Data Sheet

Cisco 1710 Security Access Router

The Cisco 1710 Security Access Router offers a cost-effective, business-class security solution for small and medium-sized business and branch offices. The Cisco 1710 Router features comprehensive security with virtual private network (VPN), firewall, and advanced routing functionality in an all-in-one device. The high-performance VPN and firewall functionality safeguard e-business data traveling site-to-site over the Internet and protect internal network resources from unauthorized access. The Cisco 1710 Security Access Router is the ideal security access solution for today's e-business needs.

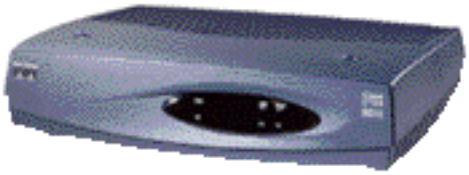
To participate fully in the digital economy, a growing number of businesses and branch offices are accessing the Internet and corporate networks using broadband digital subscriber line (DSL) and cable technologies. But these always-on Internet connections can make businesses more susceptible to intrusion and other Internet attacks. In order to help companies minimize these risks, the Cisco 1710 Security Access Router provides comprehensive security and advanced routing functionality when used in conjunction with a broadband modem.

The two Ethernet interfaces of the Cisco 1710 provide a LAN connection and a flexible, high-speed Internet connection. The router's dual Ethernet design enables an enterprise to deploy a standardized security access device across large numbers of geographically dispersed sites for use with any broadband connection.

The Cisco 1710 Security Access Router enables e-business application deployment by offering:

- Comprehensive security—Business-class security over always-on, broadband Internet connections
- High-performance VPN—Wire-speed VPN through hardware encryption
- Advanced quality of service (QoS) Features—Bandwidth optimization and traffic prioritization
- Remote manageability—Ease-of-installation, reliability, and manageability supported by Cisco Security Device Manager (SDM) and CiscoWorks

Figure 1
Photo of the Cisco 1710 Security Access Router



- All-in-one solution—Integration of multiple functions, including VPN, stateful inspection firewall, intrusion detection system (IDS), full-featured Cisco IOS® Software multiprotocol routing (IP, IPX, AppleTalk), and advanced QoS features

Part of the Cisco end-to-end security solution portfolio, the Cisco 1710 Security Access Router runs Cisco IOS Software, the accepted industry standard networking operating system for the Internet. This advanced software platform provides comprehensive security, advanced QoS, and routing functionality not found on simple broadband access devices.

For service providers, the Cisco 1710 Security Access Router provides an add-on security solution to basic broadband services. By delivering managed VPN services to small and medium-sized businesses and small branch office customers, service providers can help customers deploy e-business applications that leverage their current equipment investments.

The Cisco 1710 Security Access Router delivers a comprehensive feature set, including support for:

- Secure Internet, intranet, and extranet access with VPN and firewall
- Dual Ethernet for flexibility in using any high-speed broadband connection
- Standards-based IEEE 802.1Q virtual LAN (VLAN)
- Point-to-Point Protocol over Ethernet (PPPoE)
- Dynamic Host Configuration Protocol (DHCP) client and server
- Network Address Translation (NAT)/Port Address Translation (PAT)
- Tunneling with generic route encapsulation (GRE), Layer 2 Tunneling Protocol (L2TP), and Layer 2 Forwarding (L2F)

Comprehensive Security

To support global networking and e-business today requires more than broadband WAN connectivity. Businesses need cost-effective, comprehensive security capabilities, including integrated VPN and firewall support. The Cisco 1710 Security Access Router delivers the latest VPN tunneling technology, including an integrated VPN hardware encryption module that accelerates IP Security (IPSec) 3DES performance up to full duplex T1/E1 speeds. Integrated firewall technology prevents unauthorized Internet users from accessing the enterprise LAN. Additionally, remote management applications, such as Cisco Security Device Manager (SDM), make it easier than ever to deploy and monitor VPN and Cisco IOS Firewall on your Cisco 1710 Security Access Router.

VPN

VPNs enable companies to securely connect their branch offices, mobile workers, and business partners over public networks, dramatically lowering costs compared to a private line. By taking advantage of the vast, shared communications infrastructure of the Internet or a shared service provider backbone, companies avoid the service charges of traditional private networks. Using today's technologies, VPNs deliver a wealth of benefits, enabling companies to

- Improve data security
- Increase network performance and availability
- Reduce recurring WAN costs
- Simplify network operations

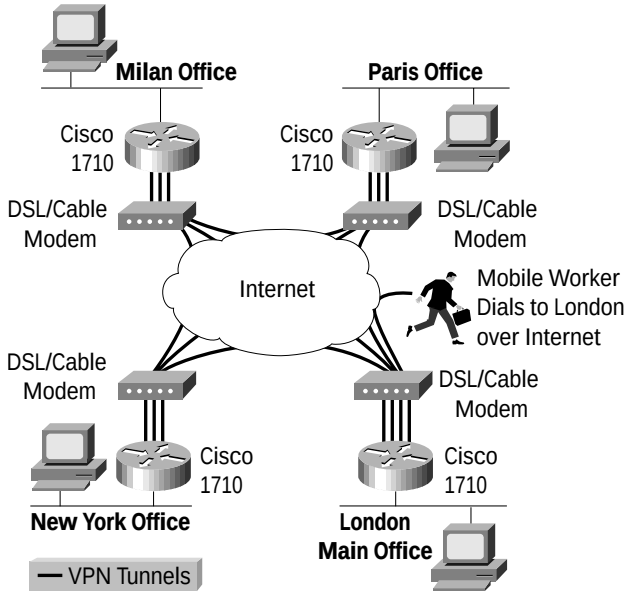
VPNs are making broadband networking affordable for enterprises with large numbers of branch offices that need to communicate securely with one another and to access resources at corporate headquarters or regional sites. Each site—a franchise dealership, a medical clinic, a sales branch, or any satellite office—simply connects its local Ethernet LAN to the Cisco 1710 Router and establishes a secure broadband Internet connection through a cable modem or DSL link.

The ability to offer managed VPN services to business customers, along with such value-added services as stateful inspection firewall and remote management, can help service providers tap new services and revenue streams while improving customer satisfaction. By deploying the Cisco 1710 Router to business customers, service providers can extend their service demarcation point beyond the broadband modem to encompass a business-class security router.

High-Performance VPN

VPN performance is essential to ensuring that e-business applications deliver maximum performance. The Cisco 1710 delivers hardware-assisted VPN functionality allowing users to encrypt data using the strongest encryption available, 3DES at wire-speed (T1/E1). Using high-performance VPN encryption and tunneling technologies, the Cisco 1710 Security Access Router establishes a secure tunnel across the Internet to the corporate network. The virtual network connection lasts only as long as it is needed, so enterprises no longer pay for idle capacity on costly leased lines. Using the Cisco 1710, a VPN can scale to support up to 100 concurrent tunnels or sites in a fully meshed, fully secure global communications web.

Figure 2
Site-to-Site/Mobile User VPN



The Cisco 1700 Series routers support the Cisco Easy VPN Remote feature that allows the routers to act as remote VPN clients. As such, these devices can receive predefined security policies from the headquarters' VPN head-end, thus minimizing configuration of VPN parameters at the remote locations. This solution makes deploying VPN simpler for remote offices with little IT support or for large deployments where it is impractical to individually

configure multiple remote devices. While customers wishing to deploy and manage site-to-site VPN would benefit from Cisco Easy VPN Remote because of its simplification of VPN deployment and management, managed VPN service providers and enterprises who must deploy and manage numerous remote sites and branch offices with IOS routers for VPN will realize the greatest benefit.

The Cisco 1700 Series routers also support the Cisco Easy VPN Server feature that allows a Cisco 1700 router to act as a VPN head-end device. In site-to-site VPN environments, the Cisco 1700 router can terminate VPN tunnels initiated by the remote office routers using the Cisco Easy VPN Remote. Security policies can be pushed down to the remote office routers from the Cisco 1700 router. In addition to terminating site-to-site VPNs, a Cisco 1700 router running the Cisco Easy VPN Server feature can terminate remote access VPNs initiated by mobile and remote workers running Cisco VPN client software on PCs. This flexibility makes it possible for mobile and remote workers, such as sales people on the road, to access company intranet where critical data and applications exist.

Remote Access VPN

In an age of increasing mobility, workers on the move need secure, cost-effective access to corporate e-mail, databases, and network resources. Remote access VPNs meet this need by enabling mobile users to establish a secure tunnel to the corporate network from virtually any location—a home office, hotel room, or conference site—using the Internet as the transport medium.

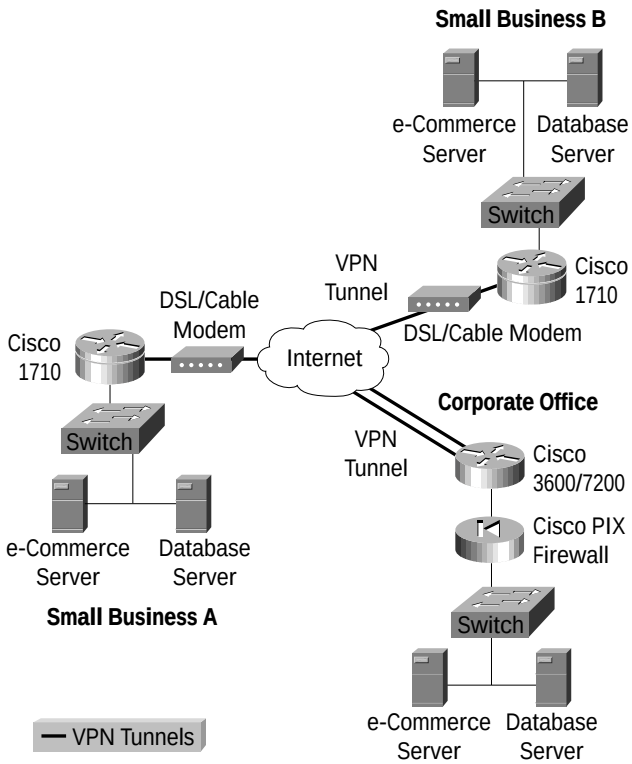
Mobile users simply dial in from their PC or laptop computer to an Internet service provider's local point of presence (POP). Their data is encapsulated inside a second protocol such as IPSec or L2TP and transported across the Internet to the Cisco 1710 Security Access Router at the main office. With Cisco IOS routing support, the Cisco 1710 provides a multiprotocol remote access solution for IP, IPX, and AppleTalk traffic.

Extranet VPN

The Cisco 1710 Security Access Router also enables small and medium-sized businesses to evolve their organization into e-businesses by participating in their enterprise customers' VPN-based extranets. These larger enterprises are increasingly using extranets to provide their suppliers and partners with secure, real-time access to selected enterprise data to enable collaboration, maximize supply chain efficiency, improve sales force effectiveness, or improve e-business operations.

By deploying a Cisco 1710 router, small and medium-sized businesses position themselves to participate in these trusted relationships over a secure VPN tunnel. Secure extranet access up-to-the-minute inventory information, high-level support services, or database resources can give a supplier a competitive advantage over competitors who do not have advanced VPN capability.

Figure 3
Extranet VPN



Firewall

With an always-on broadband connection to the Internet, it is essential to protect the internal network against unwanted intrusion or malicious Internet attacks. The integrated stateful inspection firewall in the Cisco 1710 Security Access Router enables secure Internet access by internal users while defending the enterprise network against denial-of-service attacks and other forms of unauthorized access.

The Cisco 1710 integrates robust firewall functionality and intrusion detection system (IDS) for every perimeter of the network. It adds greater depth and flexibility to Cisco IOS security solutions such as authentication and encryption by including state-of-the-art security features such as stateful, application-based filtering, Context-Based Access Control (CBAC), denial of service protection, dynamic per-user authentication and authorization, defense against network attacks, Java blocking, and real-time alerts.

The Power of Cisco IOS® Technology

Powered by Cisco IOS technology, the Cisco 1710 includes a host of powerful software features to enable secure communications among branch offices or between remote offices and a corporate headquarter while providing unsurpassed network control, maximizing the value of existing infrastructure investments, and reducing costs.

- Advanced QoS Features. Cisco IOS QoS features control the allocation of VPN bandwidth to mission-critical applications. The Cisco 1710 supports advanced QoS features such as committed access rate (CAR), policy routing, Low-Latency Queuing (LLQ), Priority Queuing/Class-Based Weighted Fair Queuing (PQ/CBWFQ), Weighted Random Early Detection (WRED), Generic Traffic Shaping (GTS), Resource Reservation Protocol (RSVP), and DiffServ.
- Multiprotocol Routing. With Cisco IOS Software, the Cisco 1710 offers optional multiprotocol routing (IP, IPX, and AppleTalk), IBM/Systems Network Architecture (SNA), and transparent bridging. Competing security solutions cannot match the full-featured routing functionality (RIP, OSPF, IGRP, EIGRP, and BGP) of the Cisco end-to-end network solution.
- IEEE 802.1Q VLAN. Using the IEEE 802.1Q VLAN standard, the Cisco 1710 enables enterprises to set up multiple VLANs and route between them for added security within the internal corporate network and ease of network resource management.
- Dynamic Host Configuration Protocol (DHCP) Server/Client. DHCP provides a way for network administrators to centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. With DHCP server, the Cisco 1710 is the central point for assigning IP addresses to individual IP devices on the network. DHCP client allows enterprises and service providers to deploy the Cisco 1710 without having to statically assign IP address information to the Ethernet WAN interface.
- PPP over Ethernet (PPPoE). This Cisco IOS Software feature enables the router to be authenticated on a service provider's network or corporate home gateway using PPP, providing support for service provider access control as well as usage tracking and service billing.

Cisco IOS Software is the industry standard networking software and delivers proven reliability. The use of Cisco IOS technologies ensures that a VPN can scale reliably to large networks through the support of Internet Key Exchange (IKE) and digital certificates with leading certificate authorities (CAs), scalable routing protocol features such as Open Shortest Path First (OSPF) protocol and Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), and reliability services such as Hot Standby Router Protocol (HSRP).

Ease of Configuration and Remote Management

The Cisco 1710 supports a range of ease-of-installation and management tools:

- Cisco Security Device Manager (SDM) is an intuitive, easy to use, web-based device management tool embedded within the Cisco IOS access routers. SDM enables resellers and customers to quickly and easily deploy, configure and monitor a Cisco access router without requiring knowledge of Cisco IOS Command Line Interface (CLI). Through smart wizards, SDM can automate best practices for NAT, ACLs, VPN and firewall deployment. Other common LAN, WAN, and routing protocol configurations can also be easily performed through SDM. Network resellers and customers can further fine-tune router configurations for changing business needs and preview the Cisco IOS CLI for each configuration through SDM. For more information visit www.Cisco.com/go/sdm.
- CiscoWorks2000, the industry-leading Web-based network management suite, provides the ability to remotely configure, administer, monitor, and troubleshoot the Cisco 1710. CiscoWorks2000 provides increased visibility into network behavior and quickly identifies performance bottlenecks and long-term performance trends. It also provides sophisticated configuration tools to optimize bandwidth and utilization across expensive and critical WAN links in the network.

- CiscoView is a Web-based tool that graphically provides real-time status of the Cisco 1710. It can drill down to display monitoring information on interfaces, provide dynamic status, statistics, and comprehensive configuration information.
- Cisco Secure Policy Manager (CSPM) is a Windows NT based software tool that allows users to define, distribute, enforce, and audit network-wide security policies from a central location. CSPM streamlines the tasks of managing complicated network security elements, such as IPSec-based VPNs. CSPM can dramatically simplify Firewall and IPSec VPN deployments for enterprise customers, allowing administrators to visually define high-level security policies from one central tool.
- For service providers, Cisco VPN Solutions Center (VPNSC) release 2.0 offers an extensive suite of service management solutions to enable service providers to effectively plan, provision, operate, and bill for VPN services. As service providers build VPNs that include WAN switches, routers, firewalls, VPN concentrators, and Cisco IOS software, they need to seamlessly manage these devices across the network infrastructure and provide service-level agreements (SLAs) to their customers. They also need to enable business customers to personalize their access to network services and applications. VPNSC now offers a cost-effective, carrier-class VPN service management for service providers to rapidly deploy outsourced VPN services that many businesses want today. The portfolio combines robust IPSec VPN services with all the other features of Cisco IOS software on platforms for every site, from the small office to corporate headquarters.

All-in-One Solution

The Cisco 1710 provides a complete security access solution in a single device, with high-speed encryption, stateful inspection firewall, intrusion detection system (IDS), VPN tunnel server, and Cisco IOS® multiprotocol routing. This integration reduces deployment and management time and expense because fewer devices and cables need to be installed and configured. An integrated product also saves space and increases reliability because fewer standalone devices are needed to build a solution. The Cisco 1710 simplifies ongoing support of small branch offices from a central site through remote configuration, monitoring, and troubleshooting of all integrated functions in the security router.

Extending Cisco End-to-End Security Solutions

Cisco IOS Software supports an extensive set of basic and advanced network security features, including access control lists (ACLs); user authentication, authorization, and accounting (such as PAP/CHAP, TACACS+, and RADIUS); and data encryption. To increase security, integrated Cisco IOS Firewall protects internal LANs from attacks with context-based access control (CBAC). IPSec tunneling with Data Encryption Standard (DES) and 3DES encryption provides standards-based data privacy, integrity, and authenticity as e-business data travels through a public network.

The Cisco 1710 Security Access Router is part of the Cisco end-to-end security portfolio. As part of the Cisco 1700 Series of access routers, the Cisco 1710 enables businesses to extend a cost-effective, secure network infrastructure to the small branch office. In addition to the fixed configuration Cisco 1710, the Cisco 1700 Series includes two modular access routers: the Cisco 1720, optimized for data-only connections, and the Cisco 1751, which supports both voice and data integration. Based on Cisco IOS technology, the Cisco 1700 Series integrates seamlessly with the entire range of Cisco LAN and WAN connectivity products for a comprehensive security solution across the network infrastructure.

Table 1 Key Features and Benefits

Features	Benefits
Security	
Stateful inspection firewall. The Cisco IOS Firewall includes context-based access control for dynamic firewall filtering, denial-of-service detection and prevention, Java blocking, and real-time alerts	Allows internal users to access the Internet with secure, per-application-based, dynamic access control while preventing unauthorized Internet users from accessing the internal LAN
High-performance VPN encryption. IPSec DES and 3DES VPN module for high-speed, hardware-based encryption	Provides high-speed hardware-assisted encryption up to T1/E1 performance Enables creation of wire-speed VPNs by providing industry-standard data privacy, integrity, and authenticity as data traverses public networks
Device authentication and key management. IKE, X.509v3 digital certification, support for Certificate Enrollment Protocol (CEP) with certificate authorities (CAs) such as Verisign and Entrust	Ensures proper identity and authenticity of devices and data. Enables scalability to very large IPSec networks through automated key management.
VPN tunneling with IPSec, GRE, L2TP, L2F	Choice of standards-based tunneling methods to create VPNs for IP and non-IP traffic Allows any standards-based IPSec or L2TP client to interoperate with Cisco IOS tunneling technologies
Cisco Easy VPN Remote	Allows the router to act as remote VPN client and have VPN policies pushed down from the VPN concentrator
Cisco Easy VPN Server	Allows the router to terminate remote access VPNs initiated by mobile and remote workers running Cisco VPN client software on PCs; and allows the router to terminate site-site VPNs initiated by IOS routers using the Cisco Easy VPN Remote feature
Cisco SDM	Simplifies router and security configuration through smart wizards to enable customers to quickly and easily deploy, configure and monitor a Cisco access router without requiring knowledge of Cisco IOS Command Line Interface (CLI).
Advanced QoS	
Quality of Service (QoS). (CAR, policy routing, LLQ, WFQ, PQ/CBWFQ, GTS, FRTS, RSVP, DiffServ)	Allocates and optimizes bandwidth to priority applications for improved performance
All-in-One Solution	
Device integration. Integrated advanced routing, firewall, encryption, VPN tunnel server in a single device.	Reduces costs and simplifies management compared to solutions based upon multiple separate devices
Enhanced Management	
IEEE 802.1Q VLAN	Enables efficient traffic separation, provides better bandwidth utilization, and alleviates scaling issues by logically segmenting the physical LAN infrastructure into different subnets so that packets are switched only between ports within the same VLAN

Features	Benefits
Dynamic Host Configuration Protocol (DHCP) Server	Reduces the work necessary to administer an IP network by enabling the hosts on an IP network to obtain their IP address from the Cisco 1710 router
Dynamic Host Configuration Protocol (DHCP) Client	Provides a mechanism for centrally managing the IP addresses for remote Cisco 1710 routers
Network Address Translation (NAT)/Port Address Translation (PAT)	Simplifies deployment and reduces Internet access costs
Auxiliary (AUX) port	Enables dial-up connection for remote management
Manageable via SNMP, Telnet, and console port	Allows remote monitoring, configuration, and diagnostics for all functions integrated in the Cisco 1710, reducing management time and costs
Ease of use and installation. Cisco SETUP configuration utility, AutoInstall, color-coded ports/cables, and LED status indicators	Simplifies and reduces deployment time and costs with graphical LAN/VPN policy configurator; command-line, context-sensitive configuration questions; and straightforward cabling
Flexibility	
Feature-rich Cisco IOS support including multiprotocol routing (IP, IPX, AppleTalk, IBM/SNA) and bridging	Provides industry's most robust, scalable, and feature-rich internetworking software support using the accepted standard networking software for Internet and private WANs
Dual-Ethernet configuration	Takes advantage of broadband access technologies such as cable and DSL to increase WAN connectivity speeds and reduce WAN access costs Offers the flexibility to connect any broadband modems
Autosensing 10/100 Fast Ethernet	Simplifies implementation in mixed Ethernet environments

Figure 4
Rear Panel, Cisco 1710 Security Access Router

Physical Interfaces/Ports

10/100BaseTX Fast Ethernet port (RJ-45)

- Automatic speed detection
- Automatic full/half duplex negotiation

10BaseT Ethernet port (RJ-45)

- Full/half duplex support (manual selection)

Auxiliary (AUX) port

- RJ-45 jack with EIA/TIA-232 interface
- Asynchronous serial data terminal equipment (DTE) with full modem controls Carrier Detect (CD), data sheet ready (DSR), Request To Send (RTS), Clear To Send (CTS)
- Asynchronous serial data rates up to 115.2 kbps

Console port

- RJ-45 jack with EIA/TIA-232 interface (plug compatible with Cisco 1600/1700/2500/2600 series console ports)
- Asynchronous serial DTE
- Transmit/receive rates up to 115.2 kbps (default 9600 bps, not a network data port)
- No hardware handshaking such as RTS/CTS

DRAM and Flash Memory

Run from RAM architecture

Flash—ships with 16 MB

- Onboard (fixed/default): 16 MB
- Maximum: 16 MB
- Support dual Flash bank

DRAM—ships with 64 MB

- Onboard (fixed): 32 MB
- One DIMM slot—populated with 32 MB DIMM
- Maximum DRAM: 96 MB

Dimensions

Width: 11.2 in. (28.4 cm)

Height: 3.1 in. (7.85 cm)

Depth: 8.7 in. (22.1 cm)

Weight (minimum): 2.6 lb (1.18 kg)

Weight (maximum): 2.9 lb (1.32 kg)

Power

Locking connector on power socket

AC input voltage: 100 to 240 VAC

Frequency: 50 to 60 Hz

AC input current: rated 1 A, measured 0.5 A

Power dissipation: 20W (maximum)

Environmental

Operating temperature: 32 to 104 F (0 to 40 C)

Nonoperating temperature: –4 to 149 F (–20 to 65 C)

Relative humidity: 10 to 85% noncondensing operating; 5 to 95% noncondensing nonoperating

Safety

UL 60950

CSA 22.2—No. 60950

EN60950

AS/NZS 3260

ETSI 300-047

BS 6301 (power supply)

IEC 60950 (power supply)

GB 4943 (power supply)

Emission

EN55022, 1998, class B

CISPR22, 1997, class B

CFR47, Part 15, Subpart B, 1995, class B

EN61000-3-3 Voltage Fluctuation and Flicker

Immunity

CISPR24, 1997

EN 55024:1998

IEC 61000-4-2:1995

IEC 61000-4-3:1995

IEC 61000-4-4:1995

IEC 61000-4-5:1995

IEC 61000-4-6:1996

IEC 6100-4-8: 1003

IEC 61000-4-11:1995

Service and Support

Leading-edge technology deserves leading-edge support. From installation and implementation services (Total Implementation Solutions), to industry leading operational support (SMARTnet), Cisco and its best in class service partners are available to help you align your networks with your business needs. Service and support for the Cisco 1710 is available on a one-time or an annual contract basis. SMARTnet support options range from help-desk assistance to proactive, onsite consultation.

All SMARTnet support contracts include:

- Major Cisco IOS Software updates including protocol, security, bandwidth, and feature improvements
- Full access to Cisco.com for technical assistance, electronic commerce, and communications information
- 24-hour-a-day access to the industry,s largest dedicated technical support staff

A support contract maximizes the value of your technology investment throughout its lifecycle, ensuring optimum performance and availability. Augment your Internet staff's capabilities by taking full advantage of Cisco expertise.

Contact your local sales office for further information.

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

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

ETMG 203078—MS 07/03