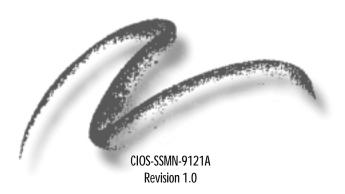
Cisco Hardware and the IOS



Wave Technologies International, Inc. is an independent entity from Cisco Systems, Inc. and is not affiliated with Cisco Systems, Inc. in any manner. This study guide and/or material is not sponsored by, endorsed by, or affiliated with Cisco Systems, Inc. Cisco[®], Cisco Systems[®], CCDATM, CCNATM, CCDPTM, CCNPTM, CCIETM, CCSITM, the Cisco Systems logo and the CCIE logo are trademarks or registered trademarks of Cisco Systems, Inc. in the United States and certain other countries. All other trademarks are trademarks of their respective owners.

Cisco Hardware and the IOS CIOS-SSMN-9121A Revision 1.0 ©1988-2000 Wave Technologies International, Inc. Practical Cisco Routers, Joe Habraken • ©1999 by Que Corporation* All rights reserved.

Printed in the United States of America. No part of this book may be used or reproduced in any form or by any means, or stored in a database or retrieval system, without prior written permission of the publisher. Making copies of any part of this book for any purpose other than your own personal use is a violation of United States copyright laws. For information, contact Wave Technologies International, Inc., 10845 Olive Blvd., Suite 250, St. Louis, Missouri 63141.

This book is sold as is, without warranty of any kind, either express or implied, respecting the contents of this book, including, but not limited to, implied warranties for the book's quality, performance, merchantability, or fitness for any particular purpose. Neither Wave Technologies International, Inc., nor its dealers or distributors shall be liable to the purchaser or any other person or entity with respect to any liability, loss, or damage caused or alleged to be caused directly or indirectly by this book.

Wave Technologies International, Inc. is an independent entity from Cisco Systems, Inc. and is not affiliated with Cisco Systems, Inc. in any manner. This study guide and/or material is not sponsored by, endorsed by, or affiliated with Cisco Systems, Inc. Cisco[®], Cisco Systems[®], CCDATM, CCNATM, CCDPTM, CCNPTM, CCIETM, CCSITM, the Cisco Systems logo and the CCIE logo are trademarks or registered trademarks of Cisco Systems, Inc. in the United States and certain other countries. All other trademarks are trademarks of their respective owners.

*Portions of chapter 4 and the glossary of *Practical Cisco Routers* were used in the writing of this book.

Trademarks

Trademarks and registered trademarks of products mentioned in this book are held by the companies producing them. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

The Wave logo is a registered trademark of Wave Technologies International, Inc., St. Louis, Missouri.

Copyright of any screen captures in this book are the property of the software's manufacturer.

Mention of any products in this book in no way constitutes an endorsement by Wave Technologies International, Inc.

 $10 \ 9 \ 8 \ 7 \ 6 \ 5 \ 4 \ 3 \ 2 \ 1$

SELF STUDY Contents

Introduction	1
Course Purpose	1
Course Goals	
Technology Walkthroughs	2
Simulations	3
Videos	
Assessment	
Hardware Requirements	4
Chapter 1—Introduction	5
Objectives	6
Pre-Test Questions	6
Introduction	7
Router Ports	
Router Port Definition	
Ethernet Ports	
Serial Ports	
Basic Rate Interface (BRI) Ports	
Port Configuration Basics 10	
Telnet Session	
Direct Cable Connection 10	
Physical Connections 10	
Loading a Configuration	
Nonvolatile RAM1	
Trivial File Transfer Protocol Server12	
Summary12	
Post-Test Questions12	2
Chapter 2—Cisco IOS 15	5
Objectives	6
Pre-Test Questions10	
Introduction	7
How to Read a Cisco Command Display18	8
IOS Overview	
Navigation from the Command Line	5
Command Structure	6

Command Modes	28
User Exec and Privileged Exec Modes	. 29
Configuration Mode	
Basic IOS Commands	33
Basic Configuration with the Setup Command	
Common Commands	
Using Help	52
Summary	
Post-Test Questions	
Chapter 3—Managing the IOS on a Router	57
Objectives	58
Pre-Test Questions	58
Introduction	
Memory Types	
Passwords	
Enable Password	. 62
Enable Secret Password	. 62
Line Password	. 64
Login Command	. 64
Console Password	
Virtual Terminal Password	. 66
Setting Up Usernames and Passwords	. 68
Disabling the Enable Password	. 68
Getting Around Lost Passwords	. 69
Loading the IOS	70
Router Boot Sequence	. 71
Boot System Command	. 72
The IOS and TFTP	72
Working with Configuration Files	. 73
Copying Configuration Files to the Network	. 73
Copying Configuration Files from the Network	. 73
Cisco Discovery Protocol	
Checking Out the Internetwork Neighborhood	
Viewing CDP Neighbors	
Summary	78
Post-Test Questions	79

Chapter 4—Router Configuration	81
Objectives	82
Pre-Test Questions	
Introduction	
Anatomy of a Router	
Router Components	
Router CPUs	
Router Memory	86
Setting Up a New Router	
Connecting the Console	
Setting Up Terminal Emulation Software	
Establishing Communications between the Router and Console	90
Connecting the Router to the Network	91
A Final Word on Physical Router Connections	
Basic Router Configuration	95
Configuring the Router	
Working with the System Configuration Dialog Box	
Saving a Configuration	103
Loading a Configuration	105
Interfaces	106
Router Interfaces	106
LAN Interfaces	110
Serial Interfaces	110
Logical Interfaces	110
Port Configuration	112
Network Configuration	
Summary	
Post-Test Questions	114
1 · · · · · · · · · · · · · · · · · · ·	117
Objectives	118
Pre-Test Questions	118
Introduction	119
Managing the Configuration	120
Configuration Registry	120
Boot Options	120
Backup and Restore	
Backing Up Configuration Files to a TFTP Server	
Restoring Configuration Files from a TFTP Server	
Back Up and Upgrade the Cisco IOS Using tftp	125

Monitoring Network Traffic	136
Common Monitoring Options	
Debugging	136
Network Security and Session Monitoring	137
Access Lists and vty Control	138
Standard Access List Configuration	138
Controlling vty Access	144
Extended Access lists	145
Configuring Extended Access Lists	145
Named Access Lists	146
Summary	148
Post-Test Questions	148
Chapter 6—Advanced LAN Design	151
Objectives	152
Pre-test questions	152
Introduction	153
LAN Standards	153
IEEE Standards	154
Ethernet	156
Token Ring	159
FDDI	160
LAN Encapsulation	161
Encapsulation and OSI Layers	162
Addressing and Header Formats	
LAN Packet Structure	164
VLAN Packet Structure	166
LAN Switch Configuration	167
Catalyst 1900 Nomenclature	167
Catalyst 1900 Features	
Basic Configuration of the Catalyst 1900	
Summary	
Post-Test questions	203
Appendix A—Answers to Pre-Test and Post-Test Questions	205
Glossary	211
Index	239

SELFSTUDY

Introduction

COURSE PURPOSE

This manual is a component of the curriculum offered by Wave Technologies International for Cisco CCNA[™] certification. This training program is designed to provide network professionals and support staff with the knowledge they need to achieve CCNA certification.

This self-study manual, *Cisco Hardware and the IOS*, along with the companion manuals, *Introduction to Networking* and *Protocols and the Network*, will cover the major components and skills needed to achieve CCNA certification.

In this manual, you will be introduced to Cisco hardware and Cisco's Internetworking Operating System (IOS). IOS is your access point to router hardware and network configuration. This book covers the concepts and procedures used to configure and manage Cisco routers, including detailed information about console commands. You will also be introduced to Cisco's online help function.

The CCNA certification exam requires that you have a thorough understanding of memory management, port configuration, and selected IOS commands. This manual covers these topics.

The CCNA exam also requires you to have a thorough understanding of networking concepts and protocol configuration. These topics will be covered in the companion manuals, *Introduction to Networking* and *Protocols and the Network*.

It is assumed that anyone using this material has a basic understanding of networking and network protocols.

COURSE GOALS

This course will provide you with information related to the following topics:

- Cisco hardware overview
- Types of memory in a Cisco router
- Configuration files
- Loading the Internet Operating System (IOS)
- Managing the configuration
- Configuring ports
- Types of ports on a router
- Reading the screen
- Login modes of the IOS
- Controlling passwords
- The command-line interface (CLI)
- Use of a TFTP server
- Router startup
- Copying a router configuration
- Saving a router configuration
- Router access lists
- Backup and upgrade of a router

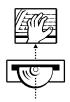
TECHNOLOGY WALKTHROUGHS

The walkthroughs in this manual are designed to give you samples of various Cisco IOS commands. In most cases, you will need access to a Cisco router to complete the walkthroughs. However, this may not always be convenient. If you do not have access to a router, read through the sample to familiarize yourself with the technology.

NOTICE:

The walkthroughs in this self-study product are designed to be used on a system that is designated for training purposes *only*. Practicing on a LAN or workstation that is used for other purposes may cause configuration problems, which could require a reinstallation and/or restoration of the original configuration. Please keep this in mind.

SIMULATIONS



Throughout the course, you will see icons asking you to practice the concepts you have learned in that chapter using NEXTSim. NEXTSim is an interactive simulation product that provides you with scenario-based training and hands-on experience in a *safe* environment. NEXTSim is part of the Interactive Learning CD-ROM that is included with this course. This tool should be used strictly as a supplement to the course and not to replace the course content.

VIDEOS



Digital video is a key element of the Interactive Learning CD-ROM that is included with this course. Digital video lessons describe key concepts covered in the manual. Often concepts are best understood by drawing a picture. Digital video segments provide a graphical illustration, accompanied by an instructor's narration. These lessons are ideal both as introductions to key concepts and for reinforcement.

ASSESSMENT



As reinforcement and review for the certification exam, *Challenge! Interactive* is a helpful tool. *Challenge! Interactive* is part of the Interactive Learning CD-ROM that is included with this course. *Challenge! Interactive* contains sample questions relating to the certification objectives. The sample questions are presented in multiple choice, screen simulations, and scenario format to help prepare you for the CCNA certification exam. It is a good idea to take the *Challenge! Interactive* test, read the self-study material, and then take the test again. This test material is intended as a study aid. It is recommended that you take the tests as often as necessary to reinforce the learning process.

HARDWARE REQUIREMENTS

All of the technology walkthroughs in this course require that you establish a telnet session with a Cisco router. This connection does not require great computing power. If you have access to equipment that fits the following guidelines, you will be able to use the computer to view the Interactive Learning CD-ROM and to telnet into a router. The computer used for this purpose should meet the following minimum hardware requirements:

- 486 DX2, 66 MHz processor (or higher)
- 32 MB of RAM
- 200-MB hard disk
- CD-ROM drive
- VGA display (or better)
- Modem or network adaptor with outside connection
- Windows 9x operating system



Remember, there is always help available online. Please refer to the Support pages in Getting Started for further information regarding online support.

Introduction

СНАРТЕ

R

MAJOR TOPICS

►

Objectives	6
Pre-Test Questions	6
Introduction	7
Router Ports	7
Port Configuration Basics	10
Loading a Configuration	11
Summary	12
Post-Test Questions	12

OBJECTIVES

At the completion of this chapter, you will be able to:

- Describe the basic hardware structure of Cisco router interfaces.
- Define the types of Cisco router ports.
- Configure Cisco router ports.

PRE-TEST QUESTIONS

The answers to these questions are in Appendix A at the end of this manual.



INTRODUCTION

Routers manufactured by Cisco Systems currently carry the vast majority of Internet traffic worldwide. Cisco routers are powerful devices specifically designed to move information quickly and efficiently between networks. The comprehensive family of Cisco routers range in size and capacity from small, modular access routers designed to power small offices and departments to powerful models designed to enable entire cities.

This chapter will lay the groundwork for a basic understanding of Cisco router hardware and router configuration. The information provided will give you the basic skills necessary to build scaled networks of increasing complexity. Each command outlined provides the background information and directions for when and how it is used. A display of what the command should look like on the screen is also provided.



Stop now and view the following video presentation on the Interactive Learning CD-ROM:

Router Fundamentals Router Hardware

ROUTER PORTS

Cisco routers are dedicated hardware devices. They are not designed for any task other than moving data between networks and users.

Cisco routers are designed around hardware interfaces used to connect the router to various types of networking media. Cisco interfaces are also commonly referred to as ports.

| \searrow |
 | |
|------------|------|------|------|------|------|------|------|------|------|------|--|
| |
 | |
| |
 | |

The following topics will be covered in this section:

- Router Port Definition
- Ethernet Ports
- Serial Ports
- Basic Rate Interface (BRI) Ports

Router Port Definition

Cisco routers use several types of ports. Most router ports are physical interfaces on the router. The exception is the virtual terminal port, which is used to establish a remote connection to the router.

The physical ports are connected to networking devices or media. When the appropriate port is connected and configured correctly, Cisco routers provide the capability to move data between networks of differing technologies and protocols. Cisco routers can route between Token Ring and Ethernet networks as well as Digital Equipment Corporation's DECnet and Banyan Vines networks.

Examples of common port types are Ethernet, Serial, and BRI. Ethernet ports are used to connect to local area networks via Ethernet hubs. Since Ethernet networks comprise the vast majority of networks, integration of Cisco routers into existing Ethernet networks is relatively common.

Ethernet Ports

The Attachment Unit Interface port on the back of the router (labeled AUI) is connected to a transceiver. The transceiver is then connected to Ethernet networks using a standard cable. This design allows Cisco routers to be connected to Ethernet networks regardless of the physical medium.

The Ethernet transceiver is used to convert the Ethernet traffic from one cable type to another. Ethernet cable types include Thin Ethernet, Thick Ethernet, unshielded twisted pair, and fiber-optic cable.

Serial Ports

Serial ports are connected to WAN devices, such as high-speed modems or digital devices. Leased lines typically consist of a physical path connected at the customer end to a Data Terminal Element (DTE). The service provider typically has Data Communications Equipment (DCE) that is used to connect to the DTE at the customer site. The DTE takes care of establishing and maintaining communication with the DCE at the other end. Clock speeds and data transmission speeds are controlled by the DCE.

These devices are connected to physical media at a central location in the network. The point where the internal network is connected to the external network is called the point of presence, or POP. The POP is usually where the central network routers reside. Central, or premise, routers are typically more powerful than routers at outlying or branch offices. These premise routers are responsible for moving information within an enterprise.

Routers that comprise the endpoint of a network are called autonomous system routers. The autonomous system router is generally configured to support a differing set of communication protocols in addition to the protocols used to route within the internal network.

Basic Rate Interface (BRI) Ports

Basic Rate Interface (BRI) ports are used to connect the router to Integrated Services Digital Network (ISDN). BRI ports use leased telephone lines. ISDN BRI consists of two channels used for data transmission and one channel used for establishing connectivity and maintaining control. The two data channels run at speeds of up to 64 Kb, while the control channel is typically a 16-Kb channel. The ISDN BRI interface can operate at speeds of up to 128 kilobits per second.

<u>)</u>	 		

PORT CONFIGURATION BASICS

Configuring Cisco routers involves providing each of the ports with the correct parameters necessary for connectivity. The Internet Operating System (IOS) is used to configure ports.

The following topics will be covered in this section:

- Telnet Session
- Direct Cable Connection
- Physical Connections

Telnet Session

A telnet session is used to connect with routers that have already been configured. Telnet is an Application-layer protocol included in the TCP/IP protocol suite. Telnet is included with Windows 95 and Windows 98. To start a telnet session, use the Windows 95 **Start** menu and select **Run**. Type "telnet" and the IP address of a router. This will connect to the router using a virtual (logical) terminal connection.

Direct Cable Connection

To connect to a new or unconfigured router, it is necessary to physically connect a cable to the console router port. Console sessions are also used to connect to a router if a telnet session cannot be established.

The console port is labeled "Con." Use the connector and cable provided with the router to establish a console session. Since a console session is a physical connection to the router, it is unsecure.

Physical Connections

A router must be physically connected to the network before it will operate correctly. Cisco cables are blue and usually ship with the router. Cisco ports are connected through 60-pin serial cables, unshielded twisted-pair network cables (models with a built-in hub), or to the AUI port using a transceiver.

LOADING A CONFIGURATION

The configuration file is loaded after the router has been initialized, performs several selftests, and loads the operating system. The configuration file is a text file that the router uses line by line to configure interfaces to communicate with each other and the surrounding network. The configuration file is stored in Random Access Memory (RAM), which is lost when the router is powered down.

When a router is powered on, the configuration file can be loaded from either of two locations:

- Nonvolatile RAM
- Trivial File Transfer Protocol Server

Nonvolatile RAM

1

Configuration files are stored in physical memory on the router in a location called nonvolatile RAM (NVRAM). NVRAM is located on physical memory chips and is considered a form of permanent memory. The NVRAM file is similar to the hard drive on a personal computer and is not lost when the router is powered down.

When a router is rebooted, the configuration file is automatically loaded from NVRAM. If the files are not located in NVRAM, the router can be configured to look for these files on a network server using the trivial file transfer protocol server.

Trivial File Transfer Protocol Server

The Cisco IOS uses the Trivial File Transfer Protocol (TFTP) server to transfer files to and from the router. TFTP is an Application-layer protocol that does not use password authentication, so files can be transferred to and from the TFTP server without using passwords. TFTP server software for Windows 95/98/NT is available free of charge from Cisco Connection Online (Cisco's Web site). Once the TFTP server software is installed, any personal computer can operate as a TFTP server. Configuration files can be stored on a TFTP server to recover from corrupted configuration files in NVRAM or to load new configuration files. A TFTP server is also used to upgrade the software on a router.

SUMMARY

In this chapter, you were introduced to the following:

- Basic hardware structure of Cisco router interfaces
- Configuration of Cisco interfaces, or ports, to operate with hardware connected to that port
- Purpose of configuration
- Port configuration basics

POST-TEST QUESTIONS

The answers to these questions are in Appendix A at the end of this manual.

1. Which type of Cisco port is connected to local area networks?

.....

2. Which type of Cisco interface is typically connected to a high-speed modem?

.....

3.	What device is usually connected to the Ethernet ports of Cisco routers?
4	
4.	What is usually connected to a BRI port on a Cisco router?
5.	What is the termination point where the telephone equipment meets the internal network called?
6.	Configuration of Cisco routers is primarily concerned with configuration of what?

Cisco IOS

CHAPTER

2

MAJOR TOPICS

Objectives	16
Pre-Test Questions	16
Introduction	17
How to Read a Cisco Command Display	18
IOS Overview	25
Command Modes	
Basic IOS Commands	
Using Help	52
Summary	55
Post-Test Questions	56

OBJECTIVES

At the completion of this chapter, you will be able to:

- Define the basics of the Internetwork Operating System (IOS).
- Log in to the router in both User Exec and Privileged Exec modes.
- Use the context-sensitive help.
- Describe the basic Cisco IOS command structure.
- Control router passwords and identification.
- Use the command history and editing functions.

PRE-TEST QUESTIONS

The answers to these questions are in Appendix A at the end of this manual.

Q

- 1. What is an operating system?
 -
 -
- 2. What kind of operating system is used by Cisco routers?

.....

-
- 3. If you wish to see a list of all available User Exec commands, what would you type at the User Exec prompt?

.....

4. What command would you use to enter Global Configuration mode?

.....

INTRODUCTION

A router, like a computer, needs an operating system to run. Without an operating system, a router is just a collection of hardware. The operating system used by Cisco routers is called the Cisco Internetwork Operating System, or IOS. The Cisco IOS is designed to move information between networks in an enterprise setting.

The information moved between networks or segments of a given network is the raw material data frames are formed from. The process of correctly selecting a path for a given data frame then forwarding that frame based on its network layer destination address is called routing. The Cisco IOS controls the processes and parameters associated with routing.

The Cisco IOS is a text-based network operating system. It is intended for use by system administrators and others who design, build, and support data and voice networks. In contrast, the Windows family of operating systems is graphics-based and designed for use on a personal computer by an end user.

The Cisco IOS, like any other operating system, uses files for configuration and memory for storage. Cisco products do not have hard drives, unlike computer-based network operating systems. Cisco routers use flash memory and nonvolatile RAM (NVRAM) for permanent storage. RAM stores information used by the router when in an operational state.

Flash memory can be loosely compared to hard drive storage space. Flash memory is where the operating system resides. NVRAM is used to store configuration and registry settings. Routers use a registry loosely comparable to the Windows registry to control hardware and bootup parameters.

While highly complex, the Cisco IOS contains an excellent context-sensitive help system. This help system can speed advanced configuration tasks by showing all available command options at the current command prompt. There is also a highly developed online technical documentation system available on Cisco's Web site that provides answers to almost any question or possible configuration scenario.

$ \rightarrow $	 	 	 	



Stop now and view the following video presentation on the Interactive Learning CD-ROM:

Router Fundamentals Router Command Line-Interface (CLI) Router Configuration Basics Privileged Mode vs. User Mode Router Boot Options and Password Recovery Boot System Commands

HOW TO READ A CISCO COMMAND DISPLAY

The router's console interface, or a telnet connection to a given router, provides the vehicle for you to configure your router as well as observe statistics regarding your router's operation. The router's console, consisting of either a terminal or PC connected directly to the router or accessing it remotely, is the primary interface between the administrator and the IOS.

The information displayed on the console screen will vary depending upon the commands you enter and the mode from which you enter the commands. Both permanent and temporary changes can be made to your router's configuration from the command prompt displayed on the router's console.

The console's command prompt can be compared to a DOS prompt. Before you can start a DOS program, you must switch to the appropriate directory and type the command to start the particular program. In a similar manner, a specific router component can only be configured from the correct prompt.

The following example lists the screen output of the **show config** command and illustrates the basic components of a configuration file's output. While this example is not meant as a comprehensive reference, it is a starting point for understanding the topics covered later in this and subsequent chapters.

After issuing the **show config** command at the router's console prompt and pressing *ENTER*, the first line of output looks like the following:

```
Using 805 out of 32762 bytes !
```

This shows the size of the configuration file in bytes. The configuration file gets larger as more parameters are added or changed and smaller as port configurations are dropped. There is an exclamation point following each section of the configuration file's output to distinguish between sections.

The next section of output appears as follows:

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

This section of the configuration file shows the IOS version number and the services that are automatically configured on the router.

The next line lists the name given to the router, if any.

```
hostname RouterB
```

In this example, the currently configured host name is RouterB.

The next section of the configuration file begins describing the interfaces of the router, as shown in the following excerpt:

```
!
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast
!
```

This section displays information about interfaces configured on the router's ports, in this case the first Ethernet port. Ethernet ports are connected to a local area network. Port numbers on Cisco routers start with zero and proceed upward. The second Ethernet port would be labeled Ethernet1. Any additional ports would follow this convention.

The following sections display information about the configuration of other ports on this router.

```
!
interface Serial0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
no fair-queue
clockrate 4000000
!
interface Serial1
ip address 192.168.1.2 255.255.255.0
no ip directed-broadcast
!
```

The previous sections display information about serial ports. Serial ports are normally connected to wide area networking devices. An example of a WAN device is the high-speed modem that is connected to a leased line. Serial ports follow the same numbering convention as Ethernet ports.

The following section of output describes the configuration of an optional installed component on the router.

```
!
interface BRIO
no ip address
no ip directed-broadcast
shutdown
!
```

After serial interface configurations, the configuration of any optional installed components is displayed. The word "interface" in the previous section designates that this is a physical connection to some type of networking device or medium. BRI, or Basic Rate Interface, describes this as a physical port used to connect to ISDN BRI devices.

The section that follows describes additional configuration information, as shown below:

```
router rip
network 10.0.0.0
network 192.168.1.0
network 192.168.2.0
network 192.168.3.0
```

Routing protocol information, if configured, constitutes the next section of the configuration file. The router from which this configuration file was captured is configured to use the Routing Information Protocol (RIP). RIP is described later in this course. The network statement identifies the network addresses in use on this router. Host addresses, or addresses that are specific to a given interface on the router, are configured as interface configuration parameters.

The routing configuration parameters shown previously are network numbers and represent the networks this router is responsible for reaching.

Ĵ	 	 	

The following is an example of the next section of output:

```
!
line con 0
exec-timeout 0 0
password cisco
login
transport input none
!
```

This section describes any lines installed on the router. A line is similar to a port, but can represent a logical connection entity or a physical port entity. The "line con 0" reference designates this interface as a console line, or the line through which the console (terminal or PC serial cable) is connected directly.

The parameters that follow, as shown below, are configuration parameters describing the console port on this router.

```
!
line aux 0
line vty 0 3
password cisco
login local
line vty 4
password sparky
login
!
```

Illustrated in this section are the auxiliary and vty lines. The "line aux 0" reference is presently unconfigured. Auxiliary lines can be connected to a modem for dial-up support. Virtual terminal lines, or vty lines, are logical ports. Logical ports are not used for physical connections but rather for remotely connecting to the router. The "password" lines describe the configuration parameters for the virtual terminal lines. In this example, there are three lines, and two of them are configured with passwords.

At the end of the configuration file displayed on the console, you will see the following section, which denotes the end of the configuration file:

end ! Another example of a command's output on a console or Telnet display follows. The following output results from entering the **show interface Ethernet0** command. Statistics and configuration information regarding the Ethernet0 interface will be displayed on the router console. In this example, there are no exclamation points denoting changes in section; the following command output would be listed on consecutive lines on a router console. Line 1 appears as follows:

EthernetO is up, line protocol is up

The first line of this output describes the physical device as Ethernet port 0, and displays the status of the layer 2 and layer 3 protocols. "Ethernet0 is up" means that the interface itself is operational and enabled. The "line protocol is up" reference means the protocol bound to the interface is operational.

In the next line, the name and MAC address of the port are listed.

Hardware is Lance, address is 0010.7b7f.b6a6 (bia 0010.7b7f.b6a6) In this example, the port has been assigned the name Lance.

The next output line shows the Ethernet0 port's IP address.

Internet address is 208.212.225.15/23

The IP address is also known as the network layer address.

The following line of output begins describing more technical parameters, as follows:

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255 This line indicates the Maximum Transmission Unit (MTU) the device is set to use. Next, it lists the bandwidth available to the interface, the delay time in milliseconds, the reliability of the interface, and the current load on the interface.

Proceeding to the next line of output, we find other parameters, as shown below:

Encapsulation ARPA, loopback not set, keepalive set (10 sec) ARP type: ARPA, ARP Timeout 04:00:00

This section gives information about the encapsulation type used by the device. Encapsulation tells the device how to structure data frames before passing the frame onto the wire for transmission across the network media.

The following output shows a number of additional statistics and parameters:

```
Last input 00:00:04, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 1 packets/sec
7675 packets input, 731792 bytes, 0 no buffer
Received 7375 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
126108 packets output, 8050080 bytes, 0 underruns
37 output errors, 0 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred
37 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

This section is where troubleshooting information regarding the interface is located. It is also the section of the command output that contains the most statistical data pertaining to the interface's performance. The previous output sample shows statistics for an interface with very little traffic.

Now let's move on to discuss the Cisco IOS in more detail.

IOS OVERVIEW

Most Cisco routers and switches, including the PIX firewall system, have at least a partial implementation of the Cisco IOS. While some commands vary between devices, there are many commands that are common to most Cisco products. Some of these common commands will be described in this section.

It is important to note that the information presented here is not meant to serve as a comprehensive guide to the hundreds of commands and combinations of commands that are possible when configuring Cisco products. Rather, this section will familiarize you with some of the basic concepts of configuring Cisco products from the Command-Line Interface (CLI).

The CLI, accessible through a directly connected terminal or in-band (over the network) via telnet, is the vehicle through which configurations are created, changed, altered, copied, and sometimes distributed. The commands you will use in this section can be grouped together to form configuration scripts, which are useful when configuring multiple routers requiring similar parameters.

The following topics are discussed in this section:

- Navigation from the Command Line
- Command Structure

Navigation from the Command Line

Although commands will vary in parameter and syntax, there is some commonality regarding the command line. There are a number of commands that are common to all modes and perform essentially the same function irrespective of where in the IOS the command is used. Such commands tend to be indispensible to the average administrator, as there are few people who could memorize the thousands of commands and parameters supported by the Cisco IOS.

In order to utilize the CLI, it is first necessary to log in to the device in question. Some routers display an opening message or help screen when you log in; others do not. Later in this chapter, there is a demonstration of how to display such an opening message at login.

Logging in to the router prior to passwords being set is a simple matter. It is important to note here that all Cisco routers ship without passwords, so when you are configuring a router for the first time, press *ENTER* whenever prompted to enter a password. Pressing *ENTER* at the Login prompt gives you the User Exec mode prompt, similar to the following:

```
router1>
```

From this prompt, type the word "enable" and press *ENTER*. You will be prompted as shown below:

router1#

You have just entered Privileged Exec mode. Note that the last character of the prompt changes after entering Privileged Exec mode.

Moving from Privileged Exec mode to Configuration mode is also accomplished with a single command. Type "config" from the Privileged Exec mode, press *ENTER*, and the prompt changes as shown below:

router1# router1#(config)

Configuration mode has many sublevels accessible by aggregating commands. A compound command such as **config interface** would cause the prompt to change, reflective of the sublevel in question.

Commands can be entered in any of three modes that are described in detail later in the chapter: User Exec, Privileged Exec, and Configuration. Some commands work the same way in all three modes; some do not. There are many commands that are mode specific, particularly in the case of Configuration mode.

Command Structure

The structure of a Cisco IOS command varies with the command. Most commands are simple. Often a command is simply a word, combination of words, or an abbreviation of the commands in question. Some commands are compounded by adding other commands and/or switches and parameters.

Using the IOS commands, you can start or stop an interface on a given router or switch; configure ports, passwords, and interfaces; or accomplish a vast array of configuration tasks.

The command-line interface features a prompt like the following:

```
router1#
```

This prompt changes when the command mode changes.

It is possible to configure your router to display a custom prompt as well. A custom prompt might contain the system name, a code set by you, or a number or symbol. The prompt first appears after a user logs in to a Cisco device for the first time.

Cisco routers are configured using a CLI. Commands are interpreted and executed by a command interpreter. The command-line interface prompt has several modes to designate which router component the EXEC commands will configure.

Cisco commands are designated as EXEC commands because they are executed as soon as the *ENTER* key is pressed. EXEC commands are stored in RAM on the router when they are entered but not saved to NVRAM. This means that you can test configuration changes without saving them. If you make a mistake, you can quickly restore the original configuration.

Cisco's recommended procedure for restoring the previous configuration is to enter the command as follows:

Router1#copy startup-config running-config

Since the commands are not stored until you specifically save them, even in the worst case, you can simply reboot the router to restore the startup configuration.

Cisco commands follow a basic structure consisting of the command followed by the router parameter. The command will be one of the IOS commands, such as **show**. The router parameter is the item you want the command to act on.

For example, the command for restoring the previous configuration that was noted earlier illustrates the basic components of a command. This is shown below:

Router1#copy startup-config running-config

In this example, the command is "copy", and "startup-config" and "running-config" are parameters that tell the command interpreter exactly where to perform the copy operation. In this case, a configuration file called startup-config will overwrite the current configuration running in RAM.

The following table illustrates how commands are indicated in Cisco documentation and gives some examples of commonly used router commands.

Syntax	Operation	Example
boldface	Typed exactly as shown	show ip route
italics	You must supply this information	trace ip destination
[a]	Optional components	router isis [tag]
{a b c }	You must select one of the components	show access-lists [access-list-number name]
[a{b c}]	There is a default option or optional components	encapsulation [novell-ether {arpa sap snap}]

COMMAND MODES

The Cisco IOS has three basic modes of operation from which commands can be entered: User Exec, Privileged Exec, and Configuration. User Exec is the base mode from which a limited number of commands is available. Privileged Exec (sometimes called Enable mode) allows the administrator to adjust more parameters and see more global information about the router. Configuration mode allows more granular adjustments to be made to any facet of a router's operation, including interfaces, subinterfaces, protocols, ports, lines, and other entities.

Privileged Exec mode is only accessible from User Exec, and Configuration mode is only accessible through Privileged Exec. This hierarchy of IOS structure aids in preventing unauthorized access to the router's parameters and configuration.

In order to distinguish one mode from another, the command prompt changes its appearance depending upon the IOS mode from which you are working. The differences between these prompts are described in detail later in this section.

The following topics will be covered in this section:

- User Exec and Privileged Exec Modes
- Configuration Mode

User Exec and Privileged Exec Modes

User Exec mode allows users to enter commands that allow observation of basic router operations. This mode allows the user to connect to other devices via telnet, perform simple diagnostics, and display system information at the console screen. Configuration changes cannot be made from User Exec mode.

Privileged Exec mode allows the user to access all of the commands in User Exec mode, as well as additional configuration, troubleshooting, and maintenance commands. As mentioned previously, the two modes are differentiated by the router prompt, as shown in the following table:

Mode	Prompt
User Exec	router>
Privileged Exec	router#

There are differences in the available options based on whether you are in User Exec or Privileged Exec mode. A good example of this is the **show** command.

In User Exec mode, the **show** command is used to review settings for command history, configured hosts, active sessions, terminal configuration parameters, active users, and the IOS version.

In Privileged Exec mode, the **show** command allows all of the User Exec commands and can also be used to look at almost all router settings. There are well over 100 basic **show** commands, with most of those commands having many additional parameters and commands.

As previously mentioned, you can only access the Configuration mode from the Privileged Exec mode.

Accessing Privileged Exec Mode from User Exec Mode

The first mode entered when you connect to the router is User Exec. To access Privileged Exec mode, use the **enable** command and enter the enable secret password. Notice the change in the router prompt from router1> to router1#, as shown in the following sample:

```
router1>enable
Password:
router1#
```

To exit Privileged Exec mode and return to User Exec mode, type "disable" from the Privileged Exec mode prompt, as shown below:

```
router1#disable
```

To completely exit a currently active session, type "logout" or "quit" from either of the Exec modes.

The Exit Command

The **exit** command will produce different results depending on the mode you are in. In the Privileged Exec or User Exec modes, the **exit** command will terminate your connection to the console. If login is enabled on your router, you will have to log in again to begin a new session. In Configuration mode, the **exit** command will back you out of Configuration mode to the Privileged Exec mode.

The following is an example of the exit command:

```
router1(config-if)#exit
router1(config)#exit
router1#
```

In the previous example, you are two layers deep in Configuration mode. Having configured the interface, you type "exit", which returns us to base Configuration mode. Typing "exit" again returns us to Privileged Exec mode.

Configuration Mode

As stated previously, you cannot enter Configuration mode except through Privileged Exec mode. Since you can enter Privileged Exec mode only from User Exec mode, you are then three nested levels deep in the command structure when you enter Configuration mode. Configuration mode has many subsections and subinterfaces.

Configuration mode processes commands slightly differently from how User Exec and Privileged Exec modes process them. User Exec and Privileged Exec commands are twopart requests, requiring you to specify the command and what you want it to act on. In contrast, Configuration commands require that you execute several commands. These commands, layered together, change the parameters related to a particular interface, a particular protocol, the global settings for the router itself, or a number of other configuration parameters. For example, let's say that you want to select the WAN protocol that you will use on a particular serial interface on the router. In the following example, you will use port Serial1.

There are many different Configuration modes. The Configuration mode is determined by which interface, protocol, line, or other parameter set you wish to alter. The command line's prompt changes its format to reflect the Configuration mode you have selected. The table below illustrates some of the more common Configuration modes.

Configuration Mode	Command Prompt
Global	Router1(config)#
Interface	Router1(config-if)#
Subinterface	Router1(config-subif)#
Line	Router1(config-line)#
Router	Router1(config-router)#
IPX-Router	Router1(config-ipx-router)#
Route-Map	Router1(config-route-map)#

Each Configuration mode is used for different purposes. The basic functions of each are described below:

• Global Configuration mode

This mode is used to configure global parameters, such as router passwords, to enable routing protocols, default routes, the configuration registry, boot order, and other parameters that affect all router components.

• Interface Configuration mode

This mode is used to configure interface-specific parameters such as the IP address of a given interface.

• Subinterface Configuration mode

This mode is used to configure multiple virtual interfaces on one physical interface. This mode is used most often on interfaces connected to Frame Relay circuits.

Line

This mode is used to configure Virtual Terminal Lines, which are used in the establishment of telnet sessions.

• Router

This mode is used to configure IP routing protocols.

• IPX-Router

This mode is used to configure IPX routing protocols.

• Route-Map

This mode is used to manually configure routing tables and source and destination addresses.

It is important to note that commands entered in Configuration mode are not automatically saved. In order to save configuration changes, use the **write** command or the **copy** command as described below:

```
router1#write mem
```

or

router1#copy running-config startup-config

This writes the configuration changes you just made into NVRAM. Recall that NVRAM is the area of memory that stores the configuration file, so the router will use that configuration file on startup.

BASIC IOS COMMANDS

This section introduces you to some commonly used commands that will allow you to view and change router parameters. This subset of commands contains the most common commands and will give you a starting point to build your knowledge and experience on. Starting with the most basic **setup** command, you will learn how to configure individual interfaces and ports.

The following topics will be covered in this section:

- Basic Configuration with the Setup Command
- Common Commands

Basic Configuration with the Setup Command

Setup mode is used to bring up a minimal router configuration quickly. New, unconfigured routers or routers with corrupted startup files will automatically enter Setup mode, which will prompt you for basic configuration information.

The **setup** command is issued from the Privileged Exec mode. Setup is a Configuration mode that prompts you for basic commands that are used to initially configure a router. The **setup** command configures basic router elements only. It may be necessary to use the CLI to configure additional options for optimal router operation. Each section of the setup configuration dialog is explained in the next section.

Setup Command

The following output shows the **setup** command being entered from Privileged Exec mode.

```
router1#setup
         --- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Refer to the 'Getting Started' Guide for additional help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes]:
First, would you like to see the current interface summary? [yes]:
               IP-Address
                              OK? Method
Interface
                                             Status
                                                       Protocol
Ethernet0
               204.32.23.81
                              YES manual
                                             up
                                                       down
Serial0
               unassigned
                               YES not set administratively down
 down
Serial1
               unassigned
                               YES not set administratively down
 down
```

Global Parameters

The Setup Configuration mode has several components, the first being global parameters. Global in this context means these parameters affect all interfaces and ports. Examples of global configuration parameters are routing protocols, passwords, router host names, and SNMP management configuration.

```
Configuring global parameters:
Enter host name [router1]: router1
```

The enable secret is a one-way cryptographic secret password used instead of the enable password when it exists.

```
Enter enable secret [<Use current secret>]: cisco
```

The enable password is used when there is no enable secret and when using older software and some boot images.

```
Enter enable password [ciscol]: ciscol
Enter virtual terminal password [cisco]:
```

These configuration dialog options set the router name and password options.

The following section deals with network and routing protocols.

```
Configure SNMP Network Management? [no]:
Configure IP? [yes]:
Configure IGRP routing? [yes]: n
Configure RIP routing? [no]: y
Configure Vines? [no]:
Configure IPX? [no]:
Configure AppleTalk? [no]:
Configure Apollo? [no]:
Configure DECnet? [no]:
Configure XNS? [no]:
Configure CLNS? [no]:
Configure bridging? [no]:
Configure LAT? [no]:
```

Interface Parameters

The next section of the setup configuration dialogue deals with interface configuration parameters. Interface parameters are used to configure Ethernet and serial ports. Interface-specific information such as IP and IPX addresses, subnet addresses, and the interface shutdown are configured in this portion of Setup Configuration mode.

```
Configuring interface parameters:

Configuring interface Ethernet0:

Is this interface in use? [yes]:

Configure IP on this interface? [yes]:

IP address for this interface [204.32.23.81]:

Number of bits in subnet field [0]:

Class C network is 204.32.23.0, 0 subnet bits; mask is

255.255.255.0

Configuring interface Serial0:

Is this interface in use? [no]:
```

```
Configuring interface Serial1:
Is this interface in use? [no]:
```

After you are finished entering configuration information, you are shown the script that is automatically created and you are prompted as to whether you want to use the script.

```
The following configuration command script was created:
hostname router1
enable secret 5 $1$yaHK$s04ZGjzNPCRDNftc3b3Ph0
enable password ciscol
line vty 0 4
password cisco
no snmp-server
ip routing
no vines routing
no ipx routing
no appletalk routing
no apollo routing
no decnet routing
no xns routing
no clns routing
no bridge 1
interface Ethernet0
ip address 204.32.23.81 255.255.255.0
no mop enabled
Interface SerialO
shutdown
no ip address
interface Serial1
shutdown
no ip address
router rip
network 204.32.23.0
end
Use this configuration? [yes/no]: y
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
router1#
```

Common Commands

The following subsections give a basic overview of the more commonly used Cisco IOS commands, and in many cases provide a demonstration of the console screen output when such a command is issued.

show config

The **show config** Privileged Exec command is used to display the current running configuration file in NVRAM. Configuration changes made to the router take place immediately and are stored in RAM. You can review changes before saving the running configuration to the startup configuration. This is a very handy way to avoid making changes that you might not want to save. If you make a mistake, you can restore the original configuration from NVRAM. A sample of the console screen output after issuing the **show config** command as follows:

```
Router1#show config
Using 464 out of 32762 bytes
!
version 10.3
service config
service udp-small-servers
service tcp-small-servers
!
hostname Router1
L
enable secret 5 $1$dnKx$ZP34XME.oGEZzhn2TtU5G.
enable password ciscol
!
T
interface Ethernet0
  ip address 192.168.0.1 255.255.255.0
 no mop enabled
```

```
!
interface SerialO
  ip address 192.168.1.1 255.255.255.0
1
interface Serial1
 no ip address
  shutdown
  --More--
                               !
!
!
line con 0
 exec-timeout 0 0
line aux O
 transport input all
line vty 0 4
 password cisco
 login
ļ
end
```

Much in the same manner as the output depicted earlier in this course, the sections of the configuration list are separated by an exclamation point.

Editing Commands

The Cisco IOS has several hot-key shortcuts that can simplify entering long or complex commands as you configure multiple interfaces or protocols.

Frequently, when editing, you may wish to repeat the previous command, move the cursor, or allow the IOS to finish a command for you. There are several useful key combinations that will assist you in your editing. Each Cisco router has a command history buffer, which is an area of memory that stores the last ten commands you entered. Becoming familiar with these editing commands could save you time and effort during configuration.

The following table describes several of the most common keyboard shortcuts available in all modes of the CLI:

Key Sequence	Action
CONTROL+A	Moves the cursor to the beginning of a command line
CONTROL+ B	Moves the cursor backward one character
CONTROL+E	Moves the cursor to the end of a command line
CONTROL+F (or RIGHT ARROW)	Moves the cursor forward one character
CONTROL+N (or DOWN ARROW)	Having gone back more than one command in the command bufffer, this key sequence allows you to move forward one command.
CONTROL+P (or UP ARROW)	Shows you the command entered previous to the line you are on
CONTROL+R	This repeats the previous command line, including a fresh command prompt. This is particularly useful in situations where your command entry is interrupted by system messages.
ESCAPE+B	Moves the cursor backward to the first character of the previous word
ESCAPE+F	Moves the cursor forward to the first character of the next word
BACKSPACE	Deletes characters as it moves the cursor to the left
ТАВ	Finishes a command for you if you have entered enough characters to uniquely identify that command in your current mode

The **terminal no editing** command turns off editing commands. This command is useful when you have finished editing and don't want anyone to change your configuration.

)	 	 	

The **show history** command is used to review the last ten commands entered, which are stored in the command buffer. Here is an example of the output of the **show history** command.

```
Routerl# show history
debug ipx sap activity
show ipx traffic
show ipx sap
show ipx servers
show ip route
show ipx routing
show ipx rout
copy startup-config running-config
show interfaces
show history
```

By default, only the last ten commands entered are stored in the terminal history buffer. You can change this value to any number between zero and 256 by using the following command format:

```
terminal history size <0-256>
```

Storing a larger number of commands is useful when you make configuration changes on a router and wish to keep track of what commands you entered. The terminal history buffer only stores the commands from the current session. In other words, if the router is restarted, the buffer clears regardless of the value of this setting.

show version

The **show version** command is used to display the IOS version, configuration registry settings, and other settings for the router's firmware and software. This command is important when attempting to verify the operating system version. Also, this command is useful in determining how the boot process is currently being accomplished by listing the configuration registry setting. (The configuration registry setting is described in detail later in this course, but for the purpose of this discussion, the configuration registry tells the router where the boot file is found.)

The following is an example of output from the **show version** command. Note that the third line displays the IOS version and the last line displays the configuration registry settings.

```
Router1#show version
Cisco Internetwork Operating System Software
IOS (am) 3000 Software (IGS-J-L), Version 10.3(7.4), MAINTENANCE
  INTERIM SOFTWARE
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Tue 28-Nov-95 19:35 by vatran
Image text-base: 0x0302E398, data-base: 0x00001000
ROM: System Bootstrap, Version 4.14(9.1), SOFTWARE
Router1 uptime is 1 day, 2 hours, 28 minutes
System restarted by reload
System image file is "igs-j-1.103-7.4", booted via flash
cisco 2500 (68030) processor (revision D) with 16384K/2048K bytes of
 memory.
Processor board serial number 01696155
SuperLAT software copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software (copyright 1994 by TGV Inc).
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
Bridging software.
1 Fthernet/IFFF 802.3 interface.
2 Serial network interfaces.
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)
```

Configuration register is 0x2102 The show version command is available from any mode.

show flash

Since IOS files can be renamed at will, the **show flash** command will show the name and size of the current IOS file. The following example shows why you would use the **show version** command rather than the **show flash** command to verify the IOS version.

The following is an example of the screen output from a **show flash** command. Notice that the complete IOS filename and size are displayed as well as the available flash memory.

```
RouterC#show flash

System flash directory:

File Length Name/status

1 6788464 c2500-d-1_120-4.bin

[6788528 bytes used, 1600080 available, 8388608 total]

8192K bytes of processor board System flash (Read ONLY)
```

show processes

The **show processes** command is used to display information about processor utilization, process IDs of active processes, and information about the function of active processes.

Route	Router1#show processes												
CPU utilization for five seconds: 39%/2%; one minute: 6%; five minutes: 5%													
ΡID	Q T	PC	Runtime (ms)	Invoked	uSecs	Stacks	ΤΤΥ	Process					
1	М *	0	20064	2546	7880	1096/ 2000	0	Exec					
2	LΕ	303F68E	2885920	27794	103832	928/1000	0	Check heaps					
3	ΜE	30666CA	0	2	0	964/1000	0	Timers					
4	LΕ	3095BB2	0	1	0	954/1000	0	ARP Input					
5	LΕ	30BF2FE	0	1	0	924/1000	0	Probe Input					
6	ΜE	30BEE96	0	1	0	962/1000	0	RARP Input					
7	ΗE	30B1668	0	1	0	1942/ 2000	0	IP Input					
8	ΜE	30D7C0A	272	19091	14	944/1000	0	TCP Timer					
9	LΕ	30D98EE	0	31	0	884/1000	0	TCP Protocols					
10	ΜE	30BC042	0	1	0	796/1000	0	BOOTP Server					

show protocols

The **show protocols** command shows which protocols are configured globally as well as the status and protocol address on each interface. You can also use this command to troubleshoot the Network and Data Link layers of the OSI Model. If the interface is up and the line protocol is down, the problem is most likely a layer 2 connectivity issue. Check to see if the port is properly connected. If the port is down, troubleshooting would begin with the layer 3 configuration. For information about layer 2 and 3 of the OSI Model, refer to the *Introduction to Networking* manual.

The same information about the status of interfaces is available with the **show interfaces** command. The **show protocols** command is a more concise method to quickly check which protocols are configured as well as the status of layer 2 and 3 connectivity.

The following example demonstrates that the router is probably not connected to anything and is most likely a demonstration unit. While both IP and IPX are enabled, only IP is configured. Although Serial0 is configured as a Novell subinterface, there is no network addressing configured.

```
Router1#show protocols
Global values:
Internet Protocol routing is enabled
Novell routing is enabled
Ethernet0 is up, line protocol is down
Internet address is 192.168.0.1 255.255.255.0
Serial0 is down, line protocol is down
Internet address is 192.168.1.1 255.255.255.0
Serial0.1 is down, line protocol is down
Serial1 is administratively down, line protocol is down
```

>	 	 	 	 	 	

show memory

The **show memory** command displays information regarding the memory usage of the router, the process memory location, and free memory pool statistics. The following example shows there are console sessions in process that are taking memory space in addition to the command interpreter and Exec functions.

Router1#s⊦	Router1#show memory											
Head	FreeL	ist	Т	otal(b) (Jsed(b)	Free(b)	Largest(b)				
Processor	5EE54	2 E	EEO 1	6384428	86	675084	15709344	15709216				
I/0	400000	00 2 F	B74 2	097152		335420	1761732	1742388				
Processor	memory											
Address	Bytes	Prev.	Next	Ref	PrevF	NextF	Alloc PC	What				
5EE54	24 0		5EE90	1			311DC42	*Init*				
5EE90	2508	5EE54	5F880	1			3050118	TTY data				
5F880	2000	5EE90	60074	1			3052208	TTY Input Buf				
60074	512	5F880	60298	1			3052238	TTY Output Buf				
60298	2000	60074	60A8C	1			3040586	*Init*				
60A8C	2000	60298	61280	1			30785AC	Exec				
61280	2000	60A8C	61A74	1			30785AC	Exec				
61A74	52	61280	61ACC	1			3051A9E	Exec				
61ACC	60	61A74	61B2C	1			3051A9E	Exec				
61B2C	24	61ACC	61B68	1			3088340	*Init*				
61B68	3440	61B2C	628FC	1			303F792	Reg Service				
628FC	2040	61B68	63118	1			303F792	Reg Function				
63118	1136	628FC	635AC	1			304949C	Registry				

show flash

The **show flash** command is used to display the names and sizes of files stored in flash memory. This is typically the IOS file. Information about the total size in bytes of available, used, and free flash memory is displayed. It is very important to check the size of IOS files against the size of flash memory available before upgrading the IOS version.

```
Routerl#show flash

System flash directory:

File Length Name/status

1 5569984 igs-j-l.103-7.4

[5570048 bytes used, 2818560 available, 8388608 total]

8192K bytes of processor board System flash (Read ONLY)
```

show ip route

A

The **show ip route** command is used to display the current contents of the Internet Protocol routing table. When a router learns how to send information to a network, it adds the information as an entry to its routing table. The routing table is built dynamically and maintained in RAM.

Since information in RAM is lost when the router is powered down, the routing table must be rebuilt each time the router is powered down. Therefore, it is not a good idea to reboot a router unless it is absolutely necessary.

```
RouterC#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
  B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
 default
       U - per-user static route, o - ODR
       T - traffic engineered route
Gateway of last resort is 208.212.224.1 to network 0.0.0.0
С
     192.168.1.0/24 is directly connected, Serial1
S*
     0.0.0.0/0 [1/0] via 208.212.224.1
     208.212.224.0/23 is directly connected, Ethernet0
С
```

show running-config

The **show running-config** command is used to display the current running configuration file, which is always stored in RAM. This command will let you review configuration changes before saving the configuration to NVRAM. NVRAM is used to hold the startup configuration files that are loaded during the router boot processes.

```
router1#show running-config
hostname Router1
!
boot system flash igs-j-l.103-7.4
boot system igs-j-1.103-7.4 208.212.225.71
boot system rom
enable secret 5 $1$dnKx$ZP34XME.oGEZzhn2TtU5G.
enable password ciscol
L
ipx routing 0000.0c3b.b4f2
!
interface Ethernet0
  ip address 192.168.0.1 255.255.255.0
 no mop enabled
!
interface SerialO
  ip address 192.168.1.1 255.255.255.0
```

```
ļ
interface Serial0.1
!
interface Serial1
 no ip address
  shutdown
!
router rip
 network 192.168.0.0
 network 192.168.1.0
!
ip default-network 192.168.1.1
!
banner motd ^Cwelcome to router 1, authorized users only^C
!
line con O
 exec-timeout 0 0
 password cisco
 login
line aux O
 transport input all
line vty 0 4
 password cisco
 login
ļ
end
```

show startup-config

The **show startup-config** command is used to display the contents of the file used by the router to load configuration information during the boot process. The startup-config file is stored in NVRAM. The startup-config file can be loaded if configuration changes do not have the desired result or if the running configuration has been altered.

)	 	 	 	

telnet

The **telnet** command allows you to connect to other hosts using VT100 emulation. You can use this to connect to other routers or computers that support telnet sessions. This command is very useful when troubleshooting routers remotely. If the on-site technician runs the setup configuration and a basic configuration is established, you can then telnet in and remotely configure advanced parameters.

Message of the Day

The message of the day, once configured, is displayed whenever a telnet or console connection is established to the router. It can be used to identify the router and the function of the router or the banner can be something fun and informative. The message of the day is configured from the Global Configuration mode, an example of which follows.

```
Router1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#banner motd !Welcome to Router1!
Router1(config)#exit
Router1#
```

Once configured, the message of the day (Banner mode) is stored in the running configuration until the **copy running-config startup-config** command is issued, at which point it is copied into NVRAM and will be part of the configuration every time the router boots.

show sessions

The **show sessions** command is used to display information about active telnet (VTY) connections to the router. The IP address of the source host and session statistics are shown.

CONTROL+SHIFT+6 followed by X

This command allows you to break out of an active telnet session and return to the router prompt without disconnecting the telnet session. Sometimes when you change the IP address of an interface, your telnet session will hang. You can break out of the session using the *CONTROL+SHIFT+6* key combination, followed by the *X* key, then telnet back in and find the session using the **show sessions** command. You can clear the session using the **disconnect** <1-20> command.

configure

The **configure** command is used to enter configuration information. There are three ways to configure a router using the **config** command.

- The **configure memory** command loads the configuration file from NVRAM. This has the same effect as the **copy startup-config running-config** command.
- The **configure network** command loads configuration information from a network host using the trivial file transfer protocol.
- The **configure terminal** command allows you to input global and interfacespecific configuration commands such as protocol and address configuration, routing protocol configuration, and subinterface configuration commands.

hostname

This Global Configuration command, as shown below, allows you to change the router identification.

```
Router1(config)#hostname router
router(config)#^Z
router#
```

AT R	Ď	 	 	 	 	 	

show interfaces

The **show interfaces** command is used to check the status of all interfaces. Information about the state of the interface, interface address, maximum transmission unit size, encapsulation type, and traffic statistics is displayed.

```
SerialO is up, line protocol is up
 Hardware is HD64570
 Internet address is 192,168,1,1/24
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
   1/255
 Encapsulation HDLC, loopback not set, keepalive set (10 sec)
 Last input 00:00:00, output 00:00:02, output hang never
 Last clearing of "show interface" counters never
 Queueing strategy: fifo
 Output queue 0/40, 0 drops; input queue 0/75, 0 drops
 5 minute input rate 0 bits/sec, 1 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
    125995 packets input, 4440501 bytes, 0 no buffer
    Received 123920 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    12617 packets output, 740789 bytes, 0 underruns
    O output errors, O collisions, 3 interface resets
    O output buffer failures, O output buffers swapped out
    5 carrier transitions
    DCD=up DSR=up DTR=up RTS=up CTS=up
```

ip address

This interface-specific configuration command is used to set interface IP addresses. The syntax is **ip address** *ip address subnetmask*.

```
Router1(config-if)#ip address 192.168.2.1 255.255.255.0
```

To change the IP address on an interface using older versions of the IOS, you must first remove the existing IP address. To remove an IP address, use the **no ip address** *ip address subnetmask*.

```
Router1(config-if)#no ip address 192.168.2.1 255.255.255.0
```

CONTROL+Z

This shortcut command will allow you to exit completely out of Configuration Mode. Remember that configuration changes take place as soon as you press *ENTER* and that changes are saved into the running configuration, stored in RAM. Unless you save your configuration changes to the startup configuration file stored in NVRAM, your changes will be lost when the router reboots.

write memory

This is an older command retained for backward compatibility. It is the same as the **copy running-config startup config** command. The commands *CONTROL+Z* and **write memory** should only be used if you are absolutely sure the changes you made are correct. This shortcut combination achieves the same result as the **exit** and **copy running-config startup-config** commands.

Cisco recommends exiting out of the Configuration mode and using the **show running-config** command to review your changes. Once you are sure your changes meet the desired results, then issue the **copy running-config startup-config** commands. If you use the **write memory** command, you will not be able to check to see if your commands were accurately entered. This could result in network traffic coming to a halt as you re-enter configuration commands. If you notice you have entered incorrect configuration information, you can simply restore the original configuration information using the **copy startup-config running-config** command.

```
router(config)#^Z
Router1#write memory
Building configuration...
[OK]
```


Syslog

The **syslog** command, available from Privileged Exec mode, allows you to keep track of error messages in real time. Each error message created by the IOS is shown on the console screen as it occurs. This is a very useful feature when troubleshooting and is useful occasionally when in normal operation. However, it can become an annoying interruption when trying to enter commands–particularly large commands or multiple commands.

Perhaps a more effective method of checking error messages if you are entering commands on the console would be to issue the **logging buffered** command. This will save the IOS error messages in a buffer on the device. When you wish to view the messages later, issue the **show logging** command.

Debug

Debug is a useful command in troubleshooting your device. There are a number of monitoring points upon which **debug** can be enabled, including ICMP tracings and other packets. Through the various debug options, you can track packets sent to and from specific interfaces, or all interfaces. You can also track a specific protocol on a given interface. **Debug** is particularly useful when you have isolated a problem to a given interface or port.

If you use **debug** on a router that is currently in production, be careful not to bog the system down with excessive debug messages. For example, running a **debug** command such as **debug packet** on a busy interface could flood the system with enough error messages to bring the interface (or even the router) down.

USING HELP

If you don't know a command, or you know only part of a command, the Cisco IOS supports both context-sensitive and word help formats. Context-sensitive will be of help if you don't know exactly what command to use; word help is great if you don't know how to complete an argument.

No matter what mode you are in, the Cisco IOS can provide help. Suppose you are in User mode and would like to see a complete list of the commands available. Type "?" and then press *ENTER*.

Assume that after checking out the commands available in User mode, you find that you would like to use a particular command but would like additional help on how that command should be entered at the prompt.

For example, let's say you would like to see how to use the **show** command. Type "show" at the prompt, followed by a space and then "?", and then press *ENTER*. (Be sure to place a space between **show** and the question mark, or you will get a "bad command" notification.) You will be provided with help specific to the chosen command.

After providing help on the specific command, the command is automatically retyped for you at the command prompt. You can then add specific parameters to the command and press *ENTER* to execute it.

For example, in the case of the **show** command, you can add **version** to the command and then press *ENTER*. Parameters related to the IOS currently installed on the router will be displayed on the screen.

The help system is also available in Privileged and Configuration modes. The Privileged mode help is similar to that found in the User mode. You can receive general help by typing "?" or access more specific help by typing a command followed by a space and "?".

To learn more about how to use the online help system, you can type "help" from the router prompt. This will give you explicit instructions on how to use the help system, as illustrated below.

```
routerl>help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must back up until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
command argument (e.g., 'show ?') and describes each possible
argument.
2. Partial help is provided when an abbreviated argument is entered
and you want to know what arguments match the input
(e.g. 'show pr?').
```

$ \rightarrow $					 	 	

To access context-sensitive help, you can type "?", as illustrated below:

router>?	
Exec commands:	
connect	Open a terminal connection
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
exit	Exit from the EXEC
help	Description of the interactive help system
lat	Open a lat connection
xremote	Enter XRemote mode

To use word help, type an incomplete command (as closely as possible to the correct command) followed by a question mark in place of the incomplete portion of the command. This is useful if you do not remember the complete command structure. For example, typing the following:

Router1#show i?

results in:

interfaces ip ipx isis

Choose the correct command, in this case "interfaces", from the list of available commands.

```
Router1#show interfaces
Ethernet0 is up, line protocol is down
Hardware is Lance, address is 0000.0c3b.b4f2 (bia 0000.0c3b.b4f2)
Internet address is 192.168.0.1 255.255.255.0
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 128/255,
load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 4:00:00
```

SUMMARY

During this chapter, you were introduced to the following topics:

- The Cisco Command-Line Interface
- The Exec (or executable) prompt
- Configuration mode
- IOS commands and parameters
- Logging in to the router in both User Exec and Privileged Exec modes
- Using the context-sensitive help feature
- Using the help system to identify all User Exec commands
- Using the command history and editing features
- Controlling router passwords, identification, banners, and a message of the day
- Entering an initial configuration using the setup command
- Examining the current configuration running in RAM
- Examining the startup configuration stored in NVRAM



Stop now and complete the following NEXTSim exercises on the Interactive Learning CD-ROM:

Understanding IOS View Help for the Show Command in Privileged Mode View the Router Startup Configuration View the Router Version Information

Network Protocols

View the Router Interface Details

Ż)				 	 	

POST-TE	ST QUESTIONS
The a	answers to these questions are in Appendix A at the end of this manual.
A 1.	What command would you use to enter the Privileged Exec mode from the User Exec mode?
2.	What command would you use to display a list of all available commands in the User Exec mode?
3.	What command would you use to configure the Message of the Day?
4.	What editing command would you use to repeat the last command entered?
5.	What command would you use to change the router identification?
6.	What command would you use to examine the configuration file that is not lost during reboot? The file that is lost during reboot?

Managing the IOS on a Router

СНАРТЕ

3

R

MAJOR TOPICS

Objectives	8
Pre-Test Questions5	8
Introduction	9
Memory Types6	0
Passwords	1
Loading the IOS	0
The IOS and TFTP72	2
Working with Configuration Files73	3
Cisco Discovery Protocol74	4
Summary78	8
Post-Test Questions7	9

OBJECTIVES

At the completion of this chapter, you will be able to:

- Define the basic tenets of the Cisco IOS.
- Describe the hardware architecture of a Cisco router.
- List password types and functionality.
- Describe how to load, save, and move the IOS to and from a router.

PRE-TEST QUESTIONS

The answers to these questions are in Appendix A at the end of this manual.



What is the name of the operating system on a Cisco router?
 What is stored on the Flash RAM of a Cisco router?
 What is the basic function of Cisco Discovery Protocol?
 What is the command to set an enable password?

INTRODUCTION

At the heart of each Cisco product is its operating system software, the Cisco Internetwork Operating System (IOS). Each Cisco device possesses this IOS in some form or fashion. In order to fully appreciate the abilities of a Cisco device, one must master the Cisco IOS.

This chapter will look at memory types and passwords. Loading the IOS and the relationship between the IOS and TFTP will then be covered. The chapter will conclude with a discussion on working with configuration files and the Cisco Discovery Protocol.



Stop now and view the following video presentation on the Interactive Learning CD-ROM:

Router Boot Options and Password Recovery Router Password Recovery



MEMORY TYPES

Routers not only need processing power, they also need a place to store configuration information, a place to boot the router operating system, and memory that can be used to hold dynamic information as the router does its job of moving packets on the internetwork.

Cisco routers contain four different types of memory components that provide the storage and dynamic caching required. The memory components found in a Cisco router are:

```
ROM Contains the Power-On Self-Test (POST) and the
bootstrap program for the router. The ROM chips also
contain either a subset or the complete router IOS. (For
example, the ROM on the Cisco 2505 router only
contains a subset of the IOS, whereas the 7000 series
contains the full IOS.) Because the IOS is available on
the ROM, you can recover from major disasters, such as
the wiping out of your Flash RAM. The ROM chips on
Cisco routers are removable and can be upgraded or
replaced.
```

NVRAM (Nonvolatile RAM)

Stores the startup configuration file for the router. NVRAM can be erased, and you can copy the running configuration on the router to NVRAM. The great thing about NVRAM is that it retains information even if the router is powered down. This is extremely useful considering you wouldn't want to have to reconfigure the router every time the power goes down.

Flash RAM	Flash is a special kind of RAM that you can actually erase and reprogram. Flash is used to store the Cisco IOS that runs on your router. You can also store alternative versions of the Cisco IOS on the Flash (such as an upgrade of your current IOS), which makes it very easy for you to upgrade the router. Flash RAM comes in the form of SIMMs (Single-Inline Memory Modules), and additional Flash RAM may be installed on some routers.
RAM	Similar to the dynamic memory you use on your PC, RAM provides temporary storage of information. Packets are held in RAM while their addressing information is examined by the router. RAM also holds other information, such as the current routing table and the currently running router configuration. Changes that you make to the configuration are kept in RAM until you save them to NVRAM.

Each of these memory components play an important role in what happens when you boot the router. The possibilities revolving around the router system startup and where the router finds its IOS and startup configuration files are discussed in the next chapter.

PASSWORDS

Access to your router is controlled by various levels of password protection. You can set separate passwords to allow different *levels* of access or allow different *methods* of access. Correct management of password distribution and periodic password changes will help protect your network from various methods of unauthorized entry.

You can also create individual usernames and passwords for each person responsible for administering the router. This prevents access to the router unless a valid username and password are entered after connecting to the router.

Ś	 		

There are several levels of password protection available on a Cisco router. There are also strategies for applying each level in various combinations to achieve the security level results required for your network.

In this section, we will explore the following password topics:

- Enable Password
- Enable Secret Password
- Line Password
- Login Command
- Console Password
- Virtual Terminal Password
- Setting Up Usernames and Passwords
- Disabling the Enable Password
- Getting Around Lost Passwords

Enable Password

The enable password is used to gain access to the Privileged Exec (or Enable) mode. By default, you can gain access to User Exec mode by pressing the *ENTER* key after you connect to the console port. The enable password is set up initially in setup configuration mode but is not required to gain access to the console port. It can be changed using the command **enable password** *password* in global configuration mode, as shown below.

```
Router1(config)#enable password cisco2
```

Enable Secret Password

The enable secret password also controls access to the Privileged Exec mode but uses a stronger encryption algorithm. Setting an enable secret password will require a console user to enter two passwords at the login prompt in order to access enable Privileged Exec mode.

Using an enable secret password provides added security in that it appears encrypted in the configuration file. This is useful if you are loading configuration files across a network using a TFTP server. More will be explained on securing these configuration files later.

The enable secret password cannot be the same as the enable password and is displayed in encrypted format with the show config password. The enable secret password is also set up in the initial setup configuration dialog. The enable secret password can be changed using the **enable secret** *password* command from global configuration mode.

```
Router1(config)#enable secret cisco
```

In the example below, the results of the **show config** command are displayed. Notice that the enable password is displayed in plain text while the enable secret password is encrypted.

```
Current configuration:

!

version 10.3

service udp-small-servers

service tcp-small-servers

!

hostname Router1

!

boot system flash igs-j-1.103-7.4

boot system igs-j-1.103-7.4 208.212.225.71

boot system rom

enable secret 5 $1$dnKx$ZP34XME.oGEZzhn2TtU5G.

enable password cisco2
```

/				

A

Line Password

The line password is used to secure individual lines on a router. Its primary use is in securing the console from access via telnet. If you set a line password, a user will need to know the password and log in before access to the console is granted. This example demonstrates how to set a line password:

```
RouterB#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#line con 0
RouterB(config-line) #password cisco
RouterB(config-line)#login
RouterB(config-line)#exit
RouterB(config)#line vty 0 3
RouterB(config-line) #password cisco
RouterB(config-line)#login local
RouterB(config-line)#exit
RouterB(config)#line vty 4
RouterB(config-line)#password steven
RouterB(config-line)#login
RouterB(config-line)#exit
RouterB(config)#^Z
RouterB#wr mem
```

Login Command

The **login** command enables or disables the password for establishing console and telnet sessions. You must specify the interface login command in order to require a line password for login.

Even if you set a line password, if you do not specify the interface login command, the password will be set but not required for login. So after you set passwords for console and virtual terminals, remember to issue the **login** command in the line configuration mode.

The example demonstrates a configuration file with the appropriate login commands.

```
line con 0
exec-timeout 0 0
password cisco
login
line aux 0
transport input all
line vty 0 4
password cisco
login
```

Console Password

The console password is set separately from other passwords. The console password controls access to the router console port (labeled "con" on the back of a router). The console password is disabled by default. This password is set in line configuration mode. An example shown below walks you through the steps involved.

```
Router1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#line console 0
Router1(config-line)#login local
Router1(config-line)#password steve
Router1(config-line)#^Z
Router1#
%SYS-5-CONFIG_I: Configured from console by console
Router1#wr mem
Building configuration...
[OK]
```

}	 	 	
/	 	 	

Notice the changes made to the NVRAM configuration file (**wr mem**) using the **show config** command.

```
line con 0
exec-timeout 0 0
password steve
login local
```

The **login local** command tells the router to use a password that is defined locally in line configuration mode.

Virtual Terminal Password

Virtual terminal passwords are required if you desire to support remote configuration through telnet sessions. A vty connection is a virtual terminal connection. An example of a vty connection is a telnet session. Cisco recommends setting up a separate vty line for disaster recovery. So if you configure vty lines 0 through 3 with one password and vty line 4 with a separate password, at least one vty circuit is available for disaster recovery in the event that all other lines are in use.

```
Router1#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#line vty 0 3
Router1(config-line)#login local
Router1(config-line)#password steve
Router1(config-line)#exit
Router1(config)#line vty 4
Router1(config-line)#login local
Router1(config-line)#password swannie
Router1(config-line)#password swannie
Router1(config-line)#exit
Router1(config)#exit
Router1#
```

If we check the configuration using the **show running-config** command, we will see that there are four vty lines using one password, with the last and fifth vty line reserved for disaster recovery.

```
Routerl#sho run
Building configuration...
line con 0
exec-timeout 0 0
password steve
login local
line aux 0
transport input all
line vty 0 3
password steve
login local
line vty 4
password swannie
login local
```



Setting Up Usernames and Passwords

In order to establish login requirements on your router, you must first set up usernames and passwords before disabling the enable password. The command to accomplish this is **username username password**. An example is listed below:

```
Router#lconfig t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#username steve password swannie
Router1(config)#line con 0
Router1(config-line)#login local
Router1(config-line)#
Router1(config-line)#^Z
Router1#wr mem
%SYS-5-CONFIG_I: Configured from console by steven on console
Building configuration...
[OK]
Router1#
```

Disabling the Enable Password

If you commonly store your configuration files on a network TFTP server, that practice creates a security exposure. Any network user could read the configuration file in unencrypted format, subsequently gaining access to routers by reading the enable password from the configuration file.

One way to prevent this possible exposure would be to utilize an enable secret password. Another is to disable the enable password.

Disabling the enable password automatically prompts for username and password whenever a connection to the router is established. This level of security requires that usernames and passwords for each user be set up on the router in question.

CAUTION:

If the enable password is disabled before setting up usernames and passwords on your router, your router will be inaccessible!

It is important to note that you must create global usernames and passwords before you disable the enable password and set up login requirements on your router. If you do not, you will not be able to gain access to your router.

The command to establish a username and a password associated with that username is **username** *username**password password.* An example of this sequence is illustrated below.

Router1(config)#username steve password swannie

After you have created at least one username and password, then enter into global configuration mode and disable the enable password using the **no enable password** command.

Router1(config)#no enable password

You will be prompted for a username and password each time a connection is made to the router

```
User Access Verification
Username: steven
Password:
Router1>
```

Getting Around Lost Passwords

Sometimes you just forget those passwords, which can be bad news if you need to enter the Privileged mode and change the configuration of a router.

Replacing a Lost Password

- 1. Attach a terminal or PC with terminal emulation to the console port of the router.
- 2. Turn the router off and, after waiting 5 seconds, turn it back on. As the router reboots, press *CONTROL*+*BREAK* on the terminal within 60 seconds.
- 3. You will enter the ROM Monitor mode. Type "e/s2000002" and then press *ENTER*. Write down the virtual configuration number that appears.

Ď	

- 4. Now at the prompt, type "o/r 0x2142" and press *ENTER* (this makes the router ignore the configuration file in NVRAM). Type "i" at the prompt and press *ENTER*. The router will reboot and enter the configuration dialog. Click on **No** at the dialog prompt, then press *ENTER*.
- 5. At the router prompt, type "enable" to enter the Privileged mode. Type "copy startup-config running-config" and press *ENTER* to get your original configuration into the router's RAM.
- 6. At the enabled prompt, type "config". You are now in the Configuration mode. Type "enable secret *newpassword*", where *newpassword* is your new secret password. Now you must set the register contents back to the original contents.
- 7. At the config prompt, type the config-register 0x virtual configuration number (which is the virtual configuration number that you wrote down). Press *ENTER*.
- 8. Now type "end" and press *ENTER* to get out of the Configuration mode. Reboot the router. Now you should have a new secret password, and the router should be back to its normal configuration.

Becoming familiar with the various modes of the router and the commands that they offer is an extremely important aspect of overall router management. In the next chapter, you will become more familiar with the Cisco IOS and the commands and command structure that it offers. Each of the modes discussed in this chapter will be covered in the context of the IOS commands available in a particular mode.

LOADING THE IOS

Earlier in this chapter, we discussed the four different types of memory found in the Cisco router (ROM, NVRAM, Flash RAM, and RAM). All of these memory types play a part in the boot sequence of a router. Before you walk through the sequence of steps to configure a brand new router right out of the box, some discussion is required to explain the router boot sequence and the various places that the router will look for a configuration file.

The following topics will be covered in this section:

- Router Boot Sequence
- Boot System Command

Router Boot Sequence

When you power the router on, the ROM chip runs a Power On Self Test (POST) that checks the router's hardware, including the processor, interfaces, and memory. This test is similar to the power-on test that a PC runs (RAM, CPU, and other hardware is checked).

The next step in the router bootup sequence is the execution of a bootstrap program that is stored in the router's ROM. This bootstrap program searches for the Cisco IOS. The IOS can be loaded from the ROM, the router's Flash RAM, or from a TFTP server on the network. The IOS is typically stored in the router's Flash RAM.

After the router's IOS is loaded, the router searches for the configuration file. The configuration file is normally held in NVRAM. A **copy** command is used to copy a running configuration to NVRAM. As with the IOS, however, the configuration file can be loaded from a TFTP server. Again, the location of the configuration file would be dictated by information held in the router's NVRAM.

After the router loads the configuration file, the information in the file enables the interfaces and provides parameters related to routed and routing protocols in force on the router. Keep in mind that loading the IOS from a source other than Flash RAM requires a notation in the ROM's configuration Registry. Also, to load the configuration file from a source other than NVRAM, information pointing to the location of the file has to be contained in NVRAM.

If a configuration isn't found in NVRAM or in another place specified (such as a TFTP server), the Setup mode is entered and the System Configuration dialog appears on the router console screen.

Boot System Command

You can also manually configure the router to look for the IOS file from specific locations. The command to perform this operation is **boot system**. Boot system is a global configuration command that instructs the router specifically where to look for IOS files upon bootup and the order to search for those files. You enter boot system commands in the order you want the router to search for IOS files. An example of the boot system rom is shown below.

```
Router1(config)#boot system flash igs-j-1.103-7.4
Router1(config)#boot system tftp igs-j-1.103-7.4 208.212.225.71
Router1(config)#boot system rom
Router1(config)#^Z
Router1#wr mem
%SYS-5-CONFIG_I: Configured from console by consoleBuilding
configuration...
[OK]
```

The first line tells the router to look for the IOS file igs-j-1.103-7.4 in Flash RAM, the default location. If it cannot be loaded from Flash, the second command instructs the router to look for the same file on TFTP server 208.212.225.71. The last command, **boot system rom**, instructs the router as a final failsafe to load the IOS from ROM. This could be the full IOS version, but for most router models it is a limited IOS version that will allow the router to boot so the system's administrator can correct any problems in locating the correct IOS.

THE IOS AND TFTP

You can instruct the router to look for the IOS files in various places upon bootup, but what if the IOS becomes corrupted or you need to update the IOS to support additional software feature packs?

The easiest way to upgrade the IOS is with a TFTP server, covered in depth in the Network Management chapter. Not only can you use a TFTP server to load configuration and IOS files for disaster recovery, but you can use a TFTP server to upgrade the IOS as well.

Cisco sells feature packs to add enhanced functionality to the original IOS shipped with routers. Feature packs might include support for Novell's Internetworking Packet Exchange protocol, IP Firewall Feature Pack, or encrypted Virtual Local Area Networking (IPSec 3 DES).

WORKING WITH CONFIGURATION FILES

The previous chapter explained the different configuration files used by the Cisco IOS, and you already know how to copy to and from the various configuration files. Now let's examine how you can store these files on the network for disaster recovery purposes.

It is important to note that you must thoroughly understand this section to successfully complete the CCNA exam.

The following topics will be covered in this section:

- Copying Configuration Files to the Network
- Copying Configuration Files from the Network

Copying Configuration Files to the Network

To successfully copy files from RAM (running-config), use the **copy running-config tftp** command. This command will copy the configuration file in memory to a network TFTP server. This is true of any copy operation on a router.

To successfully copy files from NVRAM, use the copy startup-config tftp command.

Notice in both examples that you specify the file you want to copy (source) before you specify the location (destination) to copy the file to.

Copying Configuration Files from the Network

To successfully copy previously saved configuration files from the network to a router, use **copy tftp {startup-config | running config}**. Notice that again the location to copy from is placed before the location where you wish to place the file. The startup config is stored in NVRAM while the running-config is stored in RAM.

CISCO DISCOVERY PROTOCOL

One of the most useful features of the Cisco IOS is the Cisco Discovery Protocol (CDP). The CDP allows Cisco routers to *find* each other on an Internetwork. In this section, we will examine the following CDP topics:

- Checking Out the Internetwork Neighborhood
- Viewing CDP Neighbors

Checking Out the Internetwork Neighborhood

When you work with internetworks, it's important to be able to gather information related to routers that are directly connected to your router. These routers are typically referred to as neighbors. Cisco routers have a proprietary protocol, Cisco Discovery Protocol (CDP), that provides you with the capability to access information related to neighboring routers. CDP uses Data Link broadcasts to discover neighboring Cisco routers that are also running CDP. (CDP is turned on automatically on routers running IOS 10.3 or newer.)

Before you use CDP to view information about other routers, you may want to check your router interfaces to make sure that CDP is enabled. This is done using the **show cdp interface** command.

Viewing CDP Interfaces

- 1. At the User or Privileged prompt, type "show cdp interface".
- 2. Press *ENTER* to execute the command.

The results of the command will appear on the router console screen (see below). The CDP information for all interfaces on the router will appear.



You can also view the CDP information for a particular interface. For example, in the screen shot above, the command that follows the initial **show cdp interface** command is **show cdp interface s0**. This provides the CDP information for just interface serial 0.

Above, you will see two pieces of information that warrant further discussion: the CDP packet send interval and the CDP holdtime. Notice that CDP packets are sent by CDP-enabled interfaces every 60 seconds. This means that they are broadcasting information to their CDP neighbors every minute.

A R	Ž	

The holdtime refers to the amount of time a router should hold the CDP information that it has received from a neighboring router. If a router doesn't receive an update message from a neighbor within 3 minutes (180 seconds), it must discard the old CDP information that it holds.

Remember that the purpose of CDP is to stay up to date on the status of your neighboring routers. So, if a line is down or some other problem causes you to lose contact with a neighbor, you don't want your router relying on old information when it makes routing decisions.

If a particular interface isn't enabled for CDP, you can enable it in the Configuration mode.

Enabling CDP on an Interface

- 1. At the Privileged prompt, type "config terminal". You are placed in the Configuration mode with the console (terminal is the source for the configuration information).
- 2. At the Config prompt, type the interface you want to enable for CDP, such as interface serial 0. Then press *ENTER*. The prompt changes to the Config-If prompt, letting you know that you can now enter information for the configuration of the designated interface.
- 3. Type "cdp enable" and press ENTER.
- 4. To end the configuration of the serial interface, press *CONTROL*+Z. You will be returned to the Privileged prompt.

르미	💻 Tera Term - COM2 VT								
Elle	Edit	Setup	Conhoi	Window	Help				
Ent pop pop pop 1d2	er c eye(eye(eye(onfig confi confi confi xSYS-	g)#int g-if)# g-if)#	n conn erface todp en rZ	seria able	a10	er line. From con		CHILZ.

Viewing CDP Neighbors

After you have viewed the status of CDP on your various interfaces, you can use CDP to take a look at platform and protocol information on a neighboring router or routers.

- 1. At the User or Privileged prompt, type "show cdp neighbor".
- 2. Press *ENTER* to execute the command.

The screen below shows the result of this command for a 2505 router that only has one neighbor, which is connected via a serial interface. The table below describes this information shown.

🗏 Tera Tem - Di	IN2 VT					
file Edit Setup	Control <u>Window</u> Help					
popeyedish cdp Capability Co	des: R - Reuter, T S - Switch, H	- Irans Brid Hest, I -	ge, B - Sourc IGMP, p - Rep	e Route Br	idge	-
Device ID elive popeye#	Local Intrfcs Sep 8	Haldtme 126	Capability R	Platforn 2585	Port ID Ser Ø	

Parameter	Meaning	Example
Device ID	The neighbor's or neighbors' host name(s) Olive	
Local Interface The interface on the local router that provides the connection to the neighbor Series		Serial O
Capability	Whether the router is configured to serve multiple functions such as routing (R), Bridging (B), and switching (S)	R (This router is only configured to route)
Platform	The type of Cisco router	2505 (The neighbor is a 2505 router)
Post ID	The interface used on the neighbor to connect to your local router	Serial O

Obviously, if you are using a higher-end router that is connected to many different neighbors via its various interface ports, the number of neighbors shown using the show **cdp neighbors** command would be greater than that shown in the previous screen.

If you want to see more details concerning your CDP neighbors, you can use the **show cdp neighbor details** command. You can enter this command at the User or Privileged prompt. Notice that this command provides the IP address of the neighbor's interface and the version of the IOS that the neighbor is running.

SUMMARY

This chapter introduced you to the heart of the Cisco router, the Internetwork Operating System (IOS). We began by looking at the following:

- Four different types of memory used by Cisco routers: ROM, NRAM, Flash RAM, and RAM
- Passwords and a number of commands used to control them
- Loading and recovering the IOS
- TFTP as it relates to the IOS
- Cisco Discovery Protocol
- Configuration files



Stop now and complete the following NEXTSim exercises on the Interactive Learning CD-ROM:

Understanding IOS

Configure VTY Password Change the Router Enable Password Copy the Startup Configuration to a TFTP Server Upgrade the IOS

POST-TEST QI	UESTIONS
--------------	----------

The answers to these questions are in Appendix A at the end of this manual.



Which command is used to display information about directly connected routers?
 What command is used to back up the running configuration on a router?
 What command would you use to back up the configuration file in NVRAM?
 What does TFTP stand for?



5. Is authentication used in TFTP?

.....

.....

6. What command is used to require a password to be used on console lines after a password is set?

.....

Router Configuration

CHAPTE

R

4

MAJOR TOPICS

►

Objectives	82
Pre-Test Questions	82
Introduction	83
Anatomy of a Router	84
Setting Up a New Router	87
Basic Router Configuration	95
Saving a Configuration	103
Loading a Configuration	105
Interfaces	106
Port Configuration	112
Network Configuration	113
Summary	114
Post-Test Questions	114

OBJECTIVES

At the completion of this chapter, you will be able to:

- Describe the basic design and configuration of the Cisco router.
- Save, upgrade, and load a backup Cisco IOS software image.
- Use the TFTP sever for router configuration storage.
- Describe some of the basic router troubleshooting methods.

PRE-TEST QUESTIONS

The answers to these questions are in Appendix A at the end of this manual.



1. What is a router?

.....

2. What is Privileged mode?

.....

.....

3. What mode should you be in to copy a running-config startup-config?

.....

.....

4. What is the syntax you would use to configure a port on a Catalyst 5000 switch?

.....

INTRODUCTION

Routers provide the hardware and software necessary for routing. They are important internetworking devices for connecting LAN subnets and for making wide area connections between subnets.

In this chapter, we will take a look at the basic design and configuration of the Cisco router. We'll examine the nuts and bolts of getting a router out of the box and ready for deployment on the network. You'll also be introduced to advanced configurations and some of the Cisco configuration tools.



Stop now and view the following video presentation on the Interactive Learning CD-ROM:

Router Fundamentals Router Memory Types Router Access Router Configuration Basics Initial Configuration Setup Mode



ANATOMY OF A ROUTER

In order to gain a comprehensive understanding of a Cisco router, it is necessary to familiarize oneself with its architecture. The design of a Cisco router allows it to perform the tasks it needs to perform without any added hardware that could hinder network performance.

The following topics will be covered in this section:

- Router Components
- Router CPUs
- Router Memory

Router Components

Cisco routers must be able to build routing tables, execute commands, and route packets across network interfaces using routing protocols. This means that the router must have processing power, some sort of storage capacity, and available random access memory. It is also necessary for the router to have appropriate software, such as an operating system, that can be used to configure routing protocols.

Several Cisco router models are available, each designed to satisfy a particular networking need. The number and type of ports vary from model to model. Many of the higher-end routers allow you to customize the type and number of interfaces found on the router.

The figure below shows the front and back of the Cisco 2505 Router. The 2505 router provides three interfaces: one LAN and two serial interfaces. The 2505 is typically used to connect subnets over serial connections, such as ISDN, T1 leased lines, and other WAN alternatives.



Router CPUs

Routers are similar to PCs in that they contain a microprocessor. And just like PCs, different Cisco router models come with different processors.

For example, the Cisco 2505 Router contains a 20-MHz Motorola 68EC030 processor. A higher-end router like the Cisco 7010 Router contains a 100-MHz Motorola RISC CPU.

Many of the lower-end routers use the same Motorola processors that are used in a variety of Apple Macintosh computers. Some of the very high-end routers use RISC processors that you would typically find on miniframe computers or very high-end servers.

Router Memory

Routers not only need processing power, they also need a place to store configuration information, a place to boot the router operating system (IOS), and memory that can be used to hold dynamic information as the router does its job of moving packets on the internetwork. Cisco routers contain different types of memory components that provide the storage and dynamic caching required.

There are four different memory components found in a Cisco router: ROM, NVRAM (nonvolatile RAM), Flash RAM, and RAM. We'll discuss each of these in turn.

ROM

The router's ROM contains the Power-On Self-Test (POST) and the bootstrap program for the router. The ROM chips also contain either a subset of the Cisco IOS or the complete router IOS. For example, the ROM on the 2505 router only contains a subset of the IOS, whereas the 7000 series contains the full IOS.

Because the IOS is available on the ROM, you can recover from major disasters such as the corruption or deletion of your Flash RAM. The ROM chips on Cisco routers are removable and can be upgraded or replaced.

NVRAM (Nonvolatile RAM)

NVRAM stores the startup configuration file for the router. NVRAM can be erased, and you can copy the running configuration on the router to NVRAM.

The major advantage of NVRAM over standard RAM is that it retains the information that it holds even if the router is powered down. This is useful because it eliminates the necessity of reconfiguring the router after power outages. The router's configuration file is normally stored in NVRAM. Thus, when the router boots, the configuration file loads faster than if it were stored on disk.

Flash RAM

Flash is a special type of RAM that is erasable and capable of being reprogrammed. Flash is used to store the Cisco IOS that runs on your router. You can also store alternative versions of the Cisco IOS on the Flash (such as an upgrade of your current IOS), which makes it easy to upgrade the router.

Flash RAM comes in the form of SIMMs (Single-Inline Memory Modules). Depending on the router you have, additional Flash RAM may be installed.

RAM

Similar to the dynamic memory you use on your PC, RAM provides the temporary storage of information. For instance, packets are held in RAM while their addressing information is examined by the router, and RAM is used to hold the current routing table. The currently running router configuration is also held in RAM; changes you make to the configuration are kept in RAM until you save them to NVRAM.

SETTING UP A NEW ROUTER

It's now time to walk through the steps of getting a new router out of its box and connecting it to the LANs that it will service. This connection can be made either by direct connection using a LAN port such as an Ethernet port or by connecting LANs using WAN connections.

Before you attempt to connect the router, it makes sense to take a look at the contents of the box that were shipped to you by Cisco or your Cisco reseller. Make sure you got what you paid for. Check the cable specifications (they are printed on the cable near the connectors). Check the IOS that was shipped (the router won't work with the wrong IOS version). And make sure that the router contains the interfaces you ordered.

If anything is missing or the router doesn't contain the correct cables or interfaces, get on the phone to Cisco (1-800-462-4726) or your local Cisco reseller.

After you have inventoried the router, cables, and software that you were shipped, you can begin to assemble the router.

The following topics will be discussed in this section:

- Connecting the Console
- Setting Up Terminal Emulation Software

)	 	 	

- Establishing Communications between the Router and Console
- Connecting the Router to the Network
- A Final Word on Physical Router Connections

Connecting the Console

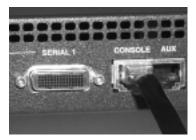
Make sure that the router is turned off, then connect the router's power cable to the router and a power source. The next step is to connect a PC to the router to act as the router's console. The console PC can be any PC that has a serial port and can run some type of terminal emulation software. The PC, in effect, becomes a dumb terminal and provides you with the interface that you use to configure and monitor the router.

The console computer and the router are connected by the roll-over cable that ships with the router. The cable is terminated on both ends with RJ-45 connectors.

The router also comes with several different serial adapters that contain an RJ-45 port so that they can be connected to the router, then to the serial port on the PC that you will use as the router's console. After you've selected the appropriate serial adapter, you are ready to connect the router and the console.

Connect the Router and the Console

1. Place the RJ-45 male adapter on the roll-over cable into the port on the back of the router marked CONSOLE.



2. Attach the serial adapter to the appropriate serial port on the PC that will serve as the console.

With the physical connection of the router to the PC taken care of, you now must set up some type of terminal emulation software on the PC. Terminal emulation software and the communication settings necessary to talk to the router are covered in the next section.

Setting Up Terminal Emulation Software

The PC serving as the console communicates with the router using terminal emulation software. A number of these software packages are readily available, such as HyperTerminal (included with Windows 95, 98, and Windows 2000 Professional operating systems) and ProComm Plus (a commercial communication program that offers faxing, terminal emulation, and other communication possibilities). A number of other possibilities are available on the Internet and can be downloaded as freeware or shareware. One such option is Tera Term Pro, an extremely easy-to-use-and-configure terminal emulator. Tera Term Pro is shown below and is used throughout this manual.



After you have installed the terminal emulation software package of your choice, you must set up the communication parameters for the serial port on the router. The table shows the communication settings to be used by the software.

Parameter	Setting
Terminal Emulation	VT100
Baud Rate	9600
Parity	None
Data Bits	8
Stop Bits	1 (2 stop bits for 2500 series router)

Establishing Communications between the Router and Console

Each terminal emulation package will operate a little differently, but each will provide some sort of menu/dialog box system that gives you access to the various settings for the software.

The Serial port setup dialog box in Tera Term Pro is shown below. Communication settings are configured using drop-down boxes.

Pert	000M2	<u>.</u>	OK
Send rate:	5600	+	
Quita:	0 bit	Ŧ	Cancel
Parity:	none	¥	
Stop:	2.68	٠	Belb
		-	

After you've correctly configured the console's terminal emulator, you must establish communications with the router.

Establish Communications between the Router and the Console

- 1. Start your terminal emulator. Make sure that you have selected the appropriate serial port for communications and set the communication parameters as shown in the previous table.
- 2. Power on the router. For many Cisco routers, there is a rocker switch on the back for powering the router on or off. For some models, you may need to unplug the router's power cable in order to power up or down.

The banner for the router should appear. If you have a connection with the router, check your serial and console connections on the roll-over cable and make sure that you have specified the correct serial port for the communication session in the terminal emulator.

Routers right out of the box will not normally be configured. This means that none of the interfaces have been prepared for communications nor have the appropriate routed and routing protocols been configured for operation on the new router.

Connecting the Router to the Network

After the router is connected to the console, you have a means to configure the various router parameters. The next step is connecting the router to the networks that it will service.

As previously discussed, several different interfaces can be available on your router, depending on the router model and the selected configuration. For a basic walkthrough of some of the connection options, we will take a look at a 2505 Cisco Hub/Router.

LAN Connections

Depending on the type of router you have, LAN connections are typically made to an Ethernet or Token Ring interface port on the router and then to a hub or Multistation Access Unit (MAU) that supplies the connections for the various computers on the network.

Let's assume that we are connecting an Ethernet LAN to our router. Typically, a hub will be connected to the Ethernet port using Category 5 unshielded twisted-pair cable (CAT 5) since the router's Ethernet interface provides an RJ-45 female port. The various computers on the network will then be connected to the hub.

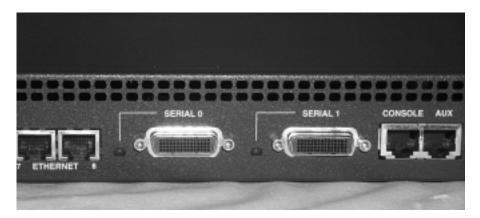
To use a straight-through CAT 5 twisted-pair cable to connect PCs to hubs, you must switch the MDI/MDI-X switch on the router to the MDI-X position. For routers such as the Cisco 2505 and 2507 Routers that don't have the MDI/MDI-X switch, the router must be connected to a hub using a crossover cable. A crossover cable is a modified straight-through twisted-pair cable where the pairs have been reorganized to reverse the transmit and receive electrical signals.

Some routers, such as the Cisco 2505 Router, actually provide the Ethernet interface in the form of a hub (below). This negates the need for a separate hub, and PCs can be plugged directly into the hub ports available on the router. If more hub ports are required, a crossover cable can be used to connect one of the hub ports on the router to a port on an additional hub.



Serial Connections

Serial connections on the router can be configured for several different WAN protocols. The actual physical serial connection on Cisco routers is a 60-pin female port.



The Cisco 2505 Router supplies two serial ports. The serial port supports several different signaling standards, including V.35, X.21bis, and EIA-530.

)	 	 	

The figure below shows a V.35 cable that supplies the male 60-pin connector for connection to the router's serial port. The other end of the V.35 cable would typically be placed in a CSU/DSU or other device in WAN connections. The table lists some of the signaling standards supported by Cisco serial interfaces.



Standard	Specification	
V.35	Synchronous communication between networks and packet-switching WANs	
X.21 bits	Defines communication between DTEs and DCEs in an X.25 WAN	
EIA-530	RS-232 standard for unbalanced serial communications	

A Final Word on Physical Router Connections

Determining whether you should configure the router before connecting it to the serial and LAN interfaces that it will service or connect the router and then configure it is a matter of individual preference. In some situations, one might prefer to begin configuration using a directly connected PC as a terminal, then finish configuration via a telnet connection after the router is connected to the network. Others may prefer to complete the configuration using a directly connected console PC, then connect the router to the network after all of the interfaces are configured.

Connecting the various LAN and WAN devices, if possible, before you configure the router allows you to fully configure and test the connections immediately. However, if the router is placed in an area that is somewhat difficult to access (such as a small closet on a hub rack), it might be difficult to directly connect a PC to the router for configuration purposes.

BASIC ROUTER CONFIGURATION

In this section, you will learn the basic configuration steps and boot sequence of the Cisco router. Also, you will look at the system configuration dialog box. Finally, you will look at the different router modes.

The following topics will be covered in this section:

- Configuring the Router
- Working with the System Configuration Dialog Box

Configuring the Router

Setting up a basic configuration for a router is a matter of enabling the various interfaces on the router and setting the software settings for the routed and routing protocols. For example, if you are routing IP, the interfaces must be assigned appropriate IP addresses. Routing protocols must also be configured. If you are going to use RIP or IGRP, you must configure these protocols. And any serial interfaces that you use must also be configured with an appropriate WAN layer 2 protocol (such as HDLC or Frame Relay). Basic configuration information may also include bandwidth information and timing information for WAN connections.

3	 	

Bottom line, the configuration file for your router uses software settings that tell the router what to route and how to route it. All of the commands that you use to configure the router are part of the Cisco IOS command set.

Below we discuss several different ways that you can configure the router.

Router Console

Of all of the configuration methods available, probably the simplest is configuring the router by directly connecting a PC to the router console port. This not only allows you to quickly set up a basic configuration on the router using the router System Configuration dialog, but it also allows you to fine-tune your configuration in the router Configuration mode.

Virtual Terminal

If the router has already been provided a basic configuration that gets at least some of the interfaces up and running on the network (such as an Ethernet port), you can telnet to the router via a virtual terminal. This simply means that a computer on the network that is running a telnet program can connect to the router and configure the router. In order to gain access via telnet, you will need to know the router's IP address and password if any are assigned.

Network Management Workstation

Routers can also be configured from a workstation on the network that runs special network management software, such as Cisco's CiscoWorks or a similar product from Hewlett Packard known as HP OpenView.

TFTP Server

A configuration for a router can be loaded from a TFTP server on the network. Saving configurations to a TFTP server and then downloading them to a particular router is very straightforward. TFTP servers will be discussed later in this course.

Working with the System Configuration Dialog Box

When you boot up a new router (or a router where the configuration file has been deleted), the System Configuration dialog is loaded (see below). This Setup mode asks a series of questions. The answers to those questions provide a basic configuration for the router.



Working through the Setup dialog is very straightforward. You will need to know certain parameters related to the configuration of the router, such as which network protocols you will route (IP, IPX, AppleTalk, etc.) and the parameters related to the various interfaces.

1

For example, if you route IP, you will need to know the IP addresses of the router interfaces that you want to configure. The following steps provide sample addresses. If you have a router that you want to configure, follow the steps provided.

Start the Setup Dialog

The Setup dialog can ask you quite a few questions related to setting various passwords for the routers and configuring the interfaces on the router. The first part of the setup configuration relates to setting up enable and virtual terminal passwords for the router.

Start the configuration process with the Setup dialog.

- 1. You will be asked, "Would you like to enter the initial configuration dialog?" Press *ENTER* to answer yes (the default option) and continue.
- 2. You will then be asked if you want to see the current interface summary. This allows you to view the interfaces on the router. Press *ENTER* to continue. A summary of the interfaces on the router will be provided, as shown below. Note that the Ethernet 0 interface is up, but that both the serial interfaces on this router are down. Also, no IP numbers have been assigned to the interfaces.

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Would you like to enter the initial configuration dialog? [yes]:
First, would you like to see the current interface summary? [yes]:
Bay interface listed with OK? value "NO" does not have a valid configuration
Interface
                                 IP-#ddress
                                                         OK? Method Status
                                                                                                         Protocol
                                                         NO
NO
                                 unassigned
Ethernet8
                                                              unset up
unset down
                                                                                                          up
down
Seria18
                                 unassigned
 Seriali
                                 unassigned
                                                         NO
                                                               unset
                                                                         dous
                                                                                                          down
 Configuring global parameters:
   Enter host name [Router];
```

- 3. Next, you are asked to provide a name for the router. Type a name (such as ciscokid) and then press *ENTER*.
- 4. The next Setup dialog question asks you to provide an enable secret password. This password is encrypted and will provide you with access to the router's Privileged Exec or Enable mode (the mode that allows you to make changes to the router's configuration). Type an appropriate password and then press *ENTER*.

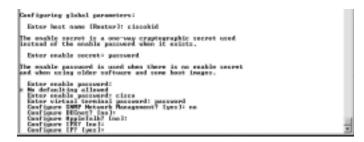
- 5. You are then asked to provide an enable password. This may seem redundant because you have already provided a secret password for the Enable mode. This second password is related to earlier versions of the Cisco IOS that didn't provide the capability to create an encrypted password for the Enable mode. Because you aren't allowed to leave this password blank (even though you won't use it), type a value (something you can remember but isn't apparent to someone trying to access the router who shouldn't). In this case, we will use "password." Press *ENTER* to continue.
- 6. You will then be asked to provide a virtual terminal password for the router. This password is used by virtual terminals that telnet to the router over the network. This enables you to monitor (and even configure a router) from a remote workstation on the network. Provide a virtual terminal password and press *ENTER* to continue.
- 7. The next Setup dialog question asks you if you want to enable SNMP (Simple Network Management Protocol). This protocol provides baselines for network operations and provides a method for monitoring changes in the network using a management station (which requires software such as CiscoWorks). If you don't use management software to manage the routers, there is no reason to enable SNMP. In this case, you won't enable it. Type "no" at the prompt and press *ENTER* to continue.

Configure Routed Protocols

The next portion of the Setup dialog is related to the configuration of routing protocols that will be used on the router. You will be asked if you want to enable each of the routed protocols supported by your version of the IOS and to choose which routing protocols you want to enable.

Configure protocols with the Setup dialog.

- 1. In the case of the 2505 router we are using in our example, the next prompt asks if DECnet should be enabled. DECnet is a protocol stack supported by the Digital Equipment Corporation. The default response is No. Press *ENTER* to continue.
- 2. In the case of our 2505 router, the next dialog prompt asks if AppleTalk should be configured. For now, you will respond with no (the default). You will learn more about Routing AppleTalk, later in this course, covering the ins and outs of AppleTalk routing. Press *ENTER* to continue.
- 3. The next dialog prompt asks if IPX should be configured. IPX is also covered in this course. To answer no, press *ENTER*.
- 4. The next prompt asks if IP should be configured, and the default answer is yes. This enables you to get the router up and running on the network, and then you can further configure the router using a virtual terminal or by loading a ready-made configuration file from Cisco ConfigMaker or a TFTP server. Press *ENTER* to answer yes and continue.



- 5. You will then be asked if you want to configure IGRP on the router. IGRP is one of the IP routing protocols. Configuring IGRP and RIP will be covered later in this course, so for the moment you can say no. Type "no" and press *ENTER* to continue.
- 6. You will then be asked to configure RIP. No is the default, so press *ENTER* to continue.
- 7. The next dialog asks if bridging should be enabled on the router. No is the default. Press *ENTER* to answer no and continue.

Configure Router Interfaces

The next part of the Setup dialog is related to the configuration of the router's interfaces. You will be asked which router interfaces will be in use on the router (such as Ethernet and serial interfaces). Also, because IP was enabled for routing, you will have to supply IP addresses for the various interfaces on the router. How these IP addresses were arrived at will be discussed in another chapter in this course.

Configure interfaces with the Setup dialog.

- 1. The next prompt relates to the first interface on the router, which in the case of the 2505 router in this example is the Ethernet 0 interface. You will be asked if this interface is in use. Yes is the default value, so to enable the interface, press *ENTER*.
- 2. The next prompt asks if IP should be configured on the interface (E0). The default value is Yes; press *ENTER* to continue.
- 3. The next prompt asks for the IP address of the interface (interfaces on the router use IP addresses just like any other node on the network). Type "10.16.1.1" as the address for the E0 interface. Then press *ENTER* to continue.

Casfiguring interface parameters:	
Configuring interface Ethernet@: In this interface in usef (gen):	
Casfigure IP on this interface? Iges 1: IP address for this interface? S0.16.1.1	Ξ

- 4. The next prompt asks how many bits are in the subnet field. This number relates to how many IP subnets have been created for your internetwork. For our purposes, we have divided the available network addresses (which are class A addresses) into 14 subnets, which requires 4 bits in the subnet field. Type "4" and press *ENTER*.
- 5. Because the 2505 router's E0 interface is actually an eight-port hub, you are asked if you want to enable all ports on the hub. The default is Yes, so press *ENTER* to continue.
- 6. You are then asked if you want to configure the next interface on the router, which in this case is serial 0. Yes is the default. Press *ENTER* to continue.



- 7. You are then asked if you want to configure IP on the S0 interface. Press *ENTER* and continue.
- 8. You are given the option of configuring the S0 interface as IP unnumbered (this means that the interface will route IP but doesn't require its own IP number). This is done to actually save your IP addresses (from the pool of IP addresses that you have available). Configuring serial interfaces with IP addresses will be handled in more detail later in this course. For now, press *ENTER* to say no.
- 9. You are then asked to provide an IP address for the S0 interface. Type "10.32.1.1". Then press *ENTER*.
- 10. You will then be asked to provide the subnet field bits. This is defaulted to 4, which was entered in step 4. Press *ENTER* to use the same bit count.
- 11. You are now asked to configure the Serial 1 interface. Press *ENTER* to say yes.
- 12. Press *ENTER* to say no to IP unnumbered.
- 13. Type the IP address "10.48.1.1" at the prompt. Then press *ENTER*.

Configuring interface parameters:	
Configuring introduce Ethernetit: Is this introduce in one? Ignol: Configure IF on this interface? Ignol: If address for this interface? Ignol: Mandawar of hits is underful 201: 4 Charm & article is underful 201: 4 Charm & article is underful interface? Upul: Enable all had parts on this interface? Upul:	
Casfiguring interface SerialBi In this interface in use? [sen]: Casfigure IF on this interface? [sen]: Casfigure IF uneashered as this interface? Use]: IF address for this interface; 18, 22.1.1 Randow of him is interface? [sel] 41: Close B actuarts in 10.8.8.4.4 saket bits; much is /12	
Canfiguring interface Serial: Is this interface is one? Ignel: Canfigure IF on this interface? [yes]: Canfigure IF uncanbered on this interface? Evol: IF address for this interface? 18.43.1.	

- 14. The next prompt is where you enter the subnet bits (4 is supplied as the default number of subnet bits). Then press *ENTER*.
- 15. After you press *ENTER*, the screen will scroll rapidly, showing link tests for the interfaces that you have configured. You will be asked if you want to use the current configuration. Type "yes" and then press *ENTER* to save the configuration file that you created using the System dialog. The router will build the configuration file and save it to NVRAM.
- 16. The next time you press *ENTER*, the router will take you to the router's User mode prompt. You are now ready to view the configuration parameters on the router or edit the configuration of the router.

SAVING A CONFIGURATION

When you configure the various interface and protocol parameters for a router, this information is stored in the router's RAM. It's important that you store this information somewhere in case the router loses power. In the Privileged mode, you can save your running configuration to NVRAM where it becomes the router's startup configuration and is loaded if the router is rebooted.

The Privileged mode also allows you to examine the contents of RAM and NVRAM using the **show** commands. These commands aren't available in the User mode.

View the Running Configuration

- 1. At the User prompt, type "enable" and then press *ENTER* (if you aren't in the Privileged mode).
- 2. Type the Privileged mode password and press *ENTER*. You are now in the Privileged mode.



- 3. Type "show running-config" and then press *ENTER* to execute the command. The command results will appear on the router.
 - Der Brannen (1994) The [28] Song Capton (2)view (54) Inserfece Etherport Ip address 130.10.04.11 255.255.255.214.0 Interfece Eterial Ip address 130.10.22.1 255.255.214.0 Interfece Eterial Castorial Interfece Interfece Terial description Comments CincelS85.1 description Comments researching S. 8.8.0 restars is 8.8.8.0 restars is 8.8.0 restars is 8.8.0
- 4. To advance through the information on the screen, press *SPACEBAR* for an entire screen or *ENTER* to advance line by line.

The running configuration provides information on how the different interfaces are currently configured and which routing protocols have been enabled. It also shows the passwords that have been set on the router. However, remember that the Privileged mode secret password is encrypted, so you can't tell what it is.

The **running-config** command provides a complete picture of the parameters running on the router, and this is why it is a Privileged mode command; its information is important to the router's administrator, so it should be protected.

As you fine-tune your running configuration, a time will come when you will want to save it to NVRAM as the startup configuration. The great thing about the **copy** command is that you can copy information from RAM to NVRAM (running to startup). Or if you mess up your running configuration, you can copy information from NVRAM to RAM (startup to running). The command you use to copy information from one type of memory to another is **copy**.

Copy the Running Configuration

- 1. In Privileged mode, type "copy running-config startup-config".
- 2. Press *ENTER* to execute the command.

The router will pause for a moment. Building configuration will be displayed on the screen. Then "[OK]" will appear. The running configuration has been copied to the startup configuration.

You can quickly check your new startup configuration with the ' command. The output will be similar to the running-config shown in the previous figure. The results of this command also show you how much NVRAM is being used on the system to store the configuration file.

Another memory type on the router is Flash RAM. This is where the router's IOS is stored. You can view the contents of Flash in both the User and Privileged mode.

LOADING A CONFIGURATION

When you load a configuration, you are copying a previously written configuration file into RAM. Once the configuration file is in RAM, it becomes the running configuration on your router.

Loading a configuration is basically the same as saving a configuration, except instead of copying the file to storage, you are copying it into memory. You can either load a configuration from NVRAM or from a TFTP server. To load a configuration from NVRAM or a TFTP server into the running configuration in RAM, use the **copy** command. The parameters are **copy {tftp | startup-config} running config**. Remember that if two commands are in brackets, you must choose one of the available options. You must specify the file to copy before you specify its destination.

A A	Zj

INTERFACES

In this section, you will look at router interfaces. An interface supplies the physical connection between the router and a particular network media type.

Cisco interfaces are often referred to as ports. Each port is physically designed to support the appropriate LAN, WAN, or console interface.

For example, a LAN interface, such as an Ethernet port on the router, will consist of a female RJ-45 connector that is connected to an Ethernet hub using a twisted-pair cable with male RJ-45 connectors on either end.

The following interfaces will be discussed:

- Router Interfaces
- Lan Interfaces
- Serial Interfaces
- Logical Interfaces

Router Interfaces

Built-in ports are designated by their connection type followed by a number. For example, the first Ethernet port on a router would be designated as E0. The second Ethernet port would be E1, and so on. In some cases, the Ethernet port will be set up as a hub, such as on the 2505 router. Serial ports are designated in a similar manner, with the first serial port being S0.

The figure shows two serial ports and their numeric designation on a Cisco 2505 Router and the Ethernet 0 hub ports (1 through 8).



Cisco routers, such as those in the 2500 Series family, are off-the-shelf routers that come with a predetermined number of LAN, WAN, and serial ports. Higher-end routers like the Cisco 4500 are modular and actually contain empty slots that can be filled with several different interface cards.

Not only are different interface cards available (such as LAN versus WAN), but the number of ports on the card can also be selected. For example, one of the three empty slots on the 4500 router can be filled with an Ethernet card that contains six Ethernet ports.

A

The Cisco ConfigMaker hardware configuration screen for the Cisco 4500 Router is shown below. Three slots are available (shown on the right of the screen) and can be filled with several different cards (listed on the left of the screen).

Cince 4500 Wizard - HW Configuration To Add: Drag the Network interface on To Remove: Select the Network interface of	rd into an empty slot.
Network Interface Cards C 2 Ethernet C 2 Ethernet C 3 Ethernet C 4 Serial C 4 Serial C 5 Ethernet C 5 Ether	Configuration:
< Back Me	d) Cancel Help

Modular routers (like the 4500) designate their ports by connection type, followed by slot number, followed by port number. For example, the first Ethernet port on an Ethernet card placed in the router's first slot would be designated as Ethernet 1/0 (the slot is designated first, followed by the port number).

Viewing the interfaces (and their status) on a particular router is handled by the **show interfaces** command. The results of the **show interfaces** command on a 2505 router that has one Ethernet port (E0) and two serial ports (S0 and S1) are shown below. The status of the various ports is related to whether the ports have been connected physically to the internetwork and whether they have been configured.



Configuring a particular interface depends on the type of network protocol used by the network the interface port is connected to. For example, an Ethernet port connected to an IP network will be configured for the routing of IP.

AL R	

LAN Interfaces

Cisco routers support several common LAN interfaces. The most common LAN router interfaces are Ethernet, Fast Ethernet, IBM Token Ring, and Fiber Distributed Data Interface (FDDI).

All of these LAN protocols utilize the same Data Link layer addressing system (i.e., the MAC hardware address on a NIC or the MAC hardware address found on the controller of the router interface). These addresses are unique for each device, regardless of LAN interface.

Serial Interfaces

Serial router interfaces provide a way to connect LANs using WAN technologies. WAN protocols move data across asynchronous and synchronous serial interfaces (on routers), which are connected via leased lines and other third-party telecommunications technologies.

Logical Interfaces

Before we conclude our discussion of router interfaces, we must take a look at logical interfaces. A logical interface is a software-only interface and is created using the router's IOS.

Logical interfaces don't exist as actual hardware interfaces on the router. You can think of logical interfaces as virtual interfaces that have been created with a series of router software commands.

These virtual interfaces can be viewed by devices on the network as real interfaces, just as a hardware interface such as a serial port is a physical interface. You can configure different types of logical interfaces on a router, including Loopback interfaces, Null interfaces, and Tunnel interfaces.

Loopback Interfaces

A Loopback interface is a software-only interface that emulates an actual physical interface on the router. Loopbacks are typically configured on a high-end router that serves as the core router between two corporate internetworks or between a corporate network and the Internet. Routers serving as core routers will be configured with an exterior gateway protocol, such as Border Gateway Protocol, that routes the packets between two separate and autonomous internetworks.

Because the router serves such an important link between internetworks, you don't want it dumping data packets if a particular physical interface on the router goes down. So the Loopback virtual interface is created and configured as the termination address for the Border Gateway Protocol (BGP) sessions. In this way, the traffic is processed locally on the router, which assures that the packets get to their final destination.

Null Interfaces

Another logical interface is the Null interface. It is set up on a router using the appropriate router commands and serves as a virtual wall that can be used to keep out certain traffic. For example, if you don't want traffic from a particular network to move through a particular router, you can configure the Null interface so that it receives and dumps any packets that the network sends to the router. Normally Access lists are used to filter traffic on an internetwork and define valid routes for certain networks. The Null interface is pretty much a sledgehammer approach to a process that is normally handled with jeweler's tools.

Tunnel Interfaces

A Tunnel interface is another logical interface that can be used to move packets of a particular type over a connection that doesn't typically support these types of packets. For example, a Tunnel interface can be set up on each of two routers that are responsible for routing AppleTalk packets from their LANs. These two routers are connected by a serial connection. The Tunnel interface can be configured to route IP. And although AppleTalk would not be typically routed over an IP interface, the AppleTalk packets are encapsulated (stuffed in a generic envelope) and then moved across the Tunnel as if they were IP packets. Cisco routers provide the Generic Route Encapsulation (GRE) Protocol, which handles the encapsulation of packets moved over a Tunnel interface.

PORT CONFIGURATION

Individual ports are configured in interface configuration. For the purposes of this section, we will confine our discussion to how to enter the different interface configuration modes and some of the basic commands needed to activate them.

The first step in configuring a port is entering configuration mode with the **configure terminal** (**config t**) command. Interface configuration mode can only be accessed from global configuration mode.

The next step in configuring interfaces is selecting the port you wish to configure. In this example, we will configure the IP address for the Ethernet zero port. The command **interface ethernet 0**, as with most Cisco commands, can be abbreviated. Interface tells the router to enter into interface configuration mode, while Ethernet 0 specifies the interface to configure.

Another important component on the LAN interface is the Network layer address. Examples of Network layer protocol addresses you might configure are IP, IPX, AppleTalk, and DECnet. In the example below, the command **ip address** *ip-address subnetmask* is used to configure the IP address on interfaces.

The final command, **no shutdown**, is used to activate the interface. Cisco routers ship with the ports shut down by default. Once the port is configured with an address, you must inform the router that the port is no longer in a state of shutdown.

One of the first ports commonly configured on a router is the LAN interface. By configuring the LAN interface first, you can simplify troubleshooting if you have difficulties configuring the other ports. Once the LAN port is enabled, it also opens the option of using telnet to remotely complete configuration of the remaining ports, such as WAN or additional LAN ports.

```
RouterC#config t
RouterC(config)#int e0
RouterC(config-if)#ip address 208.212.225.15 255.255.255.0
RouterC(config-if)#no shutdown
```

NETWORK CONFIGURATION

A router must be configured correctly in order to become part of the network. You should spend some time investigating the network that the router is joining. Make sure that in addition to the IP addresses the router will use, you obtain a list of the routing protocols, default gateways in use on the network, and the subnet mask of the network segment the router will serve. The more information you have about the router's environment, the easier it will be to troubleshoot any configuration problems you may encounter.

Once the router interfaces are configured with Network layer addresses, the router is ready to become part of the network. This is accomplished by ensuring that the router can connect to the rest of the network. If you are using static routes, you must configure the router to forward all data to a specific gateway. The gateway then becomes responsible for distributing network traffic to its destination.

Use the **ip route 0.0.0 0.0.0** *gateway-address* command to set up static routes. This command tells the router that all IP traffic from any (first 0.0.0.0 octet) bound for any destination (second 0.0.0.0 octet) address is to be sent to the gateway address. In this type of configuration, there is no routing taking place; all traffic is sent to the same address for further distribution across the internetwork.

If you are using RIP, IGRP, OSPF, or other IP routing protocols, and you configured the protocols without using the setup command, you must enable IP routing using the **ip routing** command. This global configuration command starts the IP routing process on the router.

RouterC(config) #ip routing

If you are using IPX RIP, IPX SAP, or NLSP, you must enable IPX routing once the interface is configured. The command **ipx router** enables IPX routing on Cisco routers. As with **ip routing**, **ipx router** is a global configuration command.

Ź	 	 		

RouterC(config)#ipx routing

SUMMARY

In this chapter, you learned about the following:

- The basic design and configuration of the Cisco router
- How to save, upgrade, and load a backup Cisco IOS software image
- How to use the TFTP server for router configuration storage
- Some of the basic router troubleshooting methods



Stop now and complete the following NEXTSim exercises on the Interactive Learning CD-ROM:

Understanding IOS

Configure HyperTerminal for Console Access

Network Protocols

Use the Setup Mode to Configure the Router

POST-TEST QUESTIONS

The answers to these questions are in Appendix A at the end of this manual.



 Which show ______ config command generates the following first line? Using 1,312 out of 32,762 bytes

.....

.....

2. A _______ is used to copy configuration files to and from a router.

3. Which command is used to enable routing of the IPX protocol? IP protocol?

.....

.....

4. It is best to configure the router port that will be connected to the _____ first.

.....

.....

- 5. Router ports are not shut down prior to initial configuration.
 - A. True
 - B. False

_ ^

- 6. Which command would enable interface configuration mode?
 - A. Router1#int ser 0
 - B. Router1(config)>int lan 0
 - C. Router1(config)#int ser 0
 - D. Router1(config-if)#int ser 0

)			

Network Management

CHAPTE

5

R

MAJOR TOPICS

►

Objectives 118	}
Pre-Test Questions118	}
Introduction119)
Managing the Configuration)
Backup and Restore122	?
Monitoring Network Traffic136	;
Access Lists and vty Control138	}
Extended Access lists145	5
Summary	3
Post-Test Questions	3

OBJECTIVES

At the completion of this chapter, you will be able to:

- Back up and restore configuration files. •
- Back up and restore the IOS file. •
- Define the basics of network management.
- Configure standard and extended access lists.

C . 1

PRE-TEST QUESTIONS

The answers to these questions are in Appendix A at the end of this manual. TOC



1.	why is a backup of the Cisco IOS recommended?
2.	What type of server is used to back up and restore Cisco files?
0	

3. If a server version of the IOS fails, can the IOS be restored?

1 10

....

....

. . . .

....

- 4. Configuration files stored on a TFTP server are secured using password authentication.
 - True Α.
 - B. False
- 5. What will be the result of the ACE command access-list 101 10.10.2.0 0.0.0.255 10.20.1.1?

.....

INTRODUCTION

The overall configuration of Cisco products consists of many interconnected components. The Internetwork Operating System version will dictate what functionality and command structure you must use when configuring router options.

The configuration files dictate how the individual components will operate as well as what features are enabled from the myriad of available protocols and routing options. The configuration registry controls how the router hardware will operate, along with boot options that take priority over any software configuration options.

It is essential to understand how these individual components interoperate to allow routers to move information across many interconnected systems. Once configured properly, these operations are transparent to end users. Administrators must manage each of the individual components correctly to ensure optimal operation of internetwork traffic flow. This chapter will explore how to manage each of these components and how they interoperate to make operation of routers possible.



Stop now and view the following video presentation on the Interactive Learning CD-ROM:

Router Configuration Basics Router Configuration File Management Upgrading Router IOS Image Router Boot Options and Password Recovery Router Configuration Register

	>
(FTK	1
J-X-C	

MANAGING THE CONFIGURATION

Managing the configuration of a router involves understanding how each of the router components interact with each other. This involves configuring each hardware component, taking into account how this will affect all other components.

The following topics will be discussed in this section:

- Configuration Registry
- Boot Options

Configuration Registry

The configuration registry is a 16-bit software registry stored in NVRAM. The least significant 4 bits form the boot field. The boot field controls various boot options on Cisco routers, such as forcing the system into the bootstrap monitor, specifying a boot source and default filename, loading operating system software from ROM, enabling booting from a TFTP server, and controlling broadcast addresses. To view the current configuration registry settings, use the **show version** command.

Boot Options

The boot field of the configuration registry can be configured to instruct the router to boot from ROM. The configuration registry setting to boot from ROM is 0x2101, using the configuration files found in NVRAM. Once you have upgraded the IOS, you must reset the configuration registry to tell the router to boot from Flash. The configuration registry setting to boot from Flash using the configuration files in NVRAM is 0x2102.

Editing the Confirmation Registry

To edit the configuration registry, use the **config-register** *parameter* global configuration command.

```
Router1(config)#config-regis 0x2101
Router1(config)#^Z
Router1x
%SYS-5-CONFIG_I: Configured from console by steven on console
Router1#show version
Configuration register is 0x42 (will be 0x2101 at next reload)
This command tells the router to boot from the IOS in ROM and use the
   configuration files in NVRAM. This setting is commonly used to
   upgrade the IOS.
```

Returning Registry to Original Settings

After the IOS upgrade, it is recommended to set the configuration registry back to the original settings.

```
Router1(config)#config-regis 0x4202
Router1(config)#^Z
Router1#
%SYS-5-CONFIG_I: Configured from console by steven on console
Router1#
```


BACKUP AND RESTORE

When planning for disaster recovery, it is recommended that you back up data and configuration files for mainframes, network servers, and workstations. It is not often mentioned that you should also keep backup copies of router files.

The following topics will be covered in this section:

- Backing Up Configuration Files to a TFTP Server
- Restoring Configuration Files from a TFTP Server
- Back Up and Upgrade the Cisco IOS Using tftp

Backing Up Configuration Files to a TFTP Server

The easiest way to back up configuration files is through the use of a TFTP server. We have covered copying configuration files thoroughly in this book. Once they are stored on a TFTP server, they can be added to routine network backup cycles. If the TFTP server crashes, you will lose your images if they are not backed up during regular network backups.

copy running-config tftp

The **copy running-config tftp** command is used to place a backup of the currently running configuration file in RAM on a network server.

```
RouterC#copy running-config tftp
Address or name of remote host []? 208.212.225.63
Destination filename [running-config]?
!!
1145 bytes copied in 6.380 secs (190 bytes/sec)
RouterC#
```

copy startup-config tftp

The **copy startup-config tftp** command is used to place a backup of the configuration file stored in NVRAM on a network TFTP server.

```
RouterC#copy startup-config tftp
Address or name of remote host []? 208.212.225.63
Destination filename [startup-config]?
!!
1145 bytes copied in 0.236 secs
```

Restoring Configuration Files from a TFTP Server

If a configuration file becomes corrupt, or configuration changes cause the router to malfunction, a backup can be restored. Files can only be restored if they were previously copied to a TFTP server.

)	 	 	

copy tftp startup-config

The **copy tftp startup-config** command is used to load a configuration file from a network TFTP server.

```
RouterC#copy tftp startup-config
Address or name of remote host []? 208.212.225.63
Source filename []? startup-config
Destination filename [startup-config]?
Accessing tftp://208.212.225.63/startup-config...
Loading startup-config from 208.212.225.63 (via Ethernet0): !
[OK - 1145/2048 bytes]
```

1145 bytes copied in 10.844 secs (114 bytes/sec)

copy tftp running-config

The **copy tftp running-config** command is used to load a configuration from a network TFTP server to the configuration currently running in RAM.

```
RouterC#copy tftp running-config
Address or name of remote host [208.212.225.63]?
Source filename [startup-config]? running-config
Destination filename [running-config]?
Accessing tftp://208.212.225.63/running-config...
Loading running-config from 208.212.225.63 (via Ethernet0): !
[OK - 1145/2048 bytes]
```

1145 bytes copied in 5.528 secs (229 bytes/sec)

Back Up and Upgrade the Cisco IOS Using tftp

This section will show the steps involved in backing up and upgrading the IOS on Cisco routers. Before the IOS is upgraded, the existing IOS should be backed up to a TFTP server. This makes it possible to restore the previous IOS file if there are problems with the upgrade. All configuration files should have been backed up before the upgrade is done.

Back Up the IOS Using tftp

The Internetwork Operating System is a file stored in Flash memory on the router. To back up the IOS file, you copy it to a TFTP server using a simple four-step process:

1. Use the **show flash** command to get the name of the IOS file.

```
System flash directory:

File Length Name/status

1 6788464 c2500-d-l_120-4.bin

[6788528 bytes used, 1600080 available, 8388608 total]

8192K bytes of processor board System flash (Read ONLY)
```

2. Write down the name of the IOS file, in this case, c2500-d-l_120-4.bin.

)	 	 	

3. Make sure the TFTP server is up, using the **ping** command.

```
RouterC#ping 208.212.225.63
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 208.212.225.63, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/2/4 ms
```

4. Use the command **copy flash tftp** to initiate the dialog. After answering the onscreen prompts, the copy operation will begin.

Upgrade the IOS

While you cannot add to the existing IOS of a Cisco router, you can add functionality by replacing the entire IOS file with a new file that enables the options you desire.

Routers come with different levels of software support for protocols. If you purchase a router that does not come with the functionality you desire, you must obtain the IOS Feature Pack that contains the functionality you desire and replace the entire IOS file with the new file. A feature pack is a product you purchase from your vendor at the time of purchase or at the time you need to expand the capabilities of your router.

Some routers also require an IOS upgrade to support virtual private networking.

Upgrading the IOS is a six-step process:

1. Using **show version**, write down the current configuration registry settings. In the example shown below, the current configuration registry is set to 0x2102. This is the most common configuration registry setting for Cisco 2500 series routers.

```
Success rate is 100 percent (5/5), round-trip min/avg/max =
 1/2/4 ms
RouterC#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(4), RELEASE
 SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 14-Apr-99 21:21 by ccai
Image text-base: 0x03037C88, data-base: 0x00001000
```

ROM: System Bootstrap, Version 11.0(10c), SOFTWARE BOOTFLASH: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c), RELEASE SOFTWARE (fc1)

```
RouterC uptime is 1 hour, 40 minutes
System restarted by power-on
System image file is "flash:c2500-d-1_120-4.bin"
```

)	 	 	

```
cisco 2500 (68030) processor (revision N) with 14336K/2048K bytes
of memory.
Processor board ID 11157008, with hardware revision 00000001
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)
```

Configuration register is 0x2102

2. The second step in upgrading the IOS is to change the configuration registry to allow the router to boot using the IOS in ROM. This is necessary because an IOS in use cannot be erased. The configuration files in NVRAM should be used to allow the router to boot with network connectivity. Use the setting 0x2101 to accomplish this boot process. The "2" instructs the router to use the configuration files in NVRAM. If you wanted to boot from ROM with no configuration files, use the configuration registry setting 0x101.

```
RouterC#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterC(config)#config-register 0x2101
RouterC(config)#^Z
RouterC#
```

Verify the configuration registry changes using the **show version** command. If the command was entered correctly, the last line of the show version display should be identical to the last line in the example below.

RouterC#show version

Text has been removed.

Configuration register is 0x2102 (will be 0x2101 at next reload)

3. Use the **show flash** command to show the name of the IOS file and size. Use the **copy flash tftp** command to back up the IOS. It is a good idea to rename the file to fileneme-backup.bin in case a restore is necessary. Notice the shortcut below: if a known filename is to be copied, the filename can be entered instead of flash. This will save time answering the dialog.

```
RouterC#show flash
System flash directory:
File Length Name/status
    6788464 c2500-d-l 120-4.bin
 1
[6788528 bytes used, 1600080 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
RouterC#copy c2500-d-1_120-4.bin tftp
Address or name of remote host []? 208.212.225.63
Destination filename [c2500-d-l 120-4.bin]?
 c2500-d-1 120-4backup.bin
111111111111111111
11111111111111111
......
6788464 bytes copied in 115.632 secs (59030 bytes/sec)
RouterC#
```



4. After obtaining the correct filename and ensuring the file is on the TFTP server, it is time to reboot the router and initiate the upgrade. The process of upgrading a router involves erasing the current IOS and replacing it with the new version of the IOS. The **copy tftp flash** command is used to copy the new IOS onto the router. The router should reboot, and a new prompt is displayed. The prompt should include the router name followed by the word "boot" if the router has been booted from the IOS in ROM. Since the startup configuration in NVRAM was specified, the passwords should be the same as before the reboot.

```
RouterC#reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload? [confirm]
01:57:51: %SYS-5-RELOAD: Reload requested
System Bootstrap, Version 11.0(10c), SOFTWARE
RouterC(boot)>en
Password:
RouterC(boot)#copy tftp flash
System flash directory:
File Length
           Name/status
 1
     6788464 c2500-d-l 120-4.bin
[6788528 bytes used, 1600080 available, 8388608 total]
Address or name of remote host [255.255.255.255]? 208.212.225.63
Source file name? c2500-d-l 14-120-4.bin
Destination file name [c2500-d-l_14-120-4.bin]?
 c2500-d-l 120-4.bin
Accessing file 'c2500-d-l_14-120-4.bin' on 208.212.225.63...
Loading c2500-d-1_14-120-4.bin from 208.212.225.63 (via
 Ethernet0): ! [OK]
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'c2500-d-l 14-120-4.bin' from server
 as 'c2500-d-l_120-4.bin' into Flash WITH erase? [yes/no]y
Loading c2500-d-l 14-120-4.bin from 208.212.225.63 (via
 Ethernet0): !!!!!!!!!!!
[OK - 6788464/8388608 bytes]
```

```
Verifying checksum... OK (0xEE19)
Flash copy took 0:03:25 [hh:mm:ss]
RouterC(boot)#
```

5. After the file copy, it is necessary to reset the configuration registry to its original settings using the **config-registry** command. After changing the configuration registry, use the **show version** command to ensure the configuration registry settings will be correct at next reboot.

```
RouterC(boot)#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterC(boot)(config)#config-register 0x2102
RouterC(boot)(config)#exit
RouterC(boot)#show
0:11:39: %SYS-5-CONFIG_I: Configured from console by
 consoleversion
Cisco Internetwork Operating System Software
IOS (tm) 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c),
  RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Fri 27-Dec-96 17:33 by loreilly
Image text-base: 0x01010000, data-base: 0x00001000
ROM: System Bootstrap, Version 11.0(10c), SOFTWARE
RouterC uptime is 11 minutes
System restarted by reload
```

Running default software

A


```
cisco 2500 (68030) processor (revision N) with 14336K/2048K bytes
of memory.
Processor board ID 11157008, with hardware revision 00000001
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
Basic Rate ISDN software, Version 1.0.
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
1 ISDN Basic Rate interface.
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
```

Configuration register is 0x2101 (will be 0x2102 at next reload)

6. The final step in upgrading the IOS is to reboot the router and verify the router is still operating correctly. A good way to ensure the router is operating correctly is to ping several neighbors. A good way to ensure proper operation is to use the **trace** command to a site on the Internet. After the trace route operation, use **show ip route** to the same site using the IP address. If the router is operating correctly, it will return the port the router is using to send the traffic to and how the route was learned. If these steps are successful, the router is operating correctly and the IOS upgrade was successful. If these steps are not successful, start troubleshooting the configuration fields to ensure that they match the original configuration.

```
RouterC(boot)#reload

System configuration has been modified. Save? [yes/no]: n

Proceed with reload? [confirm]

0:13:37: %SYS-5-RELOAD: Reload requested

System Bootstrap, Version 11.0(10c), SOFTWARE

Copyright (c) 1986-1996 by cisco Systems

2500 processor with 14336 Kbytes of main memory
```

<pre>%SYS-4-CONFIG_NEWER: Configurations from version 12.0 may not be correctly understood.</pre>
F3: 6700084+88348+451572 at 0x3000060
Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive San Jose, California 95134-1706
Cisco Internetwork Operating System Software IOS (tm) 2500 Software (C2500-D-L), Version 12.0(4), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 14-Apr-99 21:21 by ccai
Image text-base: 0x03037C88, data-base: 0x00001000
cisco 2500 (68030) processor (revision N) with 14336K/2048K bytes of memory.
Processor board ID 11157008, with hardware revision 00000001
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
1 ISDN Basic Rate interface(s)

```
32K bytes of non-volatile configuration memory.
 8192K bytes of processor board System flash (Read ONLY)
Press RETURN to get started!
00:00:27: %LINK-3-UPDOWN: Interface BRIO, changed state to up
00:00:27: %LINK-3-UPDOWN: Interface Ethernet0, changed state to up
00:00:28: %LINK-3-UPDOWN: Interface SerialO, changed state to down
00:00:28: %LINK-3-UPDOWN: Interface Serial1, changed state to up
00:00:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRIO,
  changed state to down
00:00:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface EthernetO.
  changed state to up
00:00:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface SerialO,
  changed state to down
00:00:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1,
  changed state to up
00:00:31: %LINK-5-CHANGED: Interface BRIO, changed state to
  administratively down
00:00:32: %LINK-5-CHANGED: Interface SerialO, changed state to
  administratively down
00:00:32: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1,
  changed state to down
00:00:32: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRIO:2,
  changed state to down
00:00:33: %SYS-5-CONFIG_I: Configured from memory by console
00:00:33: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(4), RELEASE
  SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 14-Apr-99 21:21 by ccai
RouterC>
The router prompt should return to normal after the reboot.
```

RouterC#ping www.microsoft.com
Translating "www.microsoft.com"...domain server (255.255.255.255)
[OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 207.46.131.30, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5)
RouterC#ping 208.212.224.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 208.212.224.1, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

	-

MONITORING NETWORK TRAFFIC

Network traffic can be displayed using several Debug commands. Debug commands tell the router to display network information on the screen. This information can be used to detect common router problems. This process uses a large amount of system resources and should be used with care.

The following topics are covered in this section:

- Common Monitoring Options
- Debugging
- Network Security and Session Monitoring

Common Monitoring Options

You can monitor common router operations using the **debug** Privileged Exec command. A list of the many available debug options can be obtained by typing "debug ?". The **debug** command is used to display router operations on the console or virtual terminal screens.

Debugging

If a router is not operating correctly and the configuration files have been checked, it is possible to monitor individual components to verify that they are operating properly. Common problems include incorrect modem settings. If a modem attached to a dial-in access server does not operate correctly or loses its settings when the power is reset, the router configuration files can be set up to force the initialization string into NVRAM on the modem each time the port attached to the modem is reset. This is a common problem when troubleshooting Cisco 2509 and 2511 access servers. It is important to note that each debugging operation requires additional processor and memory overhead. Debugging options should be turned off once the problem is identified and corrected.

Enabling

Use the **debug {option}** command to turn debugging on. This command is executed from the Privileged Exec command prompt.

Disabling

To disable debugging operations, run the command **no debug {options}**. The screen might be scrolling with debug options. Ignore these and type the command. The router will accept the command even if it does not appear at a single command prompt. If the router does not accept the command, try retyping it. This is a little confusing, but it is something that cannot be changed.

Network Security and Session Monitoring

It is possible to monitor active telnet sessions on the router. This is useful to monitor what a user is doing during a telnet session with the router. If a user is attached and entering commands, the session can be disconnected. If a user from a particular IP address is continually accessing the router, the address can be blocked using network security options. Commonly used network security methods include using an access list to filter who can and cannot access the router based on IP address. By requiring an individual username and password for each user allowed to access the router, network security can be further increased. Individual username and password security was discussed in earlier chapters of this book.

$ \rightarrow $		 	

ACCESS LISTS AND VTY CONTROL

The Cisco IOS provides security functionality with the use of Access Control Lists (ACLs) to permit or deny traffic across a specific interface. ACLs are created using sequential permit or deny conditions. The IOS examines each of the Access Control Entries (ACEs) against addresses and once a match is made, the software ends the process. Because of the sequential nature of this process, the order of ACEs in the access list is extremely important. This section will examine the process of configuring a standard access list and discuss how an access list can be used to control virtual terminal line access.

The following topics will be covered in this section:

- Standard Access List Configuration
- Controlling vty Access

Standard Access List Configuration

Standard access lists differ from extended access lists in that standard access lists can only be used to filter traffic via the source IP address. Source IP addresses are compared to a wilcard mask. A wildcard mask defines the subset of the 32 bits in an IP address that must be matched.

Wilcard Masks

The CCNA exam will require you to understand how a wildcard match is used to define the subset of an IP address in access lists. Matching is performed by the IOS by comparing the wildcard mask against the packet's source IP address. Mask bits of the binary value 1 (decimal 255) are considered wildcards, allowing the corresponding bit positions in the source IP address to be any number. Mask bits of the binary value 0 require that the same bit positions in the source IP address are matched. The following table explains the process.

Access List IP Address	Access List IP Binary Equation	Source IP Address	Source IP Binary Equation	Access List Wildcard Mask	Result
1.10.88.4	0000 0001 0000 1010 0101 1000 0000 0100	1.10.88.111	0000 0001 0000 1010 0000 0000 0110 1111	0.0.0.0	The wildcard mask of 0.0.0.0 requires that all bits match. The last octet of 111 does not match 4. The packet will be dropped.
1.10.88.0	0000 0001 0000 1010 0101 1000 0000 0000	1.10.88.111	0000 0001 0000 1010 0101 1000 0110 1111	0.0.0.255	The wildcard mask of 0.0.0.255 requires that the first three octets match, and they do. The packet will be forwarded.

Access List IP Address	Access List IP Binary Equation	Source IP Address	Source IP Binary Equation	Access List Wildcard Mask	Result
1.10.0.0	0000 0001 0000 1010 0000 0000 0000 0000	1.10.56.7	0000 0001 0000 1010 0011 1000 0000 0111	0.0.255.255	The wildcard mask of 0.0.255.255 requires that the first two octets match, and they do. The packet will be forwarded.
0.0.0.0	0000 0000 0000 0000 0000 0000 0000 0000	5.10.22.5	0000 0000 0000 1010 0001 0110 0000 0101	255.255.255. 255	The wildcard mask of 255.255.255. 255 dos not require that any octets match and will forward all packets.

Configuration of Standard Access Lists

As previously mentioned, standard (and extended) access lists are created in a sequential order that the Cisco IOS uses to permit or deny packets.

The following two steps are involved in the creation of access lists:

- 1. Create an access list by specifying an access list number (or name) and Access Control Entries (ACEs).
- 2. Apply the created access list to interfaces or terminal lines.

The following types of access lists are supported by the Cisco IOS. A definition of each will be given, however, the CCNA exam will only address standard and extended access lists.

• Standard access lists

Standard access lists use source addresses for matching operations.

• Extended access lists

Extended access lists can match the following criteria:

- Source address
- o Subsets of the source address using wildcard masks
- Destination address
- o Subsets of the destination address using wildcard masks
- Protocol type (TCP, UDP, ICMP, IGRP, IGMP, etc.)
- Source port
- o Destination port
- Established (matches all TCP flows except the first flow)
- IP TOS

-

o IP Precedence

• Dynamic access lists

Dynamic access lists are extended access lists that allow the Cisco IOS to add a temporary ACE to the list. The user must telnet into the router and supply a username and password. Once authenticated, the Cisco IOS adds the entry for the user. The temporary entry will not be deleted when the connection terminates, rather, the entry must be set to time out or be removed manually by an administrator.

• Reflexive access lists

Reflexive access lists allow packets to be filtered based on session information. Like dynamic access lists, reflexive access lists use extended access lists and contain temporary ACEs.

The following table displays the access list numbers and corresponding access list type.

Access List Number	Type of Access List
1-99	IP standard access list
100-199	IP extended access list
200-299	Protocol type-code access list
300-399	DECnet access list
400-499	XNS standard access list
500-599	XNS extended access list
600-699	Appletalk access list
700-799	48-bit MAC address access list
800-899	IPX standard access list
900-999	IPX extended access list
1000-1099	IPX SAP access list
1100-1199	Extended 48-bit MAC address access list
1200-1299	IPX summary address access list
1300-1999	IP standard access list expanded range
2000-2699	IP extended access list expanded range

Access List Configuration Command	Definition
<pre>access-list (1-99) (permit deny) (source address) (source mask)</pre>	Command for standard numbered access lists
<pre>access-list (100-199) (permit deny) (protocol) (source address) (source mask) (operator operand) (destination address) (destination mask) (operator operand) (established)</pre>	Command for extended numbered access lists
<pre>ip access-group (number name) (in out)</pre>	Subcommand that enables access lists
<pre>ip access-list (standard extended) (name)</pre>	Command for standard and extended access lists
<pre>deny (source) (source wildcard) (any) (log)</pre>	Subcommand for standard named access lists
<pre>permit deny (protocol) (source address) (source mask) (operator operand) (destination address) (destination mask) (operator operand) (established)</pre>	Subcommand for extended named access lists
<pre>access-class (number name) (in out)</pre>	Subcommand for standard or extended access lists
shop ip interface	Shows interface and applied access lists
show access-list	Shows all configured access lists
show ip-access list (number)	Shows IP access lists

The following table displays the access list configuration commands.



The following example shows a standard access list.

```
interface serial 0
ip access-group 1
!
access-list 1 deny 10.10.1.1 0.0.0.255
access-list 1 permit any
```

Controlling vty Access

IP access lists can be applied to one or more virtual terminal line (vty) ports to control telnet access to a Cisco router. The following example shows the creation of a vty IP access list:

```
line vty 0 2
login
password cisco
access-class 4 in
!
access-list 4 permit 10.1.1.0 0.0.0.255
```

The **access-class** command refers to access-list 4. This access list would be in effect on vty port 2 and would only allow telnet requests from the 10.1.1 subnet. The **in** keyword on the **access-class** command designates that the access list applies to incoming requests. The **out** keyword would filter outgoing telnet attempts via the destination address on a vty terminal line.

EXTENDED ACCESS LISTS

Extended access lists filter traffic by matching one or more fields in a packet. Similar to standard access lists, extended access lists are processed by the Cisco IOS in a sequential order and may be applied to an inbound or outbond interface.

The following topics will be covered in this section:

- Configuring Extended Access Lists
- Named Access Lists

Configuring Extended Access Lists

As previously mentioned, extended access lists can match the source IP address, destination IP address, protocol type, source port, destination port, and various other fields. Common to standard and extended access lists is an implied deny all traffic statement that is in effect at the end of the list. For example, if a packet fails to match the criteria of an access list, by default, the packet will be denied. However, you can use the **permit any** command at the end of the access list to permit any packet that was not matched. All statements in an ACE must match before the packet will be forwarded.

The following table provides sample extended access list commands.

Access List Command	Definition
access-list 101 deny tcp any host 10.10.1.1 eg 23	This ACE will permit packets with any source address. The header must specify TCP and the destination address must match 10.10.1.1 port 23.
access-list 101 deny tcp any host 10.10.1.1 ed telnet	This ACE will permit packets with any source address. The header must specify TCP and the destination address must match 10.10.1.1 port 23.
access-list 101 10.10.2.0 0.0.0.255 10.20.1.1	This ACE will permit packets from the subnet 10.10.2. The destination address must be 10.20.1.1.



In the previous example, the **any** keyword permits any source IP address. The **host** keyword (followed by an IP address) requires a match with the packet's destination address.

The following example shows an extended access list.

```
interface serial 0
ip access-group 100
!
access-list 100 deny ip host 10.20.1.1 10.10.1.1 0.0.0.255
access-list 100 permit ip 10.20.1.1 0.0.0.255 10.10.1.1 0.0.0.255
access-list 1 permit ip any any
```

Named Access Lists

Named access lists utilize the same logic as standard and extended access lists with added flexibility. Named access lists provide the following benefits:

- Administrators can remember named access lists easier than numbered access lists.
- Named access lists are not limited in number. Standard access lists are limited to 99, and extended access lists are limited to 100.
- ACEs can be created and removed from named access lists without re-creating the lists in their entirety. Changes to numbered access lists require the re-creation of the list.

NOTE: Names must be unique on the same router. However, named access lists with the same name can be used on multiple routers.

The following procedure demonstrates the creating and editing of a named access list called sparky.

```
conf t
Router(config)#IP access-lists extended sparky
Router(config-ext-nacl)#permit tcp host 10.10.1.1 eq www any
Router(config-ext-nacl)#deny udp host 10.10.1.1 0.0.0.0 255.255.255.0
Router(config-ext-nacl)#deny ip 10.10.2.0 0.0.0.255 10.10.1.2
    0.0.0.255
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#^z
```

Once the named access list is created, you can view the configuration with the **sh run** command, as shown in the following example:

```
Router#sh run
Building configuration...
Current configuration:
.
. (uninportant statements omitted)
.
!
ip access list extended sparky
permit tcp host 10.10.1.1 eq www any
deny udp host 10.10.1.1 0.0.0.0 255.255.255.0
deny ip 10.10.2.0 0.0.0.255 10.10.1.2 0.0.0.255
permit ip any any
```

The following example demonstrates how to edit a specific ACE in the named access list with the **no** command.

```
conf t
Router(config)#IP access-lists extended sparky
Router(config-ext-nacl)#no deny udp host 10.10.1.1 0.0.0.0
255.255.255.0
Router(config-ext-nacl)#^z
```

The **show access-list** command will verify that the entry has been removed.

```
Extended IP access list sparky
permit tcp host 10.10.1.1 eq www any
deny ip 10.10.2.0 0.0.0.255 10.10.1.2 0.0.0.255
permit ip any any
```

\mathbf{r}	 				 	

SUMMARY

During this chapter, you were introduced to some important tools for managing the Cisco IOS:

- Configuration files
- Procedures for backing up and restoring configuration files
- Ways to monitor network traffic, including debugging and session security procedures
- Implementing access lists

POST-TEST QUESTIONS

The answers to these questions are in Appendix A at the end of this manual.



1.	What command is used to verify configuration registry changes prior to reload?
2.	What configuration registry setting is used to boot the router into ROM monitor mode?
3.	What does the "2" signify in the configuration registry setting 0x2101?
4.	What router prompt designates the router has booted from the IOS in ROM?

5. What will be the result of the ACE command access-list 101 deny tcp any host 10.10.1.1 eg 23?

6. What command is used to turn on debugging on the router?
7. What is one way to verify correct router operation following an IOS upgrade?



Advanced LAN Design

CHAPTE

6

R

MAJOR TOPICS

►

Objectives	152
Pre-test questions	152
Introduction	153
LAN Standards	153
LAN Encapsulation	161
LAN Switch Configuration	167
Summary	203
Post-Test questions	203

OBJECTIVES

At the completion of this chapter, you will be able to:

- List and explain major IEEE LAN standards.
- Identify and explain the reasoning behind LAN segmentation.
- Configure and deploy the Cisco Catalyst 1900 switch.
- Configure VLANs on the Cisco Catalyst 1900 switch.

PRE-TEST QUESTIONS

The answers to these questions are in Appendix A at the end of this manual.



Which IEEE standard applies to Ethernet?
 What is the basic unit of transmission at the physical media?
 What is one advantage of token passing over bus architecture?
 What is one advantage of token passing over bus architecture?
 Can a Cisco Catalyst 1900 switch support multiple transmission media?

INTRODUCTION

Early LAN administrators used many techniques to conserve bandwidth, from using faster, nonroutable protocols to daisy-chaining managed hubs.

The advent of switched networks forced administrators to evaluate more intelligent bandwidth conservation. Modern applications, particularly video and streaming applications, require increasing amounts of this already scarce resource. While processors' capacities tend to double every 12 to 18 months, significant baseband-to-broadband migration and evolution takes considerably longer.

The excessive network congestion so pervasive in Internet-enabled, multiplatform LANs has spawned an entirely different approach to bandwidth conservation than in years past. LAN design is now an important and ongoing responsibility of every network administrator and IT department. No longer can businesses simply react to changes in the computing landscape; it is necessary to be proactive in network design.

To that end, Cisco offers a wide range of networking products, from low-end Layer 2 switches like the Catalyst 1900 to high-end multimedia switches like the Catalyst 5500. These and other network-switching products help make the network design task easier and provide more capability and flexibility for the network.

LAN STANDARDS

As the battle for networking standards continues to be waged, one organization's standards has withstood the test of time to become not only the de jure leader but the de facto leader in networking standards. The Institute of Electrical and Electronics Engineers (IEEE), or more specifically the IEEE's Project 802 committees and working groups (collectively called the Project 802 group), are constantly refining and revising LAN standards. The Project 802 group is also called the LAN/MAN (Local Area Network/Metropolitan Area Network) Standards Committee, or LMSC.

The more common LAN topologies, such as Token Ring, FDDI, and most notably Ethernet, all have their roots with their respective IEEE 802 committees. In this section, we will not detail the intricacies of each specification; rather, we will take a look at the general tenets of each specification. This section will deal with the more popular LAN standards in generally descriptive terms, framing our discussion of LAN packet construction later in this chapter.

The following topics will be covered in this section:

- IEEE Standards
- Ethernet
- Token Ring
- FDDI

IEEE Standards

Originally, the IEEE intended to develop only *one* networking standard with Project 802 of the IEEE Computer Society Local Network Standards Group. In February 1980, when the first IEEE 802 committee met, it was soon decided that the original standard should be divided into three layers: physical layer (media), Media Access Control, and Higher Level Interface. The original access method chosen by the group was similar to Carrier Sense Multiple Access/Collision Detection (CSMA/CD), as it was their preferred bus topology.

Since then, other standards have subdivided the group, known to the IEEE as the LMSC as a reflection of changes in its overall mission. As of this writing, there are sixteen working groups and Technical Advisory Groups (TAGs), overseen by a sponsor executive committee.

The following URL is for all standards committees:

http://grouper.ieee.org/groups/802/dots.html

IEEE 802 Standards, Status, and Description

The following table lists and describes the IEEE 802 LAN/MAN standards committees.

Designation	Status	Committee Title
802.1	Active	Higher Layer LAN Protocols Working Group
802.2	Inactive	Logical Link Control Working Group
802.3	Active	Ethernet Working Group
802.4	Inactive	Token Bus Working Group
802.5	Active	Token Ring Working Group
802.6	Inactive	Metropolitan Area Network Working Group
802.7	Inactive	Broadband TAG
802.8	Active	Fiber Optic TAG
802.9	Active	Isochronous LAN Working Group
802.10	Active	Security Working Group
802.11	Active	Wireless LAN Working Group
802.12	Active	Demand Priority Working Group
802.14	Active	Cable Modem Working Group
802.15	Active	Wireless Personal Area Network Working Group
802.16	Active	Broadband Wireless Access Working Group
RPRSG	Active	Resilient Packet Ring Study Group

Each of these committees has the responsibility for discussion, debate, and publishing of its respective standards. Further, each committee publishes interpretations of its standard as necessary when requested.

For more information about IEEE standards, please see the IEEE Standards Association Web site:

http://standards.ieee.org/catalog/olis/index.html

The following are some shorter descriptions of applicable topology standards. While not as exhaustive as the descriptions provided elsewhere in this course, they are overviews of three more common standards and their implementation on Cisco routers and switches.

Ethernet

Ethernet, defined by the IEEE 802.3 committee specifications, is by far the most common networking standard. The CSMA/CD access method, whereby a bus topology with shared media access is defined, is a simple yet powerful idea. The standard, though reinterpreted in response to advances in hardware, has proven remarkably durable.

The standard, written by the IEEE, originally specified physical layer standards and access methods. However, over the years, the standard has been revised as the technology has matured.

Cisco products offer a full range of Ethernet support, from 10 Mbps to 1,000 Mbps (Gigabit Ethernet) and everything in between.

Half Duplex vs. Full Duplex

The duplex state of a signal refers to its direction across a physical medium. If a media is full-duplex capable, it can support both incoming and outgoing transmission traffic simultaneously.

For instance, a Category 5 twisted-pair cable is capable of supporting both incoming and outgoing traffic at the same time, with the outgoing traffic on one wire and the incoming traffic on another.

Half duplex means that the same wire on a physical medium is used both to transmit and receive binary data. It is the nature of a half-duplex connection that while one station is transmitting, the other must be listening. The signal travels in both directions in half-duplex communication, but only flows in one direction at time.

Ethernet, briefly outlined as follows, is capable of supporting full-duplex connections, as are Token Ring and FDDI. Full-duplex Ethernet is by far the most common of the three.

Standard Ethernet

Standard Ethernet is the base specification for 10-Mbps Ethernet, sometimes called 10BaseT. 10BaseT is shorthand for 10-Mbps Baseband communication over twisted-pair cable.

Standard Ethernet is venerable but still viable. Most often used in hub-to-workstation or switch-to-workstation installations, it can provide sufficient bandwidth for a basic slate of applications, including e-mail and desktop computer productivity software. Often, networks with Internet-connected routers or firewalls will use a 10BaseT circuit to transmit data received from slower WAN connections to the main network by a router or firewall.

Fast Ethernet

100-Mbps Ethernet, or Fast Ethernet, is rising to prominence as its adoption begins to permeate the marketplace on a mass scale. Many modern applications, including those optimized for network or Internet performance, continue to require more and more bandwidth.

In answer to the problem of baseband bandwidth squeeze, the IEEE 802.3u committee developed the 100BaseT standard. From this, the 100BaseFX specifications for 100 Mbps over fiber-optic cable were spawned.

Gigabit Ethernet

Gigabit Ethernet, originally a group of proprietary competing standards operating on different vendors' backplanes, was eventually addressed by the IEEE 802 project. This standard, specifying speeds of up to 1,000 Mbps over its media, is gaining acceptance not only as a means of high-speed data transfer within a switch or router, but as a means of connecting them.

3	 	 	

Certain applications, if sufficiently network intensive, could eventually benefit from Gigabit Ethernet. For now, Gigabit Ethernet remains relegated primarily to backbone networking and backplane networking. However, judging by the current pace of technological advances and the speed at which a given technology matures in the IT market, it won't be long before Gigabit Ethernet is running between switches, between servers, and eventually between workstations.

Packet Structure in Ethernet

LAN packets have a specific structure in Ethernet. The structure of the packet header provides the information needed for switching and routing. It is important to be aware, at the very least, of where the addressing information resides within the packet.

In a standard DIX (Digital/Intel/Xerox) Ethernet packet, the header is made up of 22 bytes. The function of these bytes is as follows:

- The first 8 bytes are the packet's Preamble.
- The next 6 bytes are the packet's Destination Address.
- The next 6 bytes are the packet's Source Address.
- The next 2 bytes are the Ethernet type, which is assigned by RFC 1700.

The packet's data, followed by 4 bytes for the Frame Check Sequence (FCS), follows the above sections.

In an IEEE 802.3 Ethernet packet, the addressing information is contained in the same manner; only the Preamble is divided into a 7-byte preamble and a 1-byte Start Delimiter. The Destination and Source Address sections are unchanged, 6 bytes each. Then the 802.3 packet differs from the Ethernet DIX packet in that it contains a length field of 2 bytes. 802.2 information, routing and control information, and data follow, respectively. As with Ethernet DIX, the 4-byte FCS composes the packet trailer.

For more information on Ethernet, see the previous sections in this course, particularly in the case of Gigabit Ethernet. The following is the IEEE 802.3 project's URL:

http://grouper.ieee.org/groups/802/3

Token Ring

Token Ring, per the IEEE 802.5 specification, uses Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA) in contrast to Ethernet. In Token-Ring networks, only one station is allowed to transmit at a time, and all other stations pass this communication on to the next station.

The determination of which station is allowed to transmit is made by the possession of the *token*, an electronic entity that functions as a microphone of sorts. The token travels around the network in one direction only. Each station, or lobe, listens for the token. When the token arrives, the station checks the token to determine if one of the following is the case:

- The token is free. If the token is free, this means there is no traffic on the network, and that the station may then attach traffic to the token.
- The token contains data. If the token contains data, the station checks the destination MAC address in the destination header to determine whether the packet has reached its intended destination. If the packet is bound for this station, the station then reads the token and responds appropriately. If not, the station retransmits the token and sends it down the line.
- The token is corrupted. A new token is generated by the station.

Encountered most often in IBM networks, particularly those with legacy systems, Token Ring can accommodate speeds of 4 Mbps or 16 Mbps.

Certain vendors have developed Token-Ring products capable of 100 Mbps, but these products are not widely accepted outside established Token-Ring installations.

Packet Structure in Token Ring

As with Ethernet, it is important to note where the addressing information falls in a Token-Ring packet. It is this information that is most vital to LAN switching and routing.

A Token-Ring (802.5) header consists of the following, in the order listed:

- A 1-byte Start Delimiter, denoting the arrival of the packet
- A 1-byte Access Control Field, denoting whether the packet is a token, data, or command frame
- A 1-byte Frame Control field, which indicates priority
- The 6-byte Destination Address
- The 6-byte Source Address

This header is followed by an 802.2 header, then the packet's data. Following the data is the Token-Ring trailer, consisting of an FCS, an Ending Delimiter byte, and a Frame Status byte. The URL for the 802.5 committee follows:

http://grouper.ieee.org/groups/802/5/index.html

FDDI

Fiber Distributed Data Interchange, or FDDI, is widely regarded as one of the most reliable data transport methods, and for good reason. FDDI offers high bandwidth, nearly impermeable media when using fiber-optic cable, and long distances between repeaters. FDDI signals over fiber are not subject to interference of any kind. FDDI is also the most reliable transport medium due to its built-in redundancy.

FDDI, like Token Ring, is a CSMA/CA topology. It features token passing as its method of transit, but has a secondary ring as part of its topology. When the primary ring is experiencing problems, the secondary ring automatically takes over the traffic, often without any noticeable change in performance from the user's perspective.

FDDI is by far the most fault-tolerant topology, but is also the most expensive. Fiberoptic cabling is far more costly than the Category 5 or 5e that can be used for Ethernet or Token Ring. The interface cards for FDDI are proportionately expensive as well. Also, modules for routers and switches that feature FDDI support tend to be more expensive than their Ethernet or Token-Ring counterparts.

Packet Structure in FDDI

The structure of packets in FDDI is as important as in Ethernet and Token Ring. We will again concern ourselves with the packet header, where the information needed for switching and routing is contained.

An FDDI (ANSI) packet header is structured as follows, in the order listed:

- A 4-byte preamble
- A 1-byte Start Delimiter
- A 1-byte Frame Control section
- The Destination Address
- The Source Address

Like Token Ring, there is an 802.2 section in the packet, followed by the data and an FDDI trailer. The FCS is located in the trailer.

For more information on FDDI, see the IEEE Web site at the following location:

http://grouper.ieee.org/groups/802/8/index.html

LAN ENCAPSULATION

A thorough understanding of LAN encapsulation is integral to understanding how a LAN switch or router is able to segregate traffic. The encapsulation of data continues to become increasingly important as more sophisticated network devices continue to penetrate the market.

Encapsulation in the Cisco lexicon moves down the OSI layers, beginning with data, then moves on to segments, then to packets, then to frames, then to bits.

)	 		

The following topics will be covered in this section:

- Encapsulation and OSI Layers
- Addressing and Header Formats
- LAN Packet Structure
- VLAN Packet Structure

Encapsulation and OSI Layers

Encapsulation is the process of packaging data for delivery from one application to another by adding headers to the data. The data is then prepared and organized for transmission across the network media.

The encapsulation process begins at the Application layer of the OSI Model. At the Application layer, the user creates and inputs *data* for delivery from one application to another. A header is added by the Application layer, then the data is passed to the Presentation layer. The Presentation layer adds its header and passes the data to the Session layer. At the Session layer, another header is added.

At the next layer, the Transport layer, data is packaged into *segments*. These segments allow end-to-end transport of the data, i.e., when *data* becomes a *segment*, the *segment* has a Source and Destination Address. At this point, the segment is passed to the Network layer.

The Network layer then appends the segment with a network address, at which time the segment becomes a *packet*. The packet is then passed to the Data Link Layer.

Once the packet arrives at the Data Link layer, it is converted into *frames* in order to allow further conversion at the Physical layer.

Finally, the Physical layer converts the frames into *bits* so that the transmission across the physical media may occur.

In summary, encapsulation is the process of preparing raw data created by users at the Application layer for transmission as bits at the Physical layer. This preparation involves the adding of headers and trailers as well as several transformations as the data moves down through the OSI layers. The entire process is outlined as follows:

- Data becomes segments at the Transport layer.
- Segments become packets at the Network layer.
- Packets become frames at the Data Link layer.
- Frames become bits at the Physical layer.
- Bits are transmitted across the media.

This model is used in all Cisco hardware. It is known as the five-step encapsulation method. We will more fully explore the constructs of packets, frames, and segments in the following sections.

Addressing and Header Formats

Addressing is the method by which packets on a network are directed from their source to their destination. The different layers of the OSI Model communicate with each other and are differentiated from each other by specialized data segments called *headers*. These segments are called *trailers* if they are placed at the end of a segment, as in the case of Layer 2 (Data Link layer) information.

Each OSI layer has responsibility for providing service to its adjacent layer or layers. All of the layers work together to provide the overall structure of LAN conversations between and within stations.

Addressing and the Network Layer

As detailed elsewhere in this course, the Network layer (Layer 3) is responsible for the end-to-end deliveries of packets. It is here where the addressing of a packet takes place in terms of the overall network.

MAC addresses, a vital addressing component, provide a reference point for a particular station or interface. The MAC address is the address recorded and stored by a router when it references stations it is able to reach. At the Network layer, the router adds its own information regarding the origin or destination of the packet. This MAC-address-to-network-address relationship is similar to that of a postal address, with the MAC address being the street number and the network address being the street name.

LAN Packet Structure

It is important to understand the process of how packets are constructed. It is at this level that the distinctions are drawn between switches and routers, and where the inner workings of each are revealed. Also, the construction of data units gives insight into how routers and switches accomplish their mission of forwarding packets and frames accurately. Perhaps the most important element of value to the Networking Engineer is how the different layers that routers and switches operate are responsible for different types of tasks in networking. This will hopefully give insight into accurate LAN design based on what each device (router or switch) does well.

The construction of LAN packets varies by type, but there are many common elements. Packets encapsulated according to the OSI Model go through seven steps in their construction. A Protocol Data Unit (PDU) is the basic building block of a LAN packet. PDUs from the different OSI layers are added to the data as it travels through the seven layers. Each layer adds its own particular PDU as part of the header or trailer.

These are the activities that take place at each step in the OSI Model:

- 1. At the Application layer, the application and the user create the data. The Application layer then places an application header in front of the data and passes the data to the Presentation layer.
- 2. At the Presentation layer, a presentation header is placed in front of the application header, and the data (with headers) is passed to the Session layer.
- 3. At the Session layer, the process is repeated, and the data with headers is passed to the Transport layer.
- 4. At the Transport layer, the transport header is added. Then the data, with all PDU's, is passed to the Network layer as segments.

- 5. The process repeats at the Network layer, resulting in a data unit with a network header, a transport header, a session header, a presentation header, and an application header, followed by the data itself. This unit, now called a packet, is passed to the Data Link layer.
- 6. The Data Link layer not only adds a header to the packet, it adds a trailer as well. Now the packet is divided into frames so that the Physical layer can translate them.
- 7. At the Physical layer, the frames are converted to bits and transferred across the network medium.

At the destination of the bits, the cycle reverses itself. Each layer of the OSI Model only communicates with its counterpart on the other end. The communication that occurs between the layers consists only of the layers providing services to each other.

Within the OSI Model, there will not always be seven steps in the process of encapsulation. Very often, the upper three layers (5, 6, and 7) will add headers only on initialization. From initialization, these layers become aware of how to interpret the data, and therefore don't need to add headers in each instance when a packet is transmitted.

TCP/IP

1

In the TCP/IP network model, there are only 4 layers: Application, Transport, Internet, and Network Interface. These layers map roughly to the OSI Model in that the Application layer in TCP/IP incorporates all the functions of the upper three layers in the OSI Model. The Transport and Internet layers are nearly the same as the OSI's Transport and Network layers, respectively. Finally, the Network Interface layer maps roughly to the OSI's Data Link and Physical layers.

Data is encapsulated in TCP/IP as follows:

- 1. The Application layer creates the data.
- 2. The Transport layer adds a TCP header, which packages the data for transport.
- 3. The Internet layer adds an IP header in front of the TCP header. This header gives the network address of the station transmitting the data on the network.
- 4. The Network Interface layer adds a Data Link header and a Data Link trailer, converts the frame into bits, and transmits it across the physical medium.

Routing information in TCP/IP is carried at the Internet layer of the stack. This equates to Layer 3 of the OSI Model. Switching information is carried at the Network Interface layer of TCP/IP, equating to Layer 2 of the OSI Model.

IPX

Novell NetWare's IPX protocol stack is another common protocol that maps roughly to the OSI Model. In IPX, the Server Announcement Protocol (SAP) and NetWare Core Protocol (NCP) layers map to the upper three layers of the OSI Model. The IPX and SPX layers of the IPX stack map to the Transport and Network layers of the OSI Model, respectively. The MAC Protocols layer in IPX covers the Data Link and Physical layers of the OSI Model.

Therefore, routing information in IPX is carried at the IPX/SPX layer (Layer 3 from OSI) and switching information in IPX is carried at the MAC Protocols layer (OSI Layer 2).

VLAN Packet Structure

The structure of VLAN packets becomes slightly more complicated. Because a VLAN is a logical grouping of stations as opposed to a physical grouping, the VLAN packets must contain fields that an ordinary packet does not contain. VLAN packets, therefore, are *tagged* by various methods to denote their membership in one VLAN or another.

Two of the more prevalent VLAN tagging methods come from IEEE 802.10 and 802.1q. These standards have provided structure to a formerly unruly and vendor-specific paradigm.

The 802.1q standard sets forth the parameters for adding a VLAN tag field to a packet, allowing the VLAN to which the packet belongs to be identified by a device regardless of vendor. Q-tagging, as Cisco sometimes refers to the practice, will bring some order and consistency to the processing of VLAN traffic.

LAN SWITCH CONFIGURATION

The complexity of the modern LAN has given rise to the necessity of LAN Switching. To that end, Cisco has provided Layer 2 switching products such as the Catalyst 1900 to meet the market need.

The capability of the modern switch has adapted with its mission. As *flat* LANs have been supplanted by switched virtual LANs, so have passive hubs and bridging-only switches given way to smarter, swifter switches.

The following topics will be covered in this section:

- Catalyst 1900 Nomenclature
- Catalyst 1900 Features
- Basic Configuration of the Catalyst 1900

Catalyst 1900 Nomenclature

The Catalyst 1900 switch is Cisco's entry-level switch. The switch is available in a variety of configurations, offering either twelve or twenty-four RJ-45 10BaseT ports, and each switch also has two 100BaseX ports. All ports are half- and full-duplex capable, and duplex status is autonegotiated on 100BaseTX ports.

All RJ-45 ports are located on the front of the unit. On the rear of each unit is the power cable receptacle, a DC input port, an AUI port, and an eight-pin RJ-45 console port. The switch ships with a proprietary cable for connecting a terminal.

The front panel features LEDs for each port, plus a system power indicator and a mode indicator LED on the left side of the panel.

All Catalyst 1900 models feature two trunk ports on the right side of the front panel.

Catalyst 1900 Features

One of the more unique features of the IOS is a menu-driven interface for the Catalyst 1900 switch. The command-line interface familiar to Cisco router users is also available, but for those who prefer a menu-driven interface, the Catalyst 1900 provides one. For those segmenting a flat network for the first time, the menu-driven feature contributes to an easy setup.

Other features of the Catalyst 1900 include the following:

• IEEE 802.1d STP (Spanning Tree Protocol)

This feature includes Cisco's Port Fast technology, which allows a port to transition instantly from blocking to fowarding state.

• IEEE 802.3x flow control

This feature is available on 100Base TX ports only.

- FragmentFree and store-and-forward switching modes
- Autonegotiation of duplex on all 100-Mbps ports
- Half-duplex and full-duplex operation on all ports

This allows you to mix duplex status on your attached workstations if needed, without having to reconfigure the workstation NIC or the switch port.

Broadcast storm control

This prevents attached devices from propagating storms across the switch.

• Enhanced Congestion Control (ECC) on each half-duplex port

ECC allows transmissions to be accelerated in situations where queues have been filled.

Cisco Group Management Protocol (CGMP)

This limits the flooding of IP multicasts.

Basic Configuration of the Catalyst 1900

The Catalyst 1900 offers a menu-driven configuration program with a logically organized submenu structure. The menu-driven interface allows easier interaction, setup, and tuning of the switch. However, the command-line interface is still available for those who are well versed in the Cisco IOS.

The switch ships from the factory with the following defaults:

- No console password
- Spanning Tree and CDP enabled
- Switching mode Fragment free
- IP Address of 0.0.0.0
- Autonegotiation on 100BaseT ports
- Half duplex on 10BaseT ports

Depending on which version of the switch you are configuring, there may be other defaults. For our purposes, we will be using a Catalyst 1900 with the following:

- Twenty-four 10BaseT ports
- Two 100BaseTX ports
- One switched AUI port, model WS-C1924-EN with feature WS-C1924-A

Just as with other Cisco devices, you must first connect a console to the switch in order to configure and tune it. The console port is located on the rear of the switch, and comes with a proprietary ribbon cable with RJ-45 connectors on each end. The switch also includes both a nine-pin and a 25-pin serial adapter for the connection to the console PC.

You will need a terminal emulation program (such as Windows Terminal or HyperTerminal) on the PC you are connecting to the console port. Make sure that your serial port settings are 9,600 baud, 8 data bits, 1 stop bit, no parity, and no flow control. Connect the console cable to the rear of the switch and to the serial port on your PC, then power up the switch. The 1900 has no on/off rocker switch, so simply plug in the switch's power cable to start the switch.

On startup, the switch runs its Power On Self Test to verify hardware and internal connections and to boot the IOS. When the IOS is booted, your console should show the following screen:

```
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc. 1993-1999
All rights reserved.
Enterprise Edition Software
Ethernet Address: 00-01-96-BC-CA-40
PCA Number:
                      73-3121-04
PCA Serial Number: FAB041480PB
Model Number:
                     WS-C1924-EN
System Serial Number: FAB0414R0XD
Power Supply S/N: APQ0401025S
PCB Serial Number:
                     FAB041480PB,73-3121-04
1 user(s) now active on Management Console.
     User Interface Menu
 [M] Menus
 [K] Command Line
 [I] IP Configuration
 [P] Console Password
```

Enter Selection:

On initial configuration, you may wish to use the command line if you have a configuration script to load from a TFTP server. Selecting menu option **K** from the opening screen will take you to the standard Cisco IOS command line. For our purposes, we are going to step through some of the tasks associated with the menu-driven interface as opposed to the command line.

Selecting **M** from the opening console screen takes you to the following menu:

```
Catalyst 1900 - Main Menu

[C] Console Settings

[S] System

[N] Network Management

[P] Port Configuration

[A] Port Addressing

[D] Port Statistics Detail

[M] Monitoring

[V] Virtual LAN

[R] Multicast Registration

[F] Firmware

[I] RS-232 Interface

[U] Usage Summaries

[H] Help

[K] Command Line
```

[X] Exit Management Console

Enter Selection:

Enter your selection from your terminal's keyboard. Unlike when using the command line, there is no need to press *ENTER* after the command letter is entered; the command is processed immediately.

The following sections describe the submenus of the Main menu in detail.

Console Settings Menu

From this screen, select C for the console settings. The following menu is displayed:

Enter Selection:

It is always a good idea, for physical security, to set the management console inactivity timeout. From this screen, you can select **T** to set this timeout from 30 seconds to 65,500 seconds.

Also from this screen, you may wish to change the default mode of the status LED. The status LED can display port status, bandwidth utilization, or full-duplex operation status. The status LED, located on the front panel near the left edge of the switch, also has a button labeled MODE, which accomplishes the same function of switching between modes as the menu shown.

When displaying port status, the status LED can appear one of five ways:

Off	There is no activity on that particular port.				
Green	The link is operational.				
Flashing green	The link is experiencing activity and is operational.				
Amber	The port is not fowarding due to disabling, address violation, or suspension by Spanning Tree Protocol due to loops.				
Flashing amber/green alternating					
	Indicates a link fault. This could be a result of CRC failure, alignment errors, jabber errors, etc.				

When the status LED's mode is changed to Bandwidth Utilization mode, the LED on the front panel changes to UTL. The LEDs above each port are then treated as an aggregate, lighting up from left to right to indicate bandwidth utilization for the switch. The more port LEDs that are lit, the higher the aggregate bandwidth utilization for the switch.

When the status LED is changed to Full-Duplex operation status mode, the FDUP status LED light glows green on the left front panel. This mode will light the LEDs above each port that is operating in Full-Duplex mode. This feature is useful if you want to determine whether a given port is communicating at full duplex. Remember, however, that the default setting for all 10BaseT ports is half duplex.

Silent time upon intrusion detection (option **S** from the Catalyst 1900 **Main** menu) refers to the amount of time *after* the specified number of failed password attempts (option **P**, **Password intrusion threshold**, from the menu) that the console will disallow logins. The silent time can be set from 0 to 65,500 minutes.

The two passwords modifiable from the main menu are the login password (blank by default) and the secret password used for entering the Privileged EXEC mode from the command line. Passwords must be entered before they can be changed. The password can be four to eight characters, is not case sensitive, and can contain any combination of characters. This differs from the command line in that the new password must be entered in double quotes on the command line; the double quote is a character when entered via the menu-driven interface. The secret password can be 1 to 25 characters long. The secret password, like the unencrypted password, can contain any characters. Unlike the unencrypted password described previously, the secret password *is* case sensitive. When entered, the router encrypts this password.

A convention common to the submenu system on the Catalyst switches is that option **X** returns the user to the previous menu. Since the **Console settings** menu is only one level from the **Main** menu, **X** takes you to the **Main** menu.

)	 		

System Menu

Selecting option **S** from the **Main** menu displays the **System Configuration** menu, similar to the following:

Catalyst 1900 - System Configuration System Revision: 5 Address Capacity: 1024 System UpTime: Oday(s) O4hour(s) 51minute(s) 54second(s) ----- Settings [N] Name of system [C] Contact name [L] Location [S] Switching mode FragmentFree [U] Use of store-and-forward for multicast Disabled [A] Action upon address violation Suspend [G] Generate alert on address violation Enabled [I] Address aging time 300 second(s) [P] Network port None [H] Half duplex back pressure (10-mbps ports) Disabled [E] Enhanced congestion control (10-mbps ports) Disabled ----- Actions [R] Reset system [F] Reset to factory defaults [V] Reset VTP to factory defaults [T] Reset to enable Bridge Groups ----- Related Menus [B] Broadcast storm control [X] Exit to Main Menu

Enter Selection:

Among the many parameters you can set and adjust on this menu, the following are perhaps the most significant:

• System name

Allows you to reference the system by name. This is often used as an inventory control item, particularly in large environments.

• Switching mode

This defaults to FragmentFree. FragmentFree, also called cut-through, is the faster of the two switching methods. The other method, store-and-forward, is more reliable. It is a good idea to change this setting if you are experiencing a large amount of FCS or alignment errors on the switch.

Location

Usually, this is used to represent the physical location of the switch, such as "third-floor wire closet". In large environments, the location may be a logical location based on a schematic.

Address aging time

Allows you to enter the number of seconds the switch will store an inactive Address table entry. This parameter can have a value of between 10 and 1,000,000. This parameter can be important if a fowarding table on a given switch is near capacity, as the aging time can be shortened to prevent performance degradation. (This degradation can occur when the switch's Address table becomes full and has no space to store more addresses. It can be reasonably anticipated that some of the addresses in the switch's memory are invalid; so decreasing the interval will cause the switch not to store inactive addresses for very long. This makes more memory available for the forwarding table of 1,024 entries.)

Network port

This defines the port to which all packets with unknown unicast addresses are forwarded. This port is often the port to which a router or another switch is connected. Some important attributes of the network port are as follows. The port:

- Cannot be a secure port.
- Can only serve the bridge groups of which it is a member.
- Doesn't learn addresses as does a normal port.

When using FastEther Channel mode, VLAN, or ISL trunking, port A or B cannot be selected as the network port. The major advantage of using a network port is that unicast packets that the switch receives are not flooded (transmitted on all ports except the port that received the packet), but sent to the network port instead.

• Broadcast storm control

This has a separate menu of its own. The purpose of storm control is to prevent forwarding of broadcast packets when a threshold is reached on a particular port. When a given threshold is set from the **Broadcast storm control** menu, it applies to all ports. The **Broadcast storm control** menu also allows you to specify the following:

- The number of broadcast packets on a port that constitute a broadcast storm
- The action the switch should take when a threshold is exceeded
- Whether the port should send an SNMP alert when the threshold is exceeded
- How many packets per second constitute an end to the broadcast storm

Broadcast storm control is vital on switches that are at or near capacity. It is also important to set these parameters in large environments, adjusting both the threshold for broadcasts and the threshold for re-enabling the port after a broadcast storm to the lowest tolerable numbers.

• Reset system

This is identical to the **reset** command from the Privileged EXEC (command prompt) mode.

This overview of the **System Configuration** menu summarizes many commands available at the Privileged EXEC (enable) mode command line. For a complete list of system menu properties and explanations, please see the documentation that came with your switch.

Network Management Menu

The **Network Management** menu contains a number of key features and brings you to a number of submenus once you've made your choice.

The Network Management menu, which is similar to the following sample, will display once you've chosen [N] Network Management from the Main menu.

Catalyst 1900 - Network Management
[I] IP Configuration
[S] SNMP Management
[B] Bridge - Spanning Tree
[C] Cisco Discovery Protocol
[G] Cisco Group Management Protocol
[H] HTTP Server Configuration
[R] Cluster Management
[X] Exit to Main Menu
Enter Selection:

The options shown control most of the basic functionality of the switch. Each of the selections shown has a submenu of its own. Here is a short explanation of each option.

• IP Configuration

Allows you to adjust and configure IP address, subnet mask, default gateway, Management Bridge Group, DNS server addresses, and Domain Name. It is also from the **IP Configuration** menu that you would configure RIP; you can also ping another station or clear the DNS cached entries.

<u>)</u>	 		

SNMP Management

Allows you to set and monitor the MIB objects. The **SNMP Configuration** menu has three submenus of its own, explained below.

- READ configuration allows you to enter up to four READ community strings.
- WRITE configuration allows you to configure four community strings as well as WRITE manager names and/or IP addresses. If these are not set, any management station can write to the switch's MIB.
- TRAP configuration allows you to configure the trap community strings and managers to which the switch will send any of thirteen trap messages from warmStart to ipAddressChange.
- Bridge Spanning Tree

This allows the configuration of bridging and Spanning Tree parameters. STP (Spanning Tree Protocol) attempts to eliminate bridging loops by identifying every port and placing it in a blocking state or fowarding state. As detailed previously in this course, Spanning Tree can be useful in many networking situations. Support for STP on this switch allows you to set root bridge ID, number of STP ports, and eight other settings.

Cisco Discovery Protocol (CDP)

This allows the switch to advertise itself to other equipment supporting CDP, as well as detect other Cisco equipment. The switch advertises its size, device type, and links. CDP version 2 must be enabled in order for the switch to participate in clustering.

Cisco Group Management Protocol (CGMP)

Creates CGMP multicast groups based on multicast packets received. The settings for CGMP, from the **CGMP** submenu, are described as follows:

- Router Hold time is the amount of time a CGMP group will be kept alive before deleting the group. This parameter defaults to 600 seconds.
- CGMP is enabled by default.
- CGMP Fast Leave, which is disabled by default, allows switch ports to disassociate themselves from multicast groups faster than the normal hold time. This is also the feature that allows the switch to prune entries in the Multicast Address table if no CGMP group members from that multicast group exist on the switch.

There are also two actions you can accomplish from the **CGMP** submenu. You can list multicast addresses and remove multicast addresses manually from the Multicast Address table.

• HTTP Server Configuration

Allows you to choose the HTTP port upon which the Catalyst 1900 Switch Manager will run.

Cluster Management

Allows you to take advantage of Cisco's clustering feature for its switches. Clustering allows a number of switches to be monitored and configured as an aggregate group. One switch, dedicated as the command switch, performs all the command functions. The command switch must be a 2900 XL or a 3500 XL.

As with all menu screens, **X** brings you back to the previous menu in the hierarchy.

Port Configuration Menu

The previously described parameters, for the most part, affected the switch as a unit or all ports. The **Port Configuration** menu (shown as follows) allows you to view statistics and adjust the parameters of individual ports.

```
Identify Port: 1 to 24[1-24], [AUI], [A], [B]:
Select [1 - 24, AUI, A, B]:
```

)	 	 	

The following screen appears once you've chosen a port. In this case, we have chosen 10BaseT port 2:

```
Catalyst 1900 - Port 2 Configuration
 Built-in 10Base-T
 802.1d STP State: Forwarding Forward Transitions: 1
----- Settings -----
[D] Description/name of port
[S] Status of port
                                Suspended-no-linkbeat
[F] Full duplex
                               Disabled
[I] Port priority (spanning tree) 128 (80 hex)
[C] Path cost (spanning tree)
                               100
[H] Port fast mode (spanning tree) Enabled
----- Related Menus
[A] Port addressing [V] View port statistics
[N] Next port [G] Goto port
[P] Previous port [X] Exit to Main Menu
```

Enter Selection:

This screen allows you, by port, to adjust various parameters.

• Description

Allows you to choose a description for the port, up to 60 characters. This is often helpful in troubleshooting, as you may wish to name the port based on what equipment is connected to it.

• Status of port

Tells you the status of the port; possible statuses are described in the following table:

Port Status	Indication
Enabled	This port is ready to transmit and receive data.
Suspended-no-linkbeat	This port is suspended; normally because of a nonfunctional station at the other end of the connection, or no station connected at all. The port will change status to enabled when the condition is corrected.
Suspended-jabber	This port is suspended due to an attached node's jabbering. The port will change status to enabled when the station returns to normal operation.

Port Status	Indication
Suspended-violation	This port is suspended due to an address violation (more often than not, a duplicate address). Like the other suspension statuses, the port returns to enabled when the error condition is corrected.
Disabled-mgmt	This is a port that has been manually disabled. It will be unavailable until manually enabled.
Disabled-self-test	This port is disabled as a result of failing the switch's self-test on its port.
Disabled-violation	This port is disabled because of an address violation. In this case, the port must be manually re-enabled.
Reset	This port is in reset state.

This status information will appear on the **Port Settings** menu and will apply only to the port listed at the top of the console screen.

• Full duplex

Disabled by default on 10BaseT ports. 100-Mbps ports have an additional parameter here, allowing you to choose one of four data transfer methods: Full duplex, half duplex, Full duplex with Flow Control, or Autonegotiate. 100BaseX ports default to Autonegotiate; 100BaseFX ports default to half duplex.

The next three options apply to Spanning Tree only:

• Port priority

This option allows you to place a higher or lower priority on a given port. The default is 128, and as the number goes down, the priority goes up. For instance, if you had a file server on port 2 and a workstation on port 3, you could set the priority of port 2 to 50 and port 3 to 150. This would give the server three times the priority of the workstation.

Š	 	

• Path cost

This option is used by STP to determine which interface has more available bandwidth as compared to another. There is an inverse relationship between the path cost number and available bandwidth, so the lower the path cost number, the higher the bandwidth available. If a loop occurs, higher path cost ports are closed first.

• Port Fast mode

This option changes the mode of the port from blocking to forwarding instantaneously. Port Fast accomplishes this by eliminating the forward delay. You will recall that forward delay is the amount of time it takes for a port to change from STP listening and learning states to the forwarding state.

For 100-Mbps ports, there is the additional option of Enhanced Congestion Control (ECC) available on half-duplex ports. ECC enables a port to empty its queue more quickly, reducing congestion on the switch and decreasing the chance of dropped packets. ECC can also be set on 10-Mbps ports, but only on a global basis. The 10-Mbps configuration for ECC is accomplished using the **System Configuration** menu.

NOTE: Port addressing and port statistics submenus are addressed in the upcoming sections.

The rest of the menu options on the **Port Configuration** menu are for navigation between menus. **Next port** takes you to the next numbered (ordinal) port, and **Previous port** to the previous port. **Goto port** allows you to skip to the port you specify.

Port Addressing Menu

In order to display the **Port Addressing** submenu, you must first select the port for which you want to make changes. The following displays when you select **A** from the **Port Configuration** menu:

```
Identify Port: 1 to 24[1-24], [AUI], [A], [B]:
Select [1 - 24, AUI, A, B]:
```

Once you've chosen a port, you will see a menu similar to the following:

```
Catalyst 1900 - Port 1 Addressing
 Address : Dynamic 00-C0-4F-79-EF-A9
----- Settings
[T] Address table size
                                          Unrestricted
[S] Addressing security
                                          Disabled
[K] Clear addresses on link down
                                          Disabled
[U] Flood unknown unicasts
                                          Enabled
[M] Flood unregistered multicasts
                                          Enabled
----- Actions -----
[A] Add a static address
[D] Define restricted static address
[L] List addresses
[E] Erase an address
[R] Remove all addresses
[C] Configure port [V] View port statistics
[N] Next port [G] Goto port
[P] Previous port [X] Exit to Main Menu
```

Enter Selection:

The dynamic address on the preceding menu denotes the number of unicast addresses the port has learned. In this case, it is one number, as only one station is connected on that port. The dynamism of this addressing is that it will change automatically when another PC is connected to this port. In turn, this updates the switch's Address table.

If we had assigned unicast addresses to this port, we would see an IP address next to the Address field at the top of the preceding menu.

The settings for the port include the following options:

Address table size

Allows you to set the size of the Address table for this port if it is a secure port. A secure port can have 1 to 132 MAC addresses in its Address table. A standard port is set to 0 for this parameter.

• Addressing security

This creates secure ports. When enabled, it allows you to restrict the use of this port to only the stations you specify by MAC address. The switch will forward no packets from this port other than those from specified source addresses. Since each address allowed to send on this port must be specified, you cannot change the size of the Address table (except, of course, by adding more MAC addresses to it!). Securing a port is good from a security and tracking standpoint, in that no user can connect to your network through a secure port without your prior authorization. Also, users cannot move workstations from one port to another. Another advantage of secure ports is dedicated bandwidth. A station connected to a 10-Mbps port with its MAC address as the only one allowed on that port gets the entire 10 Mbps. For even higher security environments, you can set the **Clear addresses on link down** menu option once addressing security is enabled. This automatically clears the address associations when the link is lost.

• Flood unknown unicasts

This is an option that can prevent unknown unicast packets from being forwarded to this port. The default is that unknown unicast packets are *not* forwarded to the port. If you are enabling flood unknown unicasts, you may wish to have that particular port assigned so that *all* unknown unicast packets are forwarded through that port. This would be similar to the gateway of last resort on a router.

• Flood unregistered multicasts

This is enabled by default, allowing unknown unregistered multicast addresses forwarded on this port. In high security environments, or environments where few multicast groups exist, you may wish to disable this option on many ports. The Actions section for the port includes the following options for maintaining the address list:

• Add a static address

Allows you to add a static MAC address for this port. This address will then be recognized as registered until it is manually removed. The address is entered in six hexadecimal octets, with or without spaces. This address can be only a unicast address; attempts to add a multicast or broadcast address will cause the system to produce an error message.

• Define restricted static address

A restricted static address can be either a unicast or multicast address, and is also entered as six hexadecimal octets, with or without spaces. After entering this address, you are prompted for port numbers that are allowed to send to this address. All other ports that forward to this restricted static address are implicitly denied.

List addresses

Allows you to list all of the addresses associated with this port. This includes static and dynamic addresses.

• Erase an address

Allows you to erase one of the addresses. This works on both static and dynamic addresses.

• Remove all addresses

Clears both static and dynamic addresses on that port.

The remaining commands are primarily for navigation. Next port, Goto port, Previous port, and Exit behave exactly as they would on the previous menu. The Configure port option takes you to the Port Configuration menu, and the View port statistics option shows different statistics for the port. The port statistics report is shown in the next section.

Port Statistics Detail Menu

The Port Statistics Report displays when you select **V** from the **Port Addressing** menu. It shows a number of statistics for the port you choose, and appears much like the following:

Catalyst 1900 - Port 1	Statis	tics Report					
Receive Statistics		Transmit Statistics					
Total good frames	158		1714				
Total octets	9477	Total octets	114121				
Broadcast/multicast frames	152	Broadcast/multicast frames	1709				
Broadcast/multicast octets	28683	Broadcast/multicast octets	113391				
Good frames forwarded	158	Deferrals	0				
Frames filtered	0	Single collisions	0				
Runt frames	0	Multiple collisions	0				
No buffer discards	0	Excessive collisions	0				
		Queue full discards	0				
Errors:		Errors:					
FCS errors	0	Late collisions	0				
Alignment errors	0	Excessive deferrals	0				
Giant frames	0	Jabber errors	0				
Address violations	0	Other transmit errors	0				
Select [A] Port addressing		onfigure port					

: [A] Port addressing, [C] Configure port,

[N] Next port, [P] Previous port, [G] Goto port,

[R] Reset port statistics, or [X] Exit to Main Menu:

This screen is generally helpful in diagnosing problems with a particular port.

Monitoring Menu

Monitoring a switch is the best way to tune it for your environment and also assists in ongoing fault isolation. The Catalyst 1900 offers configuration of monitoring directly through the console port, in-band through one of the network ports, or remotely using a modem or the Internet.

In order to isolate failures and potential problems, the **Monitoring Configuration** menu is of considerable value. From this menu, you can capture traffic or monitor activity.

Enter Selection:

The monitoring offered by the 1900 is more flexible than in the past. Three options from this screen are required for monitoring to function.

- 1. The **Capturing frames to the Monitor** option must be set to "Enabled". This is the global setting that allows ports to be monitored.
- 2. The **Monitor port assignment** option must be set. The Monitor port is the switch port that is to receive the captured frames. The monitoring port can't be a member of multiple bridge groups, nor can this port's bridge group membership be changed until monitoring is disabled.
- 3. You must select Add ports to capture list and set the options for the ports.

Ĵ	

Virtual LAN Configuration Menu

One of the most advanced features of the Catalyst 1900 is Virtual LAN configuration. Recall from earlier in this course that Virtual LANs, or VLANs, consist of machines grouped together by means of logical assignment rather than physical connection.

The Virtual LAN Configuration menu is shown here.

```
Catalyst 1900 - Virtual LAN Configuration
----- Information -----
VTP version: 1
Configuration revision: 0
Maximum VLANs supported locally: 1005
Number of existing VLANs: 5
Configuration last modified by: 0.0.0.0 at 00-00-0000 00:00:00
----- Settings -----
[N] Domain name
                 Server
[V] VTP mode control
[F] VTP pruning mode
                        Disabled
[O] VTP traps
                        Enabled
----- Actions
[L] List VLANs
                        [A] Add VLAN
[M] Modify VLAN
                        [D] Delete VLAN
[E] VLAN Membership
                        [S] VLAN Membership Servers
[T] Trunk Configuration
                        [W] VTP password
[P] VTP Statistics
                         [X] Exit to Main Menu
```

Enter Selection:

From this screen, as well as from the command-line interface (CLI), you can configure management domains, trunking, and VLANs. The first task is to configure the Management domain.

Previously in this course, we defined a Management domain as the grouping mechanism for VLANs. The Management domain defines administrative responsibility for VLANs. In the entry-level Catalyst 1900, only one Management domain is supported per switch. The switch is capable of operating in one of three VLAN Trunking Protocol (VTP) modes: Transparent mode, Server mode, or Client mode. In VTP Transparent mode, the switch gets its VLAN configuration information manually. The **Virtual LAN Configuration** menu is one method for entering VLAN information. This information can also be entered from CLI or through the VLAN Trunking Protocol Management Information Base (VTP MIB).

When a trunk port is configured on a switch and no Management domain is configured, the switch is in VTP Server mode. In VTP Server mode, the switch receives advertisements from other VTP devices on the configured trunk port and sends out its own advertisements over the trunk port to other VTP-capable devices. The switch learns information about VLANs on other devices. The main difference between this mode and VTP Client mode is that in Client mode, VLAN information cannot be modified through the MIB or through the console.

In VTP Client mode, the switch does not store VLAN information in NVRAM, so it loses its VLAN configuration when shut down. In VTP Server mode, although the computer learns information about other VLANs from receiving their traffic, the information is stored in NVRAM. Also, you can alter VLAN information from the console or MIB in VTP Server mode, but not in VTP Client mode.

In VTP Client or Server mode, with no Management domain configured, the switch receives its VLAN configuration information through the trunk port, if present. Through this information, the switch obtains a Management domain name and a configuration revision number. The configuration revision number represents the latest version of the VTP configuration, according to the switch it came from.

However, if you define a Management domain on your switch, the trunk port will ignore the advertisements it receives on the trunk port that have a different Management domain name or a lower configuration revision number. It picks up the advertisements it receives on the trunk port that match the Management domain name. The switch then determines whether to forward the advertisements based on a consistency check of the information in the advertisement. If the information is consistent, the advertisement is then forwarded, and the learned information is placed in the switch's local address list. **VTP pruning mode** and **VTP traps** are the two other options affecting VTP performance. VTP pruning keeps broadcasts, multicasts, and unicast flooding restricted to only those trunk links necessary for transport. This has a positive impact on available bandwidth. VTP traps are SNMP traps for monitoring the performance of VTP. The traps that will be sent when enabled are MTU Too Big errors, Configuration revision error, or Digest error.

Virtual LAN Configuration Requirements

Before you can configure a virtual LAN, you must have the following parameters ready for configuration:

• VLAN number

This is the ordinal that uniquely identifies a VLAN and must be between 1 and 1,005 (inclusive). VLAN 0, the default VLAN to which all switch ports belong, cannot be used here.

VLAN name

This is a common name you need to give the VLAN. Each VLAN must have a unique name within its management domain.

• VLAN type

This can be Ethernet, FDDI, Token Ring, FDDI-Net or Token-Ring-Net. The two types with the -Net suffix are for Parent VLAN use only, when bridging FDDI or Token-Ring VLANs.

• MTU (Maximum Transmission Unit)

As described, this specifies the maximum size of a packet in bytes.

• VLAN state

This can be either enabled or suspended. All traffic on the switch for that VLAN is blocked when the VLAN is suspended.

• 802.10 SAID

This represents the IEEE 802.10 Security Association IDentifier for the VLAN.

• Translational Bridge

If you are bridging between two VLANs that are different types (i.e., Ethernet to Token Ring), you must set a VLAN identifier for the transitional bridged VLAN.

• Ring number

This parameter is valid for FDDI or Token Ring. If source routing is used in Token Ring, this parameter is required for routing.

Parent VLAN

A Parent VLAN can be of the FDDI-Net or Token-Ring-Net variety. This parameter refers to the VLAN ID number of the Parent VLAN. In the setup listed later in this chapter, the VLAN type must be chosen as FDDI-Net or Token-Ring-Net.

• Bridge number

This is another parameter used only in FDDI-Net and Token-Ring-Net configurations. The VLAN in this case must have a bridge number that also comes from the Parent VLAN.

• STP type

This parameter is either IBM or IEEE. IEEE is only used for Parent VLANs with FDDI-Net or Token-Ring-Net.

Once you have all of these parameters considered and their values defined, you can configure your VLAN.

On the Actions section of the **Virtual LAN Configuration** menu, there are several options. These options allow you to configure VLANs, trunks, and VTP parameters.

• List VLANs

This shows you a list of configured VLANs on this switch. When the command to list VLANs is issued, you are presented with the following screen:

This command displays a list of specified VLANs. You may specify a list of VLAN numbers to display. A VLAN number ranges between 1-1005. XB1 and XB2 in the display stands for Translational Bridge 1 and 2.

VLAN numbers should be separated by commas or spaces. A VLAN number range may also be specified. The word ALL indicates all configured VLANs. Example: 1, 2, 10-20, all

Enter VLAN numbers:

Ď	 	 	 	

In order to view the statistics on your VLANs, you must specify which VLANs to display.

Add VLAN

This allows you to add one of the following five types of VLANs:

- Ethernet
- o FDDI
- o Token Ring
- o FDDI-Net
- o Token-Ring-Net

When you have selected the type of VLAN from the choices listed, the VLAN is created. The two screens that follow illustrate the process.

```
This command selects the type of VLAN to be added.
The following VLAN types can be added:
[1]Ethernet, [2]FDDI, [3]Token-Ring, [4]FDDI-Net, or
[5]Token-Ring-Net
Select a VLAN type [1-5]: Ethernet
```

Once you've chosen the VLAN type as Ethernet, the following screen displays:

Catalyst 1900 - Add Ethernet VLAN ----- Settings -----[N] VLAN Number 2 [V] VLAN Name **VLAN0002** [I] 802.10 SAID 100002 [M] MTU Size 1500 [L] Translational Bridge 1 0 [J] Translational Bridge 2 0 [T] VLAN State Enabled [S] Save and Exit [X] Cancel and Exit

Enter Selection:

Note that the VLAN is automatically given a name, a Security Association ID (SAID), and is ready to be enabled. The Catalyst 1900 will default to the settings for MTU size if the MTU size has previously been specified under the system menu. Also note that both of the Translational Bridge numbers are 0, which is a default when no transitional bridges are defined. Selecting **S** from this menu will save the configuration of this VLAN.

• Modify VLAN

Allows you to make changes to a previously configured VLAN, regardless of whether the VLAN is enabled. It is important to note that changes made to a VLAN happen immediately. It is therefore a good idea not to make changes to a VLAN while it is in use, unless these changes are absolutely necessary.

• Delete VLAN

Allows you to delete a VLAN. As with **Modify VLAN**, it is not recommended that you do this to a functional production VLAN.

• VLAN Membership allows you to assign ports to a given VLAN. The VLAN must have been previously configured in order to assign ports to it.

The VLAN Membership Configuration submenu also allows you to determine whether membership in a VLAN is static or dynamic with regard to that port. In dynamic membership, the port will automatically be assigned to VLAN 0, and can therefore be assigned automatically to a VLAN on another switch if the port is trunked. A Static VLAN assignment, however, assigns a port to one or more VLANs on its own switch.

• VLAN Membership Servers

Allows you to view VLAN Query Protocol information and change the settings of VLAN Membership Policy Servers. You may list up to four servers, set the primary VMPS, and set the number of retries before changing servers. The Catalyst 1900 cannot function as a VMPS server on the network.

<u></u>	

Trunk Configuration

Allows you to choose one of the two trunk ports (A or B) on the switch in order to configure it for trunking or check its trunking status. Upon choosing T from the **Virtual LAN Configuration** menu, you are prompted to select A or B. Upon selecting A, you are presented with the following screen:

```
Catalyst 1900 - Trunk A Configuration Menu
 Trunking status: Off Encapsulation type: Unknown
----- Information -----
Transmit Flood traffic to VLANs
                                N/A
Receive Flood traffic from VLANs
                                N/A
Allowed VLANs
                                 1-1005
Pruning Eligible VLANs
                                2-1001
----- Settings
[T] Trunking
                                Off
 ----- Actions
[S] List VLANs that Transmit Flood traffic
[R] List VLANs that Receive Flood traffic
[V] List Allowed VLANs
[F] List Pruning Eligible VLANs
[A] Add Allowed VLAN(s) [E] Add Pruning Eligible VLAN(s)
[D] Delete Allowed VLAN(s) [C] Delete Pruning EligibleVLAN(s)
[N] Next Trunk [P] Previous Trunk [X] Exit to Vlan Menu
```

Enter Selection:

This screen shows the trunking status and allows you to change its parameters. In this case, trunking is "Off" for the port, so no statistics are shown. In the Actions section, you can specify which VLANs are pruning eligible (more than likely the VLANs that are for local traffic only, if any). You can also add to your Catalyst 1900's list of VLANs that either receive or transmit flood traffic (opposite of pruning eligible).

Three navigation choices (**N**, **P**, and **X**) allow you to navigate between trunks more easily or exit this screen.

VTP password

Enables you to change and maintain the VTP password. The VTP password is used to decipher/encipher VTP messages. The text of the VTP password console output appears as follows:

This command assigns or re-assigns the VTP password. The VTP password is used to generate a secret value. The secret is used in the calculation of MD5 digest of VTP advertisements. The MD5 digest ensures the validity of VTP advertisements. The range of VTP password length supported is 1 to 64 characters. However, for security reasons it is recommended that VTP password should have a minimum of 8 characters and a maximum of 64 characters. The password is case sensitive and can contain any character with a legal keyboard representation.

```
Current setting ===>
```

New setting ===>

As shown, the VTP password is used by the switches and routers on the network to determine the validity of VTP advertisement packets. If no password is set, this information is not encrypted.

VTP Statistics

This shows you an overview of VTP activity.

The **VLAN Configuration** menu can be an invaluable tool when configuring VLANs on your switch. The beauty of the menuing system is that you need not commit hundreds of commands and option switches to memory in order to configure the switch for Virtual LAN operations.

Multicast Registration Menu

Multicasting is a common method for reducing broadcast traffic, and hence increasing performance, across your network. The Catalyst 1900 supports multicast registration, using multicast addresses with Internet Group Multicast Protocol (IGMP) and IP multicast.

Recall that a multicast address is a network address that enables limited broadcast to only a certain subset of a network. Stations that recognize the multicast address portion of a MAC address can direct that traffic only to the stations affected, those that are part of a recognized multicast group.

In order for a multicast group to be recognized by the Catalyst 1900, it must be registered manually at the **Multicast Registration** screen or via the command line. The **Multicast Registration** screen appears as follows:

The multicast addresses you register must be associated with certain frames that you designate as part of this multicast group. You are prompted for a 6-octet hexadecimal address, then for the port or ports to which frames with this multicast address should be forwarded.

Firmware Menu

Like most Cisco devices, the Catalyst 1900 is firmware upgradeable. Updates to the switch IOS can be applied from a TFTP server, from an IP address, or from a host PC connected to the console port or one of the in-band ports.

Unlike the CLI methods of upgrade, the menu-driven upgrade process of the Catalyst 1900 is straightforward and easy to use. The console screen that allows you to upgrade and manage the firmware on your switch is shown as follows:

Enter Selection:

The firmware upgrades occur similarly to those for Cisco routers as described previously in this course. The difference is that a switch generally has a smaller update file or firmware image to download. Also, the switch offers a convenient feature that allows it to *listen* for available upgrades.

RS-232 Interface Menu

The configuration of the RS-232 interface is one of the most important configurations on the switch. Your initial connection to your new switch will almost invariably be through the RS-232 console interface, and so its configuration is compulsory to the rest of the configuration of your Catalyst 1900.

The following screen is accessible via selection I from the Main menu.

Catalyst 1900 - RS-232 Interface Configuration	
[B] Baud rate	57600 baud
[D] Data bits	8 bit(s)
[S] Stop bits	1 bit(s)
[P] Parity setting	None
Settings	
[M] Match remote baud rate (auto baud)	Enabled
[A] Auto answer	Enabled
[N] Number for dial-out connection	
[T] Time delay between dial attempts	300
<pre>[I] Initialization string for modem</pre>	
Actions	
[C] Cancel and restore previous group settings	
[G] Activate group settings	
[X] Exit to Main Menu	

Enter Selection:

In this example, the Baud rate has been changed from the standard 9,600 bps to 57,600 bps.

It is possible to connect to the console port by attaching a modem to the supplied Cisco cable and adapter. By default, the switch ships with **Auto answer** enabled and **Match remote baud rate (auto baud)** enabled, so you can dial in to the switch and configure it remotely.

Usage Summaries Menu

Usage summaries allows you to see the performance of your switch in measurable, empirical terms. This can be very useful in isolation of faults, unfavorable trends, or inefficient use of bandwidth.

The Usage Summaries screen appears similar to the following:

Catalyst 1900 - Usage Summaries [P] Port Status Report [A] Port Addressing Report [E] Exception Statistics Report [U] Utilization Statistics Report [B] Bandwidth Usage Report [X] Exit to Main Menu

Enter Selection:

A

Once you've selected which report you would like to view, it is updated in real time, every 5 seconds, as you view it.

3

Help Menu

The Help system on the Catalyst 1900 is extensive and user friendly. It provides useful information for navigating throughout the menu system and is configurable to provide different levels of assistance.

From the Main menu, entering choice H yields the following:

The Management Console offers monitoring and configuration capabilities through the terminal/modem port provided for out-ofband management. The Management Console is comprised of various menu screens, from which menu commands can be selected. The first screen displayed after correct entry of a security password is the Main menu. From the Main menu, any one of the remaining screens may be accessed.

These screens include menus through which configuration of the switch may be modified, and menus which present conditions and statistics. Together, they fully describe the operating state of the switch.

The following simple and consistent rules are implemented for the Management Console menus:

Select [N]ext help screen, [S]et help level, or e[X]it to Main menu: N $% \left[X_{1}^{2}\right] =\left[X_{1}^{2}\right] \left[X_$

Selecting N yields the following screen.

- o Menu commands that configure the switch's operational parameters are shown with the current parameter values.
- o To select a menu command, simply type the letter in square brackets that precedes or follows the selection.
- o The carriage return key is required to terminate a command value input.
- o Typing only a return in response to a command value input cancels the input and leaves any currently set value unchanged.
- o The backspace key at the beginning of a value input clears any existing value. Otherwise, it erases the character previously typed.
- o Keyed input is case insensitive except where entered as a value for a descriptive string.
- o Typing a space bar or the return key on a menu refreshes the display of that menu.
- o Typing X on a menu always returns to the parent menu. Typing X returns to the logon prompt.

Select [P]revious help screen,[S]et help level,or e[X]it to Main Menu: At this time, you can set the level of help, as explained below:

The help level determines the amount of help information displayed whenever a Management Console command is invoked. When the help level is set to [N]ovice, a detailed command description is shown for every selected command. Conversely, very little information is shown when the help level is set to [E]xpert.

Help level may be set to [N]ovice or [E]xpert:

Current setting ===> Novice

New setting ===>

Changes made to the help level take effect immediately.

Ď	

Command-Line Menu

Option **K** from the **Main** menu takes you to the familiar Cisco IOS command-line interface, or the CLI. From the CLI, the commands available are a subset of those available on Cisco routers, but follow the same formats and conventions.

On our switch named blockhead, from Enable mode, we can query the available commands just as we would on a router, with a question mark. Such a query returns the following:

blockhead#?		
Exec commands:		
clear	Reset functions	
configure	Enter configuration mode	
сору	Copy configuration or firmware	
delete	Reset configuration	
disable	Turn off privileged commands	
enable	Turn on privileged commands	
exit	Exit from the EXEC	
help	Description of the interactive help system	
menu	Enter menu interface	
ping	Send echo messages	
reload	Halt and perform warm start	
session	Tunnel to module	
show	Show running system information	
terminal	Set terminal line parameters	
vlan-membership	VLAN membership configuration	

The prompt at the CLI appears just as it would on a router; the name of the router concatenated with a > sign for EXEC mode and the name of the router concatenated with a # for Privileged EXEC mode. For example, the previous screen output example was taken from a switch called *blockhead* at Privileged EXEC mode.

SUMMARY

In this chapter, you were introduced to the following concepts:

- LAN standards
- LAN encapsulation
- LAN switch configuration



Stop now and complete the following NEXTSim exercises on the Interactive Learning CD-ROM:

LAN Switching

Configure a Cisco Catalyst 1900 for VLAN Operation Configure Spanning Tree on a Cisco Catalyst 1900

POST-TEST QUESTIONS

The answers to these questions are in Appendix A at the end of this manual.

1. Name at least two methods for configuring a Catalyst 1900 switch.

.....

2. What is one term for marking a packet with an indicator field designating that packet as part of a Virtual LAN?

.....



3. What is the maximum number of 10BaseT ports that can be configured on a Catalyst 1900?

4. What network topology is specified by IEEE 802.5?
5. What are the five types of VLANs supported on the Cisco Catalyst 1900?

SELFSTUDY

Appendix A—Answers to Pre-Test and Post-Test Questions

CHAPTER 1

Pre-Test Answers

- 1. Routers do not possess hard drives, while personal computers do.
- 2. Ethernet ports are commonly connected to local area networks.
- 3. BRI ports are directly connected to ISDN lines.
- 4. Cisco router interfaces are commonly referred to as ports.

Post-Test Answers

- 1. Ethernet ports are typically connected to local area networks.
- 2. Serial ports are typically connected to high-speed serial devices.
- 3. A transceiver is typically directly connected to Ethernet ports on Cisco routers. This transceiver is then connected to an Ethernet hub.
- 4. BRI ports are typically connected to ISDN lines. Remember, a BRI port is actually a built-in ISDN modem.
- 5. The point where the telephone company's network meets the internal network is called the Point of Presence (POP).
- 6. Configuration of Cisco Routers is primarily concerned with the configuration of interfaces.

CHAPTER 2

Pre-Test Answers

- 1. An operating system is the software used to enable computer hardware to perform specific functions.
- 2. Cisco routers use the Cisco Internetwork Operating System.
- 3. The **help** command (?) is used to display a list of all available User Exec commands.
- 4. The **configure terminal** command is used to enter Global Configuration mode from the Privileged Exec mode.

Post-Test Answers

- 1. The **enable** command is used to enter the Privileged Exec mode from the User Exec mode.
- 2. The help command ? is used to display a list of all available User Exec commands.
- 3. The **banner motd** command is used to configure the message of the day.
- 4. Use the up arrow or the *CONTROL+P* keys to repeat the last command entered.
- 5. The global configuration command **hostname** is used to change router identification.
- 6. The command **show startup-config** is used to examine the configuration file in NVRAM.

CHAPTER 3

Pre-Test Answers

- 1. Cisco routers use the Internetwork Operating System (IOS).
- 2. The IOS is stored in Flash RAM.
- 3. The Cisco Discovery Protocol is used to display information about directly connected Cisco routers.
- 4. The global configuration command **enable password** *is* used to set an enable password.

- 1. The **show cdp neighbors** command is used to display information about directly connected routers.
- 2. The **copy running-config tftp** command is used to back up the running configuration of a router.
- 3. The **copy startup-config tftp** command is used to back up the startup configuration.
- 4. TFTP stands for Trivial File Transfer Protocol.
- 5. No, TFTP does not support authentication.
- 6. After passwords are set on console or vty lines, the login command is used to specify the port requires a login password.

CHAPTER 4

Pre-Test Answers

- 1. A router is a Network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded.
- 2. Privileged mode provides all of the commands found under User mode and includes an extended set of commands for examination of the router status.
- 3. You should be in Privileged mode to copy a running-config-startup-config.
- 4. To configure a port on a Catalyst 5000 switch, type "slot/port".

- 1. show memory config
- 2. copy config
- 3. ipx routing ip routing
- 4. Network
- 5. False
- 6. C. Router1(config)#int ser 0

CHAPTER 5

Pre-Test Answers

- 1. It is reccomended to back up any operating system for disaster recovery purposes.
- 2. A Trivial File Transfer Protocol server is used to back up and restore Cisco files.
- 3. Yes, providing a copy of the IOS file has been backed up to a TFTP server.
- 4. False. Configuration files stored on a TFTP server are not secured using password authentication.
- 5. This ACE will permit packets from the subnet 10.10.2. The destination address must be 10.20.1.1.

- 1. The **show version** command is used to verify configuration registry settings prior to reload.
- 2. The configuration registry setting 0x101 is used to boot the router into ROM monitor mode.
- 3. The "2" instructs the router to use the configuration files stored in NVRAM. The "101" instructs the router to boot using the IOS stored on the ROM chip.
- 4. The Router1(boot) prompt designates the router has booted from the IOS stored on the ROM chip.
- 5. This ACE will permit packets with any source address. The header must specify TCP and the destination address must match 10.10.1.1 port 23.
- 6. The command no debug {option} is used to turn debugging options off.
- 7. Pinging a well-known Internet site and then using the command **show ip route** using the returned IP address of the well-known site is one way to check for correct router operation following an IOS upgrade.

CHAPTER 6

Pre-Test Answers

- 1. 802.3
- 2. Bits
- 3. No packet collisions, higher reliability, or reduced errors
- 4. Yes, it can support fiber optic, Category 5 STP, and UTP.

- 1. Manually by direct-connected console; downloading an image from a TFTP server; using a configuration script; in-band using a PC or management station; using the menu-driven interface; or using the CLI
- 2. Tagging, 802.1q tagging, or Q-tagging
- 3. 25; 24 ports on the front plus the AUI port on the back
- 4. Token Ring
- 5. Ethernet, Token Ring, FDDI, Token-Ring-Net, and FDDI-Net



AARP broadcast

Broadcasts to all stations on an AppleTalk network to match hardware addresses to logical destination addresses for packets.

Access list

A list of conditions called permit and deny statements that help regulate traffic flow into and out of a router.

Address Resolution Protocol (ARP)

A TCP/IP protocol used to map IP addresses to node hardware addresses.

Agent

Software watchdog used by SNMP to keep an eye on network processes.

ANDing

A method used by the router in which it compares or ANDs an IP address with its subnet mask to determine the network address.

AppleTalk

A routable networking architecture developed by Apple that provides network services to Apple Macintosh computers.

AppleTalk Address Resolution Protocol (AARP)

A Network layer protocol that resolves AppleTalk network addresses to hardware addresses. AARP sends broadcasts to all stations on the network to match hardware addresses to logical destination addresses for packets.

Area

A subset of an internetwork containing several member routers. When several areas are grouped into a higher-level subset, this organizational level is called a routing domain.

Asynchronous communication

Serial data transfer connections that rely on start and stop bits to make sure that the data is completely received by the destination device.

Asynchronous Transfer Mode (ATM)

An advanced packet-switching protocol that uses fixed packet sizes (53 bytes) called cells to increase the throughput of the data transfer. Typically run over high-speed fiber optic networks.

Attenuation

The degradation of the data signal over the run of the cable.

Autonomous system

Internet (TCP/IP) terminology for a collection of gateways (routers) that fall under one administrative entity and cooperate using a common Interior Gateway Protocol (IGP).

Bandwidth

- 1. The range of frequencies that can be transmitted through a particular circuit.
- 2. The speed at which data travels over a particular media. Bandwidth is measured in bits per second.

Banner

A message that appears on the login screen of a router on a router console or virtual terminal.

Baseband

A transmission that uses a single bit stream over the entire bandwidth available.

Beaconing

A Token Ring fault tolerance strategy where nodes on the ring can determine the state of the network in cases where cable failure has taken place or there is a problem with a neighbor down stream on the ring.

Border Gateway Protocol (BGP)

A commonly used routing protocol for interdomain routing. It is the standard EGP for the Internet. BGP handles the routing between two or more routers that serve as the border routers for particular autonomous systems.

Border router

A router used to connect autonomous systems.

Bottleneck

A device that is slowing network traffic.

Breakout box

A device used to determine whether you are getting a signal from the CSU/DSU connected to a router.

Bridge

Internetworking device that operates at the Data Link layer of the OSI Model. Bridges are used to segment networks that have grown to a point where the amount of data traffic on the network media is slowing the overall transfer of information.

Broadcast storms

A condition caused when broadcast traffic from devices on an Ethernet network overwhelms it with messages bringing down the network.

Bus network

A network topology characterized by a main trunk or backbone line with the networked computers attached at intervals along the line.

Cable range

A network designation for an AppleTalk network segment assigned by the network administrator. Cable ranges can consist of a single number designating one network on the network wire or it can be a range of network numbers specifying a number of networks on the same wire.

Campus

A portion of an internetwork that is made up of several connected LANs as one location.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

A network access strategy used by AppleTalk. A device that is ready to send data out onto the network will notify the other network nodes of its intention to place data on the network.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

A network access strategy used by Ethernet networks. If a node sending data detects that there has been a collision, it will wait to resend the data until the line is determined to be free of other data.

Cell

A packet of fixed size used by Asynchronous Transfer Mode.

Channel Service Unit/Digital Service Unit (CSU/DSU)

A device that connects LAN equipment such as a router to digital phone lines.

Circuit switching

A connectivity strategy where a dedicated connection is established between the sender and receiver on a switched network (such as the Public Switched Telephone Network). Data moves from the source to the destination along the circuit (the lines) that has been established for the particular session.

Cisco Discovery Protocol (CDP)

A Cisco proprietary protocol that operates between layer 2 and 3 of the OSI model that is used to provide information related to neighboring routers.

Class A

Large IP networks that supply more than 16 million node addresses for the network.

Class B

Large- to medium-sized IP networks that supply more than 65,000 node addresses.

Class C

Small IP networks that only provide 254 node addresses.

Class D

A class of IP network addresses used by multicast groups receiving data on an internetwork from a particular application or server service. An example of a multicast use of Class D addresses is Microsoft NetShow, which can broadcast the same content to a group of users at one time.

Class E

IP addresses that belong to an experimental class and are unavailable for general use.

Client

A computer on the network that is logged in by and receives services (such as printing or file access) from a server computer.

Clock ticks

A metric used by the IPX Routing Information Protocol. A tick is 1/18 of a second.

Command-Line Interface (CLI)

The interface provided by the Cisco IOS on a router console or virtual terminal that allows you to enter the various IOS commands.

Configuration mode

The router mode that enables you to configure the router configuration using global commands and specific interface-related commands.

Convergence

The time it takes for all routers on the network to be up to date in terms of the changes that have taken place in the network topology. The longer it takes for all routers on the internetwork to converge, the greater the possibility that packets will be routed to routes that are no longer available on the network.

Cyclic Redundancy Check (CRC)

The Data Link layer makes sure that frames sent over the physical link are received error free. Protocols operating at this layer will add a trailer on each frame called a CRC check. Basically this is a mathematical calculation that takes place on the sending computer and then on the receiving computer. If the two CRCs match up then the frame was received in total and its integrity was maintained during transfer.

Data Circuit Terminating Equipment (DCE)

Equipment that provides a connection between the network and the switched network. The DCE often provides clocking information to synchronize the communication between the network termination equipment (such as a DTE) and the switched network.

Data link broadcasts

Broadcast messages used by CDP to discover neighboring Cisco routers that are also running CDP.

Data Link Connection Identifier (DLCI)

A reference or pointing device that makes sure that packets sent over a switched network, such as Frame Relay, end up at the proper destination. This is done by mapping the logical addresses (IP addresses, for example) of the sending and receiving routers to the DLCI of the virtual circuit that they use to communicate.

Datagram

Grouping of information in the data bit stream, a datagram is also referred to as a packet or frame.

Datagram Delivery Protocol (DDP)

An AppleTalk Network layer protocol that provides a connectionless datagram delivery system (similar to UDP in the TCP/IP stack).

DECnet

A network protocol stack developed by the Digital Equipment Corporation.

Default gateway

The address of the router interface a particular LAN is connected to. Every device on the LAN uses that connected router interface address as its default gateway.

Delay

The amount of time it takes to move a packet from the interface to the intended destination. Delay is measured in microseconds.

Deny statements

Statements in an Access list that deny traffic from certain networks or nodes to enter or exit a particular router interface.

Dial-up connection

The simplest and least expensive type of data transfer connection uses a modem to connect two computers or other devices over a regular analog voice-grade telephone line.

Digital Data Service (DDS)

Leased digital lines used for data communications. DDS lines include the T-Carrier system, which provides a range of line types and data transfer rates.

Digital Terminal Device (DTE)

The termination device for a data network and connects to DCE device, which provides a connection to a switched network.

Distance-vector routing algorithms

Routing algorithms that require the router to pass their entire routing table to their nearest router neighbors (routers that they are directly connected to). This basically sets up an update system that reacts to a change in the network like a line of dominoes falling.

DOD model

When TCP/IP was developed, the Department of Defense (DOD) developed its own conceptual model-the DOD model (also known as the DARPA model)-for how the various protocols in the TCP/IP stack operate.

Dynamic algorithms

Routing tables that are built dynamically by a routing protocol.

Encapsulation

The packaging of data in a particular protocol header. For example, Ethernet data is encapsulated in an Ethernet header before being placed on the network.

Ethernet

The most commonly deployed network architecture; it provides access to the network using CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Exec

The Cisco IOS uses a command interpreter to execute your commands (it interprets the command and then executes it). The User mode and the Privileged mode are considered different levels of the Exec.

Extended segment

An AppleTalk network segment that has been assigned a range of network numbers.

Exterior Gateway Protocol (EGP)

A routing protocol that provides the mechanism for the routing of data between routing domains. Border Gateway Protocol (BGP) is an example of an EGP.

Fiber Distributed Data Interface (FDDI)

An architecture that provides high-speed network backbones that can be used to connect a number of different network types. FDDI uses fiber optic cable, wired in a ring topology, using token passing as its media access method, operating at a data rate of at least 100 Mbps, and allowing long cable distances.

File Transfer Protocol (FTP)

TCP/IP Application protocol that provides the ability to transfer files between two computers.

Flash RAM

Flash is used to store the Cisco IOS that runs on the router. Alternative versions of the Cisco IOS on the Flash (such as an upgrade of your current IOS) can also be stored, which makes it very easy to upgrade the router.

Frame relay

A packet-switching WAN protocol that uses permanent virtual circuits for communication sessions between points on the WAN. These virtual circuits are identified by a Data Link Connection Identifier (DLCI), a value provided by the frame relay service provider.

Gateway

Used to connect networks that don't embrace the same network protocol and so protocol translation is necessary between the two disparate networks. For example, a gateway can be used as the connection between an IBM AS400 miniframe and a PC-based LAN.

Global commands

Self-contained, one-line configuration commands that affect the overall global configuration of the router. Examples are hostname and enable secret.

High-Level Data Link Control (HDLC)

A synchronous Layer 2 WAN transport protocol. The HDLC used on Cisco routers is a Cisco proprietary version.

High-order bits

The first 4 bits in any octet of an IP address (on the far left of the octet) are referred to as the highorder bits.

Hop count

A metric used by RIP. A hop is the movement of the packets from one router to another router.

Hub

1. A centralized connectivity device, especially in a star topology. The computers on the network connect to the hub.

2. A device operating at the Physical layer of the OSI Model that provides the central connection point for networks arranged in a star topology.

Integrated Services Digital Network (ISDN)

Digital connectivity technology used over regular phone lines. A device called an ISDN modem is used to connect a device to the telephone network. ISDN is available in Basic Rate ISDN (BRI) and Primary Rate ISDN (PRI).

Interface

The physical connection between the router and a particular network medium type; interfaces are also referred to as ports.

Interior Gateway Protocol (IGP)

A routing protocol that provides the mechanisms for the routing of packets within the routing domain. IGPs such as RIP or IGRP would be configured on each of the routers in the router domain.

Interior Gateway Routing Protocol (IGRP)

A distance-vector routing protocol developed by Cisco in the 1980s. IGRP uses a composite metric that takes into account several variables; it also overcomes certain limitations of RIP, such as the hop count metric and the inability of RIP to route packets on networks that require more than 15 hops.

International Standards Organization (ISO)

This global standard organization develops sets of rules and models for everything from technical standards for networking to how companies do business in the new global market. They are responsible for the OSI conceptual model of networking.

Internet Control Message Protocol (ICMP)

Used for error reporting and recovery, and is a required component of any IP implementation.

Internet Package Exchange (IPX)

A connectionless transport protocol that provides the addressing system for the IPX/SPX stack. Operating at the Network and Transport layers of the OSI Model, IPX directs the movement of packets on the internetwork using information that it gains from the IPX Routing Information Protocol (RIP).

Internetwork

When several LANs are connected. This is really a network of networks (this type of network can also be referred to as a campus).

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)

The NetWare proprietary network protocol stack for LAN connectivity. IPX is similar to TCP/IP in that the protocols that make up the IPX/SPX stack don't directly map to the layers of the OSI Model. IPX/SPX gained a strong foothold in early local area networking because IPX/SPX was strong on performance and didn't require the overhead that is needed to run TCP/IP.

Internetworking Operating System (IOS)

The Cisco proprietary operating system software that provides the router hardware with the ability to route packets on an internetwork. The IOS provides the command sets and software functionality that you use to monitor and configure the router.

Interrupt Request Line (IRQ)

A unique request line that allows a device to alert the computer's processor that the device connected to that IRQ requires processing services.

Intranet

A corporate network that is internal to the enterprise (not connected to the global Internet) but uses Internet protocols such as Simple Mail Transport Protocol and HyperText Transport Protocol (the protocol used by Web browsers) to share information among corporate users.

IP unnumbered

Serial interfaces on a router configured without IP addresses (they will still route IP packets even though they are designated as IP unnumbered).

IPX network number

The first part of the IPX address, which can be up to 16 hexadecimal characters in length. This part of the network.node address is 32 bits. The remaining 12 hexadecimal digits in the address make up the node address (which makes up the remaining 48 bits of the address).

IPX Routing Information Protocol (RIP)

A routing protocol that uses two metrics, clock ticks (1/18 of a second) and hop count, to route packets through an IPX internetwork.

Keepalives

Messages sent by network devices to let other network devices know that a link between them exists.

LAN interface

A router interface providing a connection port for a particular LAN architecture such as Ethernet or Token Ring.

Leading bits

The first 3 bits in an IP network address. Rules have been established for the leading bits in the first octet of each of the classes (A, B, and C). Class A addresses must have 0 as the first bit. In Class B addresses, the first bit of the first octet is set to 1 and the second bit is set to 0. In Class C addresses, the first two bits of the first octet are set to 1 and the third bit is set to 0.

Leased line

Dedicated phone providing a full-time connection between two networks through the PSTN or another service provider. Leased lines are typically digital lines.

Load

The current amount of data traffic on a particular interface. Load is measured dynamically and is represented as a fraction of 255, with 255/255 showing the saturation point.

Local Area Network (LAN)

A server-based network of computers that is limited to a fairly small geographical area, such as a particular building.

Local Management Interface (LMI)

The signaling standard used between a router and a Frame Relay switch. Cisco routers support three LMI types: Cisco, ANSI, and q933a.

LocalTalk

The cabling system used to connect Macintosh computers (it uses shielded twisted-pair cables with a special Macintosh adapter).

Logical interface

A software-only interface that is created using the router's IOS. Logical interfaces are also referred to as virtual interfaces.

Logical Link Control (LLC)

A sublayer of the Data Link layer that establishes and maintains the link between the sending and receiving computer as data moves across the network's physical medium.

Loopback interface

A software-only interface that emulates an actual physical interface and can be used to keep data traffic local that is intended for a hardware interface that is nonfunctioning.

Lower-order bits

The first 4 bits in any octet (counting from right to left) are referred to as the lower-order bits.

Media Access Control (MAC) Address

MAC addresses are burned onto ROM chips on network interface cards, giving each of them a unique address.

Mesh topology

A network design where devices use redundant connections as a fault-tolerance strategy.

Metric

The method routing algorithms use to determine the suitability of one path over another. The metric can be a number of different things, such as the path length, the actual cost of sending the packets over a certain route, or the reliability of a particular route between the sending and receiving computers.

Multistation Access Unit (MSAU)

Token Ring networks are wired in a star configuration with a MSAU providing the central connection for the nodes. The MSAU itself also provides the logical ring that the network operates on.

Name Binding Protocol (NBP)

A Transport layer protocol that maps lower-layer addresses to AppleTalk names that identify a particular network resource such as a printer server that is accessible over the internetwork.

Nearest Downstream Neighbor (NADN)

On a Token Ring network, an NADN would be the active node directly downstream from a particular node.

Nearest Upstream Neighbor (NAUN)

In a Token Ring network, a computer that passes the token to the next computer on the logical ring would be called the nearest active upstream neighbor, or NAUN.

Neighbors

Routers that are directly connected to a particular router by LAN or WAN connections.

NetBIOS Extended User Interface (NetBEUI)

A simple and fast network protocol that was designed to be used with Microsoft's and IBM's NetBIOS (Network Basic Input Output System) protocol in small networks.

NetWare Core Protocol (NCP)

An IPX/SPX protocol that handles network functions at the Application, Presentation, and Session layers of the OSI Model.

NetWare Link Service Protocol (NLSP)

A Novell-developed, link-state routing protocol that can be used to replace RIP as the configured routing protocol for IPX routing.

Network

A group of computers and related hardware that are joined together so that they can communicate.

Network Interface Card (NIC)

A hardware device that provides the connection between a computer and the physical media of a network. The NIC provides the translation of data into bits; sometimes referred to as an adapter.

Network Operating System (NOS)

Any number of server-based software products, such as Windows NT, Novell NetWare, and AppleTalk, that provide the software functionality for LAN connectivity.

Node

Any device on the network (such as a computer, router, or server).

Nonextended segment

An AppleTalk network segment that is assigned only one network number.

Nonvolatile RAM (NVRAM)

RAM that can be used to store the startup configuration file for the router. NVRAM can be erased, and you can copy the running configuration on the router to NVRAM. NVRAM does not lose its contents when the router is rebooted.

NT domain

A network managed by an NT server called the Primary Domain Controller.

Null interface

A software-only interface that drops all packets that it receives.

Octet

Eight bits of information; one portion of the four-octet IP address used on IP networks.

Open Shortest Path First (OSPF)

A link-state protocol developed by the Internet Engineering Task Force (IETF) as a replacement for RIP. Basically, OSPF uses a shortest-path-first algorithm that allows it to compute the shortest path from source to destination when it determines the route for a specific group of packets.

Open Systems Interconnection (OSI) Model

A conceptual model for networking developed in the late 1970s by the International Standards Organization (ISO). In 1984, the model became the international standard for network communications. It provides a conceptual framework (based on seven layers called protocol stacks) that helps explain how data gets from one place to another on a network.

Packet InterNet Groper (Ping)

An IP protocol used to test the connection between two or more nodes on a network. These nodes can be host computers, servers, or routers.

Packet switching

A wide area networking strategy where the bit stream of data is divided into packets. Each packet has its own control information and is switched through the network independently.

Peer-to-peer network

A local area network that operates without a server but allows connected computers to access shared resources such as files and printers.

Permit statements

Statements in an Access list that permit traffic from certain networks or nodes to enter or exit a particular router interface.

Point-to-Point Protocol (PPP)

A synchronous and asynchronous protocol that can provide WAN connections over a number of different connection types.

Port commands

A set of commands that enable you to specify a particular interface or controller for configuration; these commands must be followed by subcommands that provide additional configuration information.

Privileged exec mode

A complete access level to the router that enables you to view, save, and erase router configuration parameters and enter the Configuration mode for the router.

Protocol

The set of software-based rules that define how networked computers send and receive data.

Public Data Network or Private Data Network (PDN)

A packet-switching network operated by a service provider. PDNs provide WAN connectivity avenues for the connection of LANs at remote sites.

Public Switched Telephone Network (PSTN)

The telephone communication infrastructure provided by the Baby Bells.

Random Access Memory (RAM)

Similar to the dynamic memory you use on your PC, RAM provides the temporary storage of information (packets are held in RAM when their addressing information is examined by the router) and holds information such as the current routing table.

Read-Only Memory (ROM)

Memory chips that contain burned-in software instructions. Router ROM contains the Power-On Self-Test (POST) and the bootstrap program for the router.

Reliability

The ratio of expected-to-received keepalives.

Repeaters

Physical devices that take the signal received from network devices and regenerates the signal so that it maintains its integrity along a longer media run than is normally possible. Repeaters are also referred to as concentrators.

Ring topology

Networked computers connected one after the other on the wire in a physical circle. Ring topology moves information on the wire in one direction with each networked computer actually resending the information it receives onto the next computer in the ring.

Roll-over cable

The cable used to connect the console computer and the router.

Routable protocol

A networking protocol that provides the necessary layer 3 protocols for the routing of packets.

Router

Internetworking devices that operate at the Network layer (layer 3) of the OSI Model. Using a combination of hardware and software (Cisco routers use the Cisco IOS-Internetwork Operating System), routers are used to connect networks.

Router console

The computer serving as the router's dumb terminal. Used to view and enter configuration settings on the router.

Router Information Protocol (RIP)

A distance-vector routing protocol that uses hop count as its metric. RIP summarizes the information in the routing table by IP network numbers (also referred to as major network numbers).

Routing protocol

Protocols that provide the mechanism for a router to build a routing table and share the routing information with other connected routers.

Routing Table Maintenance Protocol (RTMP)

A Transport layer protocol that is responsible for establishing and maintaining routing tables on routers that have been enabled to route AppleTalk.

Running configuration

The router configuration currently running in the router's RAM.

Sequenced Packet Exchange (SPX)

A connection-oriented transport protocol in the IPX/SPX stack that provides the upper-layer protocols with a direct connection between the sending and receiving machines.

Serial adapters

Adapters provided with the router used to connect the roll-over cable to the COM port on a computer.

Serial interface

A router interface providing a connection port for various WAN technologies. A router port would typically be attached to a cable such as a V.35 cable that then attaches to a WAN DCE device.

Server

The provider of data communication resources to client machines on the network.

Server-based network

A network where client computers are authenticated on the network by a server computer. The server provides centralized file storage and other centralized services such as printing and other resources.

Service Access Point (SAP)

The LLC sublayer provides these reference points so that a computer sending data can refer to the SAPs when communicating with the upper-layer protocols of the OSI stack on a receiving node.

Service Advertisement Protocol (SAP)

A protocol that advertises the availability of various resources on the NetWare network.

Service Profile Identifier (SPID)

A number used to authenticate an ISDN channel to the switch that connects the ISDN-enabled device to the phone system. Each channel must have a different SPID number.

Session

A transaction between networked nodes.

Share-level security

Typically used in peer-to-peer networks, each shared resource requires a password for access.

Simple Mail Transport Protocol (SMTP)

TCP/IP Application layer protocol that provides mail delivery between two computers.

Simple Network Management Protocol (SNMP)

A TCP/IP Application layer protocol that can be used to monitor the health of an internetwork. SNMP uses software agents that report back on a particular measured parameter related to the network.

Star topology

A network design where all computers connect together at a central hub, each with its own cable.

Static algorithms

Internetwork mapping information that a network administrator enters into the router's routing table.

Static routing

Routing where the routing tables have been entered and updated manually by the network administrator.

Subcommands

Commands that provide specific configuration information for the interface or controller that is specified with a particular port command.

Subnet mask

A four-octet mask that is used to determine which bits in the IP address refer to the network address, which bits in the IP address refer to the subnet address, and which bits in the IP address refer to the node address.

Switch

A Layer 2 internetworking device that can be used to preserve the bandwidth on your network using segmentation. Switches are used to forward packets to a particular segment using MAC hardware addressing (the same as bridges). Because switches are hardware-based, they can actually switch packets faster than a bridge.

Switching

The routing of packets on a router from an incoming interface to an outgoing interface.

Synchronous communication

Serial connections that use a clocking device that provides the precise timing of the data as it moves from sending to receiving computer across a serial connection.

Synchronous Optical Network (SONET)

A fiber optic network developed by Bell Communications Research that provides voice, data, and video at high speeds.

Telnet

A terminal emulation protocol (part of the TCP/IP stack) that enables you to connect a local computer with a remote computer (or other device such as a router).

Terminal adapter

Also known as an ISDN modem, it is used to connect a node configured for ISDN to the phone system.

TFTP server

A computer running TFTP software that can be used for the saving of router configuration files. Files can be copied from the router to the TFTP server or from the TFTP server to the router.

Time Domain Reflectometer (TDR)

A device that can diagnose shorts and breaks in a cable and can also provide information on where the short or break exists on the cable.

Token Ring

A network architecture developed by IBM that is arranged in a logical ring and uses a token-passing strategy for network access. Token Ring can run at 4 or 16 Mbps. IBM developed and supports token-passing LANs.

Topology

Networks have a physical layout or topology that will reflect, for instance, the cable type used and the actual architecture of the network (such as ring, bus, mesh, or star topology).

Transmission Control Protocol (TCP)

A connection-oriented protocol that provides a virtual circuit between user applications on the sending and receiving machines on a TCP/IP network.

Transmission Control Protocol/Internet Protocol (TCP/IP)

A routable protocol stack that can be run on a number of different software platforms (Windows, UNIX, and so on) and is embraced by most network operating systems as the default network protocol.

Trivial File Transfer Protocol (TFTP)

A stripped-down version of FTP that provides a way to move files without any type of authentication (meaning no username or password).

Tunnel interface

A logical interface that can be used to move packets of a particular network architecture type over a connection that doesn't typically support these types of packets.

Uninterruptible Power Supply (UPS)

A device that will supply power to a computer device such as a router using a battery if the electricity is cut.

User Datagram Protocol (UDP)

A connectionless-oriented TCP/IP stack transport protocol that provides a connection between Application layer protocols that don't require the acknowledgements and synchronization provided by TCP.

User mode

The basic access level to the router, User mode commands allow you to examine the router's configuration but don't allow you to change any configuration parameters.

Virtual circuit

A defined route established across a WAN cloud so that all data packets move to the destination along the same route. The use of virtual circuits in packet-switching networks can improve the overall performance of data transfers.

Virtual Loadable Modules (VLMs)

Software modules that establish and maintain network sessions between the client and server on an IPX/SPX network.

Virtual terminal

A computer or router that uses telnet to access another router.

Voltmeter

A device that can be connected to a cable to test the cable for a break or a short.

WAN interfaces

Serial interfaces or special interfaces such as ISDN interfaces that are used for WAN connectivity.

Wide Area Network (WAN)

A group of connected campuses or internetworks that span large geographical areas.

Wildcard mask

A 32-bit mask used with IP addresses to determine which portion of the IP address should be ignored in the Access list's deny and permit statements.

X.121

A telephone standard's addressing scheme (also known as International Data Numbers) used by the X.25 WAN protocol that is comprised of one to fourteen decimal digits. This number identifies the local X.121 address for your serial interface and must be configured on the router that is being enabled for X.25.

Xerox Network System (XNS)

A network operating system developed at the Xerox Palo Alto Research Center in the 1960s. NetWare is based heavily on this early networking protocol stack.

Zone

A logical grouping of different AppleTalk physical network segments. Zones are logical groupings of users (similar to the concept of workgroups in Microsoft peer-to-peer networking).

Zone Information Protocol (ZIP)

A Network and Transport layer protocol that is used to assign logical network addresses to nodes on the network.

ACRONYMS

—A—

AAL	ATM Adaptation Layer
Abend	Abnormal end
ABR	Automatic Baud Rate Detection
ACDI	Asynchronous Communications Device Interface
ACE	Access Control Entry
ACF/VTAM	Advanced Communications Function/Virtual Telecommunications Access
ACK	Method
ACK	Acknowledgment Access Control List
ACPI	Advanced Configuration and Power Interface
ACSE	Association Control Service Element
AD	Administrative Domain
ADB	Apple Desktop Bus
ADMD	Administration Management Domain
ADO	ActiveX Data Objects
ADSP	AppleTalk Data Stream Protocol
AEP	AppleTalk Echo Protocol
AFP	AppleTalk Filing Protocol
AGP	Accelerated Graphics Port
AIFF	Audio Interchange File Format
ANI	Automatic Number Identification
ANSI	American National Standards Institute
AOW	Asia and Oceania Workshop
APA	All Points Addressable
API	Application Programming Interface
APM	Advanced Power Management
APPC	Advanced Program-to-Program Communications
ARA	AppleTalk Remote Access
ARP	Address Resolution Protocol
ARPA	Advanced Research Project Agency
ARPANET	Advanced Research Projects Agency Network
ARQ	Automatic Request for Retransmission
ASCII	American Standard Code for Information Interchange
ASD	Automatic Skip Driver Agent
ASMP	Asymmetric Multiprocessing
ASN.1	Abstract Syntax Notation One
ASP	Active Server Pages
ASP	AppleTalk Session Protocol
ATM	Asynchronous Transfer Mode
	i bynomonous fruibici ividut

	۵۳۳۵	AppleTally Transaction Protocol
	ATP	AppleTalk Transaction Protocol
	AUI	Attachment Unit Interface
	AUP	Acceptable Use Policy
_	AWG	American Wire Gauge
—B—	DDC	
	BBS	Bulletin Board System
	bcp	Bulk Copy Program
	BDC	Backup Domain Controller
	BER	Basic Encoding Rules
	BIOS	Basic Input/Output System
	BISDN	Broadband ISDN
	bit	Binary Digits
	BITNET	Because It's Time Network
	BNC	British Naval Connector
	BOC	Bell Operating Company
	Bps	Bytes per second
	bps	Bits per second
	BRI	Basic Rate Interface
	BSC	Binary Synchronous Communications
	BSD	Berkeley Software Distribution
	BTAM	Basic Telecommunications Access Method
—C—		
	CAP	Competitive Access Provider
	CATV	Community Antenna Television
	CBR	Constant Bit Rate
	CBT	Computer-Based Training
	CCITT	International Consultative Committee for Telegraphy and Telephony
	CCL	Common Command Language
	CCR	Commitment, Concurrency, and Recovery
	CCTV	Closed-Circuit Television
	CD-ROM	Compact Disc Read-only Memory
	CDF	Channel Definition Format
	CERN	European Laboratory for Particle Physics
	CERT	Computer Emergency Response Team
	CGA	Color Graphics Adapter
	CGI	Common Gateway Interface
	CICS	Customer Information Control System
	CIR	Committed Information Rate
	CISC	Complex Instruction Set Computer
	CIX	Complex Instruction Set Computer Commercial Internet Exchange
		0
	CLBS	Component Load Balancing Service
	CLNP	ConnectionLess Network Protocol

	CLTP	ConnectionLess Transport Protocol
	CMIP	Common Management Information Protocol
	CMOS	Complementary Metal Oxide Semiconductor
	СМОТ	CMIP Over TCP
	CN	Common Name
	СО	Central Office
	COM	Component Object Model
	CONP	Connection Oriented Network Protocol
	COS	Corporation for Open Systems
	COSINE	Cooperation for Open Systems Interconnection Networking in Europe
	CPE	Customer Premise Equipment
	CPI	Common Programming Interface
	cps	Characters per second
	CPU	Central Processing Unit
	CRC	Cyclic Redundancy Check
	CREN	Corporation for Research and Educational Networking
	CRT	Cathode Ray Tube
	CSMA	Carrier Sense Multiple Access
	CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
	CSMA/CD	Carrier Sense Multiple Access with Collision Detection
	CSNET	Computer Science Network
	CSP	Cryptographic Service Provider
	CSU	Customer Service Unit
	CU	Control Unit
•		
	DAC	Digital to Analog Converter
	DACS	Digital Access Cross Connects
	DARPA	Defense Advanced Research Projects Agency
	DAO	Data Access Objects
	DAV	Digital Audio Video
	DB2	IBM Data Base 2
	DBCS	Double Byte Character Set
	DBMS	Database Management System
	DBO	Database Owner
	DBOO	Database Object Owner
	DCA	Defense Communications Agency
	DCE	Distributed Computing Environment
	DCE	Data Communications Equipment
	DCOM	Distributed COM
	DD	Double Density
	DDE	Dynamic Data Exchange
	DDI	Device Driver Interface

—D—

DDL	Data Definition Language
DDM	Distributed Data Management Architecture
DDN	Defense Data Network
DDP	Datagram Delivery Protocol
DES	Data Encryption Standard
DET	Directory Entry Table
Dfs	Distributed File System
DFT	Distributed Function Terminals
DHCP	Dynamic Host Configuration Protocol
DHTML	Dynamic HTML
DID	Direct Inward Dial
DIMM	Dual, In-line Memory Module
DISA	Defense Information Systems Agency
DIX	Digital, Intel, Xerox
DLC	Data Link Control
DLCI	Data Link Connection Identifier
DLL	Dynamic-link library
DMA	Direct Memory Access
DMI	Digital Multiplexed Interface
DML	Data Manipulation Language
DNA	Distributed interNet Application
DNS	Domain Name System
DOS	Disk Operating System
dpi	Dots per inch
DQDB	Distributed Queue Dual Bus
DRAM	Dynamic Random Access Memory
DS	Data Set
DS	Double-Sided
DS1	Digital Signaling Level 1
DS2	Digital Signaling Level 2
DS3	Digital Signaling Level 3
DSA	Directory System Agent
DSDD	Double-Sided, Double-Density
DSE	Data Service Equipment
DSHD	Double-Sided, High-Density
DSP	Digital Signal Processor
DSU	Data Service Unit
DTC	Distributed Transaction Coordinator
DTE	Data Terminal Equipment
DTR	Data Terminal Ready
DTS	Data Transformation Service
DUA	Directory User Agent

	DVD	Digital Video Disc or Digital Versatile Disc
	DXF	Drawing Exchange Format
	DXI	Data Exchange Interface
—Е—		
	E-mail	Electronic mail
	EARN	European Academic and Research Network
	EBCDIC	Extended Binary-Coded Decimal Interchange Code
	ECF	Enhanced Connectivity Facilities
	ECP	Extended Capabilities Port
	EDI	Electronic Data Interchange
	EEHLLAPI	Entry Emulator High-Level Language Application Program Interface
	EFF	Electronic Frontier Foundation
	EGA	Enhanced Graphics Adapter
	EGP	Exterior Gateway Protocol
	EIDE	Enhanced IDE
	EMF	Enhanced Metafile
	EMS	Expanded Memory
	EPS or EPSF	Encapsulated PostScript File
	ER Model	Entity/Relationship Model
	ES-IS	End System-Intermediate System
	ESDI	Enhanced Industry Standard Architecture
	ESF	Extended Super Frame
	EUnet	European UNIX Network
	EUUG	European UNIX Users Group
	EWOS	European Workshop for Open Systems
—F—		
	FAQ	Frequently Asked Questions
	FARNET	Federation of American Research NETworks
	FAT	File Allocation Table
	FCB	File Control Block
	FCC	Federal Communications Commission
	FCS	Frame Check Sequence
	FDDI	Fiber Distributed Data Interface
	FEP	Front-End Processor
	FFAPI	File Format API
	FIPS	Federal Information Processing Standard
	FM	Frequency Modulation
	FNC	Federal Networking Council
	FPU	Floating Point Unit
	FQDN	Fully Qualified Domain Name
	FRICC	Federal Research Internet Coordinating Committee
	FT1	Fractional T1

	FT3	Fractional T3
	FTAM	File Transfer, Access, and Management
	FTP	File Transfer Protocol
	FYI	For Your Information
—G—		
Ū	GDI	Graphics Device Interface
	GIF	Graphics Interchange Format
	GOSIP	Government OSI Profile
	GUI	Graphical User Interface
—H—		
	HAL	Hardware Abstraction Layer
	HCSS	High Capacity Storage System
	HD	High Density
	HDLC	High-level Data Link Control
	HDX	Half-duplex
	HFS	Hierarchical File System
	HID	Human Interface Device
	HLLAPI	High-Level Language Application Program Interface
	HMA	High Memory Area
	HPFS	High Performance File System
	HTML	HyperText Markup Language
	HTTP	HyperText Transfer Protocol
	Hz	Hertz
—I—		
	IAB	Internet Activities Board
	ICM	Image Color Management
	ICMP	Internet Control Message Protocol
	IDE	Integrated Drive Electronics
	IEEE	Institute of Electrical and Electronics Engineers
	IESG	Internet Engineering Steering Group
	IETF	Internet Engineering Task Force
	IFS	Installable File System
	IGP	Interior Gateway Protocol
	IGRP	Internet Gateway Routing Protocol
	IIS	Internet Information Server
	IMHO	In My Humble Opinion
	INTAP	Interoperability Technology Association for Information Processing
	IONL	Internal Organization of the Network Layer
	IP	Internet Protocol
	IPX	Internetwork Packet Exchange
	IPXODI	Internetwork Packet Exchange Open Data link Interface
	IRC	Internet Relay Chat

	IrDA	Infrared Developers Association
	IRF	Inherited Rights Filter
	IRQ	Interrupt Request Lines
	IRTF	Internet Research Task Force
	IS-IS	Intermediate System-Intermediate System
	ISAPI	Microsoft Internet Server Application Programming Interface
	ISDN	Integrated Services Digital Network
	ISO	International Standards Organization
	ISODE	ISO Development Environment
	ISP	Internet Service Provider
	IXC	Inter-exchange Carrier
J		0
	JANET	Joint Academic Network
	JPEG	Joint Photographic Experts Group
	JUNET	Japan UNIX Network
—К—		
	KB	Kilobyte
	Kb	Kilobit
	KBps	Kilobytes per second
	Kbps	Kilobits per second
—L—		
	L2PDU	Layer Two Protocol Data Unit
	L3PDU	Layer Three Protocol Data Unit
	LAN	Local Area Network
	LAPB	Link Access Protocol Balanced
	LAPD	Link Access Protocol Device
	LAPS	LAN Adapter and Protocol Support
	LATA	Local Access and Transport Area
	LCD	Liquid Crystal Diode
	LDT	Local Descriptor Table
	LEC	Local Exchange Carriers
	LEN	Low Entry Networking
	LLAP	LocalTalk Link Access Protocol
	LMI	Local Management Interface
	lpi	Lines per inch
	LSL	Link Support Layer
	LU	Logical Unit
—M—		
	MAC	Media Access Control Sublayer
	MAN	Metropolitan Area Network
	MAP	Manufacturing Automation Protocol
	MAPI	Messaging API

—N—

MAU	Media Access Unit
MB	Megabyte
Mb	Megabit
MBps	Megabytes per second
Mbps	Megabits per second
MCGA	Multi-Color Gate Array
MDI	Multiple Document Interface
MHS	-
MHS	Message Handling System Megahertz
	0
MIB	Management Information Base
MIDI	Musical Instrument Digital Interface
MILNET	Military Network
MIME	Multipurpose Internet Mail Extensions
MIPS	Million Instructions Per Second
MLID	Multiple Link Interface Driver
MOO	Mud, Object Oriented
MPEG	Moving Pictures Experts Group
ms	Milliseconds
MSAU	MultiStation Access Unit
MTA	Message Transfer Agent
MTU	Maximum Transmission Unit
MUD	Multi-User Dungeon or Dimension
MVS	Multiple Virtual Storage
MVS-CICS	Multiple Virtual Storage-Customer Information Control System
MVS/TSO	Multiple Virtual Storage/Time-Sharing Option
NAK	Negative AcKnowledgment
NBP	Name Binding Protocol
NCC	NetWare Control Center
NCP	NetWare Core Protocol
NCP	Network Control Point
NCSA	National Center for Supercomputing Applications
NDS	NetWare Directory Services
NetBEUI	NetBIOS Extended User Interface
NetWare DA	NetWare Desk Accessory
NFS	Network File System
NIC	Network Information Center
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NLM	NetWare Loadable Module
NLQ	Near Letter Quality
NLSP	NetWare Link Services Protocol

	NMS	Network Management Station
	NNS	NetWare Name Service
	NNTP	Network News Transfer Protocol
	NOC	Network Operations Center
	NREN	National Research and Education Network
	NSAP	Network Service Access Point
	NSEPro	Network Support Encyclopedia Professional Volume
	NSEPro	Network Support Encyclopedia Professional Edition
	NSF	National Science Foundation
	NSFnet	National Science Foundation Network
	NT	Windows NT
	NT1	Network Termination 1
	NT2	Network Termination 2
	NTAS	Windows NT Advanced Server
	NTFS	New Technology File System
	NTP	Network Time Protocol
	NWADMIN	Network Administrator
—0—		
	OBS	Optical Bypass Switch
	ODI	Open Datalink Interface
	OHCI	Open Host Controller Interface
	OIW	Workshop for Implementors of OSI
	OLE	Object Linking and Embedding
	ONC	Open Network Computing
	OOP	Object-oriented programming
	OPAC	Online Public Access Catalog
	OpenHCI	Open Host Controller Interface
	OSI	Open Systems Interconnection
	OSPF	Open Shortest Path First
—P—		
	PAD	Packet Assembler/Disassembler
	PAP	Printer Access Protocol
	PBX	Private Branch Exchange
	PCI	Peripheral Component Interconnect
	PCI	Protocol Control Information
	PCL	Printer Control Language
	PCM	Pulse Code Modulation
	PCMCIA	Personal Computer Memory Card International Association
	PDC	Primary Domain Controller
	PDF	Printer Definition Files
	PDN	Packet Data Network
	PDS	Processor-Direct Slot

	PDU	Protocol Data Unit
	PID	Process Identification Number
	PIF	Program Information File
	Ping	Packet internet groper
	PMMU	Paged Memory Management Unit
	POP	Point of Presence
	POP	Post Office Protocol
	POSI	Promoting Conference for OSI
	POST	Power On Self Test
	POTS	Plain Old Telephone Service
	ppm	pages per minute
	PPP	Point-to-Point Protocol
	PPTP	Point-to-Point Tunneling Protocol
	PRAM	Parameter RAM
	PRI	Primary Rate Interface
	PRMD	Private Management Domain
	PROFS	Professional Office System
	PSN	Packet Switch Node
	PU	Physical Unit
	PUC	Public Utility Commission
	PVC	Permanent Virtual Circuit
—Q—		
	QMF	Query Manager Facility
	QoS	Quality of Service
—R—		
	RAID	Redundant Array of Independent Disks
	RAM	Random Access Memory
	RARE	Reseaux Associes pour la Recherche Europeene
	RARP	Reverse Address Resolution Protocol
	RAS	Remote Access Service
	RAS	Remote Access Server
	RBOC	Regional Bell Operating Company
	REM	REMARK
	RFC	Request For Comments
	RFS	Remote File System
	RIP	Raster Image Processor
	RIP	Router Information Protocol
	RIPE	Reseaux IP Europeene
	RISC	Reduced Instruction Set Computer
	ROM	Read-Only Memory

- ROM
 Read-Only Memory

 ROSE
 Remote Operations Service Element
 - RPC Remote Procedure Call

	RTF	Rich Text Format
	RTMP	Routing Table Maintenance Protocol
	RTSE	Reliable Transfer Service Element
-S—		
	SAA	Systems Application Architecture
	SAP	Service Access Point
	SAP	Service Advertising Protocol
	SAPI	Service Access Point Identifier
	SAPS	Service Access Point Stations
	SAR	Segmentation and Reassembly protocol
	SCSI	Small Computer Systems Interface
	SDH	Synchronous Digital Hierarchy
	SDI	Storage Device Interface
	SDLC	Synchronous Data Link Control
	SDN	Software Defined Network
	SDU	SMDS Data Unit
	SFT	System Fault Tolerance
	SGML	Standard Generalized Markup Language
	SGMP	Simple Gateway Management Protocol
	SID	Security Identifier
	SIMM	Single, In-line Memory Module
	SIP	SMDS Interface Protocol
	SLIP	Serial Line Internet Protocol
	SMDS	Switched Multimegabit Data Service
	SMI	Structure of Management Information
	SMP	Symmetric Multiprocessing
	SMS	Storage Management Services
	SMTP	Simple Mail Transfer Protocol
	SNA	System Network Architecture
	SNMP	Simple Network Management Protocol
	SONET	Synchronous Optical Network
	SPAG	Standards Promotion and Application Group
	SPE	Synchronous Payload Envelope
	SPX	Sequenced Packet Exchange
	SQL	Structured Query Language
	SRAM	Static RAM
	SRPI	Server Requester Programming Interface
	SS7	Signaling System 7
	SSL	Secure Sockets Layer
	STDM	Statistical Time Division Multiplexing
	STI	Still Image Interface
	STM	Synchronous Transport Module
		J

	STS	Synchronous Transport Signal
	SVC	Switched Virtual Circuit
	Sysop	Systems Operator
—T—	5 1	
	ТА	Terminal Adapter
	TAC	Terminal Access Controller
	TCP	Transmission Control Protcol
	TCP/IP	Transmission Control Protocol/Internet Protocol
	TDM	Time-Division Multiplexor
	TE1	Terminal Equipment Type 1
	TE2	Terminal Equipment Type 2
	Telex	Teleprinter Exchange
	TIFF	Tagged Image File Format
	TLI	Transport Layer Interface
	TNX	Teletypewriter Exchange Service
	TP0	OSI Transport Protocol Class 0
	TP4	OSI Transport Protocol Class 4
	TSA	Target Server Agent
	TSR	Terminate and Stay Resident program
	TTF	TrueType fonts
	TTL	Time to Live
	TTS	Transaction Tracking System
	TWX	Teletypewriter Exchange Service
—U—		
	UA	User Agent
	UDP	User Datagram Protocol
	UMA	Upper Memory Area
	UMBs	Upper Memory Blocks
	UNC	Universal Naming Convention
	UPS	Uninterruptible Power Supply
	URL	Uniform Resource Locator
	USB	Universal Serial Bus
	UUCP	UNIX-to-UNIX Copy Program
V		
	VBR	Variable Bit Rate
	VCI	Virtual Connection Identifier
	VDM	Virtual DOS Machine
	Veronica	Very Easy Rodent-Oriented Netwide Index to Computerized Archives
	VGA	Video Graphics Array
	VLM	Virtual Loadable Module
	VLSI	Very Large-Scale Integration
	VM/CMS	Virtual Machine/Conversational Monitor System

	VMM	Virtual Memory Manager
	VNET	Virtual Network
	VPI	Virtual Path Identifier
	VPN	Virtual Private Network
	VRAM	Video RAM
	VRC	Vertical Redundancy Check
	VRML	Virtual Reality Modeling Language
	VSE/CICS	Virtual Storage Extended/Customer Information Control System
	VT	Virtual Terminal
—W—		
	WAIS	Wide Area Information Servers
	WAN	Wide Area Network
	WATS	Wide Area Telephone Service
	WWW	World Wide Web
	WYSIWYG	What You See Is What You Get
—X—		
	XDR	External Data Representation
	XMS	Extended Memory
	XNS	Xerox Network System
—Z—		,
	ZAW	Zero Administration Initiative for Windows
	ZIP	Zone Information Protocol

SELFSTUDY

Index

В

Back Up the IOS Using tftp	125
Backing Up Configuration Files	
to a TFTP Server	122
Backup	122, 125
Basic Rate Interface	9
Boot Options	120
Boot system	72

C

Command line interface	27
Common Monitoring Options	136
config-register 0x	70
Configuration mode	31
Configuration Registry	120
Configure	49
configure memory	
configure network	49
configure terminal	
Console Password	
CONTROL+SHIFT+6 followed by X	K 48
CONTROL+Z	51
copy running-config startup config	51
copy running-config tftp	73, 123
copy startup-config running-config	. 51, 70
copy startup-config tftp	123
copy tftp	
copy tftp flash	130
copy tftp running-config	124
copy tftp startup-config	124

D

Data Communications Equipment	9
Data Terminal Element	9
Debug	136
Options	136
Debugging	

Direct Cable Connection	10
Disable	30
Disabling the Enable Password	68

Ε

Editing the Confirmation Registry	121
Enable	
Enable password	
Enable Secret Password	
Enabling CDP on an interface	
ENTER	
Ethernet	
F	
Flash RAM	61
G	
Global Configuration Mode	32
Н	
Hostname	49
I	
Interface Configuration Mode	32
IP address	
IPX-Router	
L	
Line	32
Line Password	
Login Command	
logout	
M	
Managing the Configuration	120
Message of the day	48
Monitoring Network Traffic	136

Ν

Network Security and	
Session Monitoring	
No debug	137
Options	
Nonvolatile RAM	
NVRAM	11, 37, 60

Р

Password	68
Physical Connection	10
Point of Presence (POP)	9

Q

Quit	30

R

61
11
69
122
123
121
60
32
51

S

Serial	8
Setup Command	34
show	53
show cdp interface command	74
show config	37
show flash	45
show history	40
show interfaces	48, 50
show ip route	45
show memory	44
show processes	42
show protocols	42
show running-config	

show sessions
show startup-config 47
show version
Simulation
Change the Router Enable Password 78
Configure a Cisco Catalyst 1900 for
VLAN Operation 203
Configure HyperTerminal
for Console Access 114
Configure Spanning Tree on a Cisco
Catalyst 1900 203
Configure VTY Password 78
Copy the Startup Configuration
to a TFTP Server78
Upgrade the IOS 78
Use the Setup Mode to Configure
the Router114
View Help for the Show Command
in Privileged Mode55
View the Router Interface Details 55
View the Router Startup
Configuration 55
View the Router Version Information 55
Subinterface Configuration Mode 32

Т

ТСР/ІР	10
Telnet	
Terminal history size	40
terminal no editing	39
TFTP	12
Token Ring	8
Trivial File Transfer Protocol	11
Trivial File Transfer Protocol Server	12

U

Upgrade the Cisco IOS Using tftp	125
Upgrade the IOS	126
User Exec mode	29
Username	68

V

Version	3
Video	
Boot System Commands 18	8
Initial Configuration Setup Mode	3
Privileged Mode vs. User Mode 18	8
Router Access	
Router Command-Line	
Interface (CLI) 18	8
Router Configuration File	
Management 119	9
Router Configuration Register 119	
Router Hardware	
Router Memory Types83	3
Router Password Recovery 59	
Upgrading Router IOS Image 119	
Viewing CDP interfaces	
Viewing CDP Neighbors77	
Virtual Terminal Passwords	
Virtual terminal port	
-	

W

WAN	9
Write memory5	1