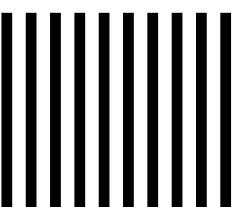




NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES



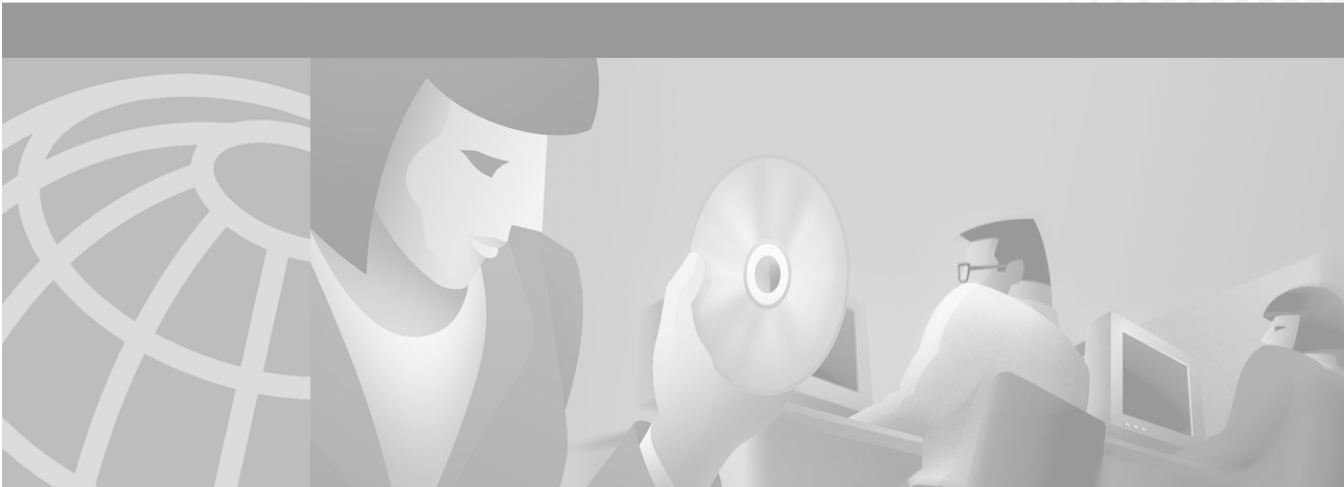
BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 4631 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

ATTN DOCUMENT RESOURCE CONNECTION
CISCO SYSTEMS INC
170 WEST TASMAN DRIVE
SAN JOSE CA 95134-9883





Cisco 1710 Security Router Hardware Installation Guide

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

Customer Order Number: DOC-7812697=
Text Part Number: 78-12697-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

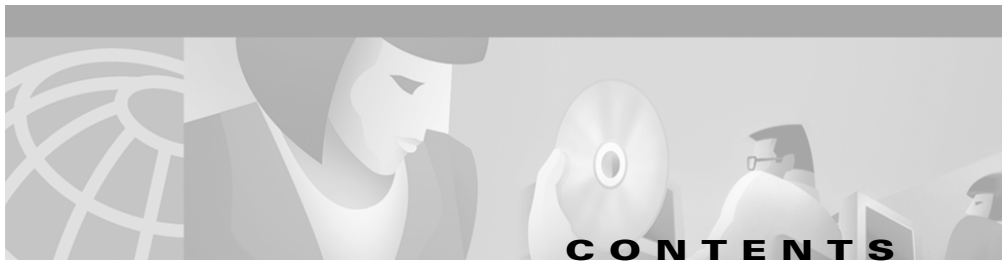
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Cisco 1710 Security Router Hardware Installation Guide
Copyright © 2005 Cisco Systems, Inc. All rights reserved.



About This Guide ix

Audience and Scope **x**

Organization **x**

Related Publications **x**

Conventions **xi**

Notes, Cautions, and Warnings **xi**

Commands **xiii**

Obtaining Documentation **xiv**

Cisco.com **xiv**

Documentation DVD **xiv**

Ordering Documentation **xv**

Documentation Feedback **xv**

Cisco Product Security Overview **xvi**

Reporting Security Problems in Cisco Products **xvi**

Obtaining Technical Assistance **xvii**

Cisco Technical Support Website **xvii**

Submitting a Service Request **xviii**

Definitions of Service Request Severity **xix**

Obtaining Additional Publications and Information **xix**

CHAPTER 1

Cisco 1710 Security Router Overview 1-1

Key Features **1-2**

Back Panel Ports and LEDs **1-4**

Front Panel LEDs **1-5**

- Router Memory **1-6**
 - Types of Memory **1-7**
 - Amounts of Memory **1-7**
- Unpacking the Router **1-8**
- Additional Required Equipment **1-8**

CHAPTER 2

Installing the Cisco 1710 Security Router 2-1

- Before Installing the Router **2-1**
- Connecting the Router **2-2**
- Connecting Power to the Router **2-5**
- Verifying Your Installation **2-6**
- Optional Installation Steps **2-7**
 - Connecting a PC **2-8**
 - Wall Mounting **2-9**

CHAPTER 3

Troubleshooting 3-1

- Contacting Your Reseller **3-1**
- Recovering a Lost Password **3-2**
 - Changing the Configuration Register **3-2**
 - Resetting the Router **3-4**
 - Resetting the Password **3-5**
 - Resetting the Configuration Register Value **3-6**
- Problem Solving **3-6**
 - Using OK LED Diagnostics **3-7**
 - Troubleshooting the Power System **3-7**

APPENDIX A **Technical Specifications** **A-1**

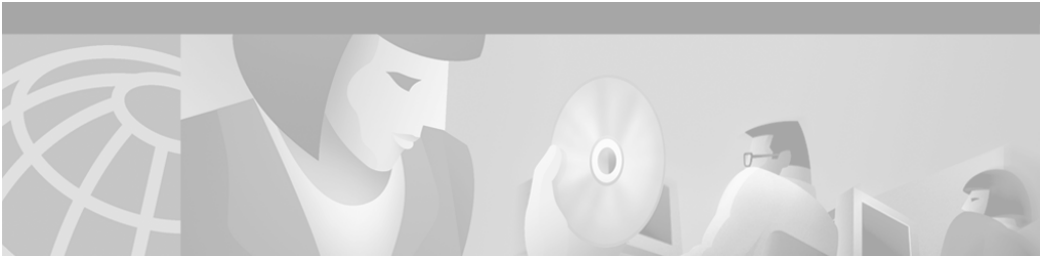
APPENDIX B **Cabling Specifications** **B-1**

Ethernet Cables **B-1**

Ethernet Network Cabling Guidelines **B-2**

Integrated Console Cable **B-2**

INDEX



About This Guide

This section discusses the intended audience, scope, and organization of the *Cisco 1710 Router Hardware Installation Guide* and defines the conventions used to convey instructions and information.

Cisco documentation and additional literature are available on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar, and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

Audience and Scope

This guide is for users who have some experience installing and maintaining networking hardware. We assume that Cisco 1710 router users are familiar with the terminology and concepts of local Ethernet and wide-area networking.

This guide describes the functional and physical features of the Cisco 1710 router and provides installation procedures, troubleshooting information, technical specifications, and cable and connector guidelines and specifications.

Organization

This guide is organized as follows:

- Chapter 1, “Cisco 1710 Security Router Overview,” describes the router features, front-panel LEDs, rear-panel LEDs, and connectors.
- Chapter 2, “Installing the Cisco 1710 Security Router,” describes how to install the router by connecting cables, power, and install WAN interface cards (WICs) and voice interface cards (VICs).
- Chapter 3, “Troubleshooting,” describes some problems that you might have with the router and how to solve these problems.
- Appendix A, “Technical Specifications,” lists the physical characteristics, environmental requirements, and power specifications for the router.
- Appendix B, “Cabling Specifications,” lists the physical characteristics of the cables and connectors used with the router.

Related Publications

The following publications provide related information on this product:

- *Cisco 1710 Router Software Configuration Guide* describes some common network scenarios and how to use the Cisco IOS command-line interface (CLI) to configure the router in these scenarios.
- *Cisco WAN Interface Cards Hardware Installation Guide* describes how to install and configure the WICs and VICs that are supported by the Cisco 1710 router.

- Cisco IOS command reference and configuration guides provide complete information about all Cisco IOS CLI commands and how to use them, as well as information on designing and configuring LANs and WANs.

Conventions

This guide uses the following conventions for instructions and information.

Notes, Cautions, and Warnings

Notes, cautions, and warnings use the following conventions and symbols:



Note

Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual.



Caution

This caution symbol means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Warning

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with the standard practices for preventing accidents.

Waarschuwing

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen.

Varoitus	Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista.
Attention	Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents.
Warnung	Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt.
Avvertenza	Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti.
Advarsel	Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker.
Aviso	Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes.

- ¡Atención!** Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes.
- Varning!** Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador.

Commands

Table 1 describes the syntax used with the commands in this document.

Table 1 *Command Syntax Guide*

Convention	Description
boldface	Commands and keywords.
<i>italic</i>	Command input that is supplied by you.
[]	Keywords or arguments that appear within square brackets are optional.
{x x x}	A choice of keywords (represented by x) appears in braces separated by vertical bars. You must select one.
^ or Ctrl	Represent the key labeled <i>Control</i> . For example, when you read ^D or <i>Ctrl-D</i> , you should hold down the Control key while you press the D key.
screen font	Examples of information displayed on the screen.
boldface screen font	Examples of information that you must enter.

Table 1 *Command Syntax Guide (continued)*

Convention	Description
< >	Nonprinting characters, such as passwords, appear in angled brackets.
[]	Default responses to system prompts appear in square brackets.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and

troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



Cisco 1710 Security Router Overview

This chapter introduces the Cisco 1710 Security router, also referred to in this guide as *the router*, and covers the following topics:

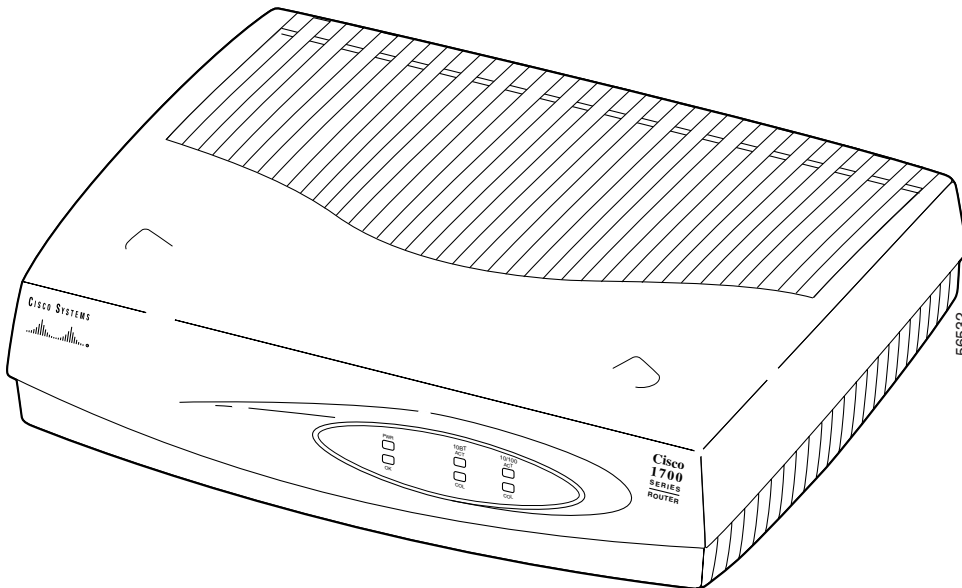
- [Key Features](#)
- [Back Panel Ports and LEDs](#)
- [Front Panel LEDs](#)
- [Router Memory](#)
- [Unpacking the Router](#)
- [Additional Required Equipment](#)

Key Features

As [Figure 1-1](#) shows, the Cisco 1710 Security router is a small desktop- or wall-mountable Virtual Private Network (VPN) router. The router is designed to provide security and privacy while accessing information across public IP networks. Useful in a variety of scenarios and configurations, the Cisco 1710 Security router can provide, for example:

- Secure site-to-site connections between remote offices, small branch offices, and corporate offices
- Secure remote access to mobile workers, telecommuters, and day-extenders
- Secure extranet access for customers and partners

Figure 1-1 Cisco 1710 Security Router



The router is equipped with a VPN module that provides hardware Triple DES (3DES) encryption.

Table 1-1 lists the key features of the Cisco 1710 Security router.

Table 1-1 Key Features

Feature	Description
One Fast Ethernet (10/100BASE-TX) port	<ul style="list-style-type: none"> • Operates in full- or half-duplex mode (with manual override available). • Supports autosensing for 10- or 100-Mbps operation.
One Ethernet (10BASE-T) port	Operates in full- or half-duplex mode; set by default to half-duplex mode (needs manual configuration for full-duplex support).
Console port	Supports router configuration and management with a directly connected terminal or PC. Supports up to 115.2 kbps.
Auxiliary port	Supports modem connection to the router, which can be configured and managed from a remote location. Supports up to 115.2 kbps.
VPN hardware-assisted 3DES encryption module	Provides IPSEC 3DES hardware encryption.
SNMP support	Router can be managed over a network using Simple Network Management Protocol (SNMP).
AutoInstall support	Configuration files can be easily downloaded to the router over a WAN connection.
Kensington security slot	Router can be secured to a desktop or other surface using Kensington lockdown equipment.
Support for Cisco IOS software features	Supports IP, IPX, AppleTalk, IBM, Open Shortest Path First (OSPF), NetWare Link Services Protocol (NLSP), Resource Reservation Protocol (RSVP), encryption, network address translation, and the Cisco IOS Firewall Feature Set.

Back Panel Ports and LEDs

This section describes the router back panel ports and LEDs, which are shown in [Figure 1-2](#) and described in [Table 1-2](#) and [Table 1-3](#).

Figure 1-2 Back Panel Ports and LEDs

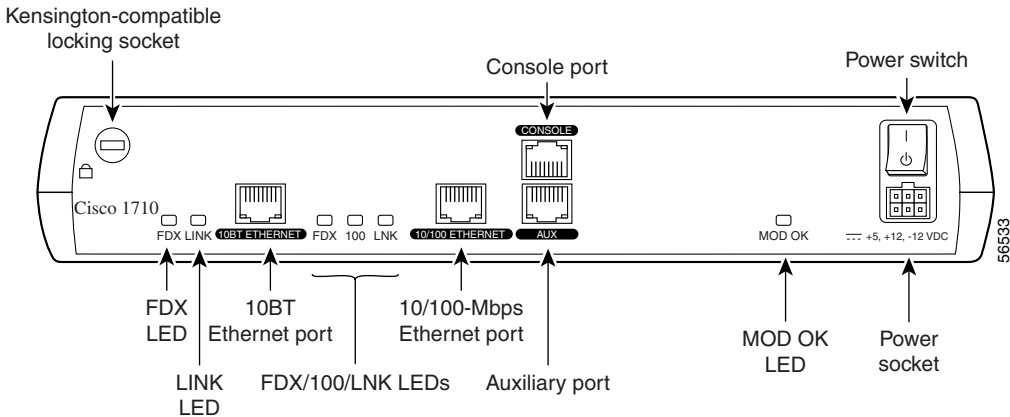


Table 1-2 Back Panel Connectors

Connector/Slot	Label/Color	Description
Ethernet port (left)	10BT ETHERNET (yellow)	Typically connects the router to the xDSL or cable modem. Can also be used to connect to the local network. This port supports both full- and half-duplex operation, but it is not autosensing. To use this port in full-duplex mode, you must use Cisco IOS software to reconfigure it from the default half-duplex setting.
Fast Ethernet port (right)	10/100 ETHERNET (yellow)	Typically connects the router to the local Ethernet network. Can also be used to connect to the xDSL or cable modem. This port autosenses the speed (10 Mbps or 100 Mbps) and duplex mode (full- or half-duplex mode) of the device to which it is connected and then operates at the same speed and in the same duplex mode.

Table 1-2 Back Panel Connectors (continued)

Connector/Slot	Label/Color	Description
Auxiliary port	AUX (black)	Connects to a modem for remote configuration with Cisco IOS software.
Console port	CONSOLE (blue)	Connects to a terminal or PC for local configuration using Cisco IOS software.
Power socket	+5, +12, -12 VDC	Connects the router to the external power supply.

Use the back panel LEDs during router installation to confirm that you have correctly connected all cables to the router.

Table 1-3 Back Panel LEDs

LED Label	Color	Description
FDX	Green	<ul style="list-style-type: none"> On solid—Ethernet port is operating in full-duplex mode. Off—Ethernet port is operating in half-duplex mode.
LINK	Green	On when the Ethernet link is operational.
100	Green	<ul style="list-style-type: none"> On solid—Fast Ethernet port is operating at 100 Mbps. Off—Fast Ethernet port is operating at 10 Mbps.
MOD OK	Green	On when the VPN hardware encryption module is installed and recognized by IOS.

Front Panel LEDs

Use the router front panel LEDs to determine network activity and status on the 10BASE-T Ethernet and 10/100BASE-TX Fast Ethernet ports. The front panel LEDs are illustrated in [Figure 1-3](#) and described in [Table 1-4](#).

Figure 1-3 Front Panel LEDs

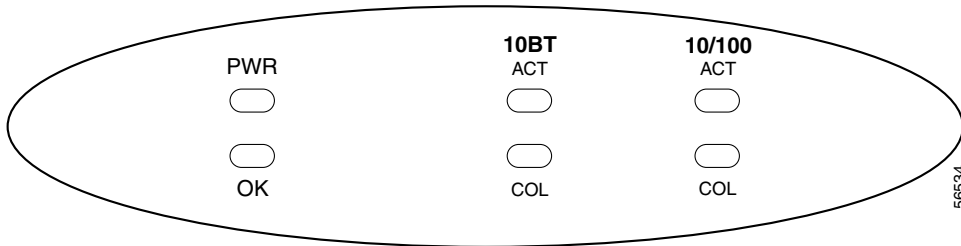


Table 1-4 Front Panel LEDs

LED Label	Color	Description
PWR	Green	On means that DC power is being supplied to the router.
OK	Green	On means that the router has successfully booted up and the software is functional. This LED blinks during the power-on self-test (POST), to indicate problems, or when the router is in ROM monitor mode. See Chapter 3, “ Troubleshooting ,” for information on how to use this LED for router diagnostics.
10BT and 10/100 ¹		
ACT	Green	Blinks when there is network activity on the associated Ethernet port.
COL	Yellow	Blinks when there are packet collisions on the Ethernet network.

1. These labels refer to the LEDs ACT and COL which are associated with each of the two Ethernet ports on the back of the router.

Router Memory

This section describes the types of memory available in the router and tells how to find out how much of each type is present.

Types of Memory

The Cisco 1710 Security router has the following types of memory:

- Dynamic random-access memory (DRAM)—This is the main storage memory for the router. DRAM is also called *working storage*. It contains the dynamic configuration information. The router stores a working copy of Cisco IOS software, dynamic configuration information, and routing table information in DRAM.
- Nonvolatile random-access memory (NVRAM)—This memory contains a backup copy of your configuration. If the power is lost or the router is turned off, this backup copy enables the router to return to operation without reconfiguration.
- Flash memory—This special kind of erasable, programmable memory contains a copy of the Cisco IOS software. You can load a new level of the operating system in every router in your network and then, when it is convenient, you can upgrade the whole network to the new level.

Amounts of Memory

Use the **show version** command to view the amount of DRAM, NVRAM, and Flash memory stored in your router. The following example of the **show version** command output displays the amount of memory stored in this router.

```
1710# show version
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-BK9NO3R2SY7-M), Experimental Version
12.2(20010418:203826) [lyhuang-sonic 141]
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 27-Apr-01 17:23 by lyhuang
.
.
cisco 1710 (MPC855T) processor (revision 0x201) with 29492K/32768K
bytes of memory.
Processor board ID JAB051004JX (986636533), with hardware revision
0000
MPC855T processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
1 Virtual Private Network (VPN) module(s)
```

32K bytes of non-volatile configuration memory.
 16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x0

Unpacking the Router

[Table 1-5](#) lists the items that come with your router. All these items are in the accessory kit that is inside the box that your router came in.

Table 1-5 Router Box Contents

• Power cord (black)
• Power supply
• Console cable, RJ-45 to DB-9 (light blue)
• Product documentation

Additional Required Equipment

Depending on your local network, you will require other items, listed in [Table 1-6](#), to complete your router installation.

Table 1-6 Additional Required Equipment

Equipment	When You Use It
Ethernet hub	A hub connects pieces of network equipment (including the Cisco 1710 Security router) to create a network. You can use a 10-, 100-, or 10/100-Mbps hub with the Cisco 1710 Security router.
Ethernet switch	A switch connects pieces of network equipment (including the Cisco 1710 Security router) to create a network. You can use a 10-, 100-, or 10/100-Mbps switch with the Cisco 1710 Security router.

Table 1-6 Additional Required Equipment (continued)

Equipment	When You Use It
An Internet connection through a broadband modem	A broadband modem is needed to provide access to the Internet. You will also need to arrange for and have an Internet Service Provider (ISP) install the necessary equipment and services for xDSL or cable Internet access, if such is not already present.
Straight-through RJ-45-to-RJ-45 cables	This cable connects the router to the Ethernet LAN and to the xDSL/cable modem. You will need one cable for each connection that requires this cable type.
Crossover RJ-45-to-RJ-45 cable and RJ-45-to-DB-25 port adapter	If you want to use a modem connection to allow for remote configuration of the Cisco 1710 Security router, you will need this type of cable and adapter.
Asynchronous modem	Connect a modem to the AUX port on the router when you want to configure the router from a remote location.

■ Additional Required Equipment



Installing the Cisco 1710 Security Router

This chapter of installation procedures for the Cisco 1710 Security router includes the following sections:

- [Before Installing the Router](#)
- [Connecting the Router](#)
- [Connecting Power to the Router](#)
- [Verifying Your Installation](#)
- [Optional Installation Steps](#)

Before Installing the Router

The Cisco 1710 Security router is shipped ready for desktop mounting. Before making the power and network connections, simply set the router on a desktop, shelf, or other flat surface.



Caution

The Cisco 1710 Security router is designed for desktop or wall mounting only. It is not to be placed in a stack of devices.



Note

For instructions on mounting the router on a wall, see the [“Wall Mounting”](#) section later in this chapter.

Be sure to read the safety information in *Regulatory Compliance and Safety Information for the Cisco 1700 Routers*, which comes with your router.

**Warning**

Read the installation instructions before you connect the system to its power source.

**Warning**

Do not work on the system or connect or disconnect cables during periods of lightning activity.

**Caution**

Do not place anything on top of the router that weighs more than 10 pounds (4.5 kg). Excessive weight on top of the router could damage the chassis.

Connecting the Router

The Cisco 1710 Security router is usually connected to your local Ethernet network through the 10/100 Fast Ethernet port, and to the Internet (by means of your xDSL/cable modem) through the 10BASE-T Ethernet port.

**Note**

These are the port assignments found in typical installations, but there is no firm requirement that the ports be connected this way. The Fast Ethernet port can be connected to the xDSL/cable modem, with the 10BASE-T Ethernet port connected to your LAN. The configuration chosen depends upon the needs and capabilities of your local network and the xDSL/cable modem you are provided with.

You must provide the following items for these connections:

- Two straight-through, RJ-45-to-RJ-45, Ethernet cables
- A 10-Mbps, 100-Mbps, or 10-/100-Mbps Ethernet hub or switch
- An xDSL/cable modem installed by your ISP

**Warning**

The ports labeled 10/100 ETHERNET, 10BT ETHERNET, and CONSOLE are safety extra-low voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits. Because BRI circuits are treated like telephone-network voltage, avoid connecting the SELV circuits to the telephone network voltage (TNV) circuits. (To see translated versions of this warning, refer to the *Regulatory Compliance and Safety Information for the Cisco 1700 Routers* document that came with the router.)

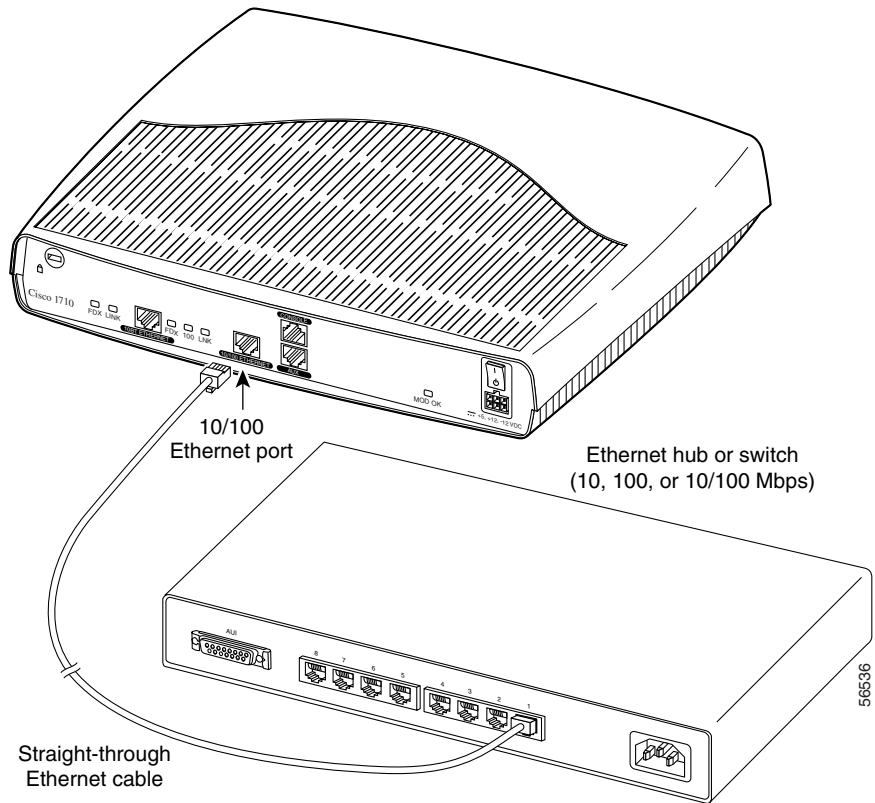
**Caution**

Always connect the Ethernet cables to the Ethernet ports on the router. Accidentally connecting a cable to the wrong port can damage your router.

To connect the router, follow these steps. See [Figure 2-1](#).

-
- Step 1** Connect one end of an Ethernet cable to the 10/100 ETHERNET port (the port on the right).
 - Step 2** Connect the other end of the cable to a network port on the hub or switch.
 - Step 3** Connect one end of a second Ethernet cable to the 10BT ETHERNET port on the router (the port on the left).
 - Step 4** Connect the other end to your xDSL/cable modem.
-

Figure 2-1 Connecting the Router to the Local Network

**Note**

The 10BASE-T Ethernet port does not perform autosensing for full-/half-duplex operation, and the default setting is for half-duplex operation. To enable full-duplex operation on the 10BASE-T port, you will need to use the CISCO IOS software to reconfigure the router.

Connecting Power to the Router

Please read the following warnings before connecting power to the router.



Warning

The power supply is designed to work with TN power systems.



Warning

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120VAC, 15A U.S. (240VAC, 16A international) is used on the phase conductors (all current-carrying conductors).



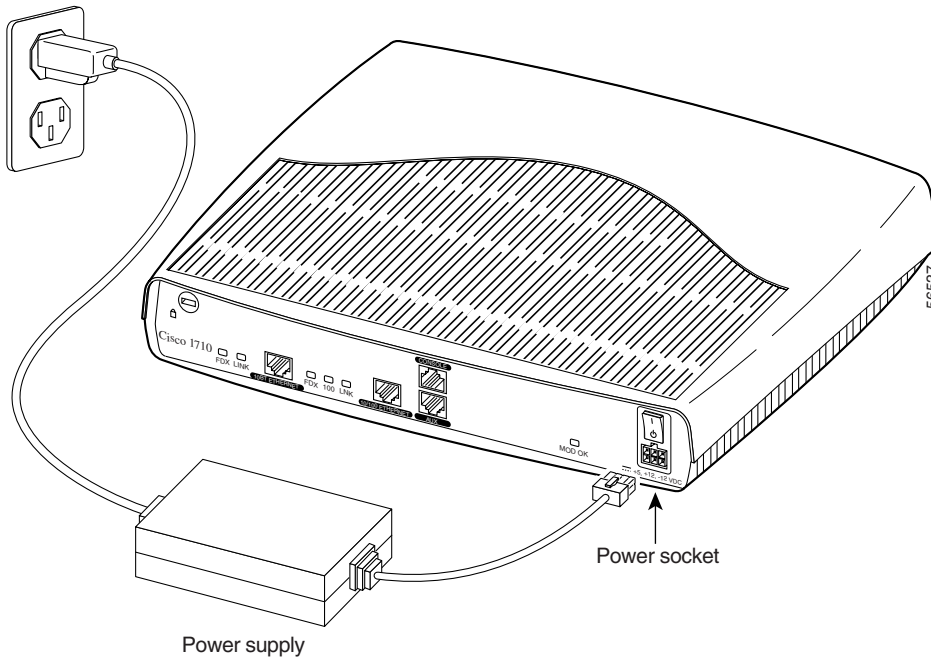
Warning

This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.

Perform the following steps (see [Figure 2-2](#)) to connect power to the router and to turn the router on:

-
- Step 1** Connect the attached power supply cord to the power socket (labeled +5,+12,-12 VDC) on the router rear panel.
 - Step 2** Connect one end of the separate power cord to the socket on the power supply.
 - Step 3** Connect the other end of the separate power cord to a power outlet.
 - Step 4** Press the router power switch to on (I).
 - Step 5** Confirm that the router has power by checking that the PWR LED on the front panel is on.
-

Figure 2-2 Connecting the Power Supply



Verifying Your Installation

You can verify that you have correctly installed the router by checking the router LEDs as described in [Table 2-1](#).

Use the front panel OK LED to determine any problems with the router. When the router first boots up, it performs a power-on self-test (POST). If the router detects a problem during the POST, the OK LED blinks in different patterns (described in Chapter 3, “Troubleshooting”) depending on the problem. A pattern consists of a specific number of blinks that is repeated until the router is turned off. If the router experiences any of these problems, contact your Cisco reseller.

Table 2-1 LEDs on the Cisco 1710 Router

LED	Panel	What to Look For
PWR	Front	On when power is being supplied to the router.
OK	Front	On when the router software is loaded and functional. Blinking when the router is running a power-on self-test (POST). Continuous blinking can indicate a problem with the router, although it will also blink if the router is in ROMMON mode. Refer to Chapter 3, “Troubleshooting,” for more information.
LNK (one for each Ethernet port)	Back	On when the router is correctly connected to the local Ethernet network through the 10BT and 10/100 ETHERNET ports.
FDX (one for each Ethernet port)	Back	On when the associated Ethernet port is operating in full-duplex mode. The 10BASE-T port does not perform autosensing for full-/half-duplex operation; the default setting is for half-duplex operation.
100 (10/100 Ethernet only)	Back	On when the 10/100 ETHERNET port is operating at 100 Mbps.
10BT and 10/100 ACT	Front	Blinking when there is network traffic on the Ethernet LAN connections.

Optional Installation Steps

This section describes some installation steps that you might or might not use, depending on your site and how you are configuring the router. This chapter describes the following procedures:

- [Connecting a PC](#)
- [Wall Mounting](#)

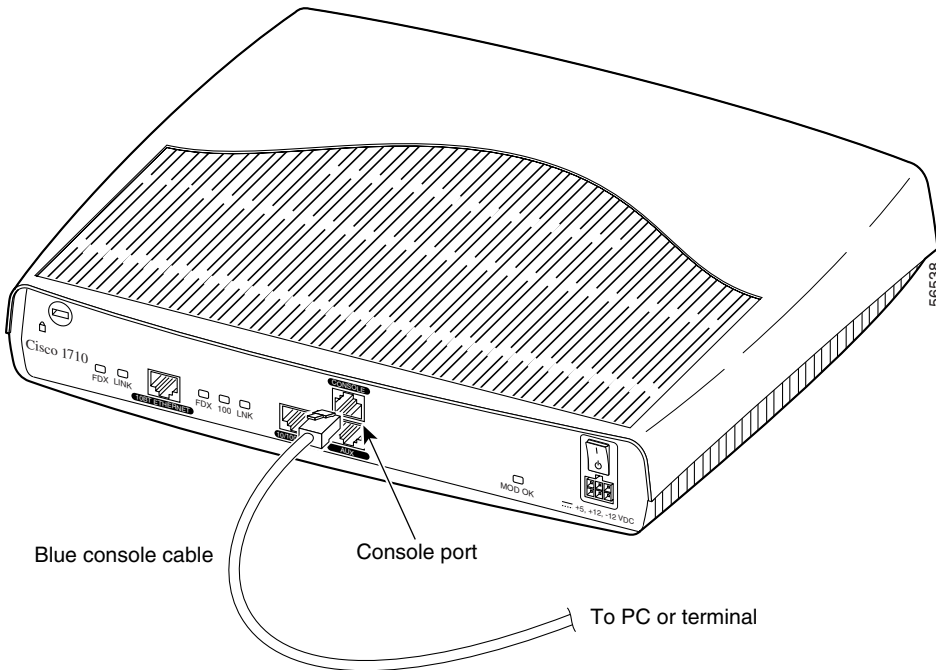
Connecting a PC

If you want to configure the router using the Cisco IOS command-line interface (CLI), you must connect the router console port to a terminal or PC. The console cable required for this connection is included with the router. You will need an available console (serial) port on the PC or terminal.

To configure the router with a PC, the PC must have some type of terminal emulation software installed. The software should be configured with the following parameters: 9600 baud, 8 data bits, no parity bits, 1 stop bit. Refer to the *Cisco 1710 Security Router Software Configuration Guide*, which comes with your router, for detailed information about configuring the router using Cisco IOS software.

Follow these steps to connect the router to a terminal or PC:

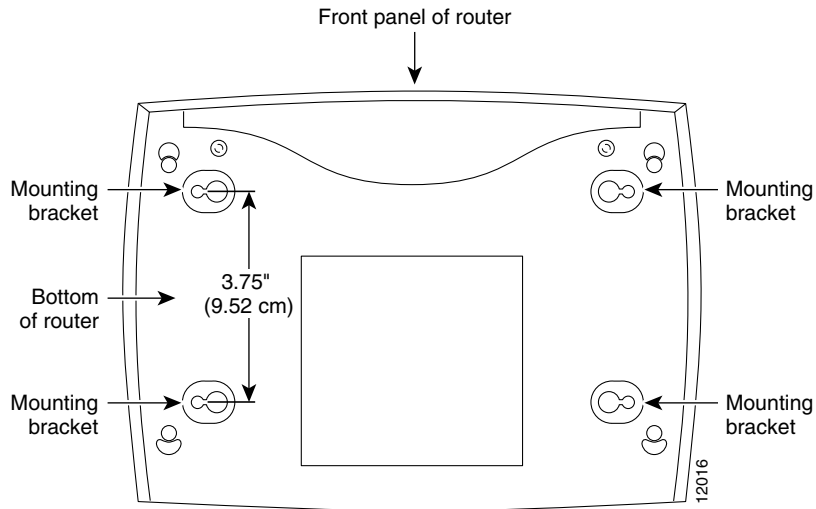
-
- Step 1** Connect the RJ-45 end of the console cable to the blue CONSOLE port on the router, as shown in [Figure 2-3](#).
 - Step 2** Connect the DB-9 end of the console cable to console (serial) port of the terminal or PC. If your terminal or PC does not have a DB-9 console port, or if the cable does not fit the port, you must provide the correct adapter for that port.
-

Figure 2-3 Connecting the Console Cable to the Router

Wall Mounting

The Cisco 1710 Security router can be wall-mounted using two number-6, 3/4-inch screws and the molded mounting brackets on the bottom of the hub. You must provide the screws. We recommend using pan-head or round-head screws.

[Figure 2-4](#) shows the locations of the wall-mounting brackets on the router.

Figure 2-4 Wall-Mounting Brackets—Bottom of Router

To mount the router on a wall or other surface:

-
- Step 1** Install the two screws 3.75 inches (9.52 centimeters) horizontally apart on a wall or other vertical surface.
- The screws should protrude 0.25 inch (0.64 centimeter) from the surface of the wall.
- Step 2** Hang the router on the screws with either the left-side or right-side mounting brackets so that
- The LEDs are visible to the user—The LEDs indicate the router operating status, so the LEDs should be easily visible.
 - The power supply does not hang from its cable—If the power supply is not supported, it might disconnect from the cable that connects it to the router.
-

**Caution**

If you install the screws in drywall, use hollow-wall anchors (1/8 inch by 5/16 inch) to secure the screws. If the screws are not properly anchored, the strain of the cables connected to the router back panel connectors could pull the router from the wall.



Troubleshooting

Use the information in this chapter to help isolate problems you might encounter with the Cisco 1710 Security router or to rule out the router as the source of the problem.

This chapter contains the following sections:

- [Contacting Your Reseller](#)
- [Recovering a Lost Password](#)
- [Problem Solving](#)

Contacting Your Reseller

If you cannot locate the source of a problem, contact your local reseller for advice. Before you call, you should have the following information ready:

- Chassis type and serial number
- Maintenance agreement or warranty information
- Type and version number of the Cisco IOS installed on your router
- Date you received the router
- Brief description of the problem
- Brief description of the steps you have taken to isolate the problem
- Output from the **show tech-support** command

Recovering a Lost Password

This section describes how to recover a lost enable or enable secret password. The process of recovering a password consists of the following major steps:

- [Changing the Configuration Register](#)
- [Resetting the Router](#)
- [Resetting the Password](#) (for lost enable secret passwords only)
- [Resetting the Configuration Register Value](#)



Note

See the “Technical Support Help” section on Cisco.com for additional information on replacing enable secret passwords.

Changing the Configuration Register

Perform the following steps to change the configuration register:

- Step 1** Connect an ASCII terminal or a PC running a terminal-emulation program to the CONSOLE port on the back panel of the router. See “[Connecting a PC](#)” in Chapter 2, “Installing the 1710 Security Router.”
- Step 2** Configure the terminal to operate at 9600 baud, 8 data bits, no parity, and 1 stop bit.
- Step 3** Reboot the router by pressing the power switch to the off position, and then pressing it to the on (|) position.
- Step 4** At the user EXEC prompt (Router>), enter the **show version** command to display the existing configuration register value (shown at the end of this example output). You will see output similar to the following:

```
1710#show version
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-BK9NO3R2SY7-M), Experimental Version
12.2(20010418:203826) [lyhuang-sonic 141]
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 27-Apr-01 17:23 by lyhuang
Image text-base: 0x800080E0, data-base: 0x80EA267C

ROM: System Bootstrap, Version 12.2(1r) XE1, RELEASE SOFTWARE (fc1)
```

```
uut_1 uptime is 2 days, 4 hours, 21 minutes
System returned to ROM by power-on
System image file is "flash:Imxiang/c1700-bk9no3r2sy7-mz.0427"

cisco 1710 (MPC855T) processor (revision 0x201) with 29492K/32768K
bytes of memory.
Processor board ID JAB051004JX (986636533), with hardware revision
0000
MPC855T processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
1 Virtual Private Network (VPN) module(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x0
```

Step 5 Record the setting of the configuration register. The setting is usually 0x2102 or 0x102.

Step 6 Record the break setting.

- Break enabled—bit 8 is set to 0.
- Break disabled (default setting)—bit 8 is set to 1.



Note To enable break, enter the **config-register 0x01 EXEC** command.

Resetting the Router

Perform the following steps to reset the router:

-
- Step 1** Do one of the following:
- If break is enabled, go to [Step 2](#).
 - If break is disabled, turn the router off, wait 5 seconds, and turn it on again. Within 60 seconds, press the **Break** key. The terminal displays the ROM monitor prompt. Go to [Step 3](#).



Note Some terminal keyboards have a key labeled Break. If your keyboard does not have a Break key, refer to the documentation that came with the terminal for instructions on how to send a break. To send a break in Windows HyperTerminal, press **Ctrl-Break**.

- Step 2** Send a break. The terminal displays the following prompt:

```
rommon 2>
```

- Step 3** Enter **confreg 0x142** as follows to reset the configuration register:

```
rommon 2> confreg 0x142
```

- Step 4** Initialize the router by entering the **reset** command:

```
rommon 2> reset
```

The router resets, and the configuration register is set to 0x142. The router boots the system image in Flash memory and displays the following:

```
--- System Configuration Dialog ---
```

- Step 5** Enter **no** in response to the prompts until the following message is displayed:

```
Press RETURN to get started!
```

- Step 6** Press **Return**. The following prompt appears:

```
Router>
```

- Step 7** Enter the **enable** command to enter privileged EXEC mode. Configuration changes can be made only in this mode:

```
Router> enable
```

The prompt changes to the privileged EXEC prompt:

```
Router#
```

- Step 8** Enter the **show startup-config** command to display an enable password in the configuration file:

```
Router# show startup-config
```

If you are recovering an enable secret password, it is not displayed in the **show startup-config** command output. Complete the password recovery process by performing the steps in the following section, “[Resetting the Password.](#)”

If you are recovering an enable password, skip the following section, “[Resetting the Router.](#)” and complete the password recovery process by performing the steps in the next section, “[Resetting the Configuration Register Value.](#)”

Resetting the Password

- Step 1** Enter the **configure terminal** command to enter configuration mode:

```
Router# configure terminal
```

- Step 2** Enter the **enable secret** command to reset the enable secret password in the router:

```
Router(config)# enable secret gobbledegook
```

- Step 3** Enter the **config-register** command and the original configuration register value that you recorded in [Step 5](#) in “Changing the Configuration Register.”

- Step 4** Press **Ctrl-Z** to exit configuration mode.

```
Router(config)# Ctrl-Z
```

- Step 5** Save your configuration changes:

```
Router# copy running-config startup-config
```

Resetting the Configuration Register Value

Once you have recovered or reconfigured a password, you need to reset the configuration register value. Follow these steps:

-
- Step 1** Enter the **configure terminal** command to enter configuration mode:
- ```
Router# configure terminal
```
- Step 2** Enter the **config-register** command and the original configuration register value that you recorded in [Step 5](#) in “Changing the Configuration Register.”
- Step 3** Press **Ctrl-Z** to exit configuration mode:
- ```
Router (config)# Ctrl-Z
```
- Step 4** Reboot the router, and enter the recovered password.
-

Problem Solving

The key to problem solving is to isolate the problem to a specific subsystem by comparing what the router is doing to what it should be doing.

In problem solving, consider the following subsystems of the router:

- Cables—Check all the external cables that connect the router to the network.
- Power system—Check the external power source, power cable, router power supply, and circuit breaker. Check for inadequate ventilation or air circulation that might cause overheating.
- VPN hardware encryption module—See the LED on the router back panel to help identify a failure.
- xDSL/cable modem configuration—Make certain that your xDSL or cable modem is configured and functioning properly.

Using OK LED Diagnostics

Use the front panel OK LED to determine any problems with the router. When the router first boots up, it performs a power-on self-test (POST). If the router detects a problem during the POST, the OK LED blinks in different patterns, depending on the problem. A pattern consists of a specific number of blinks that is repeated until the router is turned off. If the router experiences any of these problems, contact your Cisco reseller. [Table 3-1](#) describes the blinking patterns that you might observe on the OK LED.



Note

If the router is in ROMMON mode, the OK LED will blink continuously, rather than in any of the patterns described in [Table 3-1](#).

Table 3-1 OK LED Blinking Patterns

Number of Blinks	Meaning
2	The MPC855T processor dual-port random-access memory (DPRAM) failed.
3	The parameter RAM area of the MPC855T DPRAM failed.
4	The MPC855T system protection control register has a write failure.
5	The router cannot detect the dynamic random-access memory (DRAM).
6	The user-programmable machine has a write failure.
9	The router DRAM failed.

Troubleshooting the Power System

If the external power supply for the router fails, it should be returned to your Cisco reseller. [Table 3-2](#) list symptoms and possible causes of power problems.

Table 3-2 Troubleshooting the Power System

Symptom	Possible Cause(s)
Router shuts down after being on a short time.	<ul style="list-style-type: none"> • Make sure that the area in which the router is installed meets the environmental site requirements in Appendix A, “Technical Specifications,” later in this guide, and in the “Site Requirements” section in the <i>Regulatory Compliance and Safety Information for the Cisco 1700 Routers</i>, which comes with your router. • If the front panel PWR LED is not on, the power supply has failed.
The router attempts to boot, but all the LEDs remain off.	The power supply has failed.
The router is on, but the front panel PWR LED is off.	The power supply has failed.
The front panel PWR LED is on, the front panel OK LED is off, and the router does not pass console or physical layer transmission data.	The power supply has failed.



Technical Specifications

Table A-1 lists hardware and operating specifications for the Cisco 1710 router.

Table A-1 Router Specifications

Description	Specification
Console port	RJ-45
Auxiliary port	RJ-45
Ethernet ports	RJ-45
Dimensions	
H x W x D	3.1 x 11.2 x 8.7 in. (7.85 x 28.4 x 22.1 cm)
Weight	2.7 lb (1.25 kg)
Power supply	
External	Universal AC/DC switching—Supplies +5V, +12V, and -12V
On board	Supplies 3.3V
Power consumption	15W
Operating Conditions	
Operating temperature	32 to 104° F (0° to 40°C)
Storage temperature	-4 to 149° F (-20° to 65°C)
Operating humidity	10 to 85%, noncondensing



Cabling Specifications

This appendix describes cables and cabling guidelines for the Cisco 1710 Security router and contains the following sections:

- [Ethernet Cables](#)
- [Ethernet Network Cabling Guidelines](#)
- [Integrated Console Cable](#)

Ethernet Cables

This section describes the Ethernet cables that are used to connect the router to your local Ethernet network. 10/100BASE-TX routers, such as the Cisco 1710 Security routers, require Category 5 unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable.

Table B-1 *Straight-Through Ethernet Cable (RJ-45-to-45) Pinouts*

RJ-45 Pin ¹	Signal	Direction	RJ-45 Pin
1	TX+	—>	1
2	TX-	—>	2
3	RX+	<—	3
6	RX-	<—	6

1. Pins 4, 5, 7, and 8 are not used for signaling.

Ethernet Network Cabling Guidelines

Table B-2 provides some guidelines for creating Ethernet networks. Parameters might vary, depending on the manufacturer of the network equipment.

Table B-2 Ethernet Cabling Guidelines

Parameter	10BASE-T	100BASE-TX
Maximum segment length	100 meters	100 meters
Maximum number of segments per network	5	<ul style="list-style-type: none"> • With Class I repeaters: 1 • With Class II repeaters: 2
Maximum hop count ¹	4	<ul style="list-style-type: none"> • With Class I repeaters: none • With Class II repeaters: 1
Maximum number of nodes per segment	1024	1024
Cable type required	UTP Category 3, 4, or 5	UTP Category 5 or STP

1. Hop count = Routing metric used to measure the distance between a source and a destination.

Integrated Console Cable

A console cable is provided with your router. Use this DB-9-to-RJ-45 integrated console cable (blue) to connect your router to a PC or terminal.

Table B-3 describes the wiring for the router's CONSOLE port, the integrated console cable, and the console (serial) port of the PC or terminal.

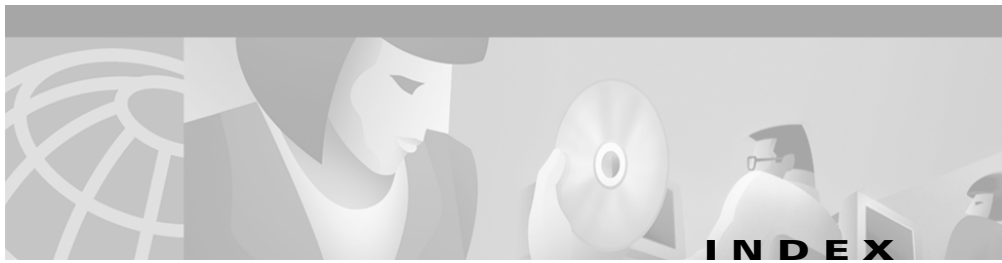
Table B-3 Integrated Console Cable Pinouts

Signal Name at the CONSOLE Port of Router	RJ-45 Pin at the Router End of the Cable	DB-9 Pin at the PC/Terminal End of the Cable	Signal Name at the PC/Terminal Port
RTS	1	8	CTS
DTR	2	6	DSR

Table B-3 *Integrated Console Cable Pinouts (continued)*

Signal Name at the CONSOLE Port of Router	RJ-45 Pin at the Router End of the Cable	DB-9 Pin at the PC/Terminal End of the Cable	Signal Name at the PC/Terminal Port
TXD	3	2	RXD
GND	4	5	GND
GND	5	5	GND
RXD	6	3	TXD
DSR	7	4	DTR
CTS	8	7	RTS

■ Integrated Console Cable



A

- accessory kit [1-8](#)
- ACT LED [1-6](#)
- adapter, included [1-8](#)
- audience [x](#)
- auxiliary port
 - description (table) [1-3](#)
 - specifications (table) [A-1](#)

B

- back panel
 - connectors
 - descriptions (table) [1-4](#)
 - illustration [1-4](#)
 - LEDs
 - descriptions (table) [1-5](#)
 - illustration [1-4](#)
- break
 - enabling [3-3](#)
 - sending to router [3-4](#)

C

- cable pinouts, Ethernet (table) [B-1](#)
- cables
 - included with router [1-8](#)
- cabling requirements for Ethernet networks (table) [B-2](#)
- caution described [xi](#)
- chassis dimensions (table) [A-1](#)
- COL LED [1-6](#)
- command
 - config-register [3-3](#)
 - configure terminal [3-5, 3-6](#)
 - copy [3-5](#)
 - enable [3-4](#)
 - enable secret [3-5](#)
 - reset [3-4](#)
 - show startup-config [3-5](#)
 - show version [3-2](#)
- command conventions [xiii](#)
- config-register command [3-3](#)
- configuration register
 - changing [3-2](#)
 - displaying [3-2](#)
 - setting [3-2, 3-4, 3-6](#)

configure terminal command [3-5, 3-6](#)

connecting

Ethernet cable [2-2](#)

power cord [2-5](#)

router to a PC [2-8](#)

console port

connecting [2-8](#)

description (tables) [1-3, 1-5](#)

illustration [1-4](#)

specifications (table) [A-1](#)

conventions

command [xiii](#)

text [xi](#)

copy command [3-5](#)

D

documentation

included [x](#)

DRAM [1-7](#)

E

enable command [3-4](#)

enable secret command [3-5](#)

Ethernet cable

connecting [2-2](#)

pinouts (table) [B-1](#)

Ethernet cabling guidelines (table) [B-2](#)

Ethernet port

connecting [2-2](#)

descriptions (tables) [1-3, 1-4](#)

illustration [1-4](#)

specifications [A-1](#)

F

Flash memory [1-7](#)

front panel

illustration [1-2](#)

LEDs

descriptions of (table) [1-6](#)

illustration [1-6](#)

H

hub

connecting to [2-3](#)

description (table) [1-8](#)

I

installation

preparing for [2-1](#)

verifying [2-6](#)

K

Kensington security slot (table) [1-3](#)

L

LEDs

back panel

description (table) [1-4](#)

illustration [1-4](#)

front panel

description (table) [1-6](#)

illustration [1-6](#)

OK LED diagnostics [2-6, 3-7](#)

using to verify installation [2-6](#)

M

memory

displaying amounts of [1-7](#)

DRAM [1-7](#)

Flash [1-7](#)

NVRAM [1-7](#)

show version command [1-7](#)

types of, in router [1-7](#)

modem

description (table) [1-9](#)

support (table) [1-3](#)

N

note described [xi](#)

NVRAM, [1-7](#)

O

OK LED

description (table) [1-6](#)

diagnostics [2-6, 3-7](#)

operating temperatures (table) [A-1](#)

organization, document [x](#)

P

password recovery [3-2 to 3-6](#)

PC

connecting to router [2-8](#)

terminal emulation settings [2-8](#)

pinouts, Ethernet cable [B-1](#)

power, troubleshooting [3-8](#)

power socket

connecting [2-5](#)

illustration [1-4](#)

power specifications [A-1](#)

problem solving [3-6](#)

publications

see documentation

PWR LED description (table) [1-6](#)

R

recovering a lost password [3-2](#)

reset command [3-4](#)

router

 unpacking [1-8, ?? to 1-8](#)

router specifications [A-1](#)

S

show startup-config command [3-5](#)

specifications, router [A-1](#)

switch

 connecting to [2-3](#)

 description (table) [1-8](#)

T

terminal emulation, settings for [2-8](#)

text conventions [xi](#)

troubleshooting

 password recovery [3-2 to 3-6](#)

 power system [3-8](#)

 using the OK LED [2-6, 3-7](#)

U

unpacking the router [1-8, ?? to 1-8](#)

W

wall mounting [2-9](#)