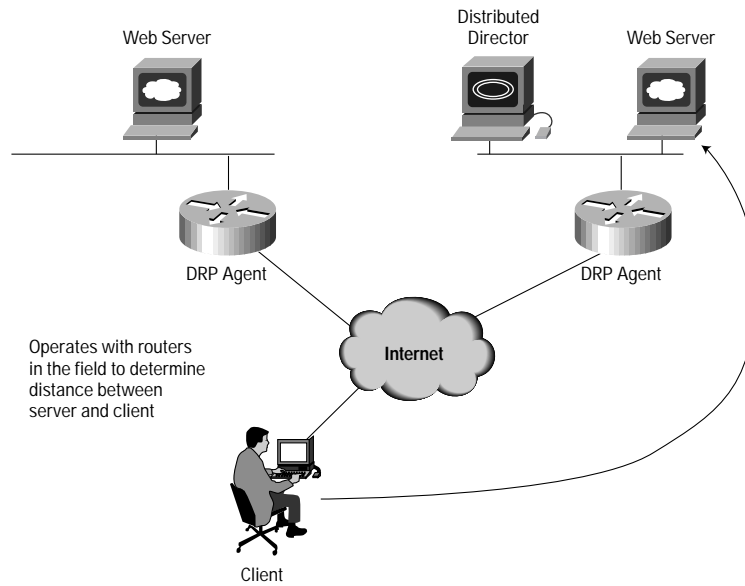
Product Marketing Contact: Kevin Dickson

DRP Server Agent

Description:

- The Director Response Protocol (DRP), a simple User Datagram Protocol (UDP)-based application developed by Cisco Systems, enables Cisco's DistributedDirector product to query routers (DRP server agents) in the field for Border Gateway Protocol (BGP) and Interior Gateway Protocol (IGP) routing table metrics between distributed servers and clients.
- DistributedDirector, a separate standalone product, uses DRP to transparently redirect end-user service requests to the topologically closest responsive server. DRP enables DistributedDirector to provide dynamic, scalable, and "network intelligent" Internet traffic load distribution between multiple, geographically dispersed servers.
- DRP server agents are border routers (or peers to border routers) that support the geographically distributed servers for which DistributedDirector service distribution is desired. Note that, because DistributedDirector makes decisions based on BGP and IGP information, all DRP server agents must have access to full BGP and IGP routing tables.
- Refer to the Cisco DistributedDirector 2501 Installation and Configuration Guide or the Cisco DistributedDirector 4700-M Installation and Configuration Guide for information on how to configure DistributedDirector.

Figure 9 Director Response Protocol (DRP)



Benefits: When used with the DistributedDirector system, DRP provides dynamic, transparent, and scalable Internet traffic load distribution between multiple topologically dispersed servers. The DistributedDirector system utilizes Cisco IOS software to transparently direct clients to the topologically closest available server, localizing Internet traffic, increasing access performance, and reducing transmissions costs.

Considerations/Platforms: When DistributedDirector makes decisions based on BGP and IGP information, all DRP server agents must have access to full BGP and IGP routing tables. This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Kevin Delgadillo

NLSP Enhancements

Description: 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.

Benefits: By interpreting the maximum lifetime field in hours, the router keeps LSP packets for a much longer time, reducing overhead on slower-speed serial links and keeping ISDN links from unnecessarily becoming active.


Considerations/Platforms: This feature is supported on these platforms: Cisco 1003/4, Cisco 1005, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Roger Farnsworth

NLSP Multicast Support

Description: NLSP multicast adds support for the use of NLSP multicast addressing for Ethernet, Token Ring, and FDDI router interfaces. With this feature, the router defaults to using multicasts on Ethernet, Token Ring, and FDDI interfaces, instead of broadcasts, to address all NLSP routers on the network. If an adjacent neighbor does not support NLSP multicasting, the router reverts to using broadcasts on the affected interface.

Benefits: Preserves bandwidth by automatically limiting broadcasts where possible.



Considerations/Platforms: This capability is possible only when the underlying Cisco hardware device or driver supports multicast addressing, and it is only available on routers running Cisco IOS Release 11.3 or later software. When routers running prior versions of Cisco IOS software are present on the same network with routers running Cisco IOS Release 11.3 software, broadcasts are used on any segment shared by the two routers.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 1003/4, Cisco 1005, Cisco 1600, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Erik Gilbert

TCP Enhancements

Release 11.3 introduces two new performance enhancements to the Cisco IOS TCP implementation - Selective Acknowledgment (described in RFC 2018) and Round-Trip Time Measurement (described in RFC 1323):-

5.1 TCP Selective-ACK Option (SACK)

Description: TCP can experience performance degradation when multiple packets are lost from one window of data. With the limited information available from cumulative acknowledgments, a TCP sender can only learn about a single lost packet per round-trip time.

Benefits: A Selective Acknowledgment (SACK) mechanism, combined with a selective repeat retransmission policy, can help to overcome these limitations. The receiving TCP sends back SACK packets to the sender informing the sender of data that has been received therefore the sender need only retransmit the missing data segments.

Platforms/Considerations: TCP Selective-Ack is incorporated into all IOS 11.3 images. It is enabled by default and it can be turned off via configuration. This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco7200 series, and the Cisco 7500 series.

5.2 TCP Round Trip Time Measurement (RTTM)

Description: Current TCP implementations base the Round-Trip Time (RTT) measurement upon a sample of only one unretransmitted packet per window. While this yields an adequate approximation to the RTT for normal data transfer, it becomes very inaccurate when there are dropped packets, and the inaccuracy in RTT estimate would cause unnecessary retransmission delay.

Benefits: This new feature allows TCP senders to place a time stamp in each data segment, and the receiver reflects these time-stamps back in Ack segments, such that a single subtraction gives the sender an accurate RTT measurement for every Ack segment.

Platforms/Considerations: TCP Round Trip Time Measurement is incorporated into all IOS 11.3 images. This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Manager: Martin McNealis

Enhanced Local Management Interface

Description: The Enhanced Local Management Interface (ELMI) feature provides an enhancement to the Frame Relay LMI protocol. ELMI enables automated exchange of Frame Relay quality of service (QoS) parameter information between the Cisco router and the Cisco StrataCom switch. Routers can base congestion management and prioritization decisions on known QoS parameters, such as the committed information rate (CIR), Committed Burst (Bc) size, and Excess Burst (Be) size. The router learns QoS parameters from the switch and can be configured to use those parameters in traffic shaping.

Benefits: ELMI simplifies and automates the loading of key QoS parameters on Cisco router platforms connected to Cisco StrataCom Frame Relay networks. This reduces configuration and setup time and reduces configuration errors for traffic shaping parameters. This provides increased frame relay scalability for Frame Relay routers in large networks with large concentrations of virtual circuits on physical ports.

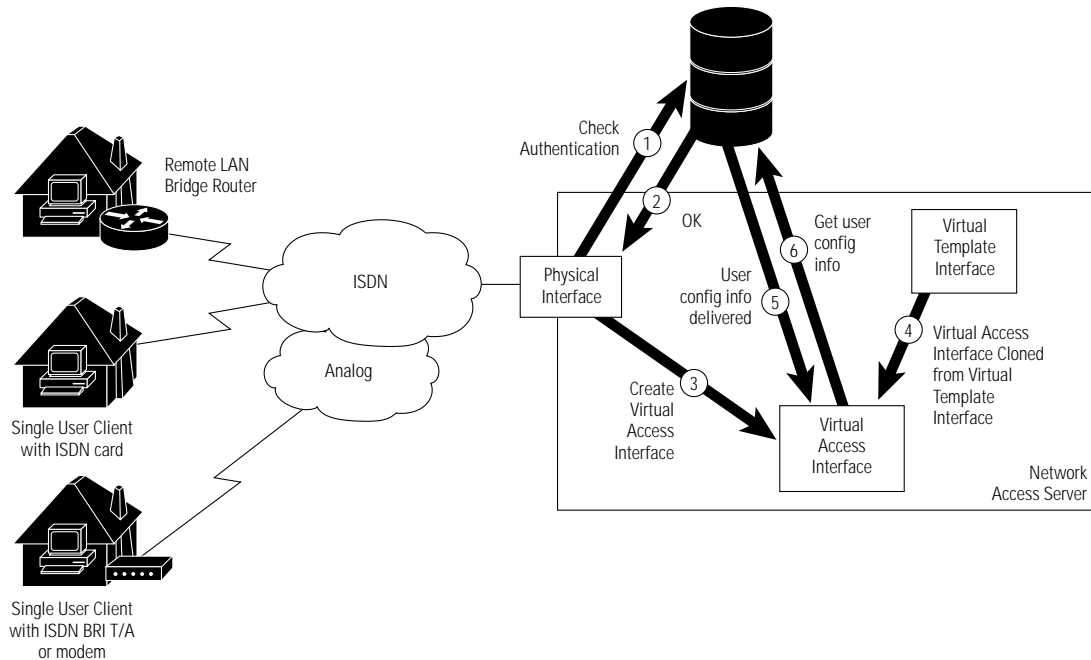
Considerations/Platforms: This enhancement works between Cisco routers and Cisco StrataCom switches (BPX/AXIS and IGX™ platforms). Specific platforms that support this feature include: Cisco 1003/4, Cisco 1005, Cisco 1600, Cisco 2500, Cisco 25FX, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Sanjay Bhardwaj

Virtual Profiles

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

Figure 10 Virtual Profiles



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

- *AAA*—the ability to change any configuration on a per-user basis currently 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 DDR 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 these limitations, but they 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.

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


Considerations/Platforms: This feature runs on all Cisco IOS platforms that support Multilink PPP: Cisco 1003/4, Cisco 1005 series, Cisco 1600 series, Cisco 2500, Cisco 25FX, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Kevin Dickson

CLNS and DECnet Fast Switching Support over PPP

Description: With Cisco IOS Release 11.3, Cisco now supports fast switching of incoming and outgoing DECnet and CLNS encapsulated packets over PPP.

Benefit: This feature provides full IOS switching performance across primary WAN protocol.



Consideration/Platforms: This feature is enabled by default and it can be turned off via configuration. This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Martin McNealis

IBM

APPN High Performance Routing

Description: High Performance Routing (HPR) is the third generation of IBM's SNA protocol. It is a major enhancement over its predecessor, APPN. Like Cisco's current APPN implementation, Cisco provides the network node (NN) implementation of HPR. Cisco will bundle APPN and HPR together as a single offering that customers can configure and deploy as required. HPR introduces a much improved flexible architecture. HPR devices can load the entire HPR functionality or a subset depending on the role in the network; the following represent the related criteria.

If the HPR devices are responsible for determining and establishing 'path' between devices and applications, they will require the entire HPR functionality:

- Rapid transport Protocol (RTP) establishes the end-to-end path over the HPR network
- Adaptive Rate Based (ARB) flow control constantly monitors network flows to avoid congestion
- Automatic Network Routing (ANR) label-forwarding mechanism operating at Layer 2
- If the HPR devices are acting as intermediary devices and are responsible for only passing HPR traffic, they only require a subset of HPR; specifically, the ANR component. HPR can nondisruptively dynamically reroute around any failures. Selective Re-transmission, of ONLY those messages dropped when dynamic rerouting can reduce and increase the traffic flow based on it's findings. Proactive congestion control is a protocol that monitors the HPR network and HPR can 'non-disruptively and dynamically re-route' around any failures that occur.

Benefits:

- Dynamic session routing around failures, transparent to the application or user; RTP detects the failure and is responsible for rerouting around the failure.
- Improved processing and increased performance through the network
- Architected for high-speed, reliable data links, Frame Relay, ATM; also supports all the traditional IBM communications types
- Limits unnecessary network traffic by retransmitting only those packets dropped
- Proactive congestion control to avoid packets being dropped
- Together with Cisco multipath channel (CMPC) support, new in Cisco IOS Release 11.3, Cisco fully supports a parallel sysplex and multinode persistent sessions (MNPS) support in the data center

Platforms/Considerations: This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco 7200, and the Cisco 7500 series. HPR, when used in conjunction with the Cisco CMPC feature on the CIP provides full support for a parallel sysplex environment. In this environment, the CIP provides the channel interface to an Escon Director interconnecting multiple IBM mainframes in the data center, where HPR is used to improve availability and flexibility in a multi-mainframe environment by providing dynamic session rerouting.

Product Marketing Contact: Mark Denny

Cisco Multipath Channel

Description: CMPC (CIP MPC) is Cisco's implementation of IBM's MPC protocol using the CIP card. IBM introduced MPC with VTAM release 4.2 as an enhanced channel protocol. MPC has been marketed as an enabling technology for HPR access to the IBM mainframe. CMPC provides this functionality on the CIP card in Cisco 7000 series routers. CMPC supports both HPR and intermediate session routing (ISR).

An overview of the CMPC implementation:

- Implemented on the CIP card
- Enables HPR
- Concurrent operation with CSNA, TN3270 server, TCP offload, TCP assist, and IP datagram support

- Supports both Enterprise System Connection (ESCON) and parallel channel
- Supports ESCON director

Benefits: CMPC insulates VTAM from the actual network topology. The MPC protocols are terminated on the CIP and converted to LLC protocols. When converted to LLC protocols, other Cisco features can be used to connect VTAM to other APPN nodes in the network. CMPC can be used in conjunction with DLSw+, RSRB, SR/TLB, SRB, SDLLC, QLLC, ATM LAN emulation, and FRAS host to provide connectivity to VTAM.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 7500 series.

Product Marketing Contact: Rod Starrett

DLSw+ SNA Type of Service

Description: DLSw+ SNA type of service (TOS) sets the IP precedence bits in the IP header of DLSw+ packets. When Advanced Peer-to-Peer (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, minimizing response time for mission critical traffic. SNA TOS dynamically maps SNA Class of Service to TCP/IP TOS. This feature prioritizes mission critical SNA transactions ahead of SNA batch or File Transfer Protocol (FTP).

Benefits: Improves SNA response time while minimizing required configuration. When used in conjunction with APPN, improves SNA interactive response time.

Product Marketing Contacts: Donna Kidder, Paul Sikorski

TN3270 Server Enhancements

The enhancements for the TN3270 server include the following:

- **LU Nailing**

Description: 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. These arrangements may be made for security or specific terminal/printer definitions. Using this feature, you can control the relationship between the TN3270 client and the LU.

Benefits: Clients from traditional TN3270 (non-TN3270E) devices can connect to specific LUs, overcoming 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, rather than at the client, providing central control.

- **LU Capping**

Description: A downstream client IP address can now be limited to a defined number of LU sessions.

Benefits: Reduces the resources allocated to a specific client IP address. Limits the resources that an IP client address can use by restricting the number of LU sessions concurrently active.

- **IP Type-of-Service/Precedence Setting**

Description: The TCP TOS bits in the TCP header can now be set to support Weighted Fair Queueing (WFQ) in the network.

Benefits: Enables bandwidth reservation of network traffic using Cisco’s WFQ algorithms.



- **RFC 1646 Printer Support**

Description: 1646 printer support implements RFC standard TN3270E printing for LU1 and LU3 sessions to client attached printers.

Benefits: Supports 3287 type printing to IP networked printers

- **Function Management Header (FMH) Support**

Description: This feature supports FMHs for printing to certain foreign character set printers

Benefits: Supports 3287 type printing to a broader range of printer types.

- **Unformatted System Services Table (USSTAB) Conversion**

Description: This feature supports SCS conversion for TN3270E clients for SSCP/LU sessions

Benefits: Enables support for a broader range of TN3270 clients for logon services.

Considerations/Platforms: These features are supported on the following platforms: Cisco Channel Interface Processor (CIP) on the Cisco 7500 series.

Product Marketing Contact: Rod Starrett

LLC2-to-SDLC Conversion Between PU4 Devices

Description: DLSw+ now 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. It also enables an SDLC-attached FEP to communicate over DLSw+ to a Cisco CIP.

Benefits: Reduces costs by allowing network consolidation of links carrying FEP traffic. It provides a smooth migration from a FEP to a CIP. It also enables DLSw+ to transport SNI traffic between FEPs when one of the FEPs is serially attached.

Product Marketing Contact: Paul Sikorski

Token Ring LANE (LAN Emulation)

Description: Cisco has added Token Ring LAN Emulation (LANE) to this release of Cisco IOS software to provide Token Ring customers increased flexibility and performance for Asynchronous Transfer mode (ATM) networking solutions.

The Token Ring LANE feature emulates an IEEE 802.5 Token Ring LAN using 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 Token Ring 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 de-encapsulated. LANE essentially bridges LAN traffic across ATM switches.

Token Ring LANE in Cisco IOS software supports all the ATM Forum LANE 1.0 functions, including LAN Emulation Configuration Server (LECS), LAN Emulation Server (LES), broadcast and unknown server (BUS), and LAN Emulation Client (LEC).

In addition, backup and redundancy is enhanced with support for Hot Standby Router Protocol (HSRP) and Simple Server Redundancy Protocol (SSRP). When used with Token Ring LANE on the Catalyst® 3900 or Catalyst 5000 switches, the Cisco 7000 and 4500 router families provide high-performance routing between LANs and emulated LANs (ELANs) along with bridging for nonroutable protocols.

Benefits: Token Ring LANE allows legacy Token Ring LAN users to take advantage of ATM's benefits without modifying end-station hardware or software. With support for Token Ring LANE, it is now possible to do high performance IP and IPX routing, source-route bridging (SRB), source-route transparent (SRt) bridging, and source route/translational bridging (SR/TLB) between Token Ring and Ethernet LANs or ELANs. In addition, Token Ring LANE in Cisco IOS software provides the following advantages:

- Facilitates backbone and server upgrades without requiring changes to the Token Ring clients, providing a high-performance solution at minimal cost
- Unparalleled IP and SNA throughput to the mainframe when an AIP or ATM Port Adapter is paired with a Channel Interface Processor (CIP) in the Cisco 7000 router family
- Enables parallel, redundant source-route bridged paths across the ATM network
- Interoperates with other LANE 1.0 compliant devices

Considerations/Platforms: Token Ring LANE is supported on the Cisco 7500 series and the CiscoRSP/7000 with the ATM Interface Processor (AIP) or ATM Lite port adapter, the Cisco 7200 with ATM Lite Port Adapter, and the Cisco 4500/4700 series with ATM Network Processor Module (NPM). Token Ring LANE client and server support is also available on the dual PHY ATM LANE module for the Catalyst 5000 family. Token Ring LANE client support is available on the Catalyst 3900.

Product Marketing Contact: Sue Sept/Donna Kidder

FRAS Host

Description: The FRAS host feature provides connectivity from an 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 (FEPs) or to LAN-attached SNA minicomputers (such as AS/400s).

Benefits: Reduces costs by allowing a Cisco router to provide host boundary access node (BAN) or BNN functions previously only available from FEPs.

FRAS host provides greatly improved economy and efficiency communicating with an SNA host, whether that host is channel attached or accessed via a LAN:

- The FRAS host LLC passthrough feature combines with a CIP-attached Cisco router's high-speed channel access to provide FEP-class performance at a fraction of what it would cost to achieve similar functionality using an FEP. FEP upgrades, such as the addition of a Frame Relay interface, an upgrade to NCP (with its associated increase in monthly charges), and a possible increase in system memory are all avoided, while the performance benefits of channel-attachment are maintained.
- The FRAS host LLC2 local termination feature provides similar benefits in LAN environments. If used with a Token Ring attached FEP, the FRAS host Cisco router shields the FEP from having to manage the interface to the Frame Relay network. This feature avoids interface, memory, and NCP upgrades as described previously. The FRAS host Cisco router simply provides LLC2 sessions to the FEP over the LAN.

If used in an environment with AS/400s, FRAS host LLC2 local termination provides an even more valuable function. Because the AS/400 is attached directly to the LAN, it must perform its own FEP functions. This drains AS/400 CPU cycles that could be better spent on user applications and increases system hardware requirements overall. The Cisco FRAS host router off-loads all of these functions from the AS/400, managing the Frame Relay connections and providing the AS/400 with simple LLC2 sessions over the Token Ring LAN.

In all environments, users may further tune the interface to the Frame Relay network by taking advantage of Cisco IOS Frame Relay features. LLC2 passthrough uses LLC window-sizing techniques to respond to network congestion and provide maximum throughput, reducing window size when required and expanding to take advantage of unused bandwidth when it's available. FRAS host LLC2 local termination responds to network BECN messages by adjusting LLC2 window sizes appropriately. Both passthrough and local acknowledgment environments support frame discard eligibility (DE) for additional congestion management. Taken together, these features increase overall throughput dramatically by comparison to generic FRADs, which typically cannot use the network with the same degree of efficiency.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 1600, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Paul Sikorski

Block Serial Tunneling (BSTUN) over Frame Relay

Description: The Block Serial Tunneling (BSTUN) over Frame Relay feature provides a tunnel mechanism for binary synchronous communications (BSC) protocol (bisync) without using TCP/IP encapsulation.


Benefits: Reduces overhead and enables network consolidation when running BSC over a frame relay network.

Product Marketing Contact: Betsy Huber

Multiple Ethernet Bridge Group Support

Description: This feature extends data-link switching plus (DLSw+) Ethernet support to support multiple bridge groups.

Benefits: Simplifies configuration and enhances control in an Ethernet environment.



Considerations/Platforms: Except where noted (for example, called out in feature name), this feature is supported on these platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series. The only exception is BSC, which is limited to the Cisco 2500, Cisco 4000, and the Cisco 7200 series.

Product Marketing Contact: Donna Kidder

DLSw+ Asynchronous TCP Enhancements

Description: TCP sessions can be started asynchronously, rather than serially, or sequentially. This is especially important in large environments. If you have ten DLSw+ peers to establish, you don't have to wait for one to finish before another one starts. When you have numerous peers, the improvement is dramatic.

Benefits: Minimizes the delay to initialize a network. The improvement is most noticeable when a single router tries to initialize many TCP connections at one time—e.g. when the data center router dials out to hundreds of branch routers.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Donna Kidder, Paul Sikorski

DLSw+ Border Peer Caching

Description: 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. Cisco's border peer caching feature extends beyond the AIW V2 standard by further reducing broadcast traffic. This feature automatically builds and maintains a distributed directory of Systems Network Architecture (SNA) and NetBIOS resources so that broadcasting only occurs the first time any branch router needs to find a network resource. With the distributed directory, requests from other branch routers are forwarded directly to the correct site.

Benefits: By eliminating subsequent broadcast traffic, Cisco's implementation greatly enhances network performance and extends scalability in a fully meshed DLSw+ environment. By comparison, AIW V2 DLSw standard requires each branch router to multicast an explorer at least once. This additional broadcast traffic can potentially impact network performance.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series

Product Marketing Contact: Donna Kidder, Paul Sikorski

DLSw+ MIB Enhancements

Description: The Cisco DLSw+ MIB enhancement feature now includes more information about the "plus" features. For example, the MIB describes the encapsulation type being used: direct, Logical Link Control, type 2 (LLC2), Fast Sequenced Transport (FST), and TCP. Furthermore, for FST and direct, which use fast cache entries instead of circuits to establish sessions, the MIB now 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 did not know about the remote peer's IP address when using direct or LLC2 encapsulation. Now the remote peer's IP address is sent through the capabilities exchange and listed in the MIB. 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.

Benefits: Simplifies management for environments using alternate DLSw+ encapsulation types or other advanced DLSw+ features.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series

Product Marketing Contact: Donna Kidder, Paul Sikorski

DLSw V2

Description: Cisco Systems, Inc. is the first vendor to announce the availability of Data Link Switching that complies with the APPN Implanters Workshop (AIW) Data Link Switching (DLSw) Version 2 (V2) standard. Cisco is also introducing two new enhancements to its Data Link Switching Plus (DLSw+) offering. These enhancements extend beyond the AIW standard by increasing network performance and scalability while decreasing network response time.

The AIW V2 DLSw standard was designed to address the scalability limitations of enterprise networks handling SNA and NetBIOS traffic between branch offices. The new standard employs an Internet protocol (IP) multicast technique to forward broadcast traffic, which can greatly reduce wide-area network (WAN) traffic in networks that require branch-to-branch communication. In addition, the new standard allows DLSw routers to communicate without specifically being configured to each other, greatly simplifying the network. This feature, called peer-on-demand, was implemented in 1995 in Cisco's DLSw+, the successor to Cisco's original DLSw solution, and is now part of the AIW V2 standard.

The AIW V2 DLSw standard focuses primarily on fully meshed networks on the scalability issues. By contrast, in hierarchical networks, Cisco's DLSw+, has proven scalability in several production networks with over 1000 branch sites. Cisco's DLSw+ has been widely deployed in over 100,000 routers worldwide.

Benefits: DLSw V2 offers the following benefits:

- Enables interoperability with non-Cisco routers supporting DLSw V2
- Increases network performance and scalability while decreasing network response time
- Can greatly reduce WAN traffic in networks that require branch-to-branch communication
- Allows DLSw routers to communicate without specifically being configured to each other, greatly simplifying the network and enhancing scalability

Considerations/Platforms: This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contacts: Donna Kidder, Paul Sikorski

DLSw+ Support For Transporting LLC1 UI Traffic

Description: DLSw lightweight circuits efficiently transport LLC1 UI traffic across a DLSw network. In the current DLSw+ implementation, noncircuit LLC1 UI frames are subject to LAN input queuing, and, periodically, a specifically routed LLC1 UI frame is broadcast to all remote peers. With DLSw lightweight circuit support, LLC1 UI frame flows will not be subject to input queuing and are guaranteed to traverse the same path (peer and remote LAN) for the duration of the flow.

In traditional DLSw, circuits are created when an exchange identification (XID) or SABME is received and DLSw knows of reachability for the destination Media Access Control (MAC) address. DLSw+ LLC1 UI support extends this to start a circuit when a specifically routed LLC1 UI frame is received and DLSw knows of reachability for the destination MAC address. The circuit setup process is identical to that of traditional DLSw. A CanUReach_cs is sent to the remote peer, the remote peer responds with an ICanReach_cs, and so on.

Circuits for a UI frame flow are referred to as lightweight because there is no active LLC2 connection for the flow and the DLSw will remain in CIRCUIT_ESTABLISHED state and will not proceed to the CONNECT state. A lightweight circuit will remain in the CIRCUIT_ESTABLISHED state until there is no UI frame flow for this MAC/SAP pair for 10 minutes.


Benefits: Enables network consolidation of LLC1 traffic (such as High Performance Routing [HPR]) with multiprotocol traffic.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Donna Kidder, Paul Sikorski

APPN Scalability

Description: APPN and HPR both allow devices and applications to initiate connections independent of a controlling host. This feature is referred to as peer-to-peer connectivity. The NNs that enable this peer-to-peer connectivity maintain a database of all available partners within an APPN/HPR network. This database is updated as changes occur (additions or deletions to the network) to reflect the most current image



of the network. When an NN receives a request to establish a peer-to-peer connection, and the requested partner is not in the database, then a 'Locate (search)' is initiated. The NN can receive multiple requests for the same destination partner one after the other. If multiple requests arrive at the NN before the first Locate (search) has completed all additional requests for the same destination partner, are 'Throttled (cached)'. After the destination partner has been found and the NN's database updated, all requests for the same destination partner will be provided the necessary information to establish the peer-to-peer connection. "LocateThrottling" lets users intelligently reduce (filter) the amount of traffic over the network. The primary focus of this feature is Wide Area Networking - making best use of expensive communications lines - but also applies to campus networks.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco 7200, and the Cisco 7500.

Product Marketing Contact: Mark Denny

APPN over Ethernet and Token Ring LAN Emulation

Description: APPN over Ethernet and Token Ring LAN Emulation allows an APPN router to participate in an ATM emulated LAN environment. It leverages Cisco's support for ATM LANE over either an Ethernet or Token Ring connection. The underlying ATM infrastructure is transparent and appears to Cisco's APPN/HPR code as an Ethernet or Token Ring segment. All the functionality of APPN/HPR is fully supported. Provides large enterprise customers with the option of deploying ATM as a high-speed backbone between campus and data center networking devices. APPN/HPR is a big part of any enterprise customer's network requirements. Support for LANE (in addition to RFC 1483, Multiprotocol over ATM), provides additional flexibility in the type of networks that can be deployed. ACF/VTAM.

Benefits: APPN over Ethernet and Token Ring LANE enables an APPN network node on an Ethernet or Token Ring LAN to participate in an ATM network without changing LAN applications.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco 7200, and the Cisco 7500 series. (ACF/VTAM 4.3 and subsequent releases).

Product Marketing Contact: Mark Denny

APPN MIB

Description: Cisco implemented support for the APPN MIB defined by the AIW, replacing Cisco's own proprietary MIB definitions for APPN.

Considerations/Platforms: This feature is supported on the following platforms: The Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Mark Denny

APPN Enhancements

Description: Contains a number of enhancements that also apply to the new HPR functionality:

- *Directed Locate*—Enables APPN/HPR customers to define parts their network statically. Customers can define the path to be used when looking for certain destination APPN/HPR partners instead of looking up this information in the local topology database maintained by the NN or generating a Locate (search) for the partner.
 - Customers can make use of both Directed Locate and the dynamic nature of APPN/HPR when designing their network to control the traffic and complexity of their APPN/HPR networks
 - Assists in reducing overall traffic due to the Locates (searches) within an APPN/HPR network
 - Reducing APPN/HPR traffic enables these networks to increase in size
- *ANR Fastswitching*—Distributes HPR traffic processing to the communications interfaces, instead of passing through the central processor of the Cisco device
 - Allows intermediary HPR devices to perform message forwarding at very high speed
 - Initial support for CIP, Token Ring, and Ethernet LAN interfaces
- Locally administered address (LAA) support in the HSRP feature
- Can configure an LAA for Token Ring, Ethernet, Fiber Distributed Data Interface (FDDI) and ATM LANE configurations, all environments that support LLC 802.2
- A customer can override the burned-in address for one of the LAN adapters with an alternate address. In this situation, a customer will configure the address of an adapter in the backup router to be the same as an adapter in the primary router. Using HSRP enables the customer to ensure that APPN/HPR traffic is dynamically cut over to the backup router.

Considerations/Platforms: This feature is supported on the following platforms: The Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Mark Denny

Backup Peer Extensions for Encapsulation Types

Description: Three types of encapsulation are supported in DLSw+: direct, 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.

Benefits: Improves network availability in DLSw+ networks using alternate encapsulation types.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 2500, Cisco 3600, Cisco 4000, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Paul Sikorski

Bisync 3780 Support

Description: Cisco's Bisync 3780 support feature has been enhanced to add a user-configurable address on contention interfaces.

Benefits: Provides extended address configurability.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 2500, Cisco 25FX, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.


Product Marketing Contact: Rod Starrett

BSC Extended Addressing

Description: The Cisco Bisync support protocol stack extended addressing feature enables you 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).

Benefits: Reduces WAN costs by consolidating onto a single backbone client/server traffic and traffic from Cisco Bisync support protocol stack devices that do not support standard addresses.

Product Marketing Contact: Rod Starrett



Frame Relay Access Support (FRAS) Boundary Network Node Enhancement

Description: 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.

Benefits: The BNN enhancement feature reduces configuration complexity; one FRAS mapping statement in the router is sufficient for multiple downstream devices. Also, end-stations can be added or deleted without reconfiguring the router.

Product Marketing Contact: Paul Sikorski

FRAS Dial Backup over DLSw+

Description: FRAS dial backup over DLSw+ is an enhancement to Cisco's FRAS implementation that allows you 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+ moves existing sessions to the alternate link automatically. When the primary link is restored, existing sessions are kept on the backup connection so they can be moved nondisruptively to the primary link at the user's discretion.

Benefits: This feature provides an auxiliary route between the end stations and the host when the DLCI connection to the Frame Relay network is lost. Backup connectivity is automatic and backup sessions stay up until the user takes action.

Product Marketing Contact: Paul Sikorski

FRAS DLCI Backup

Description: FRAS data link connection identifier (DLCI) backup is an enhancement to Cisco's FRAS implementation. It lets you 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 DLCI configured.

Benefits: This feature provides an auxiliary route between the end stations and the host when the DLCI connection to the Frame Relay network is lost.

Product Marketing Contact: Paul Sikorski

FRAS MIB

Description: The FRAS 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's SNMP application.

Benefits: Simplifies management in environments using Cisco's FRAS feature.

Product Marketing Contact: Lori Bush

NetBIOS Dial-on-Demand Routing

Description: DLSw+ now filters NetBIOS session alive packets from the WAN. This feature allows you to transport NetBIOS in a 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 dial-on-demand interfaces up and this uptime causes unwanted per-packet charges in DDR networks.

Benefits: Minimizes line charges in DDR networks by disabling connections in dial-on-demand environments using NetBIOS. This feature allows you to transport NetBIOS in a 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. These packets keep dial-on-demand interfaces up, and this uptime causes unwanted per-packet charges in DDR networks. By filtering these NetBIOS session alive packets, you reduce traffic on the WAN as well as some costs that are associated with DDR.

Product Marketing Contact: Paul Sikorski

Multimedia/Voice

Stub IP Multicast Routing

Description: 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 the dense mode. It does this by using forwarded Internet Group Management Protocol (IGMP) reports as a type of join message and selective PIM message filtering.

Benefits: Reduces the configuration and administrative burden when multicast is used in stub (that is, leaf) network segments.

Considerations/Platforms: This feature is supported on these platforms: Cisco 1003/4, Cisco 1005, Cisco 1600, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Erik Gilbert

IP Multicast over ATM Point-to-Multipoint Virtual Circuits

Description: This feature dynamically creates ATM point-to-multipoint SVCs as part of a multicast tree to handle IP multicast traffic more efficiently, allowing more efficient support to IP multicast over ATM networks.

Benefits: Can enhance router performance and link utilization because packets are not replicated and sent multiple times over the ATM interface.

Considerations/Platforms: This feature can be configured only on an ATM interface. This feature is supported on the following platforms: Cisco 4500, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Erik Gilbert

IP Multicast over Token Ring LANs

Description: Prior to this feature, IP multicast datagrams used the MAC-level broadcast address 0xFFFF.FFFF.FFFF, placing 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. 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.

Benefits: 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 process these packets.

Considerations/Platforms: 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, it is possible that other protocols are 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. This feature is available on the following platforms: Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Erik Gilbert

IP Multicast Load Splitting across Equal-Cost Paths

Description: If you have a tunnel configured with equal-cost paths to the tunnel endpoint, IP multicast traffic now automatically load splits across the physical interfaces. Prior to this feature, 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 a unicast load-splitting mechanism for the tunnel (multicast) traffic.

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

Benefits: By configuring load splitting among equal-cost paths, you can use your links between routers more efficiently when sending IP multicast traffic.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 1003/4, Cisco 1005, Cisco 1600 series, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Erik Gilbert

Management

SNMPv2C

Description: 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. Cisco IOS software will continue to support SNMPv1.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 1003/4, Cisco 1005 series, Cisco 2500, Cisco 3600, Cisco 4000, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Tom Tinor

IPX Named Access Lists

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

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

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

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

Considerations/Platforms: Consider the following before configuring IPX named access lists:

- Access lists specified by name are not compatible with releases prior to Release 11.3
- Access list names must be unique across all protocols
- Numbered access lists are also available, as described in the Release 11.2 Network Protocols Configuration Guide, Part 2

This feature is supported on the following platforms: Cisco 1003/4, Cisco 1005, Cisco 2500, Cisco 25FX, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Roger Farnsworth

Cisco Call History MIB Command-Line Interface

Description: Beginning with Cisco IOS release 11.3, a Cisco IOS software 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:

- Cisco Call History Table Max Length
- Cisco Call History Retain Timer
- 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 command-line interface is enabled by default.

Benefits: This feature provides CLI setting of parameters

Considerations/Platforms: This feature is supported on the following platforms: Cisco 1003/4, Cisco 1005 series, Cisco 1600 series, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, and the Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Tom Tinor

Cisco IOS Internationalization

Description: The Cisco IOS internationalization feature allows you to use HTML server side includes (SSIs) to customize international or noninternational HTML pages used for the Cisco Web browser interface (for example, ClickStart™ pages) and store them in Flash memory on multiple Cisco IOS platforms. In addition, this feature allows you to display 8-bit or multibyte international character sets (for example, 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.

Benefits: Simplifies creation and customization of Web pages for international use.

Considerations/Platforms: This feature is supported on these platforms: Cisco 1003/4, Cisco 1005, Cisco 1600, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Tom Tinor

Entity MIB, Phase 1

Description: 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. This 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.

Considerations/Platforms: This feature is supported on these platforms: Cisco 1003/4, Cisco 1005 series, Cisco 1600 series, Cisco 2500, Cisco 25FX series, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Tom Tinor

Frame Relay MIB Extensions

Description: 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.

Benefits: Provides improved network management granularity for Frame Relay.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 1005, Cisco 1600, Cisco 2500, Cisco 25FX, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.


Product Marketing Contact: Sanjay Bhardwaj

ATM MIB Enhancements

Description: Cisco AAL5 MIB adds a Cisco extension to the standard ATM MIB (RFC 1695) to provide per-VC statistic counters that are currently displayed in response to the Cisco IOS show atm vc vcd command 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.

The Cisco AAL5 MIB provides SNMP access to four new statistic counters defined for AAL5 virtual connections: incoming packet counter, outgoing packet counter, incoming octet counter, and outgoing octet counter. The Cisco AAL5 MIB groups these four counters in a table called cAal5VccTable.



Benefits: With the ATM MIB Enhancement feature, SNMP network Management system applications now have SNMP access to per-Virtual Circuit (VC) traffic flow statistics. Such information is ideal to assist in traffic profiling, network planning, and accounting at of individual ATM virtual circuit connections.

Platforms/Considerations: This feature is supported on these platforms: Cisco 4500 and the Cisco 7500 series with AIP

Product Marketing Contact: Keith Travis

LANE Per-subinterface Debug Messages

Description: This feature allows you to limit debug messages to those related to a particular subinterface.

Benefits: 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.

Platforms/Considerations: This feature is supported on these platforms: The Cisco 4500 and 7500 series

Product Marketing Contact: Keith Travis

Quality of Service

RTP Header Compression

Description: Real-time Transport Protocol (RTP) is a protocol used for carrying packetized audio and video traffic over an IP network. 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 IP/UDP/RTP 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 IP/UDP/RTP header without compressing it.

The RTP header compression feature compresses the IP/UDP/RTP 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.

Benefits: Using RTP header compression can benefit both telephony voice and multicast backbone (MBONE) applications running over slow links. 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 (for example, compressed audio payloads of 20 to 50 bytes). Although the some types of RTP traffic have higher payload sizes (for example, MBONE style traffic), compact encodings such as Code Excited Linear Prediction (CELP) can also help considerably.

Considerations/Platforms: RTP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. It is also supported over ISDN interfaces. This feature is implemented on the following platforms: Cisco 1003/4, Cisco 1005 series, Cisco 1600, Cisco 2500, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

Product Marketing Contact: Erik Gilbert

Frame Relay Router ForeSight

Description: ForeSight[®] is the network traffic control software used in Cisco StrataCom switches. The Cisco StrataCom Frame Relay switch can extend ForeSight messages over a User-to-Network Interface (UNI). 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. When ForeSight is enabled, a ForeSight message is periodically sent out. When a Cisco router receives a ForeSight message indicating that certain DLCIs are experiencing congestion, the Cisco router reacts by activating 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. The difference between the BECN and ForeSight methods is that BECN requires a user packet to be sent in the direction of the congested DLCI to convey the signal.

Benefits: Frame Relay Router ForeSight provides an improved mechanism for managing network traffic. It also allows Cisco routers to react to StrataCom ForeSight backward congestion notification messages. Provides guaranteed notification of traffic congestion.

Considerations/Platforms: The Router Foresight feature must be configured explicitly on both the Cisco router and the Cisco StrataCom switch. This feature is supported on the following platforms: Cisco 1005, Cisco 1600, Cisco 2500, Cisco 25FX, Cisco 3600, Cisco 4000, Cisco 4500, Cisco AS5200, Cisco 7200, and the Cisco 7500 series.

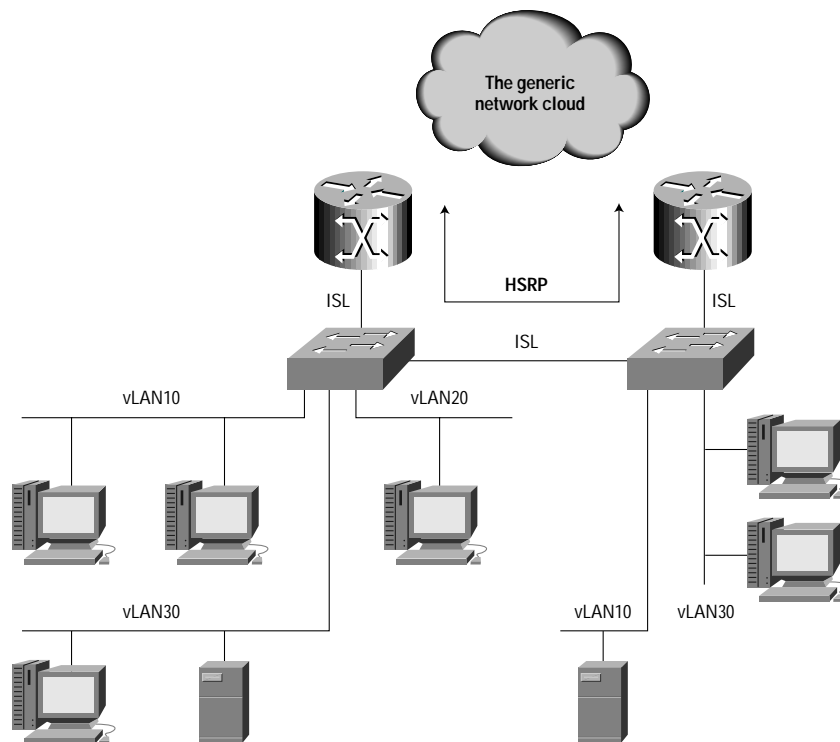
Product Marketing Contact: Sanjay Bhardwaj

Reliability

HSRP over ISL

Description: The Hot Standby Router Protocol (HSRP) is a Cisco innovation which provides excellent fault tolerance and enhanced routing performance for IP networks. HSRP allows Cisco IOS routers to monitor each other's operational status and very quickly assume packet forwarding responsibility should the current forwarder in the HSRP group fail or be taken down for maintenance. This mechanism remains transparent to the attached hosts and can be deployed on any LAN type. With Multi-Group Hot Standby, routers can simultaneously provide redundant backup and perform load-sharing across different IP subnets.

Figure 11 HSRP over ISL



Cisco IOS vLAN routers are able to take advantage of mHSRP for vLAN subnets defined via IEEE 802.10 on FDDI and ATM LAN Emulation for Ethernet starting from software release 11.2. With Cisco IOS 11.3, mHSRP can be deployed in conjunction with ISL vLANs.

Benefits: Fully redundant vLAN routing for IP in ISL switched environments.

Platforms/Considerations: HSRP for vLANs is available across any IOS platform capable of supporting Fast Ethernet, ATM or FDDI trunking media.

This feature is supported on the following platforms: Cisco 3600, Cisco 4500, Cisco 7200, and the Cisco 7500 series.

Product Marketing Manager: Martin McNealis



Please forward any questions, comments or feedback to Cisco IOS Software Release Product Manager, Ginny Vincenzini at ginnyv@cisco.com.

CISCO SYSTEMS



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
<http://www-europe.cisco.com>
Tel: 33 1 6918 61 00
Fax: 33 1 6928 83 26

Americas

Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters

Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
<http://www.cisco.com>
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco Connection Online Web site at <http://www.cisco.com>.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China (PRC) • Colombia • Costa Rica • Czech Republic • Denmark • England • France • Germany • Greece • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Russia • Saudi Arabia • Scotland • Singapore • South Africa • Spain • Sweden • Switzerland • Taiwan, ROC • Thailand • Turkey • United Arab Emirates • United States • Venezuela