Protocol Brief

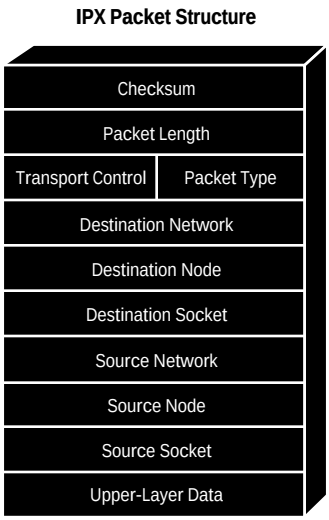
Novell IPX

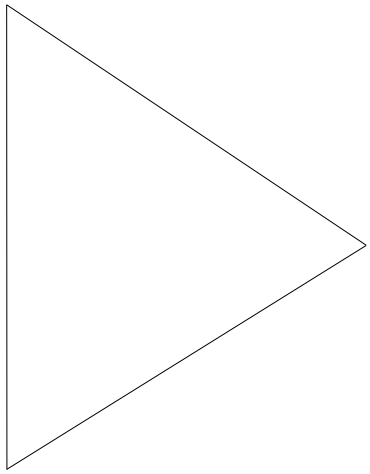
When Novell created NetWare in the early 1980s, PC networks were small and predominantly homogeneous. PC LAN workgroup communication was new, and the idea of a "personal computer" was just becoming popular.

Today, NetWare coexists with many other protocols in large, global internetworks. NetWare's market share as of September 1993 is between 50 and 75 percent (depending on the market research group performing the study) of what has been called the *network operating system* (NOS) market. With over one million NetWare networks installed worldwide, and the accelerating movement to connect networks to other networks, NetWare and its supporting protocols often coexist on the same physical channel with many other popular protocols, including TCP/IP, DECnet, and AppleTalk.

IPX Packet Format

Figure 1





The IPX Protocol Family

Internet Packet Exchange (IPX) is Novell's network-layer protocol. When a device on one network communicates with a device located on a different network, IPX routes the information to the destination through any intermediate networks that might be present. *Figure 1* shows the IPX packet format.

Although IPX was derived from the *Xerox Network Services* (XNS) protocol, it has several unique features. For example, IPX packets can employ various LAN encapsulation schemes depending on the media access protocol.

CISCO SYSTEMS

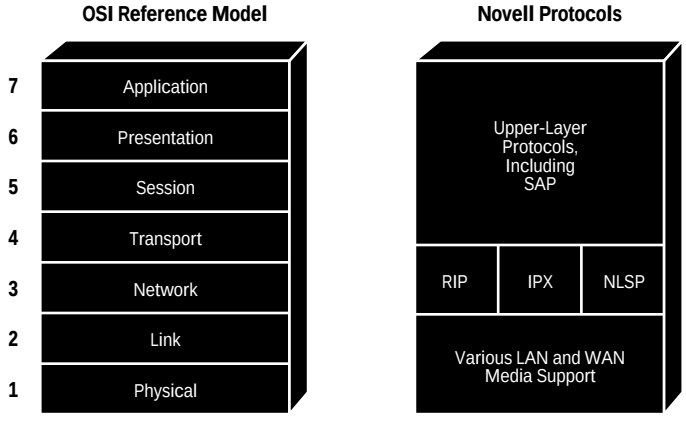
Novell IPX

Routing within Novell IPX networks usually is accomplished using the *Routing Information Protocol* (RIP). Novell recently specified the *NetWare Link Services Protocol* (NLSP), for routing in large internetworks. Although both are dynamic routing protocols, RIP has distinct limitations when used in large networks. NLSP is based on the same technology as the *Intermediate System-to-Intermediate System* (IS-IS) routing protocol created for and used in OSI and IP networks.

Novell includes the *Service Advertisement Protocol* (SAP) as part of its IPX protocol family. SAP allows nodes that provide services (such as file servers and print servers) to advertise their addresses and the services they provide. *Figure 2* shows how IPX, RIP, NLSP, and SAP relate to the OSI reference model.

Novell Protocols and the OSI Reference Model

Figure 2



Cisco's IPX Implementation

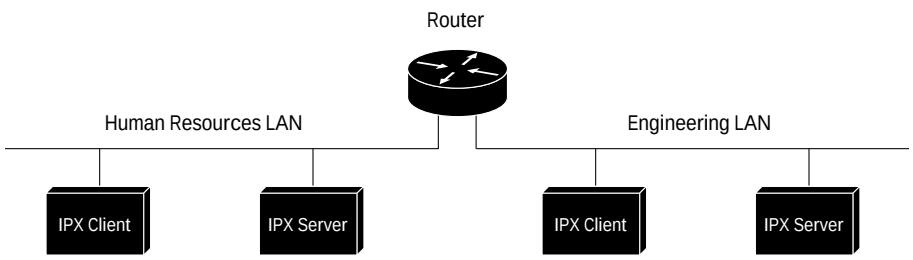
Novell sometimes refers to its routers as "internal" or "external" bridges, depending on whether the routing capability originates inside or outside its file servers. Using this definition, the Cisco Systems routers provide all the functions of a Novell external bridge, plus several additional local- and wide-area connectivity capabilities. Cisco routers can connect multiple LAN and WAN segments that represent a diverse collection of media access protocols and physical communication channels.

Security Features

As networks are connected to other networks, the potential for workstations to gain access to corporate resources grows significantly. However, in some cases, it may not be desirable for a workstation client to access a server. For example, let's assume that the connection of networks by one or more routers has provided physical access from workstations in an engineering department to servers in human resources. This situation is depicted in *Figure 3*. Unless the information on the human resource file server is somehow protected, engineers can gain access to confidential data such as employee compensation and residence addresses and phone numbers.

Access to a Human Resources LAN

Figure 3



Novell IPX

To protect this information, Cisco Systems has incorporated *access lists* into its IPX implementation. An access list permits and/or denies information exchange between network devices based on the network number or other criteria. While other security methods make the information traveling on a network more difficult to access (through password protection) or understand (with data encryption), access lists physically prevent packets from traversing particular networks. This extra security is particularly important when users have access to network analyzers, which can decode passwords and other confidential information traveling through a network.

NetBIOS is a common session-level interface found in PC networks. NetBIOS traffic is often sent by encapsulating it inside Novell IPX packets. NetBIOS names identify network nodes. Cisco includes access control filters that can look at NetBIOS information inside IPX packets, and allow network administrators to filter based on either the NetBIOS names themselves or on any byte pattern within the NetBIOS packet. Filtering on both inbound and outbound packets is supported. NetBIOS/IPX access control filters are useful for hiding private resources and restricting services in unauthorized areas.

Performance Features

The Cisco Systems routers support configurable RIP and SAP update timers on a per-interface basis. RIP and SAP normally send frequent, regular broadcast packets to inform other network devices of changes in a particular device's internal tables. These update packets can wreak havoc on network performance, particularly with large, continually changing networks containing relatively slow WAN links. By appropriately configuring RIP and SAP update timers, the network administrator can control the amount of traffic these protocols introduce to the network, thereby saving bandwidth.

To provide further control over SAP traffic, Cisco routers support SAP filters. SAP filters segregate SAP traffic based on the type of advertising device, the network number, and other fields in the SAP packet. Network administrators use this flexibility to minimize the number of entries in client SAP tables, to improve network performance, and to prevent inappropriate access to NetWare services.

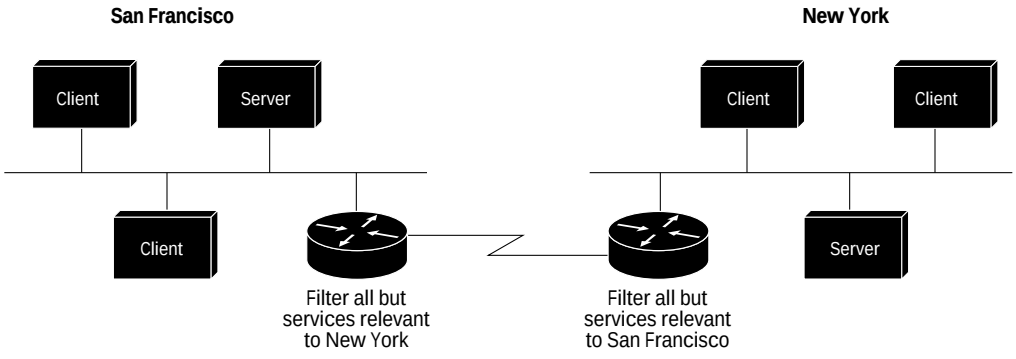
Figure 4 portrays an internetwork with servers that are at or near their SAP table entry limits. Because it is highly unlikely that users in San Francisco will need to print files on a print server in New York, the network administrator filters out all SAP table entries for print servers that are not relevant to the San Francisco installation. This action preserves SAP table entries and minimizes network traffic, saving bandwidth and money.

Cisco routers also filter on RIP fields. The concept here is the same as with SAP field filtering, but the scope is greater. SAP filters isolate certain NetWare services. RIP filters isolate entire network segments or routers. Filtering out certain routers allows the network to appear differently to different segments, logically creating parallel networks without forcing the physical isolation of those networks.

Broadcasting certain packets across an entire internetwork is an important capability, particularly when broadcast-oriented protocols such as NetBIOS name service are supported. Cisco routers support "all nets broadcasting" with an algorithm (based on the IEEE standard spanning tree algorithm) that effectively proliferates broadcasts without creating loops, thereby avoiding broadcast storms and improving network performance.

SAP Filters

Figure 4

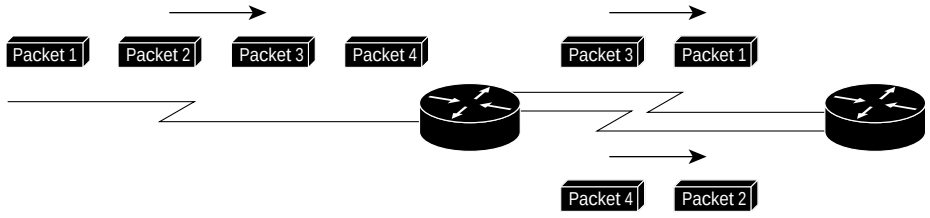


In addition, Cisco routers can simultaneously use multiple paths to a destination, providing load sharing over links, load sharing through routers, and increased tolerance of network faults. For example, *Figure 5a* depicts a situation in which two routers are connected by two high-speed serial links. The routers spread the load by alternating packets between the two links. If one link goes down, all of the traffic is automatically and immediately routed over the remaining link. This feature is particularly significant in networks where extremely important, time-sensitive data is being transferred. *Figure 5b* illustrates load sharing support across multiple internetwork paths. Another benefit of multiple paths is the optimization of throughput and reliability.

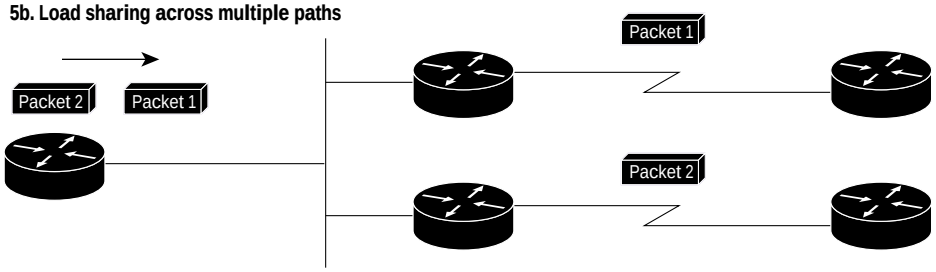
Load Sharing Across Multiple Links and Paths

Figures 5a and 5b

5a. Load sharing across multiple links



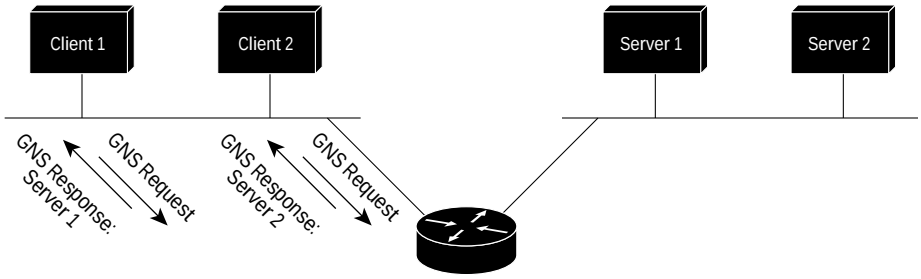
5b. Load sharing across multiple paths



When NetWare clients want to locate NetWare servers, they issue a *GetNearestServer* request. Cisco routers can read, understand, and respond to these requests, distributing clients evenly among the available servers (see *Figure 6*). Client 1 and Client 2 both issue GetNearestServer (GNS) requests. The Cisco router sends a GNS response to Client 1 telling it to communicate with Server 1. It also sends a GNS response to Client 2 telling it to communicate with Server 2. By distributing clients evenly among available servers, Cisco routers increase application availability in NetWare environments.

Proxy GetNearestServer Support

Figure 6



In situations involving slow-speed WAN links, it is often important to prioritize traffic so as to ensure expeditious processing for certain applications. For these users, Cisco offers *priority queuing* on the basis of Novell addresses, networks, and services. With this feature, users can specify that certain predefined packets will be placed in high-priority queues where requests are handled virtually immediately. An alternative scheme, called *custom queuing*, provides a different solution for optimizing traffic on a highly used link. With custom queuing, a percentage of a line's bandwidth can be reserved for a particular traffic type. With Novell traffic, this allocation can be made based on Novell addresses, networks, and service types.

Features like configurable update timers, SAP and RIP filters, all nets broadcasting, load sharing, GNS proxy service, and priority and custom queuing help Cisco routers optimize IPX performance in virtually any network.

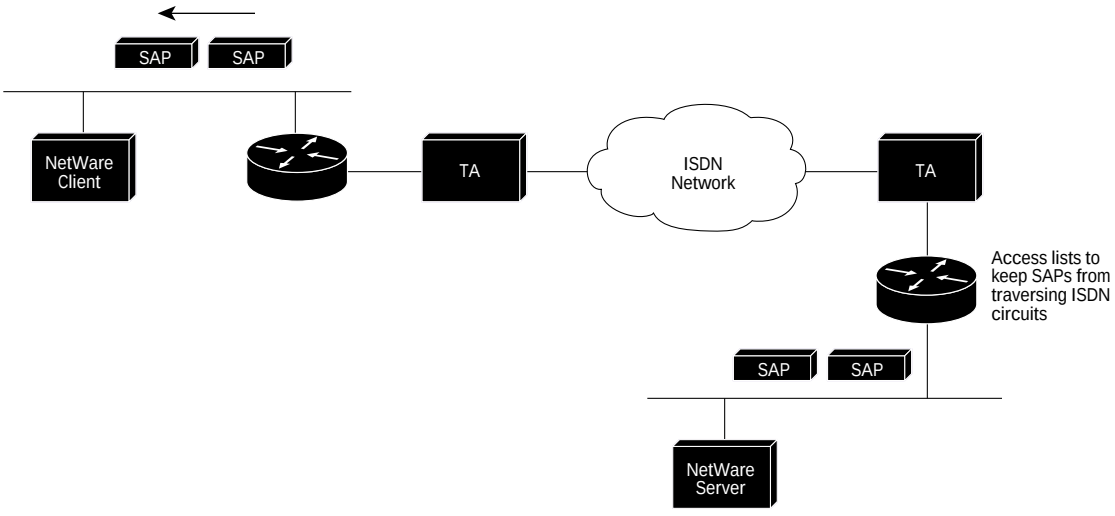
Cost Minimization Features

Increasingly, NetWare clients in one campus require communication with NetWare servers at another site. To minimize the cost of expensive WAN links between the sites, Cisco provides a feature called *dial-on-demand routing* (DDR). DDR provides for the use of the dial-up telephone network, ISDN, or any other circuit-switching data network to provide "on-demand" connectivity without incurring the cost of a dedicated, private-line circuit.

Figure 7 shows a DDR configuration where a remote server is separated from the client by an ISDN network. To prevent unneeded SAP messages from crossing the ISDN network, SAP filters are established in the server-side router. Static SAPs are set up in the client-side router so that the client knows what applications are available to it at the other site. When the Cisco router receives a client request, it consults a static SAP table to determine the appropriate outbound router interface. Once the interface is known, the router can issue a call through the ISDN network (via the native ISDN interface on some Cisco models, or via an external ISDN TA that acts like an ISDN "modem"). With ISDN bandwidth used on demand and SAPs prevented from traversing the ISDN network, overall network performance improves and costs decrease.

IPX Dial-on-Demand Routing

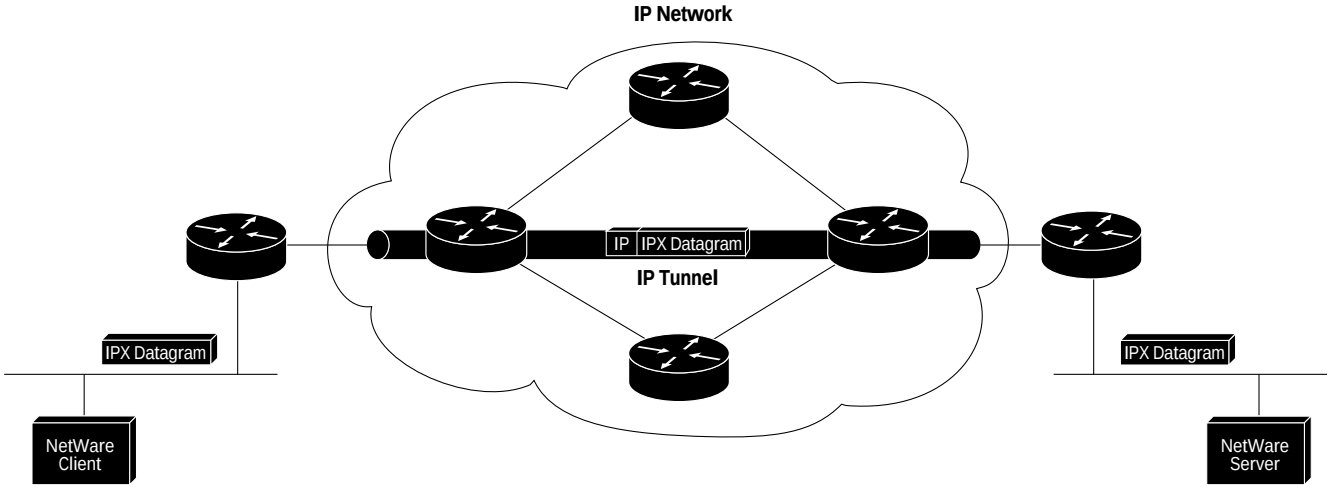
Figure 7



Another feature designed to optimize remote client/server communication is *IPX tunneling.* Tunneling is a generic term used to describe how communication between two like environments can occur through a dissimilar environment. *Figure 8* shows an example. Two NetWare/IPX LANs are separated by an IP WAN of arbitrary size and topology. With IPX tunneling enabled, Cisco routers at the IP WAN's periphery can encapsulate IPX datagrams in IP packets for transmission through the IP WAN.

IPX Tunneling

Figure 8



Novell IPX

Although many routers can be traversed inside the IP WAN, IPX routing protocols see the entire IP WAN as one hop. By lowering the hop count for end-to-end communication between the two NetWare LANs, network scalability improves. Further, all supported IP routing protocols and the many specialized IP features that make up Cisco's IP routing implementation can be used. Application availability increases as route selection is improved and rerouting (convergence) times diminish.

Interoperability Features

Originally, Novell packets were encapsulated in IEEE 802.3 packets without IEEE 802.2 information. Many NetWare nodes still use this encapsulation. Currently, Novell's standard encapsulation scheme is IEEE 802.3 with IEEE 802.2 information. Novell also supports *Sub-Network Access Protocol* (SNAP) encapsulation.

Cisco supports all these Novell encapsulation schemes. Further, there can be multiple encapsulations per router interface, allowing older and newer NetWare nodes to coexist on the same LAN segment without problems, and simplifying migration to IEEE 802.2. Cisco routers can read, understand, and process packets from all NetWare nodes, regardless of the encapsulation technique.

The *Point-to-Point Protocol* (PPP) is an industry-standard protocol used to convey information between two nodes connected by a serial link. Cisco's IPX implementation supports IPX encapsulation in PPP based on the IETF's draft IPXCP specification. The principle benefit of this support is multivendor WAN interconnectivity for NetWare. Thus far, interoperability has been tested and validated with 3Com and IBM, with additional testing under way.

Novell Labs-sponsored interoperability tests are also ongoing. Novell Labs provides router specifications, test suites, and compliance testing. Cisco joined the Novell Labs program in January 1993 and plans to submit each major software release for complete testing. Users benefit from the results of these tests because Cisco is committed to maintaining the highest possible level of interoperability with Novell IPX technologies and products.

Conclusion

The design and performance of Cisco routers directly reflect the company's experience in building and maintaining large networks. Cisco engineers are constantly working with customers to improve network performance and scalability. Some of these networks consist of over 1000 routers. This experience is invaluable in solving the problems that are encountered as networks expand across an enterprise.

Despite the fact that protocols such as IPX were not constructed for large internetwork environments, Cisco routers' software and hardware features allow these protocols to operate effectively in these environments while coexisting harmoniously with other protocols. Network growth reflects customer wants rather than technology constraints.

Cisco's IPX support is in continuous development. In the future, Cisco will offer support for both IPX/WAN and NLSP, two new Novell specifications. Meanwhile, Novell and Cisco continue to work together to ensure the ongoing viability of Cisco routing solutions within NetWare environments.

IPX is one of over 20 protocols that can be simultaneously routed and bridged by any Cisco router. Because many of these protocols were originally designed for use in small LANs, Cisco has added features to its implementation that optimize their performance in larger, enterprise-wide internetworks.

Corporate Headquarters
Cisco Systems, Inc.
P.O. Box 3075
1525 O'Brien Drive
Menlo Park, CA 94026
USA
Tel: 415 326-1941
800 553-NETS
(6387)
Fax: 415 326-1989

European Headquarters
Cisco Systems Europe,
s.a.r.l.
16 Avenue du Quebec
Batiment L2
ZA de Courteboeuf
91961 Les Ulis Cedex,
France
Tel: 33 1 6918 6100
Fax: 33 1 6928 8326

Intercontinental Headquarters
Cisco Systems, Inc.
P.O. Box 3075
1525 O'Brien Drive
Menlo Park, CA 94026
USA
Tel: 415 326-1941
Fax: 415 688-4646

Japanese Headquarters
Nihon Cisco Systems K.K.
Shiba Excellent Building, 5F
2-1-13 Hamamatsucho,
MinatoKu Tokyo 105
Japan
Tel: 81 3 5472 3571
Fax: 81 3 5472 3577

Cisco Systems has over 75 sales offices worldwide. Call 415 326-1941 to contact your local account representative or, in North America, call 800 553-NETS (6387).

European Offices

Belgium
Cisco Systems Belgium, SA/
NV 250, Avenue Louise
8th Floor
1050 Brussels, Belgium
Tel: 32 2 643 2626
Fax: 32 2 643 2627

Germany
Cisco Systems GmbH
Max–Planck Strasse 7
85716 Unterschleissheim,
Germany
Tel: 49 89 3215 070
Fax: 49 89 3215 0710

Italy
Cisco Systems Italy
Office No 609, 6th Floor
Via Turati 28
20121 Milan, Italy
Tel: 39 2 62 726 43
Fax: 39 2 62 729 13

Norway
Cisco Systems
Holmens gate 4
0250 Oslo, Norway
Tel: 47 22 83 06 31
Fax: 47 22 83 22 12

Spain
Cisco Systems Spain
Paseo de la Castellana 141
pl.18 Edificio Cuzco IV
28046 Madrid, Spain
Tel: 34 1 572 0360
Fax: 34 1 570 4599

Sweden
Cisco Systems
Stockholms Modecenter
S-117 60 Stockholm,
Sweden
Tel: 46 8 19 62 05
Fax: 46 8 19 04 24

Switzerland
Cisco Systems Switzerland
Sonnenberg 5
8636 Wald, Switzerland
Tel: 41 55 95 60 44
Fax: 41 55 95 64 14

United Kingdom
Cisco Systems Ltd., Unit 3
Cliveden Office Village
Lancaster Road
High Wycombe,
Bucks HP12 3YZ
United Kingdom
Tel: 44 494 464944
Fax: 44 494 465300

Intercontinental Offices

Asia
Cisco Systems
Hong Kong, Ltd.
Suite 2704
Far East Finance Center
No. 16 Harcourt Road
Hong Kong
Tel: 852 529 3534
Fax: 852 520 2676

Cisco Systems
Shell Tower, Level 37
50 Raffles Place
Singapore
Tel: 65 320 8350
Fax: 65 320 8307

Cisco Systems (HK) Ltd.
Taiwan Office
Formosa Business Center, 3F
285 Nanking East Road
Section 3
Taipei, Taiwan, R.O.C.

Australia
Cisco Systems Australia
Pty., Ltd.
Level 17, 99 Walker Street
P.O. Box 469
North Sydney, NSW 2060
Australia
Tel: 61 2 957 4944
Fax: 61 2 957 4077

Canada
Cisco Systems Canada
Limited
150 King Street West
Suite 1707
Toronto, Ontario M5H 1J9
Canada
Tel: 416 506-1500
Fax: 416 506-1506

Mexico
Cisco Systems de México,
S.A. de C.V.
Presidente Mazaryk No. 61
Col. Chapultepec Morales
C.P. 11560 México, D.F.
Tel: 525 254 0880
Fax: 525 531 9659

New Zealand
Cisco Systems New Zealand
Level 16, ASB Bank Centre
135 Albert Street
P.O. Box 6624
Auckland, New Zealand
Tel: 64 9 358 3776
Fax: 64 9 358 4442

Lit. # 010703 12/93 GP