Cisco 1700 Series Modular Access Routers
Cisco 1721 and Cisco 1720

The Cisco 1720 Modular Access Router and the enhanced Cisco 1721 Modular Access Router are designed to help organizations embrace the productivity benefits of e-business applications. The Cisco 1721 and 1720 routers enable e-business by delivering secure Internet, intranet, and extranet access with virtual private networks (VPNs) and firewall technology. The Cisco 1721 and 1720 routers offer:

- Wide array of WAN access options, including high-speed business-class digital subscriber line (DSL)
- High-performance routing with bandwidth management
- Inter-virtual LAN (VLAN) routing (Cisco 1721 only)
- VPN access with firewall option

The Cisco 1721 (shown below in Figure 1) is an enhanced version of the award-winning Cisco 1720 Modular Access Router. The Cisco 1721 offers higher performance, additional functionality, and increased memory capacity over the Cisco 1720. In addition, the Cisco 1721 supports standards-based IEEE 802.1Q VLAN routing, which enables enterprises to set up multiple VLANs and route between them for added security within the internal corporate network.

Powered by Cisco IOS® Software, the Cisco 1721 and 1720 routers provide a cost-effective solution for small and medium businesses and enterprise small branch offices to support e-business applications through a comprehensive feature set in a compact design.

The Cisco 1721 and 1720 offer the following key features:

- A RISC processor to support high-performance routing, encryption, and broadband services
- One autosensing 10/100 Fast Ethernet port
- Two WAN interface card (WIC) slots that support the same data WAN interface cards as the Cisco 1600, 2600, and 3600 routers
- One auxiliary (AUX) port (up to 115.2-kbps asynchronous serial)
- One console port
- One internal expansion slot for the hardware-assisted VPN encryption card (MOD1700-VPN)

Figure 1:

The Cisco 1721 Router delivers a versatile e-business WAN access solution.

To see a comparison of the products, review Table 1 below.

Table 1 Cisco 1721 and 1720 Product Comparison

Feature	Cisco 1721	Cisco 1720
Routing Performance (based on 64-byte packet)	12,000 packets per second	8,400 packets per second
DRAM (default/maximum)	32 MB/96 MB	32 MB/48 MB
Flash (default/maximum)	16 MB/16 MB (Nonupgradable)	8 MB/16 MB
IEEE 802.1Q VLAN Routing	Yes	No
Encryption Module LED Indicator	Yes	No

The Cisco 1700 Series supports the value of end-to-end Cisco network solutions with the following benefits:

- *Flexibility*—The modular Cisco 1721 and 1720 adapt easily to fit the needs of growing businesses. Interchangeable WAN interface cards enable easy additions or changes in WAN technologies without requiring a forklift upgrade of the entire platform. Modular data slots enable users to tailor data services as needed.

- *Security*—The Cisco 1721 and 1720 support hardware-assisted wire-speed Triple Digital Encryption Standard IP Security (3DES IPSec) VPN encryption (using optional VPN module), a Cisco IOS Software-based stateful inspection firewall, and an intrusion detection system (IDS) that allows customers to keep their data safe.

- *Business-class DSL*—Business-class DSL is delivered through the optional asymmetric DSL (ADSL) or symmetrical high-bit rate DSL (G.shdsl) WICs. The Cisco 1700 Series business-class DSL solution combines the cost benefits of DSL service with the advanced routing capability required for business use of the Internet. Through enhanced DSL quality-of-service (QoS) features, performance levels for mission-critical applications and toll-quality voice/data integration are guaranteed.

- *Traffic management*—The Cisco 1721 and 1720 are based on Cisco IOS Software, the accepted standard for Internet operations. Cisco IOS Software allows traffic prioritization by user or application, ensuring that the most strategic e-business applications and time-sensitive applications perform as expected.

E-Business Applications

VPN and Security

The Cisco 1721 and 1720 routers are part of the end-to-end Cisco VPN solution. VPNs create secure connections via the Internet to connect geographically dispersed offices, business partners, and remote users while providing security, traffic prioritization, management, and reliability equal to that of private networks.

By supporting industry standards, IPSec, Layer 2 Tunneling Protocol (L2TP), and DES and 3DES, the Cisco 1721 and 1720 routers deliver robust VPN solutions to ensure data privacy, integrity, and authenticity.

The optional VPN hardware encryption module for Cisco 1721 and 1720 routers further optimizes VPN encryption performance. By offloading encryption tasks to the VPN module, the router processor is freed to handle other operations. The VPN module accelerates the rate at which encryption occurs, speeding the process of transmitting secure data, a critical factor when using 3DES encryption.

The Cisco 1721 and 1720 routers offer integrated security features, including stateful inspection firewall functionality and IDS as an optional Cisco IOS Software feature. By deploying Cisco IOS Software firewall functionality, customers do not need to purchase or manage multiple devices, thus simplifying network management and reducing capital costs.

Cisco IOS Software firewall security features include access control lists (ACLs), user Authentication, Authorization, and Accounting (such as Password Authentication Protocol/Challenge Handshake Authentication Protocol [PAP/CHAP], TACACS+, and Remote Access Dial-In User Service [RADIUS]). These security features provide the optimal level of firewall protection to customers.

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 Unified VPN Access Server 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.

Business-Class DSL

The Cisco 1721 and 1720 routers support business-class DSL through the optional ADSL or G.shdsl WICs.

The Cisco 1721 and 1720 business-class DSL solution combines the cost benefits of DSL service with the advanced routing capability required for business use of the Internet. Through enhanced DSL QoS features, performance levels for mission-critical applications are guaranteed. (See Figure 2.)

Figure 2
The Cisco 1700 Series Deployed with an ADSL WIC
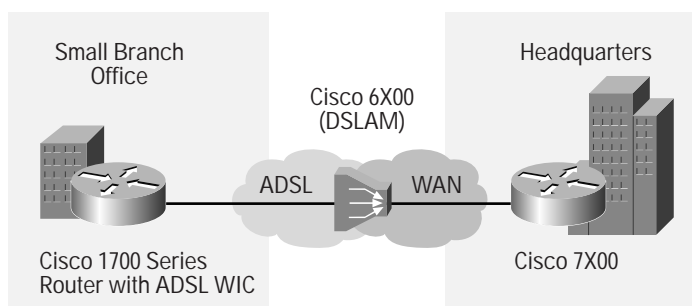
When equipped with optional Ethernet WICs, the Cisco 1700 Series supports a two- or three-Ethernet configuration, enabling deployment with an external broadband modem (such as DSL, cable modem, or wireless modem)—often supplied by a service provider as a demarcation point and deployment of a demilitarized zone (DMZ). (See Figure 3.)

Figure 3:

The Cisco 1700 Series Deployed with an Ethernet WIC and an External DSL or Cable Modem
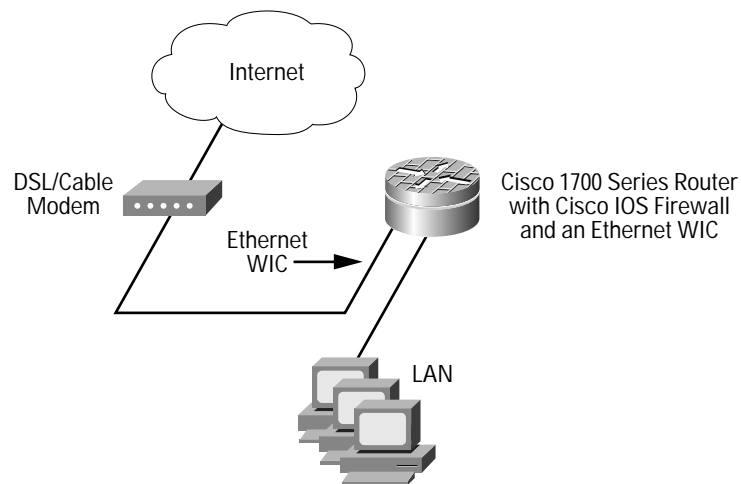
Comprehensive Feature Set and Benefits

The Cisco 1721 and 1720 offer a broad set of features designed to allow businesses to attain maximum benefits on their investment and to easily deploy e-business solutions. See Table 2 for key features and benefits.

Table 2 Cisco 1721 and 1720 Key Features and Benefits

Features	Benefits
Flexibility and Investment Protection	
Modular Architecture	• Wide array of WAN options provide flexibility and investment protection by accommodating future technologies while providing a solution to meet today's needs
WAN Interface Cards Shared with Cisco 1600, 2600, and 3600 Routers	• Reduces cost of maintaining inventory • Offers lower training costs for support personnel • Protects investments through reuse on various platforms

Table 2 Cisco 1721 and 1720 Key Features and Benefits (Continued)

Features	Benefits
Full Cisco IOS Support, including Multiprotocol Routing, QoS	• Provides industry's most robust, scalable, and feature-rich internetworking software support using the accepted standard networking software for Internet and private WANs • Constitutes part of the Cisco end-to-end network solution
Quality of Service (QoS)	• Offers support for advanced QoS features such as the Resource Reservation Protocol (RSVP), Weighted Fair Queuing (WFQ), and IP Precedence to reduce recurring WAN costs • QoS features (such as committed access rate [CAR], policy routing, low-latency queuing [LLQ], generic traffic shaping [GTS], Frame Relay traffic shaping [FRTS], and RSVP) allocate WAN bandwidth to priority applications for improved performance
Expansion Slot on Motherboard	• Allows expandability to support services such as hardware-assisted encryption
Complete Security and VPN Capability	
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 (Internet Key Exchange [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, Generic Routing Encapsulation (GRE), L2TP, L2F	• 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 polices 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

Table 2 Cisco 1721 and 1720 Key Features and Benefits (Continued)

Features	Benefits
Business-Class DSL	
Supports ADSL and G.shdsl with advanced QoS features (Multilink PPP [MLP] with link fragmentation and interleaving [LFI], LLQ, Weighted Random Early Detection [WRED], CAR, differentiated services)	• Takes advantage of broadband access technologies such as ADSL or G.shdsl to increase WAN connectivity speeds and reduce WAN access costs • Delivers business-class broadband access • Offers efficient use of bandwidth
Simplified Management and Ease of Deployment	
Device Integration (integrated router, firewall, encryption, VPN, tunnel server, data/channel service unit [DSU/CSU], and Network Termination 1 [NT1] in a single device)	• Reduces costs and simplifies management compared to solutions based upon multiple, separate devices
Manageable via Simple Network Management Protocol (SNMP) (CiscoView, CiscoWorks 2000, Telnet, and console port)	• Allows central monitoring, configuration, and diagnostics for all functions integrated in the Cisco router, reducing management time and costs
Supports Cisco ConfigMaker, SETUP Configuration Utility	• Simplifies and reduces deployment time and costs with graphical LAN/VPN policy configurator; command-line, context-sensitive configuration questions
VLAN Support (Cisco 1721 only)	• Enables inter-VLAN routing via the standards-based IEEE 802.1Q • Available in all Cisco IOS feature sets, including base Cisco IOS feature set
Support for Cisco AutoInstall	• Configures remote routers automatically across a WAN connection to save cost of sending
LED Status Indicators	• Provide at-a-glance indications for power, VPN module (Cisco 1721 only), network activity, and interface status
Reliability	
Dial-on-Demand Routing	• Allows automatic backup of WAN connection in case of a primary link failure
Dual Bank Flash Memory	• Backup copy of the Cisco IOS Software can be stored in Flash memory
Hot Standby Router Protocol (HSRP)	• Provides high network availability

Hardware/Software Options

Comprehensive WAN Support

The Cisco 1721 and 1720 support up to two of the WICs listed in Table 3. These WICs support a wide variety of WAN technologies: Integrated Services Digital Network (ISDN), asynchronous serial and synchronous serial such as leased lines, Frame Relay, ADSL, G.shdsl, Switched 56, X.25, and Switched Multimegabit Data Service (SMDS), and single-port Ethernet. Also available are WICs that integrate a DSU/CSU into the Cisco 1721 and 1720, eliminating the support costs and complexity of deploying and managing external devices.

Table 3 WAN Support for the Cisco 1721 and 1720

WIC	Description
WIC-1T	One-port serial, asynchronous and synchronous (T1/E1)
WIC-2T	Two-port serial, asynchronous and synchronous (T1/E1)
WIC-2A/S	Two-port low-speed serial (up to 128 kbps), asynchronous and synchronous
WIC-1B-S/T	One-port ISDN Basic Rate Interface (BRI) S/T
WIC-1B-U	One-port ISDN BRI U interface with integrated NT1
WIC-1DSU-56K4	One-port integrated 56/64-kbps, four-wire DSU/CSU
WIC-1DSU- T1	One-port integrated T1/fractional T1 DSU/CSU
WIC-1ADSL	One-port ADSL interface
WIC-1ENET	One-port 10BASE-T Ethernet interface
WIC-1SHDSL	One-port G.shdsl interface
VWIC-1MFT-T1*	One-port RJ-48 multiflex trunk - T1
VWIC-2MFT-T1*	Two-port RJ-48 multiflex trunk - T1
VWIC-2MFT-T1-DI*	Two-port RJ-48 multiflex trunk - T1 with drop and insert
VWIC-1MFT-E1*	One-port RJ-48 multiflex trunk - E1
VWIC-2MFT-E1*	Two-port RJ-48 multiflex trunk - E1
VWIC-2MFT-E1-DI*	Two-port RJ-48 multiflex trunk - E1 with drop and insert
VWIC-1MFT-G703*	One-port RJ-48 multiflex trunk - E1 G.703
VWIC-2MFT-G703*	Two-port RJ-48 multiflex trunk - E1 G.703

*Supported on Cisco 1721 model only, not supported on Cisco 1720 model

Hardware VPN Encryption Module

All Cisco 1700 models are equipped with an internal expansion slot to support an optional field-installable hardware VPN encryption module. The VPN encryption module offloads encryption processing from the Cisco 1700 Series RISC processor, providing performance up to T1/E1 speeds. The VPN encryption module (MOD1700-VPN) supports a maximum of 100 remote access tunnels.

Cisco IOS Software Feature Sets

Cisco 1721 and 1720 routers support a full range of Cisco IOS features, including multiprotocol routing, QoS, VPN, firewall/IDS, and legacy IBM protocol and applications in use today.

The Cisco 1721 and 1720 routers are shipped with the base Cisco IOS feature sets supporting IP routing and standards such as Network Address Translation (NAT), Open Shortest Path First (OSPF), RADIUS, Remote Monitoring (RMON), VLAN routing, basic QoS feature (Weighted Fair Queing), and Next Hop Resolution Protocol [NHRP]).

Cisco IOS IP Plus feature sets contain L2TP, L2F, Border Gateway Protocol (BGP), IP multicast, Frame Relay switched virtual circuit (SVC), RSVP, PPP over Ethernet client, NetFlow, the Netware Link Services Protocol (NLSP), Simple Multicast Routing Protocol (SMRP), the Web Cache Control Protocol (WCCP), and the Network Timing Protocol (NTP). In addition, enhanced QoS features are also supported (LLQ, FRTS, RSVP, CEF, WRED, DiffServ, MLPP with LFI).

IPSec encryption is offered in special encryption feature sets (Plus IPSec 56 and Plus IPSec 3DES). To build an IP VPN, the recommended feature sets are IP/Firewall Plus IPSec 56 or IP/Firewall Plus IPSec 3DES.

For a detailed list of features and memory requirements for a given feature set, see Cisco IOS 1700 Release Notes.

Network Management and Installation Tools

The Cisco 1721 and 1720 support a range of network-management and ease-of-installation tools.

CiscoWorks2000, the industry-leading Web-based network management suite, provides the ability to remotely configure, administer, monitor, and troubleshoot the Cisco 1721 and 1720; and increased visibility into network behavior to quickly identify 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, part of CiscoWorks2000, is a Web-based tool that graphically provides real-time status of the Cisco 1721 and 1720. It can drill down to display monitoring information on interfaces and provide dynamic status, statistics, and comprehensive configuration information.

CiscoWorks Small Network Management Solution (SNMS) is a comprehensive, Web-based network management solution that provides a powerful set of monitoring, configuration, and management tools to simplify the administration of small to medium business networks and workgroups that contain up to 20 Cisco internetworking products (switches, routers, hubs, and access servers). CiscoWorks SNMS is an ideal solution for companies that need server monitoring and network management from a single application to optimize performance and maximize network productivity. With CiscoWorks SNMS, Cisco provides a cost-effective and user-friendly solution that helps Cisco customers make the optimal use of their resources. The solution provides the following:

- Web interface for all applications—CiscoWorks SNMS can be used from any browser in the network with the appropriate user authentication.
- Simple integrated installation, autodiscovery, and automated import of devices using SNMP reduces complexities and overall setup time associated with managing the network.
- CiscoWorks SNMS provides standards-based multivendor management. The WhatsUp Gold application in CiscoWorks SNMS allows administrators to view live network information, including the status of all hosts, servers, workstations, routers, other devices, and services.
- CiscoWorks SNMS grows and adapts to the changing devices in a dynamic network. Regular device updates are provided via downloadable files from Cisco.com. This scenario ensures that users can manage the most currently available Cisco devices without waiting for new versions of CiscoWorks SNMS to be released.

Cisco ConfigMaker is a Microsoft Windows wizard-based tool designed to configure a small network of Cisco routers, switches, hubs, and other network devices from a single PC. This tool makes it easy to configure value-add security features such as the Cisco IOS Firewall Feature Set, IPSec encryption, NAT, the Dynamic Host Configuration Protocol (DHCP) server, and to establish VPN policies (including QoS and security).

Cisco 1700 Series

The Cisco 1700 Series enables deployment of a cost-effective, seamless network infrastructure for small and medium-sized businesses and small enterprise branch offices. The Cisco 1700 Series of modular access routers include the Cisco 1710, 1720, 1721,1751, 1760 (offered as a base model), Cisco 1751-V and Cisco 1760-V (offered as a multiservice-ready model.)

The Cisco 1751 and Cisco 1760 Modular Access Router is optimized for multiservice data and voice solutions. The Cisco 1721 and 1720 routers are modular devices optimized for data-access applications. The Cisco 1710 Security Access Router features comprehensive security with VPNs, Cisco IOS Firewall, and advanced routing functionality in an all-in-one device.

Service and Support

Technical Support Services

Technical Support Services for the Cisco 1721 and 1720 are available through Cisco SMARTnet™ and SMARTnet Onsite service programs. Cisco SMARTnet support augments the resources of your operations staff; it provides them access to a wealth of expertise, both on line and via telephone, the ability to refresh their system software at will, and a range of hardware Advance Replacement options.

Cisco SMARTnet Onsite provides all SMARTnet services and complements the hardware Advance-Replacement feature by adding the services of a field engineer, offering support that can be critical for those locations where staffing is insufficient or unavailable to perform parts-replacement activities. Table 4 gives features and benefits of Cisco SMARTnet support.

Table 4 Cisco SMARTnet Features and Benefits Technical Support Services

	Features	Benefits
Cisco SMARTnet Support **Cisco SMARTnet Onsite Support**	• Access 24 x 7 to software updates • Web access to technical repositories • Telephone support through the Technical Assistance Center (TAC) • Advance Replacement of hardware parts	• Enables proactive or expedited issue resolution • Lowers total cost of ownership by utilizing Cisco expertise and knowledge • Minimizes network downtime

Technical Support Services Delivery

Cisco SMARTnet support is available to customers from both Cisco directly and through Cisco channel partners. Partners purchasing direct from Cisco may offer Cisco Branded Resale of Cisco SMARTnet Software. Partners purchasing through distribution may offer Packaged Cisco SMARTnet Software.

For partners supporting the Cisco 1721 and 1720 with their own service and support infrastructure, System Integrator Support 98 (SIS98) is available.

Technical Specifications

Figure 4

Rear Panel, Cisco 1721 Access Router
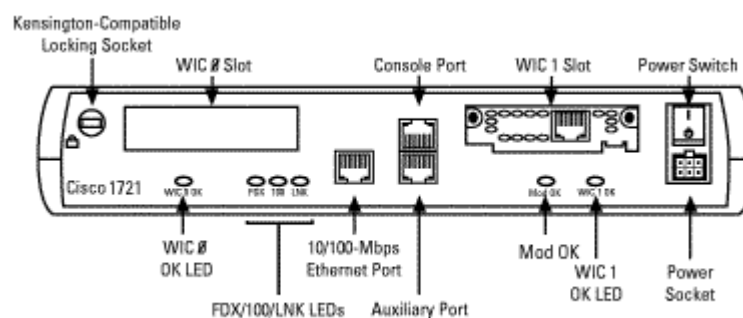
Physical Interfaces/Ports

- One 10/100BASE-TX Fast Ethernet port (RJ-45)
    - Automatic speed detection
    - Automatic duplex negotiation
    - IEEE 802.1Q VLAN routing (Cisco 1721 only)
- Two WAN interface card slots
    - Supports any combination of two WAN interface cards as shown in Table 3

- One auxiliary (AUX) port
  - RJ-45 jack with EIA/TIA-232 interface
  - Asynchronous serial data terminal equipment (DTE) with full modem controls Carrier Detect, data set ready (DSR), Request To Send (RTS), Clear To Send (CTS)
  - Asynchronous serial data rates up to 115.2 kbps
- One console port
  - RJ-45 jack with EIA/TIA-232 interface
  - 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
- One internal expansion slot for support of hardware-assisted services such as VPN encryption (up to T1/E1 performance)

WAN Interface Specifications (Optional)

- Synchronous serial interfaces on serial WAN interface cards
  - Interface speed: up to 2.0 Mbps (T1/E1)
  - Synchronous serial protocols: Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC),
    Link Access Procedure, Balanced (LAPB), IBM Systems Network Architecture (SNA)
  - Synchronous serial WAN services: Frame Relay, X.25, SMDS
  - Synchronous serial interfaces supported on the WIC-1T, WIC-2T, and WIC-2A/S cards: V.35, EIA/TIA-232, EIA/TIA-449, X.21, EIA-530
- Asynchronous serial interfaces on serial WAN interface cards
  - Interface speed: up to 115.2 kbps
  - Asynchronous serial protocols: PPP, Serial Line Internet Protocol (SLIP)
  - Asynchronous interface: EIA/TIA-232
- ADSL WAN interface card
  - Supports ATM adaptation layer 5 (AAL5) services and applications

- Interoperates with Alcatel DSL access multiplexer (DSLAM) with Alcatel chipset and Cisco 6130/6260 DSLAM with Globespan chipset
  - Complies with ANSI T1.413 issue 2 and ITU 992.1 (G.DMT)
- G.shdsl WAN interface card
  - Based on the ITU G.991.2, delivers symmetrical data rates from 192 kbps to 2.3 Mbps; speeds vary, depending on loop length and line conditions
- ISDN WAN interface cards
  - ISDN dialup and ISDN DSL (IDSL) at 64 and 128 kbps
  - Encapsulation over IDSL, Frame Relay, and PPP

Dimensions and Weight

- Width: 11.2 in. (28.4 cm)
- Height: 3.1 in. (7.85 cm)
- Depth: 8.7 in. (22.1 cm)
- Weight (maximum): 2.9 lb (1.32 kg)

Power

- Locking connector on power socket
- AC input voltage: 100 to 240 VAC
- Frequency: 47 to 64 Hz
- AC input current: 0.5 amps
- 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 1950
- CSA 22.2—No. 950
- EN60950
- EN41003

- AUSTEL TS001

- AS/NZS 3260

- ETSI 300-047

- BS 6301 (power supply)

EMI

- AS/NRZ 3548 Class A

- Class B

- FCC Part 15 Class B

- EN60555-2 Class B

- EN55022 Class B

- VCCI Class II

- CISPR-22 Class B

Immunity

- 55082-1 Generic Immunity Specification Part 1: Residential and Light Industry

- IEC 1000-4-2 (EN61000-4-2)

- IEC 1000-4-3 (ENV50140)

- IEC 1000-4-4 (EN61000-4-4)

- IEC 1000-4-5 (EN61000-4-5)

- IEC 1000-4-6 (ENV50141)

- IEC 1000-4-11

- IEC 1000-3-2

Network Homologation

- USA: ATIS/ACTA -TIA/EIA/IS - 968 (Former part 68), TIA/EIA/IS-883, T1.TRQ.6-2001, TIA/EIA/TSB-129

- Canada - CS-03

- Japan - JATE

- Australia - AS/ACIF: S-02, S-043, C-559; ACA TS-002, TS-003, TS-006, TS-016, TS-031

- New Zealand - PTC107, PTC200, PTC211, PTC270, CTR3

- European Union + Switzerland: Directive 1999/5/EC

- Russia - CTR2, CTR3, CTR21, ITU-G.992.1, ITU-G991.2

- Belarus - CTR3, CTR21

- Czechia - CTR2, CTR3, CTR21

- Poland - CTR3, PB-TE ITU-G.992.1

- Hungary - CTR2, CTR3, CTR21, ITU-G.992.1

- Singapore - IDA: TS-PSTN1, TS-ISDN1, TS-ADSL

- Taiwan - PSTN01, IS6100, ID002

- Brazil - CTR3, CS-03

- Mexico - CTR3, CS-03, FCC part 68

- South Africa- CTR3

The Cisco 1700 series, including the Cisco 1721, is in compliance with the requirements of the countries for distribution. The Cisco 1700 Series conforms to Safety, EMI, Immunity, and Network homologation standards. Details can be obtained through your Cisco reseller or account manager.

CISCO SYSTEMS

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 Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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: +65 317 7777
Fax: +65 317 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