

Cisco IOS Software Release 11.3T New Features

Introduction

This product bulletin describes new features introduced into Cisco IOS Release 11.3T.

11.3T is an Early Deployment (ED) release. This release is focused on delivering new features and platforms to market, and has greater unknowns than a more mature, Major Release. As such, it should only be used for initial “point” deployment of new features. Any ED release of software should be utilized first in a test network before being deployed in a production network.

The functionality delivered with this ED release will be incorporated in a subsequent Major Release. For more information about the Cisco IOS software release process, please see Product Bulletin #537.

Cisco strongly recommends that customers select and deploy “General Deployment” release versions of software for fundamental network infrastructure. A software release reaches the “General Deployment” (“GD”) milestone when Cisco feels it is suitable for general deployment anywhere in customer networks where the features and functionality of the release are required. These contain less unknowns and are more time proven versions of software which 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 utilized in a test network before being fully deployed in a production network.

Feature Summary

Security

IP Security (IPSec)

Description: IPSec is a framework of open standards for ensuring secure private communications over the Internet. Based on standards developed by the Internet Engineering Task Force (IETF), IPSec ensures confidentiality, integrity and authenticity of data communications across a public network. IPSec provides a necessary component of a standards-based, flexible solution for deploying a network-wide security policy.

Benefits: Customers that use Cisco’s IPSec will be able to secure their network infrastructure without costly changes to each and every computer. If a customer deploys IPSec in their network, applications gain privacy, integrity, and authenticity controls without affecting individual users or applications. Application modifications are not required, eliminating the need to deploy and coordinate security on a per application, per computer, basis. This provides great cost savings, as only the infrastructure needs to be changed.

IPSec provides an excellent remote user solution. Remote clients will be able to use an IPSec client on their PC in combination with L2TP to connect back to the enterprise network. The cost of remote access is decreased dramatically, and the security of the connection actually improves over that of dial-up lines.

Platforms/Considerations/Caveats: 1600, 2500, 2600, 3600, 4000, 4500, 5300, 7200, 7500

IPSec will not work with distributed switching on a VIP on a 7500 router. With a VIP installed, all IPSec processing will be done by the RSP.

The Encryption Service Adapter (ESA) does not support IPSec. The ESA supports Cisco Encryption Technology. A new hardware acceleration option for IPSec will be available later.

Product Marketing Contact: Terry Bernstein

Cisco IOS Firewall Feature Set

Cisco IOS security services include an array of features that enable managers to configure a Cisco router as a firewall. The Cisco IOS Firewall feature set adds greater depth and flexibility to existing Cisco IOS security solutions.

New Firewall Features:

- *Context-based access control (CBAC)*—Provides internal users secure, per-application-based access control for all traffic across perimeters, e.g. between private enterprise networks and the Internet
- *Java blocking*—Protects against unidentified, malicious Java applets
- *Denial of Service detection/prevention*—Defends and protects router resources against common attacks; checks packet headers and drops suspicious packets
- *RealTime alerts*—Logs alerts in case of denial-of-service attacks or other pre-configured conditions.
- *Audit trail*—Details transactions; records time stamp, source host, destination host, ports, duration and total number of bytes transmitted
- *ConfigMaker support*—A Windows95/WindowsNT-Wizard based network configuration tool that offers step-by-step guidance through network design, addressing and Firewall feature set implementation.

Benefits:

- *Flexibility*—All-in-one solution can perform routing, provide secure Internet connectivity, and apply distinct security characteristics according to a user-defined policy to each interface on a per-user or per-application basis.
- *Investment Protection*—Integrating firewall functionality into a multiprotocol router leverages an existing router investment.
- Routers are usually deployed to separate sensitive network segments and manage private/public network interfaces. The incremental change saves costs and management training associated with learning a new platform.
- *Easier management*—With remote management capabilities, a network administrator can implement security features from a central console over the network.
- *Seamless interoperability*—Use with other Cisco IOS software features, optimize, WAN utilization, provide robust, scalable routing, and interoperate with existing Cisco IOS-based networks (such as the Internet).

Platforms/Considerations: Cisco 1600 and 2500 series routers.

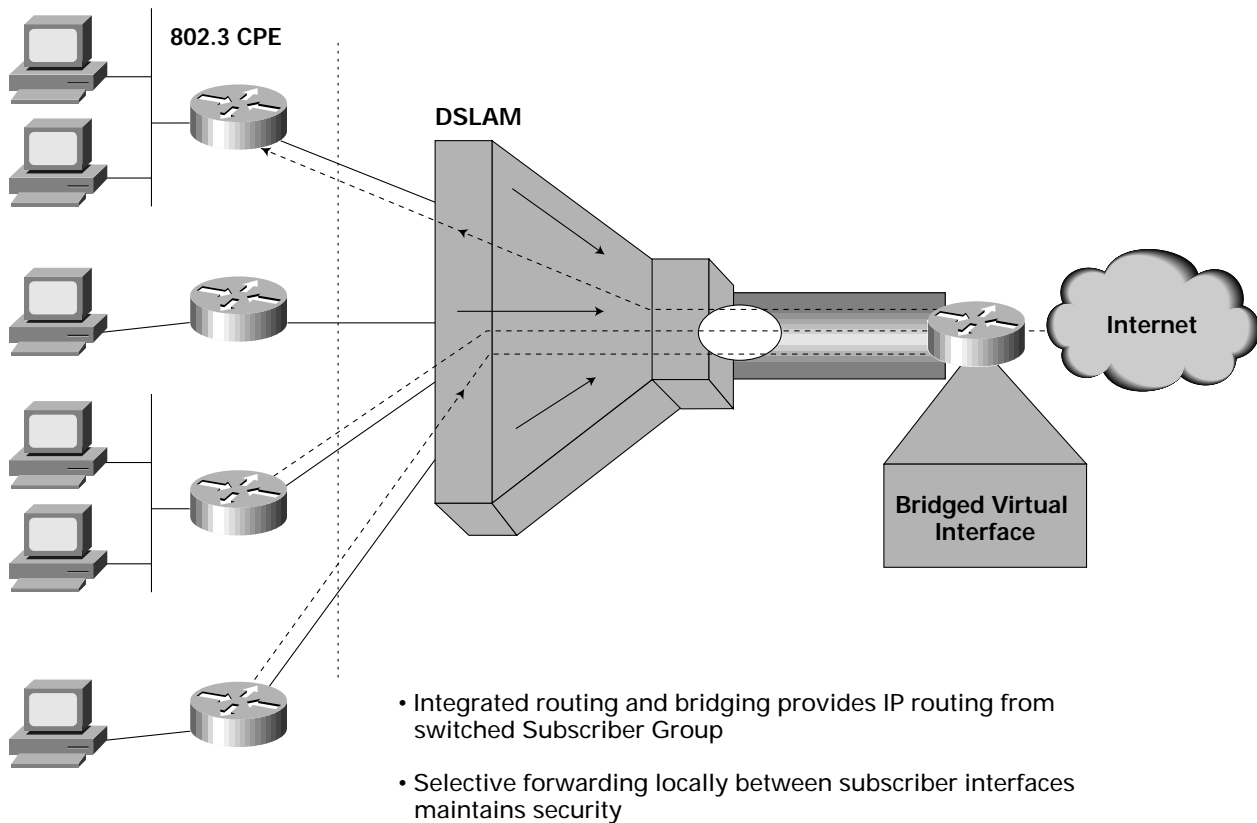
Product Marketing Contact: Jocelyne Okrent

OoS

x Digital Subscriber Line Bridge Support

Description: This feature enables an IOS platform acting as a Local Access Concentrator in a DSL environment to apply selective forwarding policy to traffic between subscribers. Typically it is deployed in conjunction with IOS Integrated Routing and Bridging (IRB) (refer to Product Bulletin 487) in an upstream routing/downstream bridging paradigm.

Figure 1 DSL Subscriber Group Support



Benefits: This provides security and enhanced performance since it contains the flooding of traffic at Layer2 between subscribers that are members of the same “*Subscriber Group*” and in particular the default subscriber policy behavior is to apply filtering intelligence to common traffic types such as ARP, Unknown Unicast, Multicast, Broadcasts etc.

Platforms: DSL Subscriber Bridging Support is available across Cisco 1000, 1600, 2500, 3600, 4x00, 5500, 7200 and 7500 IOS platforms.

Product Marketing Contact: Martin McNealis

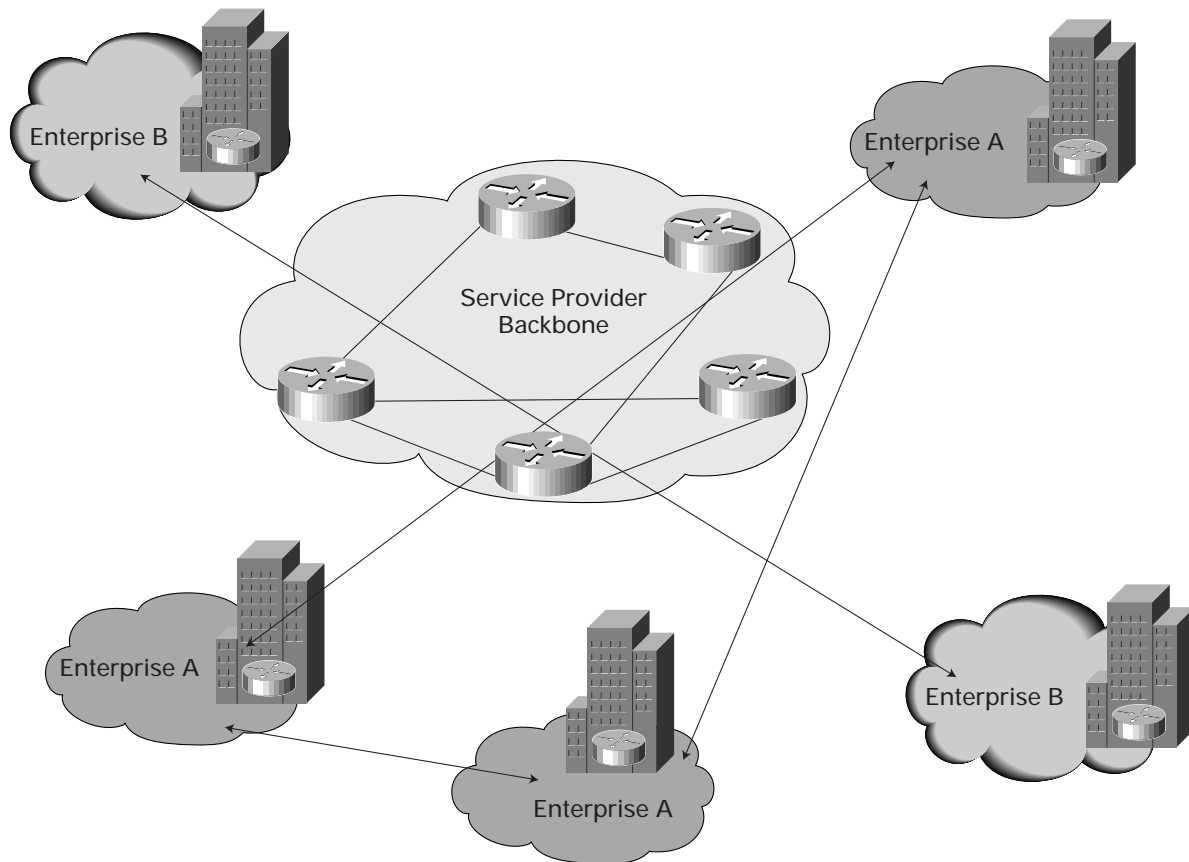
Connectivity

GRE Precedence

Description: This IOS feature integrates IP based Virtual Private Networking (VPN) technology with Layer 3 Quality-of-Service techniques.

VPNs implemented via Generic Route Encapsulation (GRE) tunneling enable overlay topologies to be defined across a common backbone network such as the Internet. This typically allows Enterprises to cost-effectively and securely communicate with other member sites as shown:

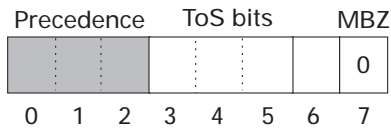
Figure 2 IP Type-of-Service Octet



And since traffic between sites is fully encapsulated, this VPN mechanism allows Enterprises the flexibility to use registered or unregistered IP addressing ranges for traffic transiting the backbone. GRE is defined in RFC1701 and RFC1702.

However in order to ensure that business critical traffic is expedited or that real-time applications receive predictable performance across the common backbone, QoS is required and in large network environments this is best delivered at Layer 3 via an enhanced IP transport since it inherently provides an end-2-end service and can be configured to differentiate between the needs of different applications and/or users. Cisco's comprehensive IOS Quality-of-Service architecture encompasses prioritized switching, smart queuing, traffic shaping and sophisticated congestion management. These mechanisms are influenced via the "IP Precedence" values associated with the Type-of-Service field in the IP header:

Figure 3 IP Precedence Reservation with GRE Encapsulation



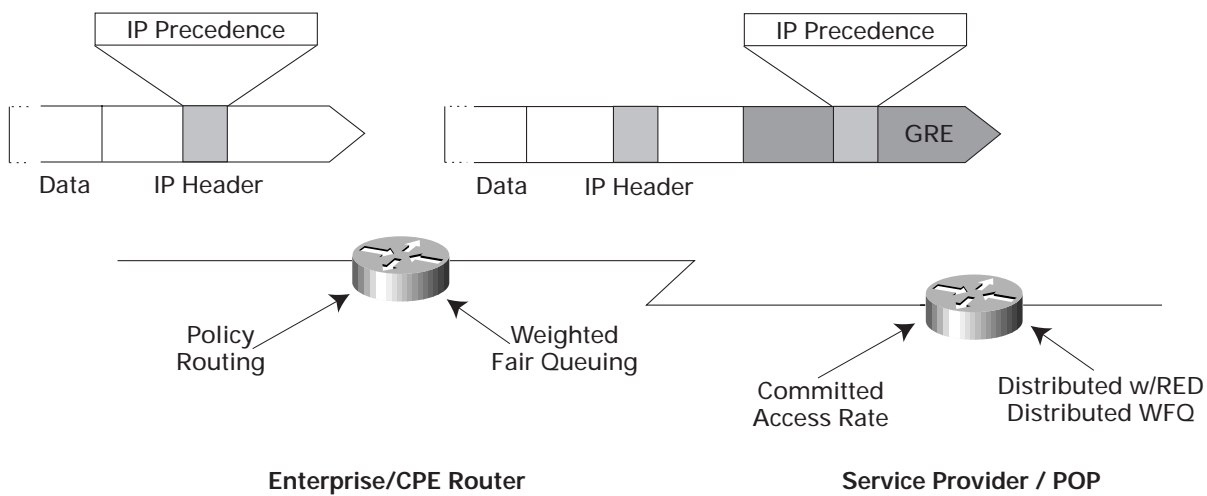
Type-of-Service bits designed to specify:

- Delay
- Throughput
- Reliability
- Cost

MBZ - 'Must be zero'

Therefore in order to have the QoS benefits apply to traffic flows transported across a GRE VPN tunnel the IOS now also carries the IP Precedence associated with received traffic flows in the GRE encapsulation. Optionally, the IOS router initiating the tunnel can classify ingressing traffic and set the appropriate Precedence value to drive upstream QoS mechanisms as shown:

Figure 4



and setting the Precedence bits can be achieved via complementary IOS functionality such as Policy Routing, Committed Access Rate or BGP Policy Propagation.

Benefits:

- Leverages existing IOS Quality-of-Service technology, e.g. Committed Access Rate, Weighted Fair Queuing, Policy Routing, Weighted Random Early Detection etc.
- IP addressing flexibility with Layer3 GRE VPNs.
- Security—IOS Network Layer Encryption can be used in conjunction with GRE Precedence to provide data confidentiality between VPN tunnel endpoints.
- QoS Policy granularity, e.g. per network, per user, per application etc.
- Deployment flexibility, i.e. applicable at Enterprise CPE or Service Provider ingress point.

Platforms: GRE Precedence is available across the Cisco C1600, C2500, C3600, C4x000, AS5x00, C5x00, C7x00 and C8500 IOS platforms.

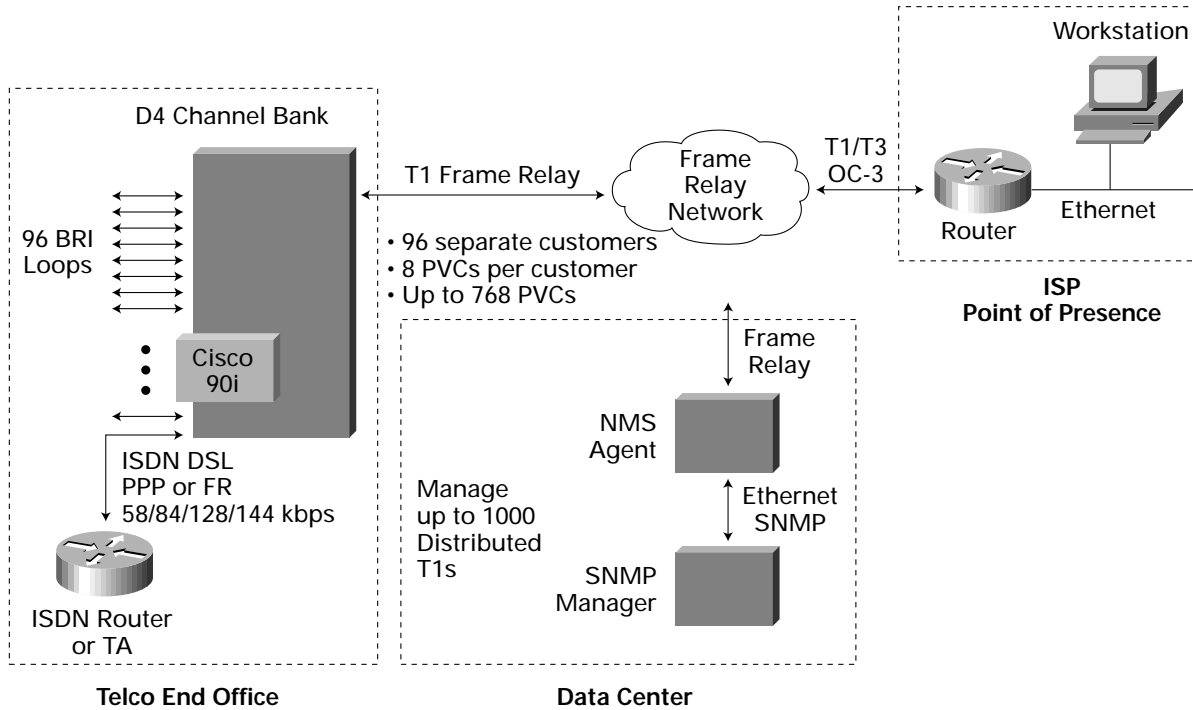
Product Marketing Contact: Martin McNealis

PPP over Frame Relay (rfc 1973)

Description: RFC 1973 defines a standardized method for transporting Point-to-Point Protocol (PPP) packets over a Frame Relay infrastructure.

This feature is especially important to the Cisco 90i IDSL product. This product accepts either a PPP or a Frame Relay connection over IDSL from a router or TA which supports leased line mode ISDN. The 90I resides in a D4 Channel bank in a CO environment with a Frame Relay backhaul to an ISP or corporate customers network. If the customer requires PPP services such as authentication, compression or encryption then it is a requirement that the router which terminates the Frame Relay link supports standards based PPP over Frame Relay.

Figure 5 A Typical Cisco 90i Environment



Benefits: Service providers offering IDSL services would prefer to use PPP access as most of their corporate customers wish to take advantage of the standardized facilities PPP offers in terms of authentication, compression etc.

It is also true that the majority of low-cost customer premises equipment which can be used with IDSL services supports PPP but not Frame Relay. Support for PPP over Frame Relay at the head-end of the network increases the market opportunity for service providers dramatically.

Considerations/Platforms:

- Only Frame Relay PVC's are supported
- IP is the only supported protocol
- Fast-switching must be used
- The only queuing method supported is FIFO

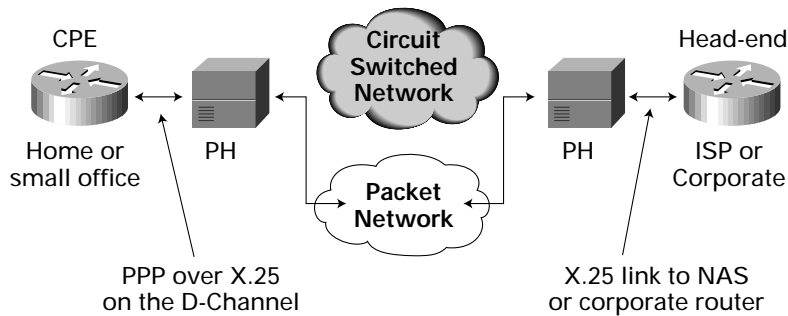
PPP over Frame Relay is supported on the 4000, 7200 and 7500 platforms.

Product Marketing Contact: Kevin Dickson

Always On/Dynamic ISDN (AO/DI)

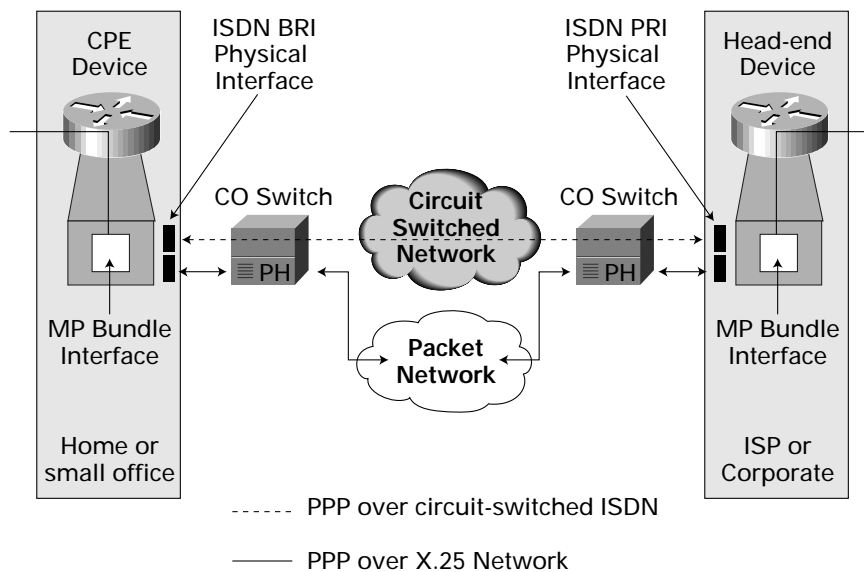
Description: Always On/Dynamic ISDN (AO/DI) is a new access connectivity solution which draws on the strengths (and tariff structures) of both packet and circuit switched networks in order to provide more efficient dial-up connectivity. Both D and B-Channel ISDN connections are used depending on the bandwidth requirements of the data being transferred at any time. The initial connection with this service is always a D-Channel X.25 long-hold switched virtual circuit call. However it is important to recognize that this X.25 connection is only a transport mechanism for the first PPP link in a Multilink Protocol (MP) bundle. When extra bandwidth is required a circuit-switched B-Channel call is made and this becomes the second link in the MP bundle. When traffic falls back to low levels the B-Channel call will be dropped and traffic will once again only use the Always On D-Channel connection.

Figure 6 The "Always On" Connection



- Initial "Always On" connection uses D-Channel and packet network
- Low-speed leased line (9.6 Kbps)
 - uses PPP over X.25 (rfc 1598)
 - first link in a MP "bundle"

Figure 7 B & D -Channels in Unison



Description (continued): Note that whilst circuit-switched calls are up MP will not load share over the D-Channel link. This link remains up but is "idled" out of use. Traffic will once again use this link once all circuit-switched calls have ended.

Benefits: A good proportion of Internet traffic is still low speed in nature. For example, downloading email in most instances does not require the full bandwidth of an ISDN B-Channel. Using an AO/DI service may provide cost savings over regular ISDN services in areas where B-Channel connection tarrifing is based on per-minute charging.

AO/DI reduces costs by increasing NAS port efficiencies.

Although this is a potential new service there are no new management or security considerations. All existing AAA functions in place for regular dial-up services can be utilized with AO/DI.

Platforms/Considerations: AO/DI services are still in their infancy. Many telcos do not have a tariffed offering for X.25 on the D-Channel.

Where ISDN Tariffing is flat rate there is no benefit to the consumer and only minor benefit to the owner of the Network Access Server pool. In this instance AO/DI may not be an appropriate solution to pitch.

Product Marketing Contact: Kevin Dickson

Multiple ISDN Switch Types


Description: The Multiple ISDN Switch Types feature allows you to configure more than one ISDN switch type per router. You can apply an ISDN switch type on a per interface basis, thus extending the existing global ISDN switch-type command to the interface level. This allows Basic Rate Interfaces (BRI) and Primary Rate Interfaces (PRI) to run simultaneously on platforms that support both interface types.

Table 1 ISDN Switch Types Summary

| Vendor | Signaling | Software | Country |
|----------------|-----------|-------------|--------------------------------------|
| Lucent 4ESS | PRI | Custom | North America |
| Nortel DMS 250 | PRI | Custom | North America |
| Nortel DMS 100 | PRI | Custom | North America |
| Nortel DMS 100 | BRI | NI | North America |
| Lucent 5ESS | PRI & BRI | Custom & NI | North America |
| AGCS GTD-5 | PRI | NI | North America |
| | BRI | NET 3 | Asia, Europe, New Zealand, Australia |
| | PRI | NET 5 | Asia, Europe, New Zealand, Australia |
| | PRI & BRI | NTT | Japan |
| | BRI | 1TR6 | Germany |
| | BRI | TS013 | Australia |
| | PRI | TS014 | Australia |

Benefits: Multiple ISDN Switch Types provides the following advantages:

- Allows you to use ISDN BRI and PRI simultaneously on the same Cisco platform.
- Allows you to add ISDN switch types per interface.
- Allows you to change the ISDN switch type without reloading the router.
- Allows you to use existing ISDN global configuration commands. The first time a switch type is added to an interface, the new value is read in and propagated to the interface level.



Platforms/Considerations: The Multiple ISDN Switch Types feature is supported on the following platforms:

- Cisco 3600 series
- Cisco 4000 series
- Cisco 5200
- Cisco 5300
- Cisco 7200 series
- Cisco 7500 series

The following restrictions apply to Multiple ISDN Switch Types:

You must configure a global ISDN switch type using the existing `isdn switch-type` global configuration command before you can configure the ISDN switch type on an interface.

Product Marketing Contact: Anita Freeman

National ISDN Switch Type for Primary Rate Interfaces

Description: National ISDN Switch Type for Primary Rate Interfaces introduces changes to ISDN switch types for Primary Rate Interfaces (PRI) by adding a the new switch type for PRI interfaces, National ISDN Primary Rate Interface (Bellcore SR3887, November, 1996). This feature also adds the ability to configure outgoing PRI B channel selection for the T1 controller in ascending order (channel 1 to channel 23) or descending order (channel 23 to channel1). Previously, the router selected a B channel for outgoing calls from the highest free channel in descending order. The E1 controller channel selection for ascending order is channel 1 to 31, and 31 to 1 for descending order.

Benefits: National ISDN Switch Types for Primary Rate Interfaces provides the following benefits:

- Unlike previous custom implementations, such as `primary-5ess`, and `primary-dms100`, the National ISDN specification is designed to be switch independent. This increases flexibility in adapting to evolving standards and future enhancements.
- The National ISDN for PRI feature addition completes Cisco IOS support for the compliment of switch types for ISDN PRI deployed in the United States public switched network. The Cisco IOS implementation of National ISDN PRI was certified by Bellcore to National ISDN Primary Rate Interface, SR3887, Issue 1, November 1996.
- Included in this feature is the highly demanded support of National ISDN PRI on the Lucent 5ESS and the AGCS GTD-5 switches.
- The ability to select PRI B channel order election for outgoing calls allows extended flexibility and compatibility with a variety of ISDN switch type service implementations. Additionally, this ability reduces ISDN switch misconfigurations, which can delay initial service activation.

Platforms/Considerations: The National ISDN Switch Types for Primary Rate Interfaces feature is supported on the following platforms:

- Cisco 3600 series
- Cisco 4000 series
- Cisco 5200
- Cisco 5300
- Cisco 7200 series
- Cisco 7500 series

The following restriction applies to National ISDN Switch Types for Primary Rate Interfaces:

The Nx64 multirate feature in National ISDN Primary Rate Interface, SR3887, Issue 1, November, 1996 is not supported.

Product Marketing Contact: Anita Freeman

NFAS with D Channel Back Up

Description: The Nortel DMS250, Nortel DMS100 and National ISDN switch types have been added to the existing Non-Facility Associated Signaling (NFAS) with D Channel Backup feature.

ISDN NFAS allows a single D channel to control multiple PRI interfaces. A backup D channel is configured for use when the primary NFAS D channel fails.

An NFAS group is a 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. Cisco IOS supports ten PRI interfaces in an NFAS group with a primary D channel and a backup D channel. Five NFAS groups are supported in a single chassis.

Table 2 NFAS Summary

| Switch Type | Type of NFAS | Release |
|----------------|------------------------------|----------|
| Lucent 4ESS | Custom | 11.3 |
| Nortel DMS 250 | Custom | 11.3 |
| Nortel DMS 100 | Customer | 11.3 |
| Lucent 5ESS | Custom-Does not support FNAS | -- |
| Lucent 5ESS | National ISDN | 11.3(3)T |
| AGCS GTD-5 | National ISDN | 11.3(3)T |

Benefits:

- Use of a single D channel to control multiple PRI interfaces can free one B channel on each PRI interface to carry other traffic.
- On the Nortel DMS100, when the single D channel is shared, multiple PRI interfaces may be configured in a single trunk group. The additional use of alternate route indexing, a DMS100 feature that provides a rotary from one trunk group to another, enables the capability of building large trunk groups in the public switched network.
- Any hard failure causes a switchover to the backup D channel and currently connected calls remain connected.

Platforms/Considerations: The NFAS with D Channel Backup feature is supported on these platforms:

- Cisco 3600 series
- Cisco 4000 series
- Cisco 5200
- Cisco 5300
- Cisco 7200 series
- Cisco 7500 series

NFAS is supported when there is an ISDN PRI capable channelized T1 controller. The router must connect to Lucent 4ESS, Nortel DMS250, Nortel DMS100, or National ISDN PRI switches.

Product Marketing Contact: Anita Freeman

Dialer Watch

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

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

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

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

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

Benefits: Dialer Watch provides the following advantages:

- *Routing*—Backup initialization is linked to the dynamic routing protocol, rather than a specific interface or static route entry. Therefore, both primary and backup interfaces can be any interface type, and they can be used across multiple interfaces and multiple routers. Likewise, Dialer Watch relies on convergence, which is sometimes preferred over traditional DDR links.
- *Nonpacket semantics*—Dialer Watch does not exclusively rely on interesting packets to trigger dialing. The link is automatically brought up when the primary line goes down without postponing dialing.
- *Dial backup reliability*—DDR redial functionality is extended to dial indefinitely in the event that secondary backup lines are not initiated. Typically, DDR redial attempts are affected by enable-timeouts and wait-for-carrier time values. Intermittent media difficulties or flapping interfaces can cause problems for traditional DDR links. However, Dialer Watch automatically reestablishes the secondary backup line on ISDN, synchronous, and asynchronous serial links.

Considerations/Platforms: This feature is supported on these platforms: Cisco 1000 series, Cisco 1600 series, Cisco 2500 series, Cisco 3600 series, Cisco 4000 series, Cisco 4500 series, Cisco 5200, Cisco 5300, Cisco 7200 series, and the Cisco 7500 series

Product Marketing Manger: April Chou

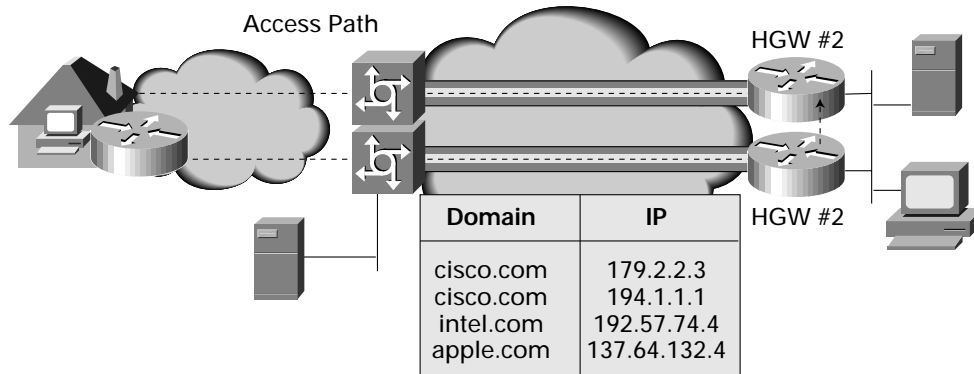
Scalability

Cisco VPDN Enhancements

L2F Stacking Home Gateways

Description: The feature permits Multilink PPP links from a single client to terminate physically at different Home Gateways while logically appearing to terminate at a single Home Gateway. This feature is a superset of the L2F load sharing feature which was available in 11.3. If the B channel calls are tunnel across different L2F tunnels and terminating at different Home Gateways, these fragmented packets are reassembled at the Home Gateway which was determined via Stack Group Bidding Protocol (SGBP).

Figure 8 L2F Stacking Home Gateways



Benefits: Organizations can scale access bandwidth by adding new devices to the MMP pool. Home Gateway Load sharing is now possible with Multilink PPP.

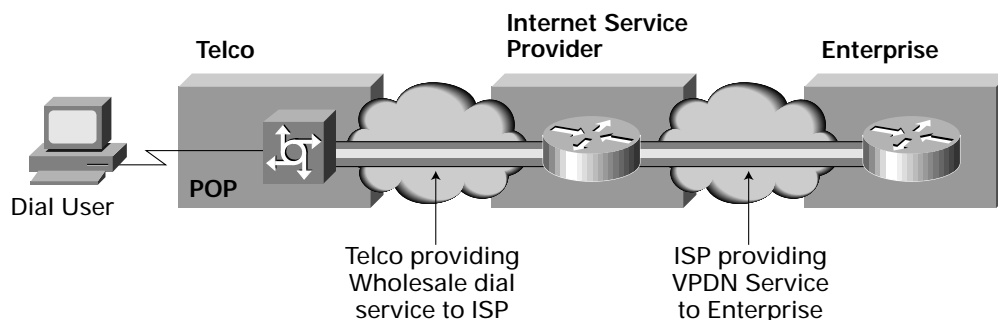
Platforms/Considerations: This feature is supported on Cisco 1000, 1600, 2500, 3600, 4000, 4500, 4700, 5200, 5300, 7200, and 7500 series. The Configuration of L2F load sharing must be done on the AAA server. The stacking Home Gateway feature is available in 11.3(3)T.

Product Marketing Contact: April Chou

L2F Multihop Support

Description: This feature will allow an extension of a L2F tunnel from a Home Gateway (tunnel termination point) to another Home Gateway. PPP is forwarded from the first Home Gateway to the Home Gateways where the tunnel is extended, in this sense the intermediate Home Gateway can be considered as an IP forwarder.

Figure 9 L2F Multihop Support



Benefits: A service provider has the ability to provide wholesale dial service to another service provider who then provides VPDN service to an Enterprise Corporation. For example, a Telco is providing wholesale dial services to an ISP. The ISP provides the virtual private dial-up network to an Enterprise Corporation. In this case, a L2F tunnel will be built to the ISP Home Gateway. This L2F tunnel will be extended to the Enterprise Corporation's Home Gateway, when remote users are trying to reach their Enterprise headquarters.

The benefit for the Telco is creating a new source of revenue in wholesale dial services while benefiting from the result of redirecting data traffic from a voice network, thus reducing network congestion. The benefits for ISPs are lowering the continuous investment in remote access equipment and concentrate on providing value-added services such as VPN services. The Enterprise Corporation also benefits by receiving the virtual private network services from an ISP.

Platforms/Considerations: This feature is supported on the Cisco 1000, 1600, 2500, 3600, 4000, 4500, 4700, 5200, 5300, 7200, and 7500 series platforms. The maximum tunnel extension is 4. This number is set to 4 in order to avoid recursive routing loops as well as to prevent a PPP time-out condition. Multihop or tunnel extension within the same stackgroup is not allowed. The VPDN tunnel configuration is also required on the intermediate Home Gateway either locally or via RADIUS server. This feature is supported in 11.3(3)T.

Product Marketing Contact: April Chou

ATM PVC Management

Description: The ATM PVC Management feature set includes new and enhanced capabilities that allow you to create and manage ATM PVCs and SVCs with more ease and improved integrity. This feature set includes the following five subfeatures:

New VC Configuration

The New VC Configuration subfeature allows you to create ATM permanent virtual circuits (PVCs), switched virtual circuits (SVCs), static maps, and associated virtual circuit (VC) parameters more easily and with fewer errors using new ATM commands in new VC command modes.

VC Integrity Management

The VC Integrity Management subfeature allows you to manage your ATM PVCs and SVCs so that you receive immediate notification of when these VCs come down in your network. Upon notification, protocols can reroute ATM packets and prevent unpredictable and relatively long timeout periods.

PVC Discovery

The PVC Discovery subfeature allows you to enable your router to automatically assign or 'discover' PVCs on an ATM interface or subinterface using information from an attached adjacent switch.

Multiprotocol Inverse ARP

The Multiprotocol Inverse ARP subfeature allows you to enable a dynamic protocol mapping between an ATM PVC and a network addresses by configuring Inverse Address Resolution Protocol (Inverse ARP) on ATM PVCs running IP or IPX.

Rate Queue Tolerance

The Rate Queue Tolerance subfeature allows you to configure a range of peak rates on a single rate queue, thereby improving ATM rate queue usage.

Benefits: Use the ATM PVC Management feature set to simplify and expedite PVC and SVC configurations and improve the management of PVC and SVC integrity. The benefits of this feature set include:

- Simplified ATM PVC, SVC, and static map configuration.
- VC management that detects connections and disconnections of PVCs and SVCs immediately, so that ATM packets are rerouted upon notification.
- Automatic assignment or 'discovery' of ATM PVCs on an ATM interface or subinterface using information from an attached adjacent switch.

- Dynamic protocol mapping between a PVC and a network address so that you no longer have to manually configure an ATM static map.
- Improved rate queue usage when you configure a range of peak rates on a single rate queue.

Considerations/Platforms: This feature is supported on the following platforms: Cisco 4500 and 4700, Cisco 7200 series, and the Cisco 7500 series. ATM rate queue tolerance is not supported on the Cisco 7200 series.

Product Marketing Manger: Keith Travis

IBM

Cisco Database Connection

Description: Cisco Database Connection turns a Cisco router into a high-speed, data-access device by enabling client-based, Open Database Connectivity (ODBC) applications using TCP/IP to connect to IBM's family of DB2 relational databases.

Benefits: This standards-based solution is easy to manage, provides complete fault tolerance, reduces expensive CPU utilization on the host, and maximizes users' IT investments by taking advantage of distributed processing and standard communication protocols. Furthermore, it offers the following benefits:

- *Leverages existing TCP/IP network*—Because Database Connection converts DRDA packets over TCP/IP to DRDA packets over APPC (LU 6.2) you can leverage TCP/IP in your enterprise.
- *Improves manageability*—You can manage enterprise-wide access to DB2 from a single centralized location within the data center.
- *Maximizes computer resources*—Database Connection takes advantage of distributed processing and standard communication protocols and reduces CPU utilization on the host.
- *Eliminates special software*—Database Connection works on your router without the need for any special software on the IBM host. It allows ODBC clients to connect to IBM's DB2 relational databases using TCP/IP without the need for communication packages on the desktop. Database Connection supports ODBC on client systems, allowing you to use applications of your choice that are enabled with ODBC. Some examples of applications that utilize ODBC are Microsoft Excel, Microsoft Access, Lotus 1-2-3, Visual Basic, Visual C++, and PowerBuilder.
- *Increases data speed access*—Cisco routers enable high-speed connections to DB2 on hosts, and these connections are faster than native host TCP/IP.

Considerations/Platforms: The Database Connection feature is supported on the following platforms and is available in the specified Cisco IOS Release software images: Cisco 4500 series routers (c4500-aejs-mz), Cisco 4700 series routers (c4500-aejs-mz), Cisco 7200 series routers (c7200-aejs-mz), and the Cisco 7500 series routers (rsp-aejsv-mz).

Product Marketing Contact: Betsy Huber



Multimedia/Voice

Voice over IP

Description: Voice over IP enables a Cisco router to carry live voice traffic (for example, telephone calls and faxes) over an IP network.

Benefits: Toll bypass, Remote PBX presence over WAN's, Unified voice/data trunking, POTS-Internet telephony gateways.

Considerations/Platforms: Feature supported on the Cisco 3600 series.

Product Marketing Contact: Mark Monday

Protocol-Independent Multicast (PIM) Version 2

Description: Protocol-Independent Multicast (PIM) Version 2 offers many improvements over PIM Version 1. PIM v2 offers a single, active rendezvous point (RP) exists per multicast group, with multiple backup Raps. This compares to multiple active Raps for the same group in PIM Version 1. Also, bootstrap router (BSR) provides a fault-tolerant, automated RP discovery and distribution mechanism. Thus, routers dynamically learn the group-to-RP mappings. Furthermore, sparse mode and dense mode are properties of a group, as opposed to an interface. We strongly recommend sparse-dense mode, as opposed to either sparse mode or dense mode only. PIM Join and Prune messages also have more flexible encodings for multiple address families. A more flexible Hello packet format replaces the Query packet to encode current and future capability options. Further, register messages to an RP indicate whether they were sent by a border router or a designated router. Finally, PIM packets are no longer inside IGMP packets; they are stand-alone packets.

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

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

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

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

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

Benefits: PIM Version 2 is a standards track protocol in the IETF.

Considerations/Platforms: This feature is supported on these platforms: Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600 series, Cisco 2500 series, Cisco 3600 series, Cisco 3800 series, Cisco 4000 series (Cisco 4000, 4000-M, 4500, 4500-M, 4700, 4700-M), Cisco 5200 series, Cisco 7200 series, Cisco 7500 series, and the Cisco AS5300.

Product Marketing Contact: Erik Gilbert

Management

SNMP Inform Requests

Description: The SNMP Inform Requests feature allows routers to send inform requests to SNMP managers.

Benefits: Informs are held in memory until a response is received or the request times out. They are more reliable than traps.

Considerations/Platforms: Informs consume more memory than traps. Feature supported on the Cisco 2500, 3600, 3800, 38xx, 4000, 4500, 5200, 7200 and 7500 series platforms.

Product Marketing Contact: Peter Long

SNMP Manager

Description: The SNMP Manager feature allows a router to server as a SNMP manager. As a SNMP manager, the router can send SNMP requests to agents and receive SNMP responses and notifications from agents.

Benefits:

Considerations/Platforms:

Product Marketing Contact: Peter Long

Reliability

MS Callback

Description: The MS Callback feature provides client-server callback services for Microsoft Windows 95 and Microsoft Windows NT clients. MS Callback supports the Microsoft Callback Control Protocol (MSCB). MSCB is Microsoft's proprietary protocol that is used by Windows 95 and Windows NT clients. MS Callback supports negotiated PPP Link Control Protocol (LCP) extensions initiated and agreed upon by the Microsoft client. MS Callback is added to existing PPP Callback functionality. Therefore, if you configure your Cisco access server to perform PPP Callback using Cisco IOS Release 11.3(2)T or later, MS Callback is automatically available.

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

Considerations/Platforms: This feature is supported on these platforms: Cisco 1000 series, Cisco 1600 series, Cisco 2500 series, Cisco 3600 series, Cisco 4000 series, Cisco 4500 series, Cisco 5200, Cisco 5300, Cisco 7200 series, and the Cisco 7500 series.

Product Marketing Manger: April Chou



MIBs Supported on Cisco IOS Release 11.3T

VPDN MIB and Syslog Facility

Description: The VPDN MIB and Syslog Facility feature provides the SNMP-based networking management support and the Syslog messages for Cisco's VPDN feature set, specifically the L2F tunneling technology and will later apply to the L2TP emerging standard.

The VPDN MIB includes four groups of objects:

- System wide information and statistics regarding VPDN (cvpdnSystemInfo)
- Information and statistics regarding active VPDN tunnels (cvpdnTunnelInfo)
- Information and statistics regarding active user sessions in active VPDN tunnels (cvpdnTunnelUserInfo)
- Information regarding failure history per user name (cvpdnUserToFailHisInfo)

The VPDN syslog mechanism provides a generic logging output for VPDN use, L2F or L2TP. The syslog messages are generated to inform of an authentication or authorization error, resource issues, including IDB's, and time-out events.

Platforms: The VPDN MIB is supported on the following platforms:

- Cisco 1003/4
- Cisco 1005
- Cisco 1600
- Cisco 2500 series
- Cisco 3600 series
- Cisco 4000 series
- Cisco 4500 series
- Cisco 5300
- Cisco 7200 series
- Cisco 7500 series

Product Marketing Contact: Anita Freeman



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