CCNA Quick Reference Sheets

Eric Rivard
Jim Doherty

ciscopress.com

shortcut
Your Short Cut to Knowledge

About the Authors

Eric Rivard, A+, MCSE, CCNP, CCSE, is an IT manager at Valley Center Municipal Water District. Over the past several years, he has taught professionals in both academic and industry settings topics on SCADA, Windows, networking, and IT security. Before joining Valley Center MWD, Eric was a network and security consultant in the San Diego area. He is the author of the first and second edition of the *CCNA Flash Cards and Exam Practice Pack*. He holds a B.S. in information technology from the University of Phoenix. He lives with his wife and two children in Oceanside, CA.

Jim Doherty is currently the director of strategic marketing with Symbol Technologies. Prior to joining Symbol, Jim worked at Cisco Systems, where he led marketing campaigns for IP telephony, and routing and switching. Over the past several years, he has taught professionals in both academic and industry settings on a broad range of topics, including networking, electric circuits, statistics, and wireless communication methods. Jim is the coauthor of *Cisco Networking Simplified* and wrote the "Study Notes" section of the *CCNA Flash Cards and Exam Practice Pack*. Jim holds a B.S. in electrical engineering from N.C. State University and an MBA from Duke University. Jim also served in the United States Marine Corps, where he earned the rank of sergeant before leaving to pursue an education.

 Please see page 311 for more details.

ICND1

Part I: Summarizing Network Technology

Section 1
Building a Simple Network

Exploring the Functions of Networking

A network is a collection of devices and end systems.

Networks consist of computers, servers, and network devices, such as switches and routers, that can communicate with each other.

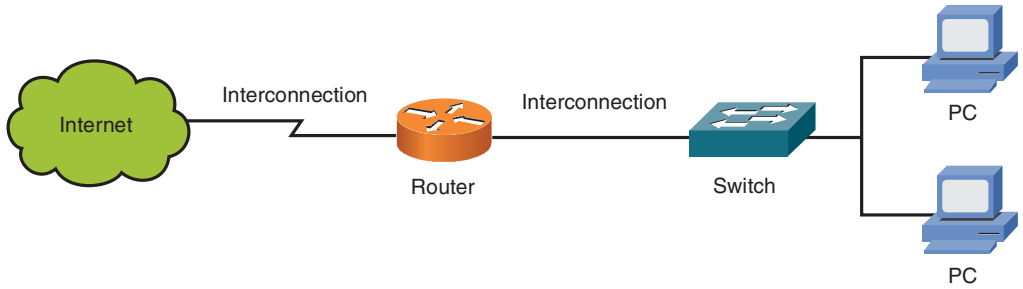
Common Physical Components of a Network

Figure 1-1 shows the four major categories of physical components on a network:

- **Personal computers (PCs):** Send and receive data and are the endpoints of the network.
- **Interconnections:** Are the components that provide a means for data to travel across the network. This includes network interface cards (NIC), network media, and connectors.
- **Switches:** Provide network access for the PCs.
- **Routers:** Interconnect networks.

 Please see page 311 for more details.

FIGURE 1-1
Network Components



Networking Fundamentals

Networking has its own jargon and common terms. The following terms are used throughout the industry and appear many times in this study guide:

- **Network interface card (NIC):** Connects a computer to a LAN.
- **Medium:** The physical transport used to carry data. Most of the time, this can be just a cable (twisted-pair or fiber), but it also includes air (for wireless transmission).
- **Protocol:** A set of communication rules used by computer or network devices.
- **Cisco IOS Software:** The most widely deployed network system software. Cisco IOS services include basic connectivity, security, network management, and other advanced services.
- **Client:** A computer or program that requests information from a server.
- **Server:** A computer or program that provides services of information to clients.
- **Network operating system (NOS):** Refers to the operating system running on servers. This includes Windows 2003 Server, Novell NetWare, UNIX, and Linux.
- **Connectivity device:** Any device that connects cable segments, connects two or more small networks into a larger one, or divides a large network into small ones.

- **Local-area network (LAN):** A network confined to a small geographic area. This can be a room, building, or campus.
- **Wide-area network (WAN):** Interconnects LANs using leased carrier lines or satellite technology over a large geographic location.
- **Physical topology:** A network's physical shape. These shapes include linear bus, ring, star, and mesh.
- **Logical topology:** The path that data takes from one computer to another.

Why Network Computers?

One of the primary functions of a network is to increase productivity by linking computers and computer networks. Corporate networks are typically divided into user groups, which are usually based on groups of employees. Remote-access locations, such as branches, home offices, and mobile workers, usually connect to the corporate LAN using a WAN service.

Resource-Sharing Functions and Benefits

Networks allow users to share resources and data. Major resources that are shared are as follows:

- **Data and applications:** Consist of computer data and network-aware applications such as e-mail.
- **Resources:** Include input and output devices such as cameras and printers.
- **Network storage:** Consists of directly attached storage devices (physical storage that is directly attached to a computer and shared server), network attached storage, and storage area networks.
- **Backup devices:** Devices that back up files and data from multiple computers.

 Please see page 311 for more details.

Networking Applications

Networking applications are computer programs that run over networks.

Network User Applications

Network user applications include the following:

- E-mail
- Web browsers
- Instant messaging
- Collaboration
- Databases

Categories of Network Applications

Network applications function in one of three ways, with each application function affecting the network in different ways:

- **Batch applications:** Started by a human and complete on their own without further interaction. FTP and TFTP are examples.
- **Interactive applications:** Include database updates and queries. A person requests data from the server and waits for a reply. Response time is typically more dependent on the server than the network.
- **Real-time applications:** Include Voice over IP (VoIP) and video. Network bandwidth is critical because these applications are time critical. Quality of service (QoS) and sufficient network bandwidth are mandatory for these applications.

 Please see page 311 for more details.

Network Administration Applications

Network administration applications help manage a network. These applications configure, monitor, and troubleshoot a network. Network administration applications fall into two general categories:

- **Network monitoring:** Examples are protocol analyzers and network sniffers. Protocol analyzers capture network packets between computers and decode the packets for easy reading. Sniffers allow you to view not only the communication between computers but also the data that is being transmitted.
- **Network management:** Helps make managing a network easier by providing device inventory, remote control of devices, software license compliance, and notifications of network problems.

Characteristics of a Network

Networks are characterized using the following terms:

- **Speed:** Also called data rate, speed is how fast data is transmitted over the network.
- **Cost:** The general cost of network components, installation, and maintenance.
- **Security:** Defines how secure the network and network data are.
- **Availability:** The measure of the likelihood that the network will be available for use when required. Calculated using the following formula: [(525,600 – Minutes downtime) / 525,600] * 100. 525,600 is the number of minutes in a year.
- **Scalability:** How well the network can accommodate more users and more data.
- **Reliability:** The dependability of the devices that make up the network (for example, switches, routers, PCs, and so on).
- **Topology:** Defines the design of the network. Physical topology defines the physical components of the network: cables, network devices, and so on. Logical topology defines the data path of the network.

Network Security

Network security involves securing the network from external and internal threats. External threats are threats external to the company or network. Internal threats are threats that originate from within the company network and might be intentional or unintentional.

Network security involves finding a balance between open and evolving networks and protecting company and private data.

Classes of Attacks

The following five classes of network attacks exist:

- **Passive:** Attacks that include capturing and monitoring unprotected communication and capturing passwords. The attacker gains access to information or data without the consent or knowledge of users.
- **Active:** Attacks that actively try to break or bypass security devices, introduce malicious code, and steal and modify data.
- **Close-in:** Attacks attempted by an individual in close physical proximity to networks or facilities, with the intent of gathering or changing data.
- **Insider:** Attacks that occur from authorized users inside a network. Can be either malicious or nonmalicious.
- **Distribution:** Attacks that focus on malicious changes to hardware or software at the factory or during distribution to introduce malicious code to unsuspecting users.

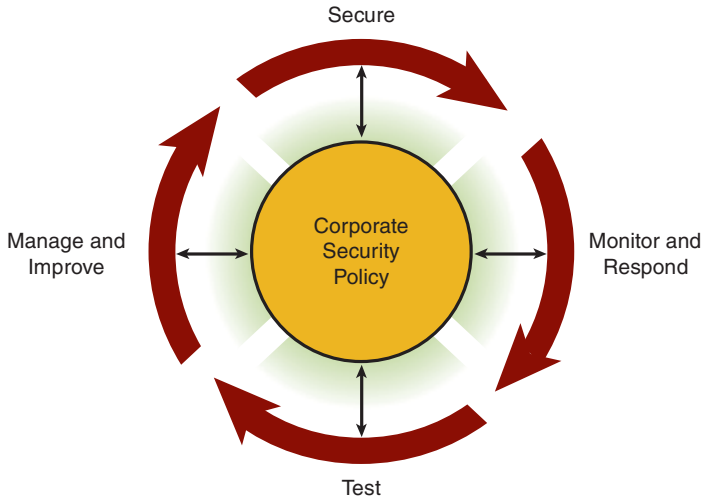
 Please see page 311 for more details.

Network Security Process

Network security is an ongoing process that continually evolves. Figure 1-2 shows the network security wheel; the four facets are as follows:

- **Secure:** Involves installing and configuring devices for security.
- **Monitor:** After the network has been secured, it must be monitored to ensure security.
- **Test:** Involves testing systems to ensure that they function properly.
- **Improve:** After monitoring and testing, you might need to improve the security of the network.

FIGURE 1-2
Network Security Wheel



Mitigating Physical and Environmental Threats

Low-risk devices are typically low-end devices where access to the physical devices and cabling does not present a high risk to the network.

High-risk devices are mission-critical devices that route and control large amounts of data, voice, and video traffic.

The four classes of physical threats are as follows:

- **Hardware:** Physical damage to the router or switch. Mitigation involves restricting access to the hardware device to only authorized personnel.
- **Environmental:** Room-temperature extremes or humidity extremes. Mitigation involves providing climate-controlled rooms for critical network devices.
- **Electrical:** Voltage spikes, brownouts, noise, and power losses. Mitigation includes using uninterruptible power supplies (UPS) and backup generators.
- **Maintenance:** Electrostatic discharge, poor cabling, and lack of critical spares.

Reconnaissance Attacks

Reconnaissance attacks are attacks that gather information about the target. These types of attacks include sniffers, ping sweeps, port scans, and Internet Domain Name System (DNS) queries.

 Please see page 311 for more details.

Access Attacks

Access attacks exploit known web services, databases, operating systems, and authentication services. The five types of access attacks are as follows:

- **Password attacks:** Attacks that try to compromise passwords. These include brute-force attacks, Trojan horse programs, IP spoofing, and packet sniffers. Mitigation of these attacks includes disabling accounts after a specific number of unsuccessful login attempts, having complex password requirements, and not using plain-text passwords.
- **Trust exploitation:** Attacks that occur when a trusted source on a network takes advantage of its trust. For example, if a trusted system on a network is compromised, it can lead to other systems being compromised on the same network.
- **Port redirection:** Attacks that use a compromised host to pass traffic through a firewall that would otherwise be dropped.
- **Man-in-the-middle attacks:** Attacks that occur when an attacker, using sniffers, captures and modifies information as it is transmitted from one network to another. These attacks require access to the network media or devices between the source and destination.
- **Buffer overflow:** These attacks exploit programming errors that can result in a memory-access exception and program termination or a breach of system security.

Application Layer Attacks

Application layer attacks try to exploit well-known vulnerabilities and passwords. They have the following characteristics:

- Exploiting well-known weaknesses in software found on servers such as send mail, HTTP, and FTP to gain elevated access rights to the computer running the software.

 Please see page 311 for more details.

- Trojan horse programs that monitor login attempts and capture account information. These programs then send the information to the attacker.
- Password stealing by prompting the user to enter the system password to gain access to the user's system or accounts.
- Java and ActiveX attacks that pass malicious programs to users through a web browser.

Application Layer Attacks and Mitigation

Several ways to mitigate application layer attacks are as follows:

- Read system and device logs.
- Subscribe to mailing lists that publicize current software vulnerabilities and attacks.
- Patch computers and devices regularly.
- Use intrusion detection systems/intrusion prevention systems (IDS/IPS) to scan and stop network attacks.

Management Protocol and Vulnerabilities

Protocols used to manage network devices, such as Telnet, can be a vulnerability because Telnet sends all session data in clear text. Instead, use Secure Shell (SSH), Secure Socket Layer (SSL), or IPsec.

Other network protocols that can be compromised and should be secured and monitored are as follows:

- Simple Network Management Protocol (SNMP)
- Syslog
- TFTP
- Network Time Protocol (NTP)

 Please see page 311 for more details.

Host-to-Host Communication Model

For different vendor hosts to communicate with each other, a consistent model or standard is needed.

OSI Reference Model

The OSI model is a standardized framework for network functions and schemes. It breaks otherwise complex network interaction into simple elements, which lets developers modularize design efforts. This method allows many independent developers to work on separate network functions, which can be applied in a "plug-and-play" manner.

The OSI model consists of seven layers, as outlined in Table 1-1.

TABLE 1-1 OSI Model

Layer	Function	Examples
Application (Layer 7)	User interface.	Telnet, HTTP
Presentation (Layer 6)	Handles encryption and other processing.	ASCII/EBCDIC, JPEG/MP3
Session (Layer 5)	Manages multiple applications.	Operating systems, scheduling
Transport (Layer 4)	Provides reliable or best-effort delivery and some error correction.	TCP, UDP
Network (Layer 3)	Provides logical addressing used by routers and the network hierarchy.	IP
Data link (Layer 2)	Creates frames from bits of data, uses MAC addresses to access endpoints, and provides error detection but no correction.	802.3, 802.2, HDLC, Frame Relay
Physical (Layer 1)	Specifies voltage, wire speed, and cable pin-outs.	EIA/TIA, V.35

 Please see page 311 for more details.

Encapsulation and De-encapsulation

Protocol data units (PDU) communicate between layers. Encapsulation is the method of adding headers and trailers. As the data moves down the communication stack, the receiving device strips the header, which contains information for that layer (de-encapsulation).

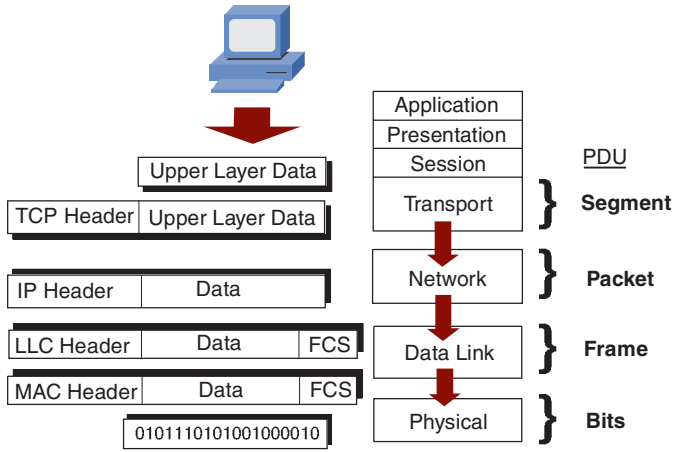
A PDU can include different information as it goes up or down the OSI model. It is given a different name according to the information it is carrying (the layer it is at). When the transport layer receives upper-layer data, it adds a TCP or User Datagram Protocol (UDP) header to the data; this is called a segment. The segment is then passed to the network layer, and an IP header is added; thus, the data becomes a packet. The packet is passed to the data link layer, thus becoming a frame. This frame is then converted into bits and is passed across the network medium. This is data encapsulation. For the ICND exam, you should know the following:

- **Application layer:** Data
- **Transport layer:** Segment
- **Network layer:** Packet
- **Data link layer:** Frame
- **Physical layer:** Bits

Peer-to-Peer Communication

For packets to travel from a source to a destination, each OSI layer of the source computer must communicate with its peer at the destination. As shown in Figure 1-3, each part of the message is encapsulated by the layer below it, and it is unwrapped at the destination for use by the corresponding layer.

FIGURE 1-3
Data Encapsulation



TCP/IP Stack

The TCP/IP suite of protocols communicates across any set of interconnected networks. These protocols, initially developed by the Defense Advanced Research Projects Agency (DARPA), are well suited for communication across both LANs and WANs. The protocol suite defines the following four layers:

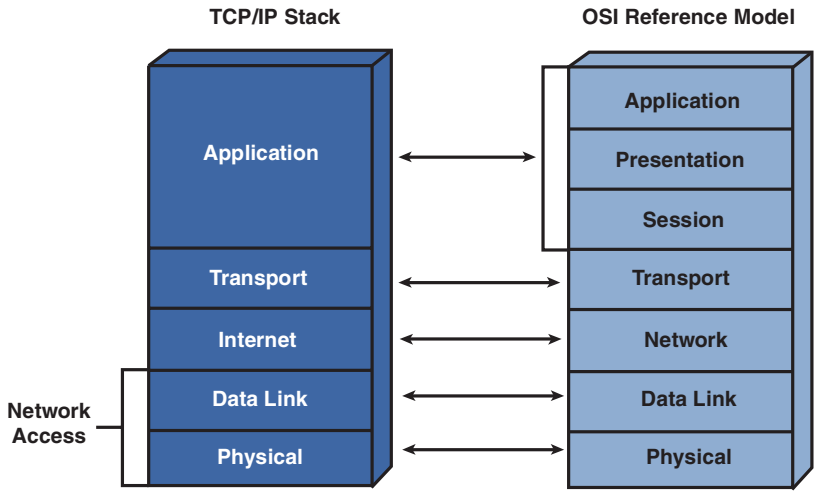
- **Network access layer:** Consists of the physical and data link OSI model layers
- **Internet layer:** Provides routing of data from the source to a destination and defines addressing schemes
- **Transport layer:** The core of the TCP/IP suite, providing communication services directly to the application layer
- **Application layer:** Provides specifications of applications such as e-mail, file transfer, and network management

 Please see page 311 for more details.

TCP/IP Stack Versus OSI Model

Figure 1-4 shows the TCP/IP model. The TCP/IP protocol stack closely follows the OSI reference model. All standard Layer 1 and Layer 2 protocols are supported (called the network interface layer in TCP/IP).

FIGURE 1-4
OSI Versus
TCP/IP Model



 Please see page 311 for more details.

Section 2
Understanding TCP/IP

TCP/IP Overview

The TCP/IP suite of protocols is used to communicate across any set of interconnected networks. The protocols initially developed by DARPA are well suited for communication across both LANs and WANs.

The protocol suite includes Layer 3 and Layer 4 specifications as well as specifications for higher-layer applications, such as e-mail and file transfer.

Internet Protocol (IP)

IP is a connectionless protocol that provides best-effort delivery routing of packets.

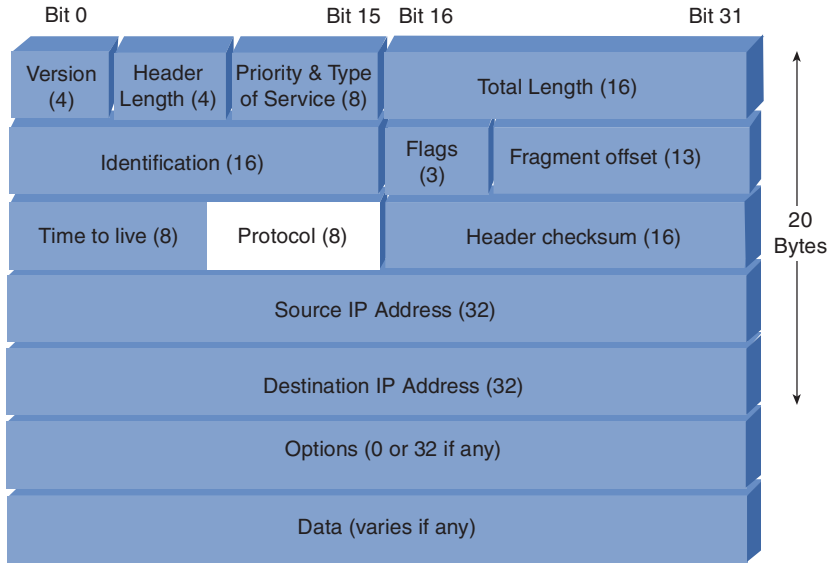
IP has the following characteristics:

- Operates at Layer 3 of the OSI (network) and Layer 2 of the TCP/IP (Internet) model
- Is connectionless
- Uses hierarchical addressing
- Provides best-effort delivery of packets
- Has no built-in data recovery

Figure 2-1 shows the IP header information.

 Please see page 311 for more details.

FIGURE 2-1
IP Header



IP Addressing

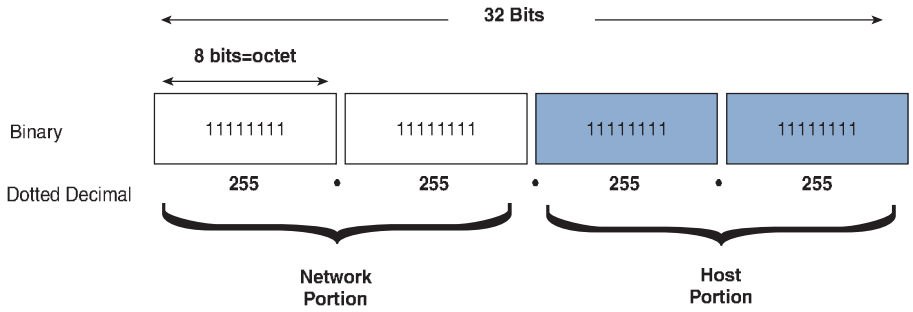
In a TCP/IP environment, each node must have a unique 32-bit logical IP address. Each IP datagram includes the source and destination IP address in the header.

As shown in Figure 2-2, IP addresses consist of two parts: the network address portion (network ID) and the host address component (host ID). A two-part addressing scheme allows the IP address to identify both the network and the host:

- All the endpoints within a network share a common network number.
- The remaining bits identify each host within that network.

 Please see page 311 for more details.

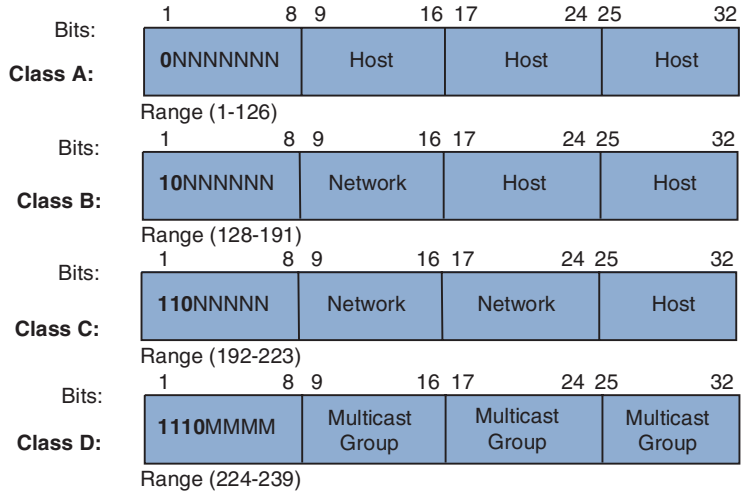
FIGURE 2-2
Two-Part IP Addresses



IP Address Classes

Five classes of IP addresses exist: classes A through E. Classes A, B, and C are the most common. Class A has 8 network bits and 24 host bits. Class B has 16 network bits and 16 host bits. Class C addresses allow many more networks, each with fewer hosts (24 network bits and 8 host bits). This scheme was based on the assumption that the world would have many more small networks than large networks. Class D addresses are used for multicast purposes, and Class E addresses are used for research. Figure 2-3 shows the address range for classes A–D.

FIGURE 2-3
A Through D IP Address Classes



 Please see page 311 for more details.

Reserved IP Addresses

Some IP addresses in TCP/IP are reserved for specific purposes. These addresses cannot be assigned to individual devices on a network. The reserved addresses are as follows:

- **Network address:** An IP address that has all binary 0s in the host bit portion of the address. For example, 172.16.0.0/16.
- **Directed broadcast address:** An IP address that has all binary 1s in the host bit portion of the address. Used to send data to all devices on the network. For example, 172.16.255.255/16.
- **Local broadcast address:** An address used if a device wants to communicate with all devices on the local network. The address is 255.255.255.255.
- **Loopback address:** Used by the TCP/IP stack to test TCP/IP by sending a message internally to itself. The address is 127.0.0.1.

Private IP Addresses

RFC 1918 defines IP addresses that are reserved for use in private networks. The IP addresses are not routed on the Internet. Three blocks of IP addresses are reserved for private networks:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

Networks using private addresses can still connect to the Internet if they use Network Address Translation (NAT).

 Please see page 311 for more details.

Tools to Determine the IP Address of a Host

- **Windows OS:** ipconfig is a command-line tool in Windows operating systems that finds the TCP/IP parameters assigned to a host.
- **UNIX/Linux:** ifconfig determines the TCP/IP information of a host.

TCP/IP Transport Layer

The TCP/IP model transport layer is responsible for the following:

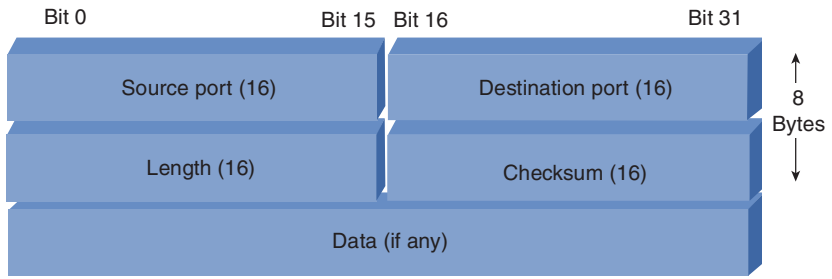
- Session multiplexing
- Segmentation
- Flow control
- Connection-oriented or connectionless transport
- Reliable or unreliable data transport

Two protocols function at the transport layer: UDP and TCP. UDP is a connectionless, best-effort delivery protocol. TCP is a connection-oriented, reliable protocol.

UDP

UDP is a connectionless, best-effort protocol used for applications that provide their own error-recovery process. It trades reliability for speed. UDP is simple and efficient but unreliable. UDP does not check for segment delivery. Figure 2-4 shows the UDP header.

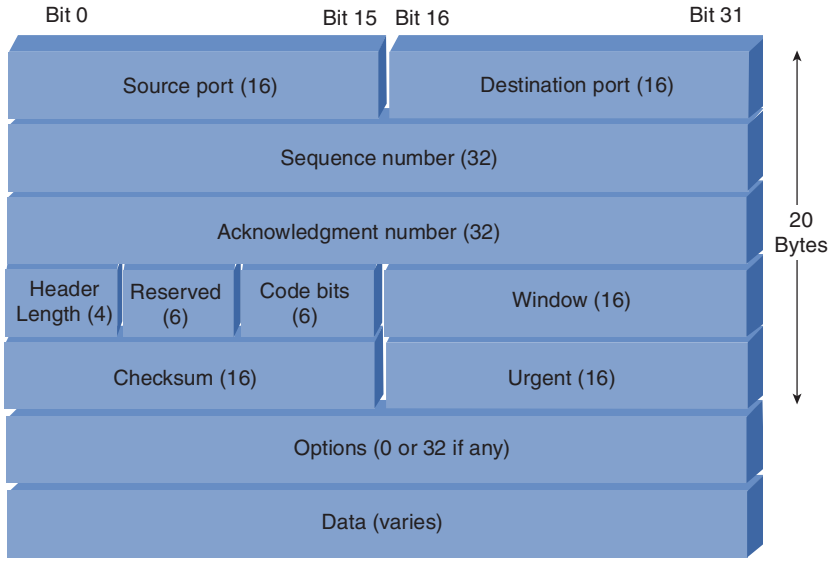
FIGURE 2-4
UDP Header



TCP

TCP is a connection-oriented, reliable protocol that is responsible for breaking messages into segments and reassembling them at the destination (resending anything not received). TCP also provides virtual circuits between applications. Figure 2-5 shows the TCP header.

FIGURE 2-5
TCP Header



TCP/IP Applications

Some of the most common TCP/IP applications are as follows:

- **File Transfer Protocol (FTP):** A TCP-based protocol that supports bidirectional binary and ASCII file transfers
- **Trivial File Transfer Protocol (TFTP):** A UDP-based protocol that can transfer configuration files and Cisco IOS Software images between systems
- **Simple Mail Transfer Protocol (SMTP):** An e-mail delivery protocol
- **Terminal Emulation (Telnet):** Allows remote command-line access to another computer
- **Simple Network Management Protocol (SNMP):** Provides the means to monitor and control network devices
- **Dynamic Host Configuration Protocol (DHCP):** Assigns IP addresses and other TCP/IP parameters such as subnet mask, DNS/WINS server addresses, and default gateways automatically to hosts
- **Domain Name Service (DNS):** Translates domain names into IP addresses

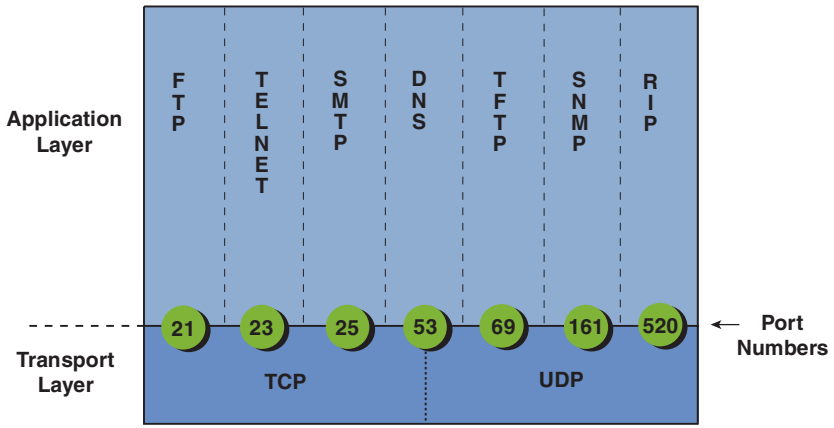
NOTE
Other examples include HTTP, HTTPS, and SSH.

Port Numbers

Both TCP and UDP can send data from multiple upper-layer applications at the same time. Port (or socket) numbers keep track of different conversations crossing the network at any given time. Well-known port numbers are controlled by the Internet Assigned Numbers Authority (IANA). Applications that do not use well-known port numbers have them randomly assigned from a specific range. Figure 2-6 shows the TCP/UDP port numbers from common applications.

 Please see page 311 for more details.

FIGURE 2-6
Port Numbers



Port number ranges are as follows:

- Numbers 1 through 1024 are considered well-known ports.
- Numbers 1025 through 49151 are registered.
- Numbers 49152 through 65535 are private vendor assigned and are dynamic.

Establishing a TCP Connection

End stations use control bits called SYNs (for synchronize) and Initial Sequence Numbers (ISNs) to synchronize during connection establishment.

Three-Way Handshake

The synchronization requires each side to send its own initial sequence number and to receive a confirmation of it in acknowledgment (ACK) from the other side. Figure 2-7 outlines the steps in the TCP three-way handshake, which are further defined in the following list:

Step 1. Host A sends a SYN segment with sequence number 100.

Step 2. Host B sends an ACK and confirms the SYN it received. Host B also sends a SYN. Note that the ACK field in host B is now expecting to hear sequence 101.

Step 3. In the next segment, host A sends data. Note that the sequence number in this step is the same as the ACK in Step 2.

FIGURE 2-7
TCP Three-Way Handshake

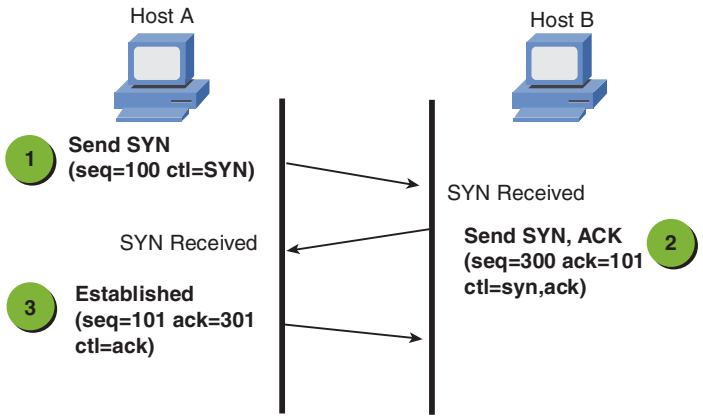
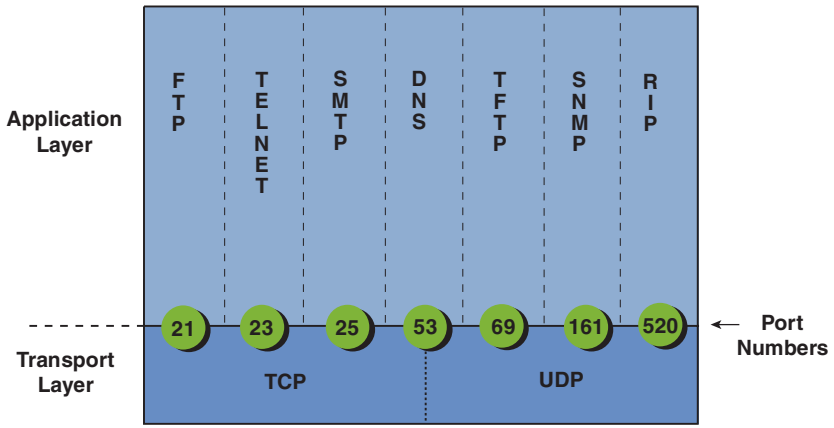


FIGURE 2-6
Port Numbers



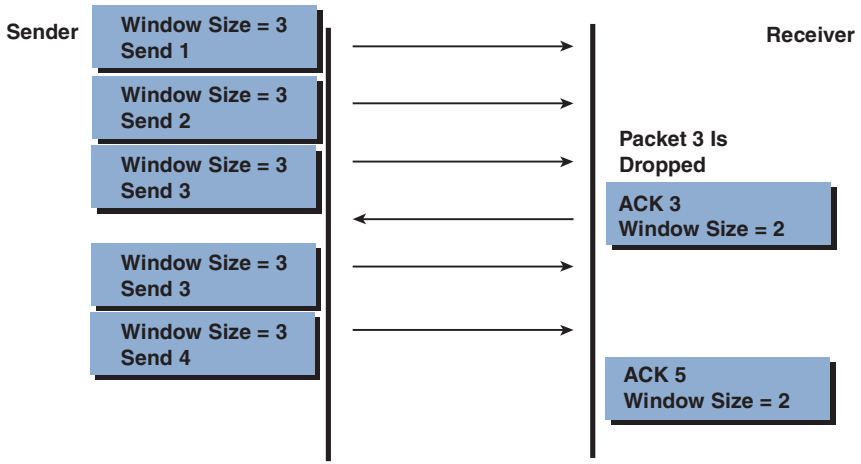
Port number ranges are as follows:

- Numbers 1 through 1024 are considered well-known ports.
- Numbers 1025 through 49151 are registered.
- Numbers 49152 through 65535 are private vendor assigned and are dynamic.

Establishing a TCP Connection

End stations use control bits called SYNs (for synchronize) and Initial Sequence Numbers (ISNs) to synchronize during connection establishment.

FIGURE 2-8
TCP Windowing Example



A TCP/IP session can have different window sizes for each node.

Exploring the Packet Delivery Process

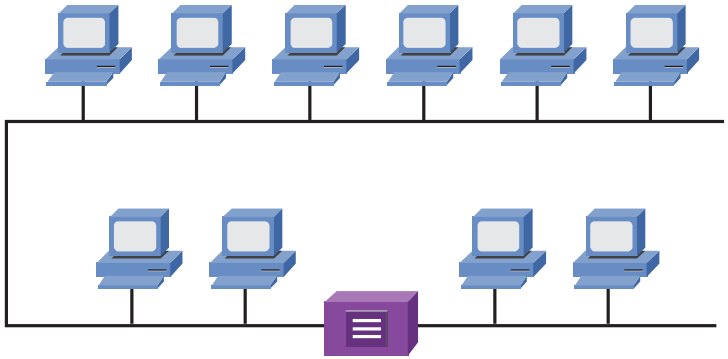
Layer 1 Devices

Layer 1 devices operate at the physical layer and are only involved in transmitting signals (moving bits). Examples include Ethernet segments, serial links, repeaters, and hubs.

Repeaters (see Figure 2-9) are necessary because a signal's quality degrades over distance, eventually becoming unreadable. Repeaters regenerate and retime (or clean up) the signal, allowing it to travel a longer distance over a given medium. Repeaters can be single-port (one in, one out) or multiport.

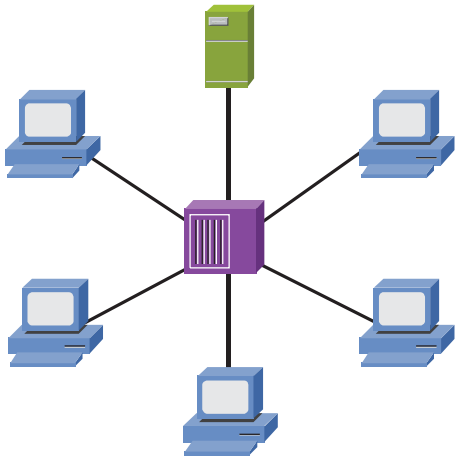
 Please see page 311 for more details.

FIGURE 2-9
Repeater



Hubs are similar to repeaters and are often called multiport repeaters (usually having from 4 to 20 ports). Hubs provide no filtering or intelligence; they simply clean up signals. Hubs also increase network reliability by isolating endpoints. Using a hub, if a single cable fails, the network continues to operate. A group of devices connected to the same physical medium is known as a collision domain. If two devices transmit a signal at the same time, a collision results. Ethernet devices use a method called carrier sense multiple access collision detect (CSMA/CD) when sending bits. When a collision occurs, both stations resend the signal after a random period. Collisions increase with the number of stations and reduce usable bandwidth (see Figure 2-10).

FIGURE 2-10
Hub



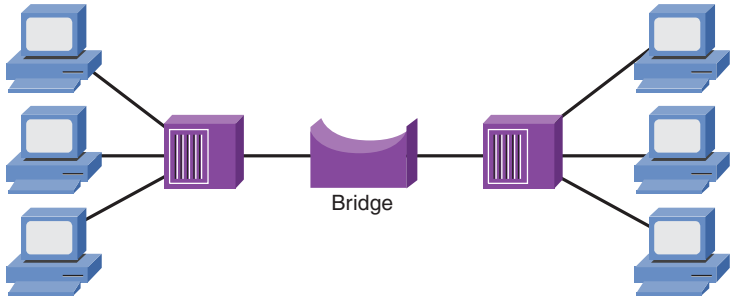
Layer 2 Devices

Layer 2 devices operate at the data link layer and, in most cases, isolate endpoints, avoiding data collisions (discussed later). Devices such as bridges and switches use MAC addresses to switch data frames.

Network interface cards (NICs) are considered Layer 2 devices because they provide MAC addresses used by other Layer 2 devices.

Figure 2-11 shows that bridges connect LAN segments and isolate collision domains, which increases bandwidth. Bridges keep local traffic from going to other LAN segments but can filter traffic intended for other LAN segments using the MAC address of the destination endpoint. Bridges keep track of destinations in MAC address tables.

FIGURE 2-11
Bridge



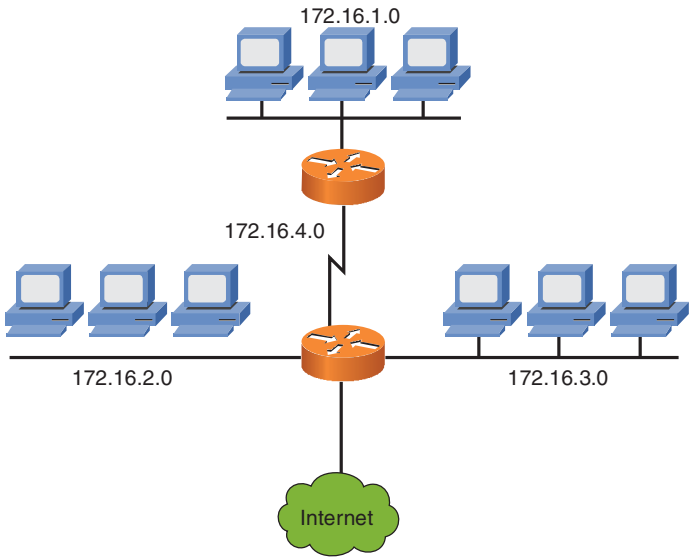
Switches (or LAN switches) are similar to bridges and have the same functionality as bridges but are typically much faster than bridges. This is because the switching functions are performed in hardware, whereas bridges use software. Switches proved more ports than bridges and also support virtual LANs (VLANs, discussed later).

Layer 3 Devices

Layer 3 devices operate at the network layer of the OSI model, which uses a different addressing scheme than Layer 2 devices. IP addresses are one type of Layer 3 address; other Layer 3 protocols exist, but they are outside the scope of the ICND1 and ICND2 exams. The two most common Layer 3 devices are routers and multilayer switches. As shown in

Figure 2-12, routers pass data packets between networks based on their IP (or possibly other Layer 3) address. Routers can make intelligent decisions about the best path a packet can take across the network. Routers can also connect different types of Layer 2 networks. Routers regulate traffic and make up the backbone of most IP networks.

FIGURE 2-12
Routers



Multilayer switches are the same as regular Layer 2 switches but can process and make switching decisions based on Layer 3 addresses. This advance was enabled because of high-speed software embedded in hardware ASICs. This has reduced the bottleneck that used to occur with software-based Layer 3 devices. Using Layer 3 addresses allows multilayer switches to implement quality and security policies.

Mapping Layer 2 Addressing to Layer 3 Addressing

For IP hosts to communicate on Ethernet networks, the IP host must know the IP address and MAC address of the destination computer. To find the MAC address of the destination, IP uses a protocol called Address Resolution Protocol (ARP).

ARP maps a known IP address to a MAC sublayer address. An ARP cache table is checked when looking for a destination. If the address is not in the ARP table, ARP sends a broadcast looking for the destination address.

 Please see page 311 for more details.

Section 3
Understanding Ethernet

Ethernet was developed in the 1970s by Digital Equipment Corporation (DEC), Intel, and Xerox. Later, the IEEE defined new standards for Ethernet called Ethernet 802.3. The 802.3 standard is the standard that is in use today.

Definition of a LAN

Local-area networks (LAN) are high-speed, low-error data networks that cover a small geographic area.

LANs are usually located in a building or campus and do not cover a large distance. They are relatively inexpensive to develop and maintain. LANs connect computers, printer, terminals, and other devices in a single building or a limited area.

LANs consist of the following components:

- **Computers:** Examples include PCs and servers.
- **Interconnections:** Provide a means for data to travel. Also include NICs and network media.
- **Network devices:** Examples include hubs, routers, and switches.
- **Protocols:** Examples include Ethernet protocols, IP, ARP, and DHCP.

Ethernet

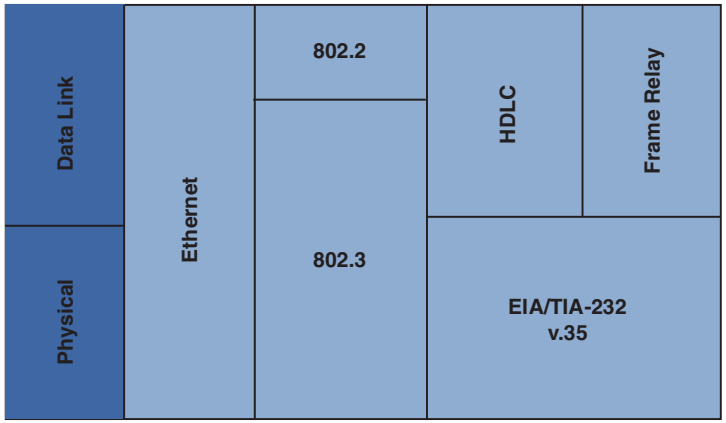
Ethernet is one of the most widely used LAN standards. As Figure 3-1 shows, Ethernet operates at Layers 1 and 2 of the OSI model.

 Please see page 311 for more details.

SECTION 3

Understanding Ethernet

FIGURE 3-1
Physical and Data Link Layers



The physical layer (Layer 1) defines cabling, connection specifications, and topology.

The data link layer (Layer 2) has the following functions:

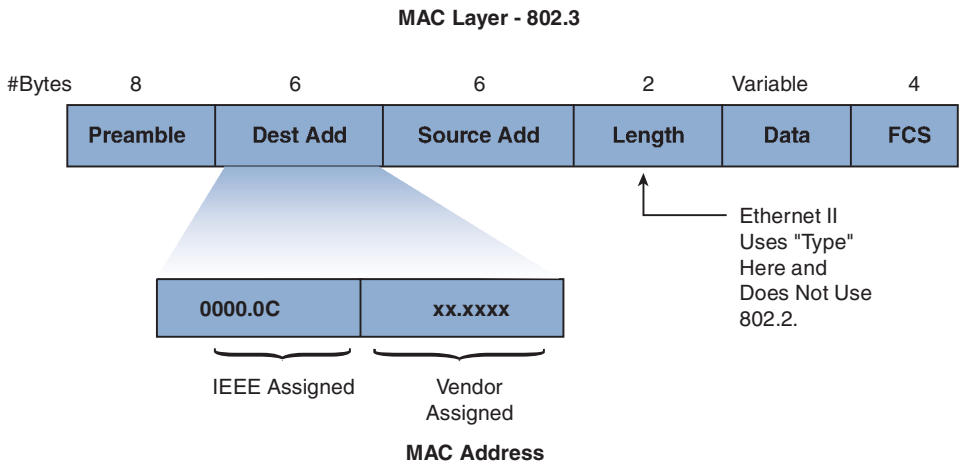
- Provides physical addressing
- Provides support for connection-oriented and connectionless services
- Provides frame sequencing and flow control

Two sublayers perform data-link functions: the MAC layer and the Logical Link Control (LLC) layer.

Figure 3-2 shows the Media Access Control (MAC) sublayer (802.3). The MAC sublayer is responsible for how data is sent over the wire. The MAC address is a 48-bit address expressed as 12 hex digits.

 Please see page 311 for more details.

FIGURE 3-2
MAC Sublayer

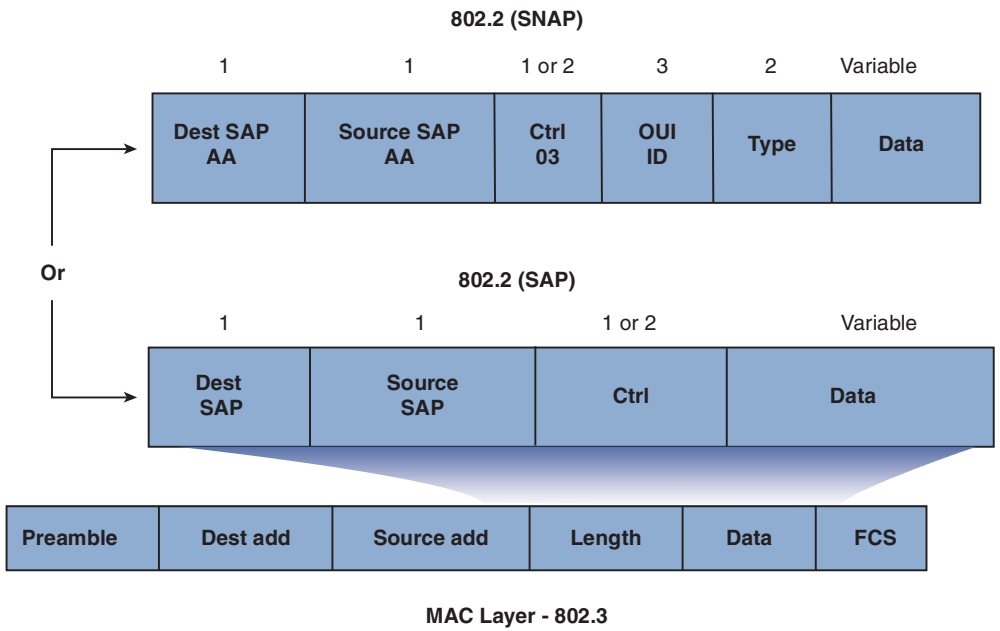


The MAC sublayer defines the following:

- Physical addressing
- Network topology
- Line discipline
- Error notification
- Orderly delivery of frames
- Optional flow control

The LLC sublayer (802.2) is responsible for identifying and encapsulating different protocol types. Two types of LLC frames exist: service access points (SAP) and Subnetwork Access Protocol (SNAP). SNAP is used to support non-802 protocols. Figure 3-3 shows the LLC sublayer frame.

FIGURE 3-3
LLC Sublayer



Role of CSMA/CD in Ethernet

All stations on an Ethernet segment are connected to the same media. Therefore, all devices receive all signals. When devices send signals at the same time, a collision occurs. A scheme is needed to detect and compensate for collisions. Ethernet uses a method called carrier sense multiple access collision detect (CSMA/CD) to detect collisions.

In CSMA/CD, many stations can transmit on the Ethernet media, and no station has priority over any other. Before a station transmits, it listens to the network (carrier sense) to make sure that no other station is transmitting. If no other station is transmitting, the station transmits across the media. If a collision occurs, the transmitting stations detect the collision and run a backoff algorithm. The backoff algorithm computes a random time that each station waits before retransmitting.

 Please see page 311 for more details.

Ethernet LAN Traffic

Three major types of network traffic exist on a LAN:

- **Unicasts:** The most common type of LAN traffic. A unicast frame is a frame intended for only one host.
- **Broadcasts:** Intended for all hosts. Stations view broadcast frames as public service announcements. All stations receive and process broadcast frames.
- **Multicasts:** Traffic in which one transmitter tries to reach only a subset, or group, of the entire segment.

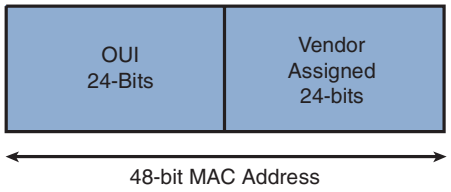
Ethernet Addresses

The Ethernet address, or MAC address, is the Layer 2 address of the network adapter of the network device. Typically burned into the adapter, the MAC address is usually displayed in a hexadecimal format such as 00-0d-65-ac-50-7f.

As shown in Figure 3-4, the MAC address is 48 bits and consists of the following two components:

- **Organizational Unique Identifier (OUI):** 24 bits. This is IEEE assigned and identifies the manufacturer of the card.
- **Vendor-assigned:** 24 bits. Uniquely identifies the Ethernet hardware.

FIGURE 3-4
MAC Addresses



Connecting to an Ethernet LAN

The term *Ethernet* encompasses several LAN implementations. Physical layer implementations vary, and all support various cabling structures. The following four main categories of Ethernet exist:

- **Ethernet (DIX) and IEEE 802.3:** Operate at 10 Mbps over coaxial cable, unshielded twisted-pair (UTP) cable, or fiber. The standards are referred to as 10BASE2, 10BASE5, 10BASE-T, and 10BASE-F.
- **Fast Ethernet or 100-Mbps Ethernet:** Operates over UTP or fiber.
- **Gigabit Ethernet:** An 802.3 extension that operates over fiber and copper at 1000 Mbps, or 1 gigabit per second (Gbps).
- **10-Gigabit Ethernet:** Defined in 802.3ae, runs in full-duplex mode only, over fiber.

Table 3-1 compares cable and connecter specifications. Fast Ethernet and Gigabit Ethernet require UTP Category 5e (or higher) or fiber cabling.

TABLE 3-1 Ethernet Media and Connection Requirements

	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX
Media	EIA/TIA Cat 3, 4, 5 UTP 2-pair	EIA/TIA Cat 5 UTP 2-pair	62.5/125 micro-multimode fiber	STP	EIA/TIA Cat 5 UTP 4-pair	62.5/50 micro-multimode fiber	9-micron single-mode fiber
Maximum Segment Length	100 m	100 m	400 m	25 m	100 m	275 m	3–10 km
Connector	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Duplex media interface (RJ-45) connector (MIC) ST	ISO 8877 (RJ-45)	ISO 8877	—	—

 Please see page 311 for more details.

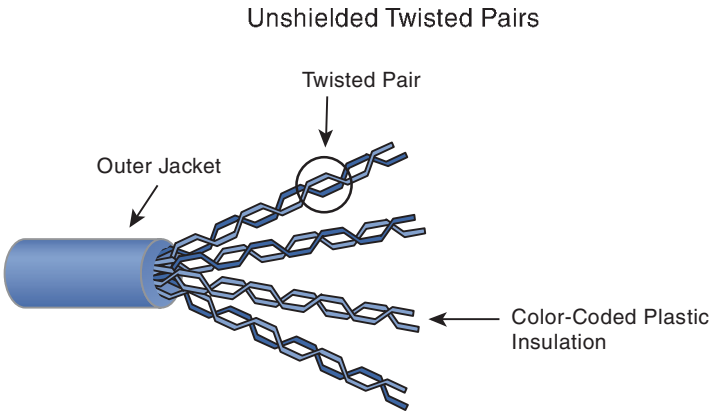
A Gigabit Interface Converter (GBIC) is a hot-swappable I/O device that plugs into a Cisco Gigabit Ethernet port. GBICs are interchangeable, and they allow you to deploy different types of 1000BASE-X technology without having to change the physical interface of the switch. GBICs support UTP and fiber media.

Network Media Types

Network media refers to the physical path that signals take across a network. The most common types of media are as follows:

- **Twisted-pair cable:** Used for telephony and most Ethernet networks. Each pair makes up a circuit that can transmit signals. The pairs are twisted to prevent interference (crosstalk). The two categories of twisted-pair cables are unshielded twisted-pair (UTP) and shielded twisted-pair (STP), defined as follows:
  - **UTP cable:** Usually connected to equipment with an RJ-45 connector. UTP has a small diameter that can be an advantage when space for cabling is at a minimum. It is prone to electrical noise and interference because of the lack of shielding. Seven categories of UTP cable exist: CAT 1, CAT 2, CAT 3, CAT 4, CAT 5, CAT 5e, and CAT 6.

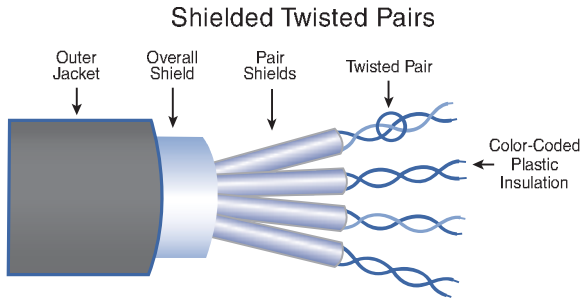
FIGURE 3-5
UTP



 Please see page 311 for more details.

- **STP cable:** Provides much better protection against electrical noise and interference than UTP but is thicker and more expensive. The cable speed and maximum length are the same as for UTP (speed is 10 to 100 Mbps, and maximum length is 100 m).

FIGURE 3-6
STP



- **Fiber-optic cable:** Allows the transmission of light signals. This offers a large jump in bandwidth over other types of cables (1 Gbps or greater). The two types of fiber-optic cables are multimode and single-mode, defined as follows:
  - **Multimode:** With this type of fiber, several modes (or wavelengths) propagate down the fiber, each taking a slightly different path. Multimode fiber is used primarily in systems with short transmission distances (less than 2 km).
  - **Single-mode:** This type of fiber has only one mode in which light can propagate. Single-mode fiber is typically used for long-distance and high-bandwidth applications.

UTP Implementation

An RJ-45 connector is use with UTP cabling. Figure 3-7 shows an RJ-45 connector and its pin connections.

The two types of connections are straight-through and crossover. Straight-through cables are typically used to connect different devices (data terminal equipment [DTE] to data communications equipment [DCE]), such as switch-to-router connections. Figure 3-8 shows the pins for a straight-through cable.

FIGURE 3-7
RJ-45 Connector

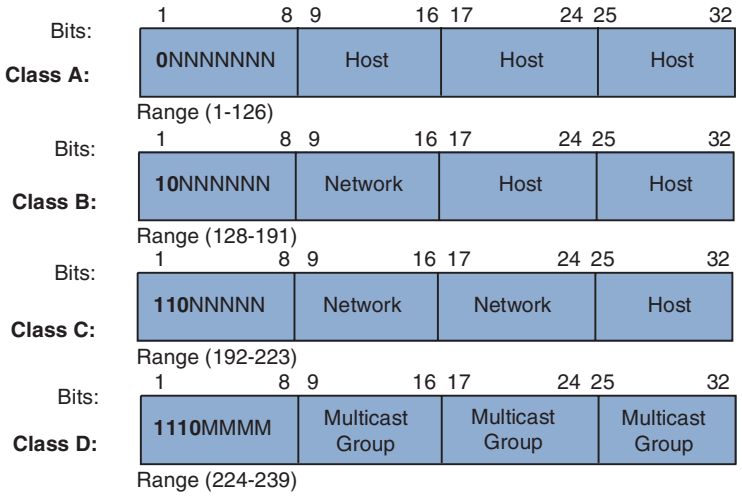
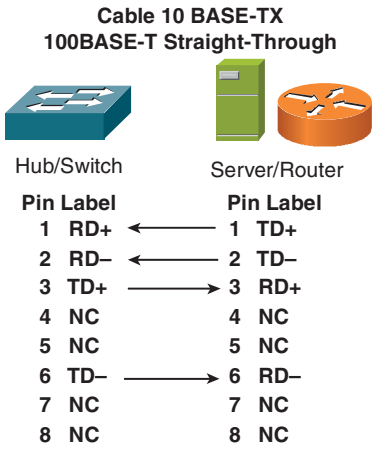
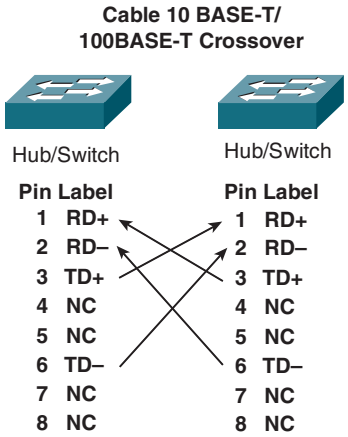


FIGURE 3-8
Straight-Through Wiring



Crossover cables are typically used to connect similar devices, such as switch-to-switch connections. The primary exception to this rule is switch-to-hub connections, which use a crossover cable. Figure 3-9 shows the pins for a crossover cable.

FIGURE 3-9
Crossover Wiring



Part II: Growing the Network (LANs)

Section 4
LAN Network Topologies

Choosing the Right Network Topology

A *topology* refers to the way in which network devices are connected.

A *physical topology* refers to the physical layout of the endpoints and the connecting cables. The three primary categories of physical topologies are as follows:

- Bus
- Ring
- Star

A *logical topology* refers to how signals travel from endpoint to endpoint. The physical and logical topologies can be the same or different. An example of this is a network in which each endpoint is connected to every other endpoint (a meshed network) but the signal can flow in only sequential order (a ring network). The following sections discuss each topology.

As shown in Figure 4-1, a bus or linear bus connects all devices with a single cable. The ends of the wire must be connected to a device or terminator, or signals will bounce back and cause errors. Only a single packet can be transmitted at a time on a bus, or the packets will collide and both will be destroyed (and must be resent).

 Please see page 311 for more details.

Figure 4-2 shows a ring topology. In a ring topology, a frame travels in a logical order around the ring, going from one end station to the next. If an end station wants to send data, it is added to the frame. The frame continues around the ring, and the data is removed at the intended destination. The frame, however, continues. In a single ring, data travels in a single direction. In a dual ring, each ring sends data in a different direction. Two rings create redundancy, or fault tolerance, which means that if one ring fails, the system can still operate. If parts of both rings fail, a "wrap" (a connection between the two rings) can heal the fault.

Star topologies are the most common physical topology in Ethernet LANs. As shown in Figure 4-3, stars have a central connection (hub, switch, or router) where all end devices meet. Stars cost more than other topologies but are more fault tolerant because a cable failure usually affects only one end device, or host. The disadvantage of a star is that if the central device fails, the entire system fails.

FIGURE 4-1
Bus Topology

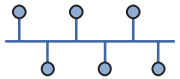


FIGURE 4-2
Ring Topology

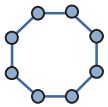
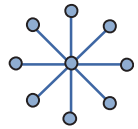
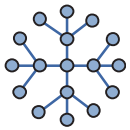


FIGURE 4-3
Star Topology



In an extended star, the central networking device connects to other networking devices, which then connect to end stations. Figure 4-4 shows an extended star topology.

FIGURE 4-4
Extended Star Topology



In a full-mesh topology, all devices are connected to all other devices. Great redundancy exists on full-mesh networks, but for networks with more than a few devices, it becomes overly expensive and complicated. Partial-mesh topologies, which have at least one device with multiple connections, provide good redundancy without the expense of full meshes. Figure 4-5 shows a full-mesh topology.

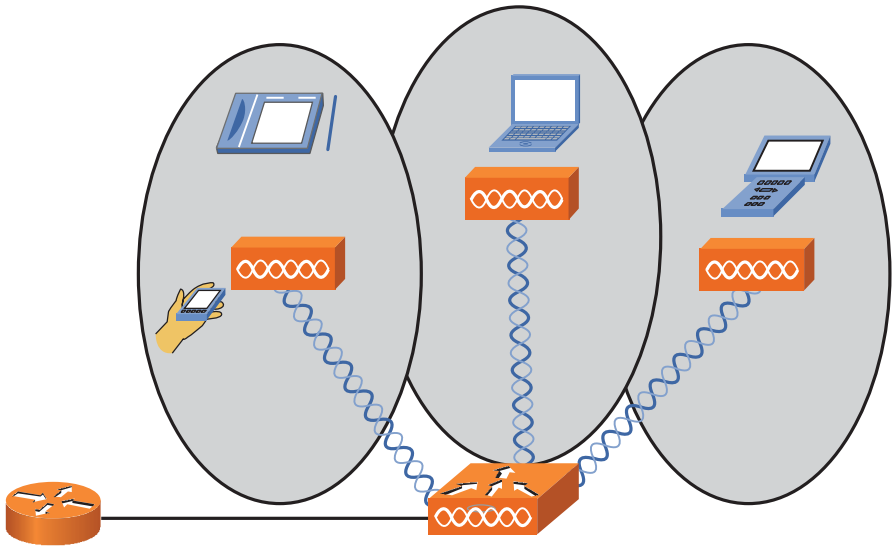
SECTION 4

LAN Network Topologies

FIGURE 4-5
Full-Mesh Topology

The last type of network topology is one that does not require the use of traditional cable connections, such as wireless networks. Wireless communications use radio frequencies (RF) or infrared (IR) waves to transmit data over a LAN. Wireless adapters must be installed on a laptop (wireless NIC) to communicate with the network. Wireless gives network designers many new options, because no physical medium is required to connect end stations (which is great for installation in old buildings or offices with inadequate space for cabling). See Figure 4-6.

FIGURE 4-6
Wireless Topology



 Please see page 311 for more details.

The Challenges of Shared LANs

An Ethernet segment is a network connection made by a single unbroken network cable. Segments can only span a limited physical distance. Any transmission beyond the physical limitation will degrade the signal. Table 4-1 lists the Ethernet segment distance limitations.

TABLE 4-1 Ethernet Segment Distance Limitations

Ethernet Specification	Description	Segment Length
10BASE-T	10 Mbps over twisted-pair	100 m
10BASE-FL	10 Mbps over fiber	2000 m
100BASE-TX	100 Mbps over twisted-pair	100 m
100BASE-FX	100 Mbps over fiber	400 m
1000BASE-T	Gigabit Ethernet over twisted-pair	100 m
1000BASE-LX	Gigabit Ethernet over fiber	Multimode: 550 m Single-mode: 10 km
1000BASE-SX	Gigabit Ethernet over fiber	62.5µ multimode: 250 m 50µ multimode: 550 m

Extending a LAN Segment

Although Ethernet has segment distance limitations, you can extend the segment by adding repeaters, hubs, or switches.

Repeaters are Layer 1 devices that amplify a signal from one segment to another.

Hubs, also called Ethernet concentrators or Ethernet repeaters, are self-contained Ethernet segments in a box. All devices connected to a hub compete for the same amount of bandwidth. Hubs let you add and remove computers without

 Please see page 311 for more details.

disabling the network but do not create additional collision domains. Hubs provide no filtering and forward all traffic out all ports regardless of where they are destined.

Switches are Layer 2 devices that amplify a signal and use Layer 2 information to route traffic.

Collisions and Collision Domains

In traditional Ethernet segments, all devices compete for the same bandwidth. The network segments that share the same bandwidth are called collision domains. All devices on the same network segment receive all signals sent on the segment. Collisions occur when two or more end stations "listen" for traffic on the segment, hear nothing, and then transmit at the same time. The simultaneous transmissions collide, and all are destroyed and must be resent. Each end station resends after a random time (called a backoff algorithm). As the number of end stations increases, collisions increase to the point where the system is virtually unusable because collisions are constantly occurring. Collisions are by-products of CSMA/CD. As networks grow, the chances that devices transmit at the same time increase, resulting in more collisions.

Repeaters and hubs amplify a signal and increase segment distance limitations; however, they cannot decrease collisions.

A collision domain is a group of devices connected to the same network segment such that if two devices access the medium at the same time, a collision results.

Solving Network Challenges with Switched LAN Technology

As networks grow and evolve, network congestion increases. The most common causes of network congestion are as follows:

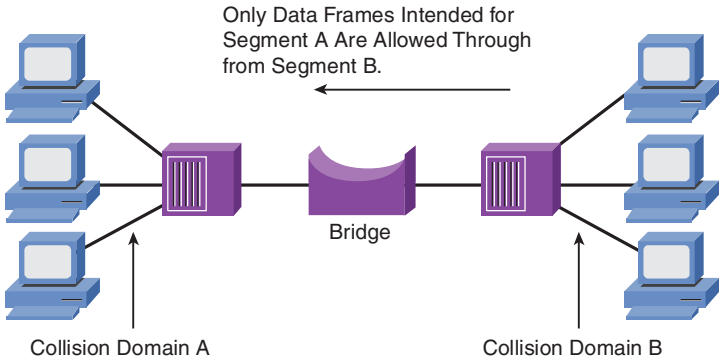
- Increases in PC speed and performance
- Increases in network data
- Bandwidth-intensive applications

 Please see page 311 for more details.

Bridges

Bridges were used as an early solution for network congestion. Bridges used the concept of segmentation to allow more end stations to be added to a LAN (called scaling). Segmentation is a method of breaking up collision domains. Bridges are more intelligent than hubs and can forward or block traffic based on the data frame's destination address (whereas hubs just send the frame to every port and end station). Segmentation is shown in Figure 4-7.

FIGURE 4-7
Segmenting a Network Through Bridges



Switches

Layer 2 switches are really just high-speed, multiport, very smart bridges. Unlike bridges that process frames using software, switches process frames in hardware through the use of application-specific integrated circuits (ASICs). Switches also have the following features:

- **High-speed backplane:** A circuit board that allows the switch to monitor multiple conversations, which increases the network's overall speed.
- **Data buffering:** A buffer is memory storage. This function allows the switch to store frames and forward them to the correct port.
- **Higher port density:** Port density is the number of ports available on a single device. A switch can have hundreds of ports.

 Please see page 311 for more details.

- **High port speeds:** Switches can support a mixture of port speeds from 10 Mbps to 10 Gbps.
- **Lower latency:** Latency is the measure of the time it takes an incoming frame to come back out of a switch.
- **Virtual LANs (VLAN):** Switches can logically segment networks into separate broadcast domains.

All these features (particularly port density) allow microsegmentation, which means that each end station has a dedicated switch port. This eliminates collisions, because each collision domain has only a single end station. Although these features can reduce some network congestion, faster PCs can flood a network with traffic. Broadcasts and multicasts also contribute to network congestion.

Switch Frame Transmission Modes

The following three primary frame switching modes exist:

- **Cut-through:** The switch checks the destination address and immediately begins forwarding the frame. This can decrease latency but can also transmit frames containing errors.
- **Store and forward:** The switch waits to receive the entire frame before forwarding. The entire frame is read, and a cyclic redundancy check (CRC) is performed. If the CRC is bad, the frame is discarded. Latency increases as a function of frame length.
- **Fragment-free (modified cut-through):** The switch reads the first 64 bytes before forwarding the frame. The minimum number of bytes necessary to detect and filter out collision frames is 64 bytes.

How Switches Segment the Ethernet Network

Ethernet switches perform three major functions in segmenting a network: forwarding, filtering, and flooding.

Switches perform these functions by the following methods:

- **MAC address learning:** Switches learn the MAC addresses of devices attached to each of their ports. These addresses are stored in a MAC database.

 Please see page 311 for more details.

- **Forwarding and filtering:** Switches determine which port a frame must be sent out to reach its destination. If the address is known, the frame is sent only on that port. If it's unknown, the frame is flooded to all ports except the one from which it originated.
- **Flooding:** Switches flood all unknown frames, broadcasts, and multicasts to all ports on the switch except the one from which it originated.

Switches in Action

A switch uses its MAC address table when forwarding frames to devices. When a switch is first powered on, it has an empty MAC address table. With an empty MAC address table, the switch must learn the MAC addresses of attached devices. This learning process is outlined below using Figure 4-8:

Step 1. Initially, the switch MAC address table is empty.

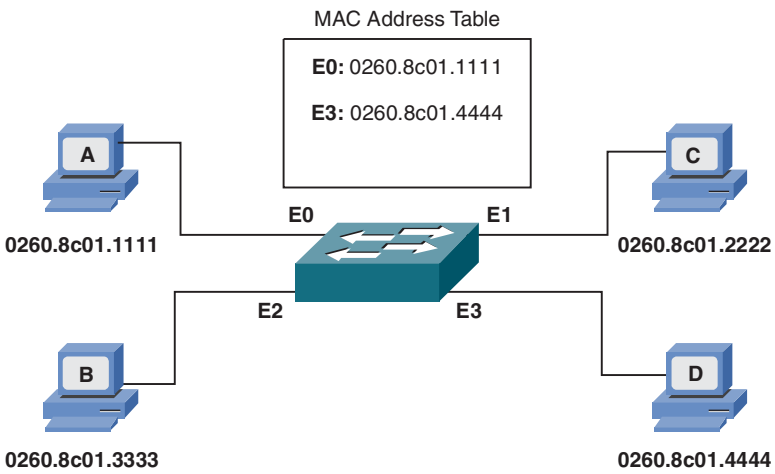
Step 2. Station A with the MAC address sends a frame to station C. When the switch receives this frame, it does the following:

- Because the MAC table is empty, the switch must flood the frame to all other ports (except E0, the frame origin).
- The switch notes the source address of the originating device and associates it with port E0 in its MAC address table entry.

Step 3. The switch continues to learn addresses in this manner, continually updating the table. As the MAC table becomes more complete, the switching becomes more efficient, because frames are forwarded to specific ports rather than being flooded out all ports.

 Please see page 311 for more details.

FIGURE 4-8
Frame Forwarding by a Switch



 Please see page 311 for more details.

Section 5
Operating Cisco IOS

Cisco IOS enables network services in switches and routers. It provides the following features:

- Carries network protocols and functions
- Connectivity
- Security
- Scalability
- Reliability

The Cisco IOS command-line interface (CLI) can be accessed through a console connection, modem connection, or Telnet/SSH sessions. These connections are called EXEC sessions.

Cisco Device Startup

When a Cisco device starts up, it goes through the following steps:

Step 1. Completes power-on self test (POST)

Step 2. Finds and loads Cisco IOS Software image

Step 3. Finds and applies device configuration

 Please see page 311 for more details.

External Configuration Sources

An IOS device can be configured from any of the following external sources:

- Console terminal
- Remote terminal (aux port)
- Telnet
- TFTP
- CiscoWorks
- SSH

Only a console connection or remote terminal connection can be used to initially configure a router or switch.

Console Connection

To establish a connection through a console port, you need a rollover cable to connect a console port to a PC. To set up the connection, follow these steps:

Step 1. Cable the device using a rollover cable. You might need an adapter for the PC.

Step 2. Configure the terminal emulation application with the following COM port settings: 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.

 Please see page 311 for more details.

Cisco IOS Software Command-Line Interface Functions

Cisco IOS uses a hierarchy of commands in its command-mode structure. For security, Cisco IOS separates EXEC sessions into these two access levels:

- User EXEC mode (user mode)
- Privileged EXEC mode (enable mode)

User EXEC mode is the first mode you enter when you log in to the IOS. This mode is limited and is mostly used to view statistics. You cannot change a router's configuration in this mode. By default, the greater-than sign (>) indicates that you are in user mode. This is how the router prompt looks in user mode:

```
Router>
```

In privileged EXEC mode, you can view and change the configuration in a router; you have access to all the router's commands and the powerful **debug** commands.

To enter privileged mode, enter the **enable** command while in user mode. By default, the pound symbol (#) indicates that you are in privileged mode. This mode is usually protected with a password. Here is an example of how to enter privileged mode. You also see the output of the prompt:

```
Router>enable
Password:
Router#
```

Keyboard Help in the CLI

Several commands built into IOS provide help when you enter configuration commands:

- **?** displays a list of commonly used commands.

 Please see page 311 for more details.

- **-More** appears at the bottom of the screen when additional information exists. Display the next available screen by pressing the spacebar. Display the next line by pressing Enter. Press any other key to return to the user-mode prompt.
- **s?** lists all commands that start with *s*.
- **show ?** lists all variants of the **show** command.

Enhanced Editing Commands

Enabled by default, enhanced editing commands allow shortcuts to speed the editing process. Table 5-1 shows the enhanced editing commands available in Cisco IOS Software.

TABLE 5-1 Enhanced Editing Commands

Command	Action
Ctrl-A	Moves the cursor to the beginning of the line
Ctrl-E	Moves the cursor to the end of the line
Esc-B	Moves the cursor back one word
Esc-F	Moves the cursor forward one word
Ctrl-B	Moves the cursor back one character
Ctrl-F	Moves the cursor forward one character
Ctrl-D	Deletes a single character
Backspace	Removes one character to the left of the cursor
Ctrl-R	Redisplays a line
Ctrl-U	Erases from the cursor to the beginning of the line

continues

TABLE 5-1 Enhanced Editing Commands *continued*

Command	Action
Ctrl-W	Erases a word
Ctrl-Z	Ends configuration mode and returns to the EXEC mode
Tab	Completes a partially entered (unambiguous) command
Ctrl-P or up arrow	Recalls commands, beginning with the most recent
Ctrl-N or down arrow	Returns the most recent commands in the buffer

Command History

A command history is available to review previously entered commands. This buffer defaults to ten lines, but it can be configured to a maximum of 256 using the **history size** command, as follows:

```
terminal history size number-of-lines      sets session command buffer size
history size number-of-lines               sets the buffer size permanently
show history                               shows command buffer contents
```

Console Error Messages

When you enter an incorrect command, you receive one of three messages detailed in Table 5-2.

 Please see page 311 for more details.

TABLE 5-2 Console Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	Not enough characters were entered to define a specific command.	Reenter the command, followed by a question mark (?), with no space between the command and the question mark.
% Incomplete command.	Keywords or values are missing.	Reenter the command, followed by a question mark (?), with a space between the command and the question mark.
% Invalid input detected at '^' marker.	The command was entered incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands or parameters that are available in this mode.

 Please see page 311 for more details.

Section 6
Configuring a Cisco Switch

Starting a Switch

When a Catalyst switch is started for the first time, a default configuration is loaded. Three main operations are performed during normal startup:

1. A power-on self test (POST) checks the hardware.
2. A startup routine initiates the operating system.
3. Software configuration settings are loaded.

Initial startup procedure:

Step 1. Before you start the switch, verify the following:

- All network cable connections are secure.
- A terminal is connected to the console port.
- A terminal application is selected.

Step 2. Attach the switch to the power source to start the switch (there is no on/off switch).

Step 3. Observe the boot sequence.

 Please see page 311 for more details.

Switch LED Indicators

Figure 6-1 shows the LEDs on the front panel of the switch. These LEDs provide information on switch status during startup, normal operation, and fault conditions. Pressing the Mode button toggles through the following LED display modes:

- Port status
- Bandwidth utilization
- Full-duplex support

FIGURE 6-1
Catalyst 2960 LEDs

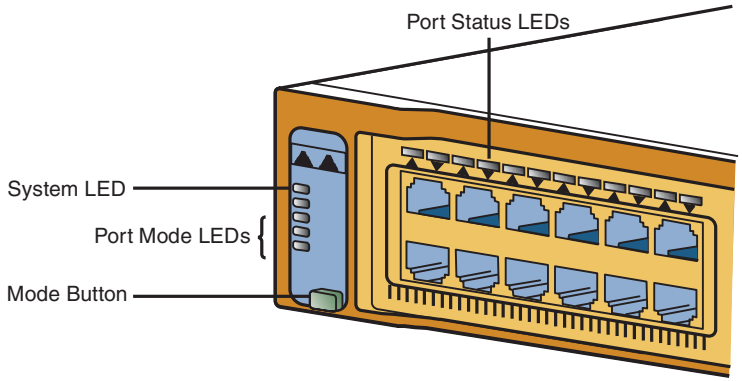


Table 6-1 details switch LED status indications for the Catalyst 2960.

TABLE 6-1 Catalyst 2960 LEDs

LED	Status
System LED	Green: System powered and operational Amber: System malfunction; one or more POST errors
Redundant power supply (RPS)	Green: RPS operational Flashing green: RPS connected but is powering another device Amber: RPS installed but not operational Flashing amber: The internal power supply and RPS have power and are powering the switch
Port status (STAT)	Green: Link present Flashing green: Link present with traffic activity Alternating green and amber: Link fault Amber: Port not forwarding
Bandwidth utilization (UTL)	Green: Bandwidth utilization displayed over the amber LED on a logarithmic scale Amber: Maximum backplane utilization since the switch was powered on Green and amber: Depends on the model
Full-duplex (FDUP)	Green: Ports are configured in full-duplex mode Off: Ports are half-duplex

Configuring a Switch from the Command Line

The following two configuration modes are available:

- **Global configuration:** Configures global parameters on a switch, such as IP address and host name
- **Interface configuration:** Configures parameters specific to a switch port

 Please see page 311 for more details.

The IOS command to enter global configuration mode is **configure terminal.**

The IOS command to enter interface configuration mode is **interface** *interface-id.*

To enter interface mode, you first need to be in global configuration mode. The *interface-id* parameter identifies the type and number of the interface you want to configure, as follows:

```
switch(config)#interface g0
switch(config-if)#
```

Configuring a Host Name

To give the switch a host name or identify it, use the **hostname** privileged IOS command, as follows:

```
switch(config)#hostname Admin-SW
Admin-Sw(config)#
```

Configuring the Switch IP Address and Default Gateway

To assign an IP address on a Catalyst 2960 switch, follow these steps:

Step 1. Enter the VLAN 1 interface. This is a logical interface used for management.

Step 2. Assign the IP address and subnet masks.

Step 3. Enable the interface by issuing the **no shutdown** command.

The following example shows the necessary command syntax for all three steps:

```
Admin-Sw(config)#interface vlan1
Admin-Sw(config-if)#ip address 192.168.0.10 255.255.255.0
Admin-Sw(config-if)#no shutdown
```

To configure the default gateway, use the **ip default-gateway** *ip-address* global configuration command, as follows:

```
Switch(config)#ip default-gateway 192.168.0.1
```

Showing Switch Status

To display the status of a switch, use one of the following commands:

- **show running-configuration** displays the currently active configuration in memory, including any changes made in the session that have not yet been saved.
- **show startup-config** displays the last saved configuration.
- **show version** displays information about the system hardware and software.
- **show interfaces** displays information on connections and ports that connect with other devices.

Managing MAC Addresses

NOTE
Some switches can be configured to dynamically learn MAC addresses associated with a port and automatically create a static entry for the learned MAC address in the MAC address table. This type of address is called a sticky address.

MAC address tables contain the following three types of addresses:

- Dynamic addresses are learned by the switch and then are dropped when they are not in use.
- Permanent and static addresses are assigned by an administrator.

MAC Address Configuration

The **mac-address-table static** global configuration command associates a MAC address with a particular switched port interface. The syntax for the **mac-address-table** command is as follows:

```
mac-address-table static mac-address vlan vlan-id interface interface-id
```

You verify the MAC address table settings using the **show mac-address-table** command.

 Please see page 311 for more details.

Understanding Switch Security

Securing a switch includes physical, environmental, and access security. Physical and environmental security is outlined in Chapter 2.

Some basic security suggestions for network devices are as follows:

- Use complex passwords for all devices.
- Limit Telnet access using access lists.
- Use SSH instead of Telnet.
- Physically secure access to the switch.
- Use banners to warn against unauthorized access.
- Set up and monitor syslog.
- Configure port security.
- Disable unused ports.

Configuring Password Security

The CLI is used to configure password security. You configure passwords to secure access to the switch. You can configure the following passwords using the CLI:

- **Console:** Password that accesses the console port
- **Telnet:** Password that accesses the virtual terminal ports on the switch
- **Enable:** Nonencrypted password that accesses privileged EXEC mode
- **Secret:** Encrypted password that accesses privileged EXEC mode

 Please see page 311 for more details.

If the enable password and the enable secret password are both set on the switch, the enable secret password will override the enable password.

The console, Telnet, and enable passwords are displayed unencrypted. To encrypt them, use the **service password-encryption** global command, as follows:

```
Cat2960(config)#service password-encryption
```

Configuring Console Password

To configure the console password, enter the following:

```
Cat2960(config)#line console 0
Cat2960(config-line)#login
Cat2960(config-line)#password CCNA
```

Configuring Telnet Password

To configure the Telnet password, enter the following:

```
Cat2960(config)#line vty 0 15
Cat2960(config-line)#login
Cat2960(config-line)#password CCNA
```

Configuring Enable and Secret Passwords

To configure enable and secret passwords, enter the following:

```
Cat2960(config)#enable password Cisco
Cat2960(config)#enable secret cisco
```

 Please see page 311 for more details.

Configuring Login Banner and MOTD

The login banner is displayed before the username and password login prompts on a Catalyst switch. The login banner is configured using the **banner login** global command, as follows:

```
Cat2960#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Cat2960(config)#banner login #
Enter TEXT message.  End with the character '#'.
Notice! Only Authorized Personnel Are Allowed to Access This Device
#
```

The message of the day (MOTD) is displayed before the login banner. It is displayed to anyone who connects to the Cisco IOS device through Telnet, console port, or auxiliary port. Use the **banner motd #** *text* **#** global configuration command to configure the MOTD. In the previous command, the # character is a delimiting character and can be any character.

```
Cat2960(config)#banner motd #      <ENTER>
Enter TEXT message.  End with the character '#'.
Warning only authorized users many access this switch. <ENTER>
#
Cat2960(config)#
```

SSH Access

Cisco recommends using SSH to encrypt communication between the Cisco device and the host. Telnet is unsecure, and all communication between the Cisco device and the host is sent in clear text. Use the following steps to configure SSH access:

Step 1. Create a local username and password on the device.

Step 2. Assign a domain name to the device.

 Please see page 311 for more details.

Step 3. Generate a security key.

Step 4. Enable SSH.

Step 5. Configure vty ports to authenticate using SSH.

The following commands demonstrate how to configure SSH access:

```
switch(config)#username eric password 0 ciscopress
switch(config)#ip domain-name cisco.com
switch(config)#crypto key generate rsa
The name for the keys will be: switch.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
switch(config)#ip ssh ver 2
switch(config)#line vty 0 15
switch(config-line)#login local
switch(config-line)#transport input telnet ssh
```

Securing vty Access

By default, any IP address can connect to a vty line. Recommended practice dictates restricting access to vty lines by IP address. This is done through standard access lists.

Standard access lists allow you to permit or deny traffic based on the source IP address. To restrict access to vty lines, you would create a standard access list that permits each authorized IP address to connect to vty and apply the access list to the vty lines.

 Please see page 311 for more details.

At the end of each access list is an implicit deny any statement. So, if a host is not specifically permitted, it will be denied.

Wildcard Masks

Wildcard masks define the subset of the 32 bits in the IP address that must be matched.

Wildcards are used with access lists to specify a host, network, or part of a network. Wildcard masks work exactly the opposite of subnet masks.

In wildcard masks, when 0s are present, the octet address must match. Mask bits with a binary value of 1 are wildcards. For example, if you have an IP address 172.16.0.0 with a wildcard mask of 0.0.255.255, the first two portions of the IP address must match 172.16, but the last two octets can be in the range of 1 to 255.

Configuring and Applying vty Access Lists

The command syntax to create a standard IP access list is as follows:

```
access-list access-list-number {permit| deny} source-address
  [wildcard-mask]
```

The *access-list-number* parameter is a number from 1 to 99 or 1300 to 1999.

The command syntax to apply an access list to an interface is as follows:

```
access-class access-list-number {in | out}
```

The following commands create access list number 10, permitting Telnet access to the vty lines from IP network 192.168.10.0/24:

```
SwitchA(config)#access list 10 permit ip 192.168.10.0 0.0.0.255
SwitchA(config)#line vty 0 15
SwitchA(config-if)#access-class 10 in    This applies the access list to telnet ports
```

 Please see page 311 for more details.

Implementing and Verifying Port Security

Port security limits the number of MAC address allowed per port and can also limit which MAC addresses are allowed. Allowed MAC addresses can be manually configured or dynamically learned by the switch. The interface command to configure port security is as follows:

```
switchport port-security [mac-address mac-address | mac-address sticky [mac-address] | maximum value |
  violation {restrict | shutdown}
```

- **switchport port-security mac-address** *mac-address*: Manually configures the port to use a specific MAC address.
- **switchport port-security mac-address sticky:** Configures the switch to dynamically learn the MAC address of the device attached to the port.
- **switchport port-security maximum** *value*: Configures the maximum number of MAC addresses allowed on the port. The default value is 1.
- **switchport port-security violation {restrict | shutdown}:** Configures the action to be taken when the maximum number of MAC addresses is reached and when MAC addresses not associated with the port try to access the port. The restrict keyword tells the switch to restrict access to learned MAC addresses that are above the maximum defined addresses. The shutdown keyword tells the switch to shut down all access to the port if a violation occurs.

The following example demonstrates how to configure port security:

```
Cat2960(config)#int f0/1
Cat2960(config-if)#switchport mode access
Cat2960(config-if)#switchport port-security
Cat2960(config-if)#switchport port-security max 1
Cat2960(config-if)#switchport port-security mac-address sticky
Cat2960(config-if)#switchport port-sec violation restrict
```

 Please see page 311 for more details.

To verify port security use the **show port-security** command, as follows:

```
Cat2960#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-------------------------------------------------------------------------
     Fa0/1             1            0                  0         Restrict
-------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8320
```

Securing Unused Ports

To secure unused ports, either disable the port or place the port in an unused VLAN.

A switch port is disabled by issuing the **shutdown** interface command.

VLANs

Users of shared LANs are usually grouped based on where people are located rather than how they use the network (physical rather than logical). Shared LANs have little embedded security, because all traffic can be seen by all end stations. It is also expensive to make moves or changes in the network setup. Virtual LANs solve these problems.

The virtual LAN (VLAN) organizes physically separate users into the same broadcast domain. The use of VLANs improves performance, security, and flexibility. The use of VLANs also decreases the cost of arranging users, because no extra cabling is required.

VLAN Characteristics

VLANs are logical broadcast domains that can span multiple physical LAN segments.

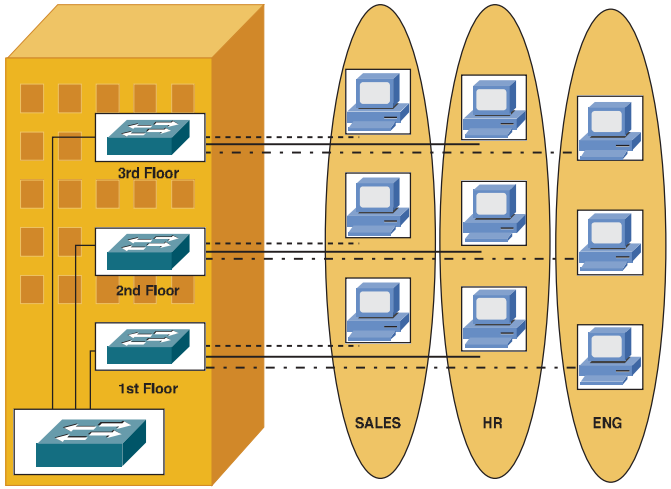
VLANs allow logically defined user groups rather than user groups defined by their physical locations. For example, you can arrange user groups such as accounting, engineering, and finance, rather than everyone on the first floor, everyone on the second floor, and so on.

VLANs are characterized as follows:

- VLANs define broadcast domains that can span multiple LAN segments.
- VLANs improve segmentation, flexibility, and security.
- VLAN segmentation is not bound by the physical location of users.
- Only ports assigned to a specific VLAN share broadcasts; other VLANs do not see other VLANs' broadcasts.
- A VLAN can exist on one or several switches.

Figure 6-2 shows a typical VLAN design.

FIGURE 6-2
VLAN Design



VLAN Operation

Each VLAN on a switch behaves as if it were a separate physical bridge. The switch forwards packets (including unicasts, multicasts, and broadcasts) only to ports assigned to the same VLAN from which they originated. This drastically reduces network traffic.

VLANs require a trunk or physical connection for each VLAN to span multiple switches. Each trunk can carry traffic for multiple VLANs.

VLAN Assignment

A port can be assigned (configured) to a given VLAN. VLAN membership can be either static or dynamic:

- **Static assignment:** The VLAN port is statically configured by an administrator.
- **Dynamic assignment:** The switch uses a VMPS (VLAN Membership Policy Server). The VMPS is a database that maps MAC addresses to VLANs. A port can belong to only one VLAN at a time. VLANs can also be assigned based on MAC addresses. This method offers flexibility but increases switching overhead (computer processing requirements).

Adding and Assigning VLANs

The **vlan** *vlan-id global* command adds a VLAN to a Catalyst 2960 switch, as demonstrated here:

```
Cat2960(config)#vlan 10
Cat2960(config-vlan)#name Admin
Cat2960(config-vlan)#vlan 20
Cat2960(config-vlan)#name Sales
```

 Please see page 311 for more details.

The **switchport access vlan** *vlan-id* interface command assigns a port to a specific VLAN, as demonstrated here:

```
Cat2960(config)#int f0/1
Cat2960(config-if)#switchport access vlan 10
Cat2960(config-if)#int f0/2
Cat2960(config-if)#switchport access vlan 20
```

Verifying VLANs

The commands to verify VLAN configurations are as follows:

- **show vlan id** *vlan#***:** Displays information about a specific VLAN
- **show vlan brief:** Displays one line for each VLAN that displays the VLAN name, the status, and the switch ports assigned to that VLAN
- **show vlan:** Displays information on all configured VLANs

Maximizing the Benefits of Switching

Microsegmentation

Microsegmentation is a network design (functionality) where each workstation or device on a network gets its own dedicated segment (collision domain) to the switch. Each network device gets the full bandwidth of the segment and does not have to share the segment with other devices. Microsegmentation reduces and can even eliminate collisions because each segment is its own collision domain.

Microsegmentation is implemented by installing LAN switches. Benefits of microsegmentation are as follows:

- Collision-free domains from one larger collision domain
- Efficient use of bandwidth by enabling full-duplex communication
- Low latency and high frame-forwarding rates at each interface port

 Please see page 311 for more details.

Duplex Communication

Duplexing is the mode of communication in which both ends can send and receive information. With full-duplex, bidirectional communication can occur at the same time. Half-duplex is also bidirectional communication, but signals can flow in only one direction at a time. Simplex runs in a single direction only. Table 6-1 provides a comparative summary of full-duplex, half-duplex, and simplex communication.

TABLE 6-1 Full-Duplex, Half-Duplex, and Simplex Communication

Full-Duplex	Half-Duplex	Simplex
Can send and receive data at the same time.	—	Data is sent in one direction only and can never return to the source over the same link.
Collision-free.	CSMA/CD is susceptible to collisions.	—
Point-to-point connection only.	Multipoint attachments.	Satellite TV downlink is an example.
Uses a dedicated switched port with separate circuits.	Can connect with both half- and full-duplex devices.	—
Efficiency is rated at 100 percent in both directions.	Efficiency is typically rated at 50 to 60 percent.	100 percent efficiency in one direction.
Both ends must be configured to run in full-duplex mode.	The duplex setting must match on devices sharing a segment.	Not used very often in internetworking.

Configuring and Verifying Port Duplex

The default port settings on a Catalyst 2960 switch are as follows:

- **Duplex:** auto
- **Speed:** auto

 Please see page 311 for more details.

To change the default settings, use the following commands:

```
Switch(config)#interface f0/1
Switch(config-if)#duplex {auto | full | half}
Switch(config-if)#speed {10 | 100 | 1000 | auto}
```

To view duplex and speed settings, use the **show interface** *interface-id* command, as follows:

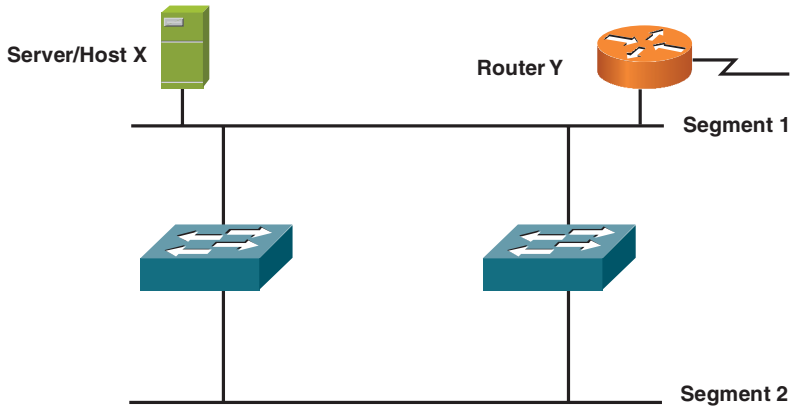
```
Cat2960#show interface f0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is Fast Ethernet, address is 0019.e81a.4801 (bia 0019.e81a.4801)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
```

Physical Redundancy in an Ethernet LAN

A redundant topology has multiple connections to switches or other devices. Redundancy ensures that a single point of failure does not cause the entire switched network to fail. Layer 2 redundancy, however, can cause problems in a network, including broadcast storms, multiple copies of frames, and MAC address table instability. Figure 6-3 depicts a redundant topology.

 Please see page 311 for more details.

FIGURE 6-3
Redundant Topology



Spanning Tree Protocol

The solution to problems caused in a redundant switched network is the Spanning Tree Protocol (STP). STP is a Layer 2 protocol that prevents looping traffic in a redundant switched network by blocking traffic on the redundant links. If the main link goes down, STP activates the standby path. STP operation is transparent to end stations.

Troubleshooting Switch Issues

When troubleshooting switch issues, remember the following:

- Switches operate at Layer 2 of the OSI model.
- Switches provide an interface to the physical media.
- Problems generally are seen at Layer 1 and Layer 2.
- Layer 3 issues could be regarding IP connectivity to the switch for management purposes.

 Please see page 311 for more details.

Identifying and Resolving Media Issues

Common switch Layer 1 issues include the following:

- Bad wires or damaged wires.
- EMI is introduced.
- New equipment is installed.

Bad wiring and EMI commonly show up as excessive collisions and noise. This is displayed by excessive collisions and runts when issuing the **show interface** command, as follows:

```
SwitchA#show interface g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet Port, address is 000d.65ac.5040 (bia 000d.65ac.5040)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<Text-Ommited>
  5 minute output rate 10000 bits/sec, 7 packets/sec
     1476671 packets input, 363178961 bytes, 0 no buffer
     Received 20320 broadcasts (12683 multicast)
     0 runts, 0 giants, 0 throttles
     3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     1680749 packets output, 880704302 bytes, 0 underruns
     8 output errors, 1874 collisions, 15 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

 Please see page 311 for more details.

Identifying and Resolving Access Port Issues

Common port access issues are as follows:

- Media-related issues
- Duplex mismatch
- Speed mismatch

Media-Related Issues

Media-related issues might be reported as an access issue; for example, a user might say that she cannot access the network. Media issues should be isolated and resolved as indicated in the previous topic.

Duplex Issues

The following items can create duplex issues:

- One end set to full-duplex and the other set to half-duplex results in a duplex mismatch.
- One end set to full-duplex and auto-negotiation on the other:
  - Auto-negotiation will fail, and the end reverts to half-duplex.
  - Results in a duplex mismatch.
- One end set to half-duplex and auto-negotiation on the other:
  - Auto-negotiation will fail, and the end reverts to half-duplex.
  - Both ends set to half-duplex causes no mismatch.

 Please see page 311 for more details.

Speed Issues

- One end set to one speed and the other set to another results in a mismatch.
- One end set to a higher speed and auto-negotiation on the other:
  - Auto-negotiation will fail, and the end will revert to a lower speed.
  - Results in a mismatch.

 Please see page 311 for more details.

Section 7
Extending the LAN

Exploring Wireless Networking

In recent years, business's need for network mobility has made wireless LANs (WLANs) common in today's networks. Unlike wired LANs, wireless devices transmit and receive data using radio frequencies (RF) or infrared signals. These frequencies or signals are sent through an access point (AP).

The AP is like a hub or switch on a wired LAN and is the connectivity point for all wireless devices to access the network.

WLANs are based on IEEE standards that define physical and data-link specifications. Because the standards define Layer 1 and Layer 2 specifications, higher-layer protocols such as IP and IPsec can function on WLANs.

The IEEE standards on WLANs, such as 802.11a/b/g, use unlicensed radio frequencies. As such, an RF license is not needed to implement WLANs.

Difference Between WLANs and LANs

The following are some of the differences between WLANs and LANs:

- WLANs use radio waves as the physical layer.
- WLANs use carrier sense multiple access collision avoidance (CSMA/CA) instead of CSMA/CD for media access.
- WLANs operate in half-duplex.

 Please see page 311 for more details.

- WLANs use a different frame type than Ethernet.
- Radio waves have problems that are not found on wires, such as
  - Connectivity issues such as coverage problems, interference, and noise
  - Privacy issues
- An access point is a shared device similar to an Ethernet hub for shared bandwidth.
- WLANs must adhere to each country's RF standards.
- WLAN devices have no physical network connection. They are often mobile and battery powered.

Radio Frequency Transmission

Radio frequencies are radiated into the air through an antenna, creating radio waves. Higher frequencies allow higher data rates but also have a shorter distance. Outside objects can affect radio waves, resulting in the following:

- **Reflection:** Occurs when RF waves bounce off objects like metal or glass
- **Scattering:** Occurs when RF waves strike uneven surfaces
- **Absorption:** Occurs when RF waves are absorbed by objects such as water

As shown in Table 7-1, several unlicensed bands are used by the ITU-R local FCC Wireless.

TABLE 7-1 ITU-R Local FCC Wireless Bands

Band	Range
900 MHz	902 to 928 MHz
2.4 GHz	2.400 to 2.483 GHz
5 GHz	5.150 to 5.350 GHz, 5.725 to 5.825 GHz

 Please see page 311 for more details.

Although these three frequencies do not require licenses, local country code regulations still exist inside the frequencies to limit characteristics such as transmission power, antenna gain, and the total summation of transmitter, cable, and antenna.

Effective Isotropic Radiated Power (EIRP) is the final unit of measurement monitored by local regulatory agencies. EIRP is calculated using the following formula:

EIRP = Transmitter power + Antenna gain – Cable loss

802.11 Standards

Table 7-2 shows the different 802.11 standards.

TABLE 7-2 802.11 Standards

	802.11	802.11b	802.11a	802.11g
Ratified	1997	1999	1999	2003
Frequency Band (GHz)	2.4	2.4	5	2.5
No. of Channels	3	3	Up to 23	3
Transmission	IR, FHSS, DSSS	DSSS	OFDM	DSSS-OFDM
Data Rates (Mbps)	1, 2	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11 and 6, 9, 12, 18, 24, 36, 48, 54

 Please see page 311 for more details.

These standards are described as follows:

- **802.11b** uses Direct Sequence Spread Spectrum (DSSS). It has four data rates: 1, 2, 5.5, and 11 Mbps. 802.11b provides up to 14 channels, but only 3 channels have nonoverlapping frequencies: 1, 6, and 11.
- **802.11a** uses Orthogonal Frequency-Division Multiplexing (OFDM). It has eight data rates: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. 802.11a provides from 12 to 23 nonoverlapping channels.
- **802.11g** uses three nonoverlapping channels: 1, 6, and 11. It uses DSSS to provide 1-, 2-, 5.5-, and 11-Mbps speeds for backward compatibility to 802.11b. It uses OFDM to provide the following rates: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

WLAN Security

With the increase of low-cost APs, hackers are finding it easier to compromise WLANs.

WLAN Security Threats

WLANs security threats include the following:

- **War driving:** A term used to describe when someone is driving around with a laptop and wireless card/antenna, looking for wireless access points to exploit.
- **Hackers:** Most hackers start by war driving. When an access point is identified, hackers try to exploit weak security keys and passwords to gain access to the network.
- **Rogue APs:** Access points installed on a WLAN that can be used to interfere with day-to-day network operation. Rogue APs are also unauthorized APs installed on the network by employees.

 Please see page 311 for more details.

Mitigating Security Threats

Three steps a network administrator can take to mitigate security threats are as follows:

- Use authentication to ensure that only authorized clients access the WLAN.
- Encrypt wireless data.
- Use intrusion detection/prevention systems to monitor, identify, and prevent WLAN attacks.

Evolution of Wireless LAN Security

Wireless security methods have evolved over time to increase security. Wireless security methods, listed from weakest to strongest, include the following:

- **Wired Equivalent Privacy (WEP):** Uses basic encryption, weak authentication, and static keys and is not scalable.
- **802.1x EAP:** Uses dynamic keys, stronger encryption, and user authentication.
- **Wi-Fi Protected Access (WPA):** Created by the Wi-Fi Alliance as a standard. Uses Temporal Key Integrity Protocol (TKIP) for encryption, dynamic keys, and 802.1x user authentication.
- **WPA2 (802.11i):** Uses Advanced Encryption Standard (AES) for strong encryption, 802.1x authentication, and dynamic keys.

Wireless Client Association

Wireless clients associate with APs as follows:

1. APs send out beacons announcing the service set identifier (SSID) and data rates.
2. The client scans all changes and sends out probe requests.

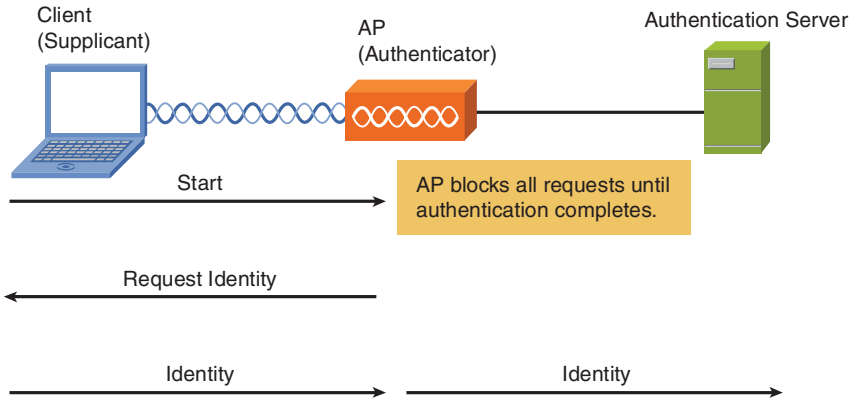
 Please see page 311 for more details.

3. The AP sends a probe response, and the client listens for the response from the APs.
4. The client associates to the AP with the strongest signal. Authentication and other security information is sent to the AP.
5. The AP accepts the association.

802.1x on a WLAN

Figure 7-1 shows how 802.1x works on a WLAN.

FIGURE 7-1
802.1x



1. The client becomes active on the medium and associates to the access point. The access point detects the client association and enables the client's port. It forces the port into an unauthorized state, so only 802.1x traffic is forwarded.
2. The access point replies with an EAP-Request Identity message to the client to obtain the client's identity. The client's EAP-Response packet, which contains the client's identity, is forwarded to the authentication server.

 Please see page 311 for more details.

3. The authentication server authenticates the client and sends an ACCEPT or REJECT packet from the authentication server to the access point.
4. Upon receiving the ACCEPT packet, the access point transitions the client's port to an authorized state and traffic is forwarded.

WPA and WPA2 Modes

WPA and WPA2 support these two modes:

- **Enterprise:** Products that are interoperable with both Pre-Shared Key (PSK) and IEEE 802.1x/EAP for authentication
- **Personal:** Products tested to be interoperable in the PSK-only authentication mode

Implementing a WLAN

802.11 supports the following two topologies:

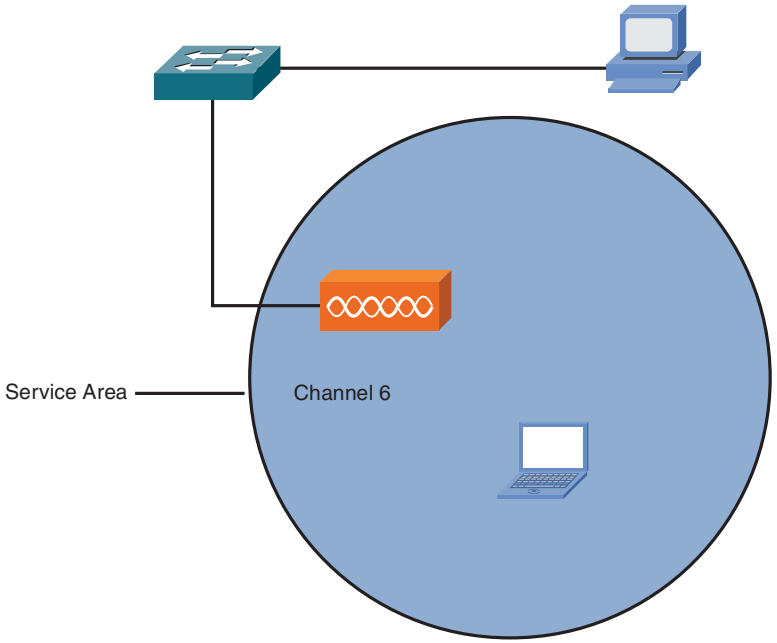
- **Ad hoc mode:** Wireless clients connect directly to each other without an access point.
- **Infrastructure mode:** Wireless clients connect through an access point. The following two modes of infrastructure mode exist:
  - **Basic Service Set (BSS):** Wireless clients connect to each other and the wireless network through one access point.
  - **Extended Service Set (ESS):** More than one access point exists, with all APs configured with a common SSID to allow roaming.

 Please see page 311 for more details.

WLAN Service Area and Data Rates

As shown in Figure 7-2, the basic service area is the access point's RF coverage area. In other words, it is the area that is covered by the access point.

FIGURE 7-2
Basic Service Area

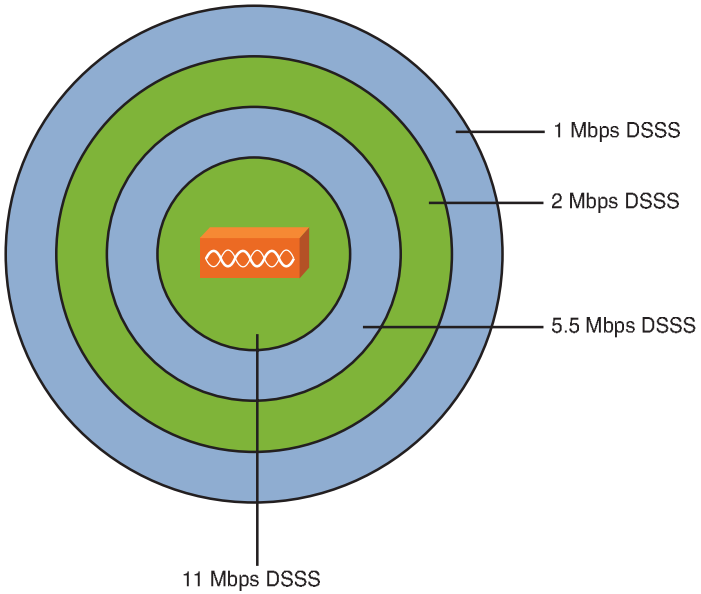


WLAN clients can shift data rates while moving. The closer a client is to an AP, the higher the data rate; the farther the client is from the AP, the lower the data rate.

Rate shifting occurs on a transmission-by-transmission basis. Clients will always try to communicate with the highest possible data rate. Figure 7-3 shows the data rates for 802.11b.

 Please see page 311 for more details.

FIGURE 7-3
802.11b Data Rates



Access Point Configuration

APs can be configured through a command-line interface or a browser GUI. APs should be configured with the following parameters:

- IP address, subnet mask, and default gateway
- Wireless protocol (802.11g, 802.11a/b/g, 802.11a)
- RF channel
- SSID
- Authentication method
- Encryption method
- Optional power adjustment

 Please see page 311 for more details.

Steps to Implement a Wireless Network

Seven basic steps are required to implement a wireless network:

Step 1. Verify wired operation, including DHCP and Internet access.

Step 2. Install the AP.

Step 3. Configure the AP with no security.

Step 4. Install and configure a wireless client with no security.

Step 5. Verify wireless connectivity.

Step 6. Configure security on the AP and client.

Step 7. Verify wireless operation.

Wireless Troubleshooting

Most wireless problems are due to incorrect configuration. Steps to troubleshoot configurations are as follows:

- Verify channel configuration.
- Verify that users have the correct passwords and encryption type.

Other common wireless problems are due to RF installation. You should verify the following:

- The radio is enabled on both the AP and the clients.
- The external antenna is connected.
- The antenna is in the optimal position.
- Check for interference from outside objects such as metal or water.

 Please see page 311 for more details.

Part III: Connecting LANs

Section 8
Exploring the Functions of Routing

Router Overview

Routing is the act of finding a path to a destination and moving data across this path from source to destination. The routing process uses network routing tables, protocols, and algorithms to determine the most efficient path for forwarding the IP packet.

Router Function

Routers have the following two key functions:

- **Path determination:** Routing tables and network addresses transmit packets through the network. The process of routing includes determining the optimum path through the network. Routers do this by using a routing protocol to communicate the network information from the router's own routing table with neighboring router's.
- **Packet forwarding:** After the path is determined, a router forwards the packets through its network interface toward the destination.

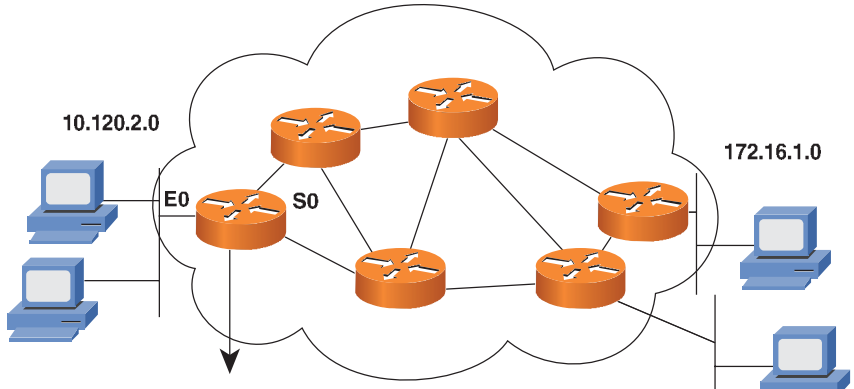
 Please see page 311 for more details.

Key Information a Router Needs

In Figure 8-1, for hosts in network 10.120.2.0 to communicate with hosts in network 172.16.1.0, a router needs the following key information:

- **Destination address:** The destination (typically an IP address) of the information being sent
- **Sources of information:** Where the information came from (typically an IP address)
- **Possible routes:** The likely routes to get from source to destination
- **Best route:** The best path to the intended destination
- **Status of routes:** The known paths to destination

FIGURE 8-1
Routing Tables



Network Protocol	Destination Network	Exit Interface
Connected	10.120.2.0	E0
RIP	172.16.2.0	S0
EIGRP	172.17.3.0	S1

Routed Protocol: IP
Routing Protocol: RIP, EIGRP

 Please see page 311 for more details.

Routing Versus Routed

Network layer protocols are either routed protocols or routing protocols. These are defined as follows:

- **A routed protocol:**
  - Is any network layer protocol that provides enough information within its address to allow the packet to direct user traffic.
  - Defines the address format and use of fields within the packet.

    Routed protocols include IP, Internetwork Packet Exchange (IPX), AppleTalk, and others.
- **Routing protocols** determine how routed protocols are used by:
  - Providing mechanisms for sharing routing information.
  - Allowing routers to update each other about network changes.

    Routing Information Protocol (RIP), Enhanced IGRP (EIGRP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) are examples of routing protocols.

Path Determination

Routing tables and network addresses transmit packets through the network. The process of routing includes determining the optimum path through the network and then moving the packets along the path.

A router can use the following types of entries in the routing table to select the best path:

- **Static routes:** Manually entered routes in the routing table
- **Dynamic routes:** Routes dynamically learned from a routing protocol
- **Default routes:** A static or dynamic route that tells the router where to route packets not explicitly in the router's routing table

 Please see page 311 for more details.

Routing Table

A router is constantly learning about routes in the network and storing this information in its routing table. The router uses its table to make forwarding decisions. The router learns about routes in one of three ways:

- Directly connected networks
- Statically (routing information entered by the network administrator)
- Dynamically (a routing process running in the network)

Information stored in a routing table includes destination/next-hop and routing metrics. Destination/next-hop tells the router whether the destination is directly connected or is available through an adjacent router.

Dynamic Routing Protocols

Routing protocols use their own rules and metrics to build and update routing tables automatically. Routing metrics are measures of path desirability. Different protocols use different metrics. Some common metrics are as follows:

- **Bandwidth:** The link's data capacity.
- **Delay:** The time required to move the packet from the current router to the destination. This depends on the bandwidth of intermediate links, port delays at each router, congestion, and distance.
- **Load:** The amount of activity on the network.
- **Reliability:** The error rate of each network link.
- **Hop count:** The number of routers the packet must travel through before reaching the destination.
- **Cost:** An arbitrary value based on bandwidth, expense, and other metrics assigned by the administrator.

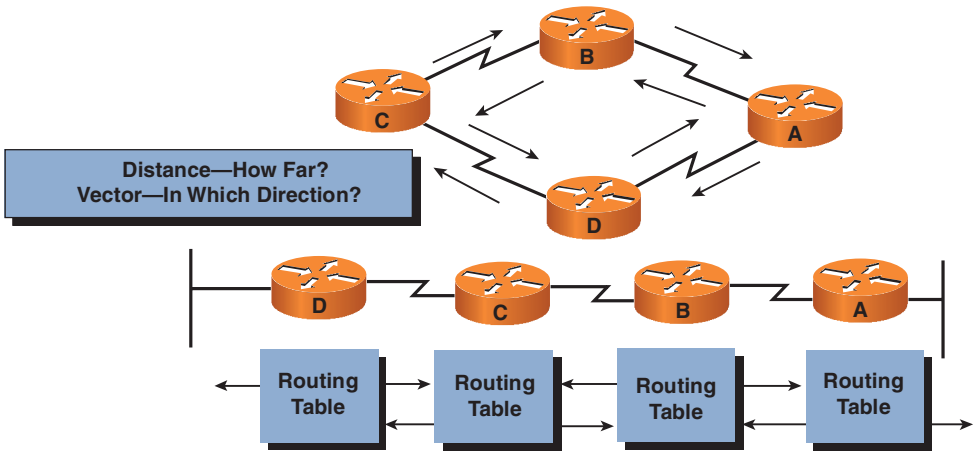
 Please see page 311 for more details.

Routing Methods

Routing protocols are designed around one of the following routing methods:

- **Distance vector routing:** Routers using distance vector–based routing share routing table information with each other. This method of updating is called "routing by rumor." Each router receives updates from its direct neighbor. In Figure 8-2, Router B shares information with Routers A and C. Router C shares routing information with Routers B and D. In this case, the routing information is distance vector metrics (such as the number of hops). Each router increments the metrics as they are passed on (incrementing hop count, for example). Distance accumulation keeps track of the routing distance between any two points in the network, but the routers do not know the exact topology of an internetwork. RIP is an example of a distance vector routing protocol.

FIGURE 8-2
Distance Vector Routing Protocols

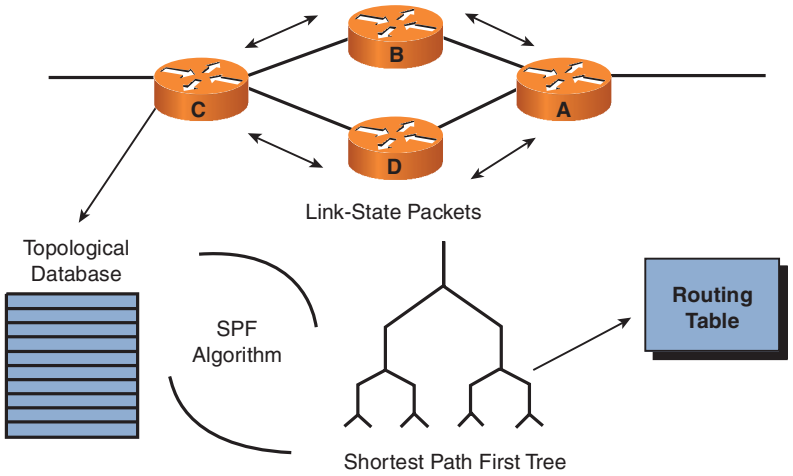


- **Link-state routing:** The link-state–based routing algorithm (also known as shortest path first [SPF]) maintains a database of topology information. Unlike the distance vector algorithm, link-state routing maintains full knowledge

of distant routers and how they interconnect. Network information is shared in the form of link-state advertisements (LSA). See Figure 8-3. Link-state routing provides better scaling than distance vector routing for the following reasons:

- Link-state sends only topology changes. Distance vector sends complete routing tables.
- Link-state updates are sent less often than distance vector updates.
- Link-state uses a two-state hierarchy (areas and autonomous systems), which limits the scope of route changes.
- Link-state supports classless addressing and summarization.
- Link-state routing converges fast and is robust against routing loops, but it requires a great deal of memory and strict network designs.

FIGURE 8-3
Link-State Routing Protocols



OSPF and Intermediate System–to–Intermediate System (IS-IS) are examples of link-state routing protocols.

- **Advanced distance vector:** Combines aspects of both distance vector and link-state protocols. Balanced hybrid routing uses distance vectors with more accurate metrics, but unlike distance vector routing protocols, it updates only when there is a topology change. Balanced hybrid routing provides faster convergence while limiting the use of resources such as bandwidth, memory, and processor overhead. Cisco Enhanced IGRP (EIGRP) is an example of a balanced hybrid protocol.

Understanding Binary Basics

Computers use a numbering system based on only 1s and 0s. This type of system is called binary or base 2. This numbering system might seem awkward at first glance, but it uses the same logic as the base 10 system we use every day. As with base 10, binary counting starts with the "ones" column until all the numbers are exhausted, and then it rolls over to the next column, which is a power of the base. For example, base 10 has ten numbers (0 through 9). When counting, you start in the "ones" column and count until you reach the highest unit. Then you move to the "tens" column. This continues with successive powers ($1, 10^1, 10^2, 10^3$). The binary system's columns or placeholders are 2^0, 2^1, 2^2, 2^3, and so on. Table 8-1 shows the values for the first seven places.

Table 8-1 Binary

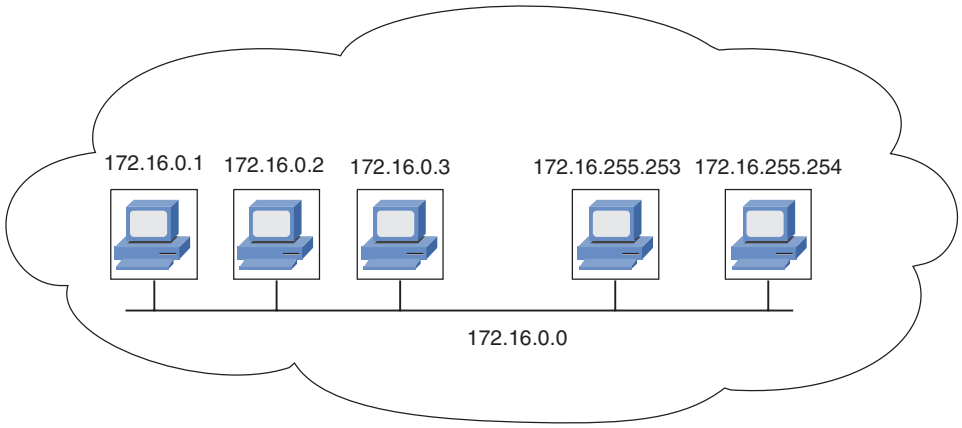
Base 2 Numbering System								
Number of Symbols	2							
Symbols	0, 1							
Base Exponent	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Place Value	128	64	32	16	8	4	2	1
Example: Convert 47 to Binary	0	0	1	0	1	1	1	1

Binary numbers are used extensively in networking. They are the basis of IP addressing. To convert between decimal and binary, it is best to build a simple table like the one just shown. To convert from binary to decimal, simply add up the "place values" of the digits that are 1s. In the preceding example, the placeholders for 1, 2, 4, 8, and 32 all contain 1s. Adding those values yields 47. (101111 in binary is 47 in decimal.) To convert from decimal to binary, again build a table. Put a 1 in the highest place value. (In this example, a 1 is placed in the column representing 32; 64 cannot be used, because it is greater than 47.) Now subtract the place value from the decimal number (47 – 32 = 15). The next value (16) is too large, so a 0 is placed in that column. A 1 is then placed in the 8 column, and the subtraction is performed again (15 – 8 = 7.) Repeat the process until the value of the subtraction equals 0.

Constructing a Network Addressing Scheme

Without subnets, an organization operates as a single network. These flat topologies result in short routing tables, but as the network grows, the use of bandwidth becomes very inefficient (all systems on the network receive all the broadcasts on the network). Figure 8-4 shows a flat network with all hosts in the same broadcast domain.

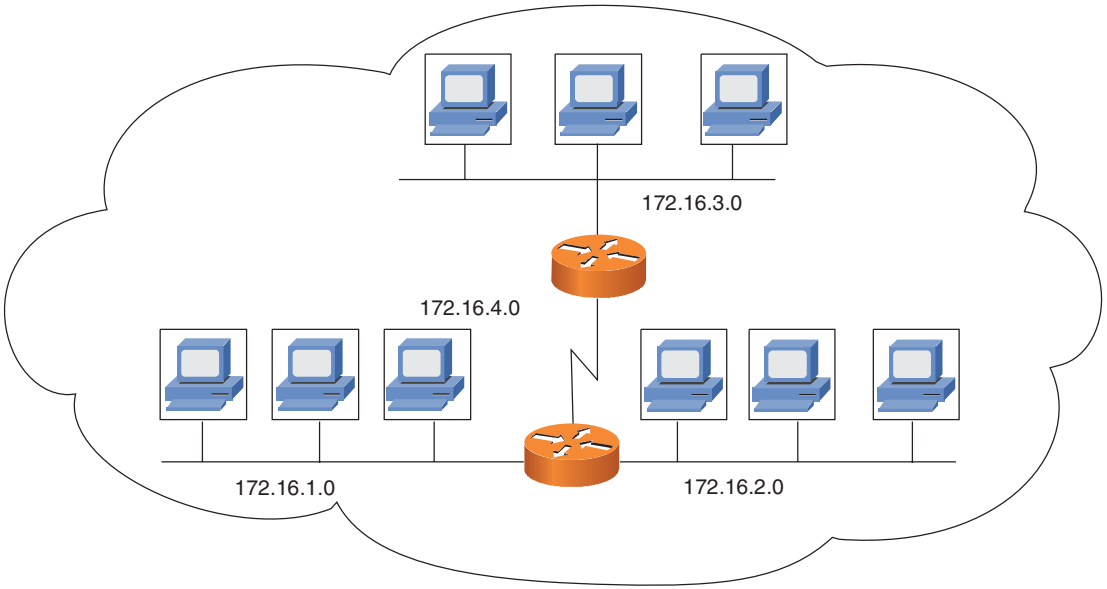
FIGURE 8-4
Flat Network Address Scheme



Network addressing can be made more efficient by breaking the addresses into smaller segments, or subnets. Subnetting provides additional structure to an addressing scheme without altering the addresses.

In Figure 8-5, the network address 172.16.0.0 is subdivided into four subnets: 172.16.1.0, 172.16.2.0, 172.16.3.0, and 172.16.4.0. If traffic were evenly distributed to each end station, the use of subnetting would reduce the overall traffic seen by each end station by 75 percent.

FIGURE 8-5
Subnetted Address Scheme



Subnet Mask

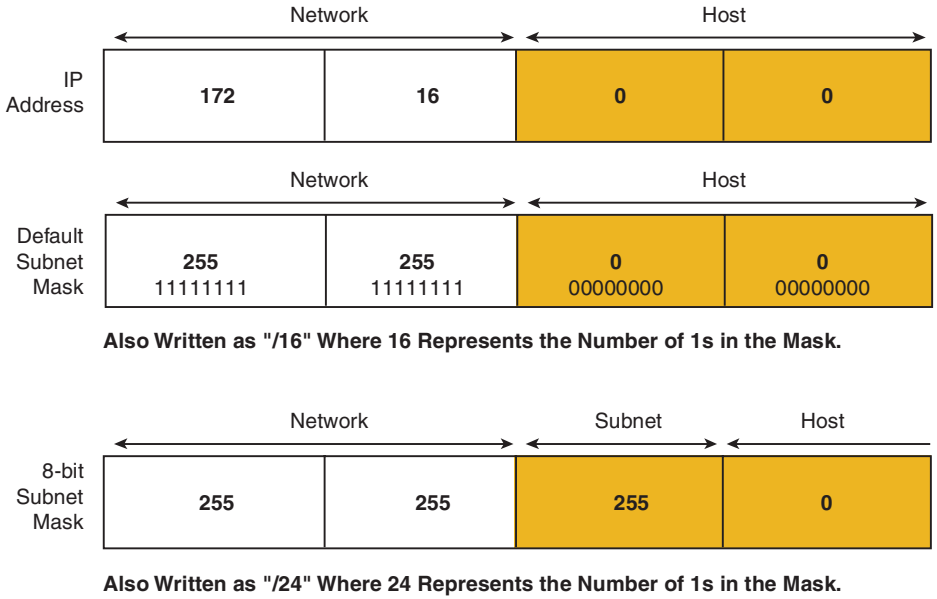
As shown in Figure 8-6, a subnet mask is a 32-bit value written as four octets. In the subnet mask, each bit is used to

 Please see page 311 for more details.

determine how the corresponding bit in the IP address should be interpreted (network, subnet, or host). The subnet mask bits are coded as follows:

- Binary 1 for the network bits
- Binary 1 for the subnet bits
- Binary 0 for the host bits

FIGURE 8-6
IP Address and Subnet Mask



Although dotted-decimal is most common, the subnet can be represented in several ways:

- **Dotted-decimal:** 172.16.0.0 255.255.0.0
- **Bit count:** 172.16.0.0/16
- **Hexadecimal:** 172.16.0.0 0xFFFF0000

 Please see page 311 for more details.

The **ip netmask-format** command can specify the display format of network masks for the router. Dotted-decimal is the default.

Default Subnet Masks

Each address class has a default subnet mask. The default subnet masks only the network portion of the address, the effect of which is no subnetting. With each bit of subnetting beyond the default, you can create 2^n–2 subnets. Figure 8-7 and Table 8-2 show the effect of increasing the number of subnet bits.

FIGURE 8-7
Default Subnet Masks

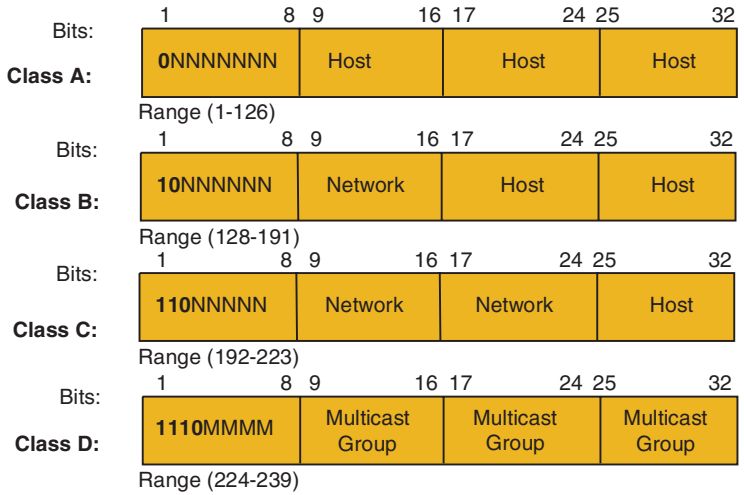


Table 8-2 Subnetting

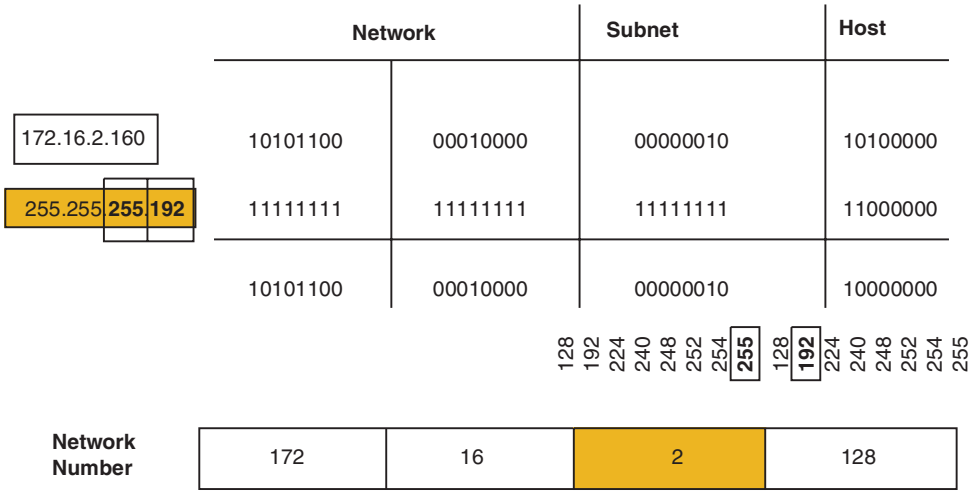
Address	Subnet Address	Number of Subnets	Comments
10.5.22.5/8	255.0.0.0	0	This is the default Class A subnet address. The mask includes only the network portion of the address and provides no additional subnets.
10.5.22.5/16	255.255.0.0	254	This Class A subnet address has 16 bits of subnetting, but only the bits in the second octet (those beyond the default) contribute to the subnetting.
155.13.22.11/16	255.255.0.0	0	In this case, 16 bits are used for subnetting, but because the default for a Class B address is 16 bits, no additional subnets are created.
155.13.10.11/26	255.255.255.192	1022	This case has a total of 26 bits of subnetting, but the Class B address can use only 10 of them to create subnets. The result creates 1024 subnets.

How Routers Use Subnet Masks

To determine the subnet of the address, a router performs a logical AND operation with the IP address and subnet mask. Recall that the host portion of the subnet mask is all 0s. The result of this operation is that the host portion of the address is removed, and the router bases its decision only on the network portion of the address.

In Figure 8-8, the host bits are removed, and the network portion of the address is revealed. In this case, a 10-bit subnet address is used, and the network (subnet) number 172.16.2.128 is extracted.

FIGURE 8-8
Identifying Network Portion of Address



Broadcast Addresses

Broadcast messages are sent to every host on the network. Two kinds of broadcasts exist:

- Directed broadcasts can broadcast to all hosts within a subnet and to all subnets within a network. (170.34.2.255 sends a broadcast to all hosts in the 170.34.2.0 subnet.)
- Flooded broadcasts (255.255.255.255) are local broadcasts within a subnet.

Identifying Subnet Addresses

Given an IP address and subnet mask, you can identify the subnet address, broadcast address, first usable address, and last usable address using the following method, which is displayed in Figure 8-9:

Step 1. Write the 32-bit address, and write the subnet mask below that.

Step 2. Draw a vertical line just after the last 1 bit in the subnet mask.

 Please see page 311 for more details.

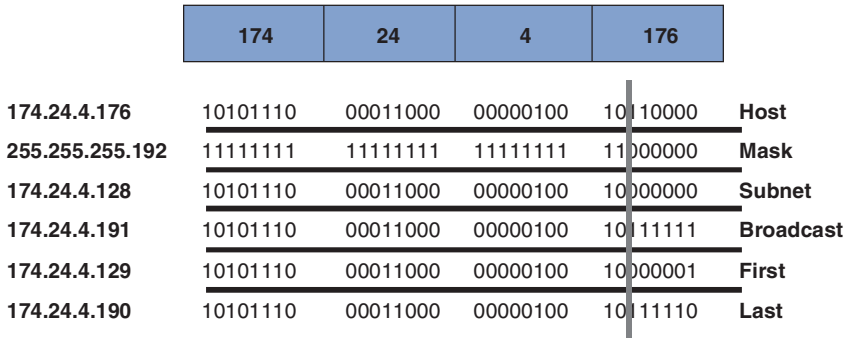
Step 3. Copy the portion of the IP address to the left of the line. Place all 0s for the remaining free spaces to the right. This is the subnet number.

Step 4. Copy the portion of the IP address to the left of the line. Place all 1s for the remaining free spaces to the right. This is the broadcast address.

Step 5. Copy the portion of the IP address to the left of the line. Place all 0s in the remaining free spaces until you reach the last free space. Place a 1 in that free space. This is your first usable address.

Step 6. Copy the portion of the IP address to the left of the line. Place all 1s in the remaining free spaces until you reach the last free space. Place a 0 in that free space. This is your last usable address.

FIGURE 8-9
Identifying Subnet Addresses



How to Implement Subnet Planning

Subnetting decisions should always be based on growth estimates rather than current needs.

To plan a subnet, follow these steps:

Step 1. Determine the number of subnets and hosts per subnet required.

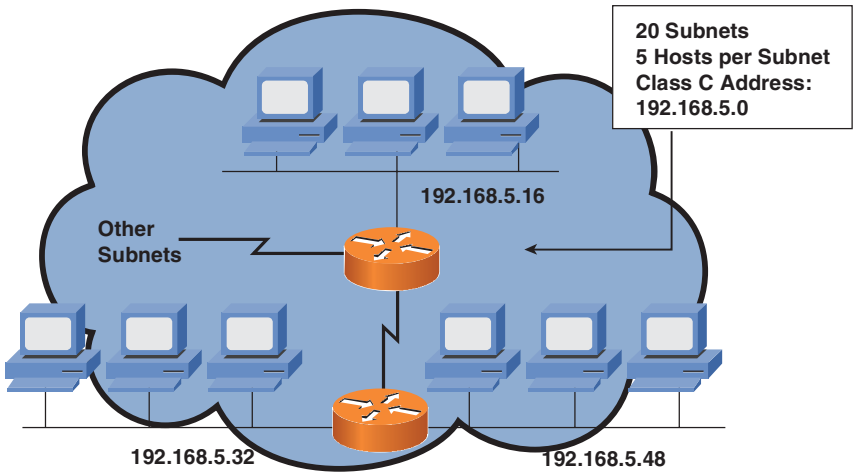
 Please see page 311 for more details.

Step 2. The address class you are assigned, and the number of subnets required, determine the number of subnetting bits used. For example, with a Class C address and a need for 20 subnets, you have a 29-bit mask (255.255.255.248). This allows the Class C default 24-bit mask and 5 bits required for 20 subnets. (The formula 2^n–2 yields only 14 subnets for 4 bits, so 5 bits must be used.)

Step 3. The remaining bits in the last octet are used for the host field. In this case, each subnet has 2^3–2, or 6, hosts.

Step 4. The final host addresses are a combination of the network/subnet plus each host value. In Figure 8-10, the hosts on the 192.168.5.32 subnet would be addressed as 192.168.5.33, 192.168.5.34, 192.168.5.35, and so forth.

FIGURE 8-10
Subnetting a Network



Configuring Static Routes

To configure a static route on a Cisco router, enter the following global command:

```
ip route destination-network [mask] {next-hop-address | outbound- interface} [distance] [permanent]
```

Here's an example:

```
RouterB(config)#ip route 172.17.0.0 255.255.0.0 172.16.0.1
```

This example instructs the router to route to 172.16.0.1 any packets that have a destination of 172.17.0.0 to 172.17.255.255.

The *distance* parameter defines the administrative distance or the route. The value for *distance* is a number from 1 to 254 (1 is the default if not defined) that rates the distance in hops of the destination. For example, a distance of 1 means that the destination is one hop away. If a router has two routes to the same destination, the route with the lowest distance is used.

The **permanent** statement specifies that the route will not be removed even if the router interface shuts down.

Default Route

A default route is a special type of route with an all-0s network and network mask. The default route directs any packets for which a next hop is not specifically listed in the routing table. By default, if a router receives a packet to a destination network that is not in its routing table, it drops the packet. When a default route is specified, the router does not drop the packet. Instead, it forwards the packet to the IP address specified in the default route.

To configure a static default route on a Cisco router, enter the following global configuration command:

```
ip route 0.0.0.0 0.0.0.0 [ip-address-of-the-next-hop-router | outbound-interface]
```

For example, the following command configures the router to route all packets with destinations not in its routing table to IP 172.16.0.2:

```
RouterB(config)#ip route 0.0.0.0 0.0.0.0 172.16.0.2
```

 Please see page 311 for more details.

Verifying Routing

The **show ip route** command, as follows, verifies routing tables:

```
RouterA#show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.10.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
D       10.1.10.0/24 [90/28416] via 10.1.10.254, 2w0d, FastEthernet0/0
D       10.1.20.0/24 [90/28416] via 10.1.10.254, 2w0d, FastEthernet0/0
C       10.1.10.0/24 is directly connected, FastEthernet0/0
S       10.0.0.0/8 [1/0] via 10.1.10.0
D       10.1.60.0/24 [90/28416] via 10.1.10.254, 2w0d, FastEthernet0/0
D       10.1.50.0/24 [90/28416] via 10.1.10.254, 2w0d, FastEthernet0/0
D       10.1.40.0/24 [90/28416] via 10.1.10.254, 2w0d, FastEthernet0/0
D       10.1.100.0/24 [90/28416] via 10.1.10.254, 2w0d, FastEthernet0/0
D       10.1.254.0/24 [90/28416] via 10.1.10.254, 2w0d, FastEthernet0/0
D    192.168.0.0/24 [90/2172416] via 192.168.1.2, 1w6d, Serial0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/30 is directly connected, Serial0/0/0
D       192.168.1.0/24 is a summary, 1w6d, Null0
S*   0.0.0.0/0 [1/0] via 10.1.10.1
```

 Please see page 311 for more details.

Section 9
Configuring a Cisco Router

Starting a Router

When a router is booted up, it goes through the following sequence (see Figure 9-1):

1. The router checks its hardware with a power-on self test (POST).
2. The router loads a bootstrap code.
3. The Cisco IOS Software is located and loaded using the information in the bootstrap code.
4. The configuration is located and loaded.

After this sequence completes, the router is ready for normal operation.

When the router is started for the first time, it does not have an initial configuration. The IOS will execute a question-derived initial configuration routine called setup mode. You can enter setup mode at any time by entering the **setup** privileged EXEC command. Setup mode configures the following:

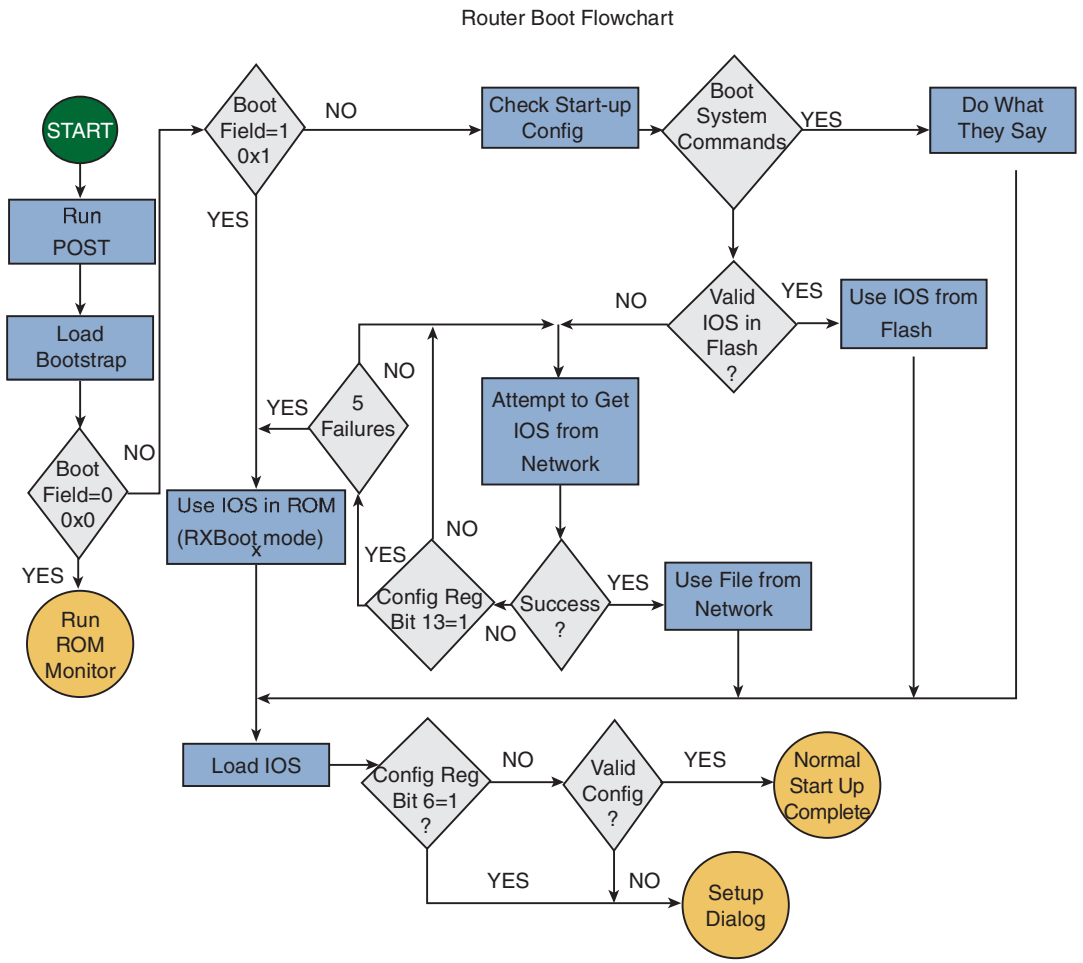
- Initial global parameters, such as host name, enable secret password, and Telnet passwords
- Initial protocols
- Interfaces
- AutoSecure

 Please see page 311 for more details.

SECTION 9

Configuring a Cisco Router

FIGURE 9-1
Router Boot
Flow Chart



 Please see page 311 for more details.

When the setup mode configuration process is completed, the setup command gives you the following options:

- **[0]:** Go to the EXEC prompt without saving the created configuration.
- **[1]:** Go back to the beginning of setup without saving the created configuration.
- **[2]:** Accept the created configuration, save it to NVRAM, and exit to EXEC mode.

Default answers appear in square brackets ([]). Pressing Enter accepts the defaults. At the first setup prompt, you can enter No to discontinue the setup. The setup process can be aborted at any time by pressing Ctrl-C.

Router Components

The major router components are as follows:

- **RAM:** Random-access memory contains key software (IOS).
- **ROM:** Read-only memory contains startup microcode.
- **NVRAM:** Nonvolatile RAM stores the configuration.
- **Configuration register:** Controls the bootup method.
- **Interfaces:** The interface is the physical connection to the external devices.
- **Flash memory:** Flash contains the Cisco IOS Software image.

Logging In to the Router

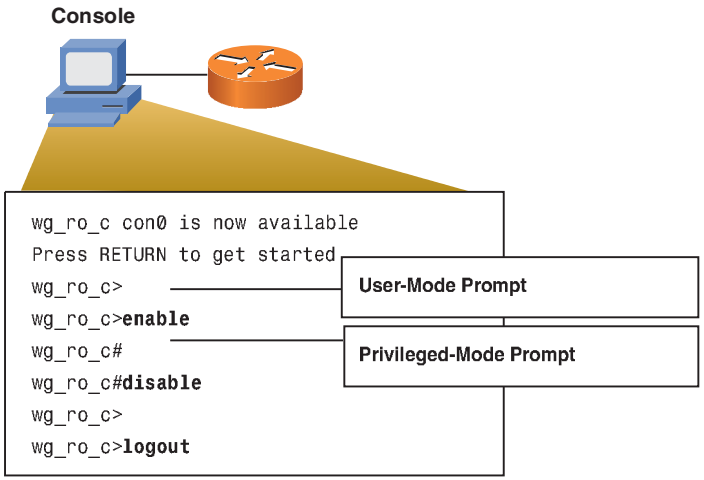
Cisco IOS Software provides a command interpreter called the EXEC. The EXEC interprets the commands that are entered and carries out the corresponding operations. To access EXEC mode, you must log in to the router through the

 Please see page 311 for more details.

command line. Two EXEC modes exist, as shown in Figure 9-2:

- **User EXEC** level provides a limited number of basic commands.
- **Privileged EXEC** (enable mode) level allows you to access all router commands. This level can be password-protected. The **enable** command allows access to this mode (disable exits to user mode).

FIGURE 9-2
Cisco IOS Software EXEC Modes



Displaying Router Status

Output from the following **show** commands provides valuable information about the router status:

- **show running-configuration** displays the currently active configuration in memory, including any changes made in the session that have not yet been saved.
- **show startup-config** displays the last saved configuration.
- **show version** displays information about the system hardware and software.
- **show interfaces** displays information on connections and ports that connect with other devices.

 Please see page 311 for more details.

Configuring a Router

From privileged EXEC mode, the **configure terminal** command provides access to global configuration mode. From global configuration mode, you can access these specific configuration modes:

- **Interface:** Configures operations on a per-interface basis
- **Subinterface:** Configures multiple virtual interfaces
- **Controller:** Supports commands that configure controllers (such as E1 and T1)
- **Line:** Configures the operation of a terminal line
- **Router:** Configures IP routing protocols

Major Command/Subcommand Relationship

Figure 9-3 shows the major command and subcommand relationships. Commands that indicate a process or interface that will be configured are called major commands.

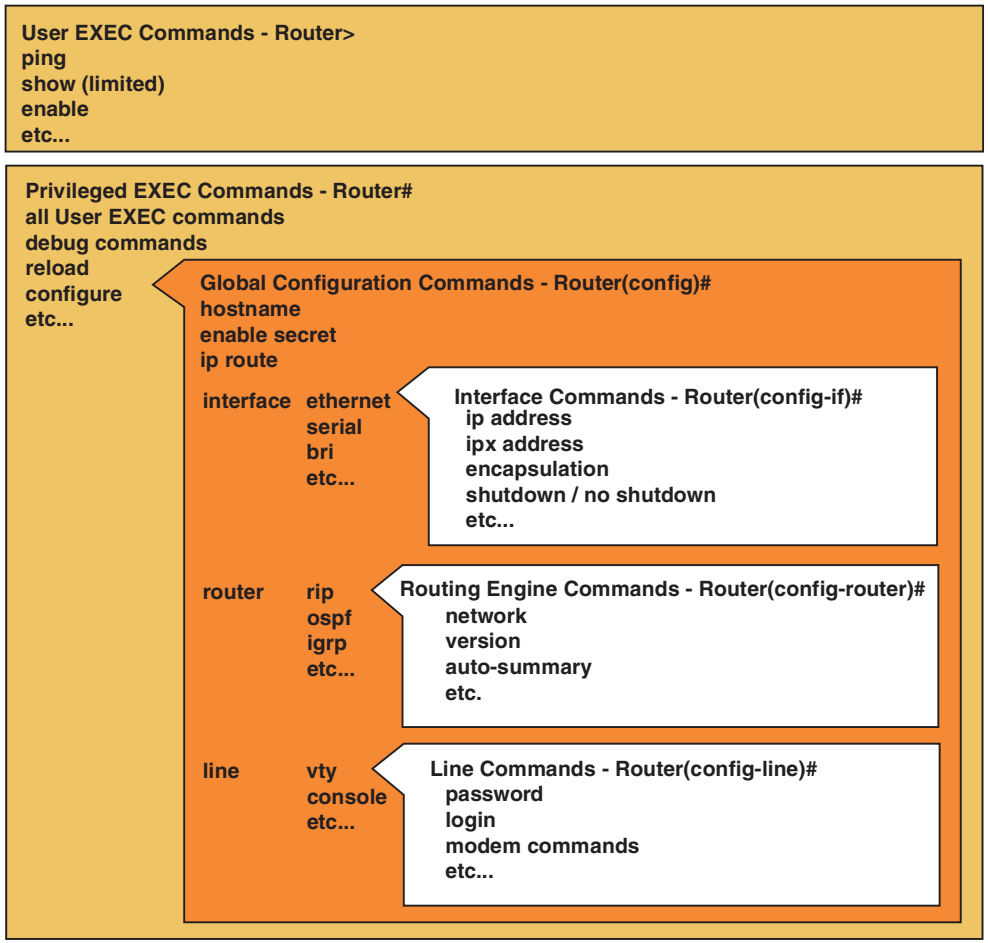
Major commands cause the CLI to enter a specific configuration mode.

Major commands have no effect unless they are immediately followed by a subcommand that supplies the configuration entry, as follows:

```
Router(config)# interface serial 0
Router(config-if)# shutdown
Router(config)# router rip
Router(config-router)# network 10.0.0.0
```

 Please see page 311 for more details.

FIGURE 9-3
IOS Command and Subcommand Relationships



 Please see page 311 for more details.

Assigning a Router Name Example

The **hostname** command, as follows, names a router (or a switch):

```
Router> enable
Router# configure terminal
Router(config)# hostname Dallas
```

Configuring a Serial Interface

NOTE
Unambiguous abbreviations of commands are allowed. Abbreviations of delimiters are not allowed. For example, a clock rate of 64,000 cannot be abbreviated as 64. The **bandwidth** command overrides the default bandwidth. The bandwidth entered has no effect on the line's actual speed; however, it changes the metric of the link as seen by routing protocols.

The following example demonstrates the command syntax needed to configure a serial interface on a router:

```
Router# configure terminal
Router(config)# interface s1
Router(config-if)# clock rate 64000
Router(config-if)# bandwidth 64
Router# show interface serial 1
Router# show controller    displays the information about the physical interface and if it is a DTE or DCE.
```

Enabling or Disabling an Interface Example

By default, all interfaces on a router are initially disabled. The following commands show you how to enable or disable a router interface:

```
Router# configure terminal
Router(config)# interface s1
Router(config)#no shutdown       enables the interface
Router(config)#shutdown       disables the interface
```

 Please see page 311 for more details.

Configuring an Interface IP Address Example

The following commands configure a router interface with an IP address:

```
Router# configure terminal
Router(config)# interface s1
Router(config)#ip address 192.168.1.1 255.255.255.0
Router(config)#no shutdown
```

Verifying Interface Configuration

The **show interface** command displays the following:

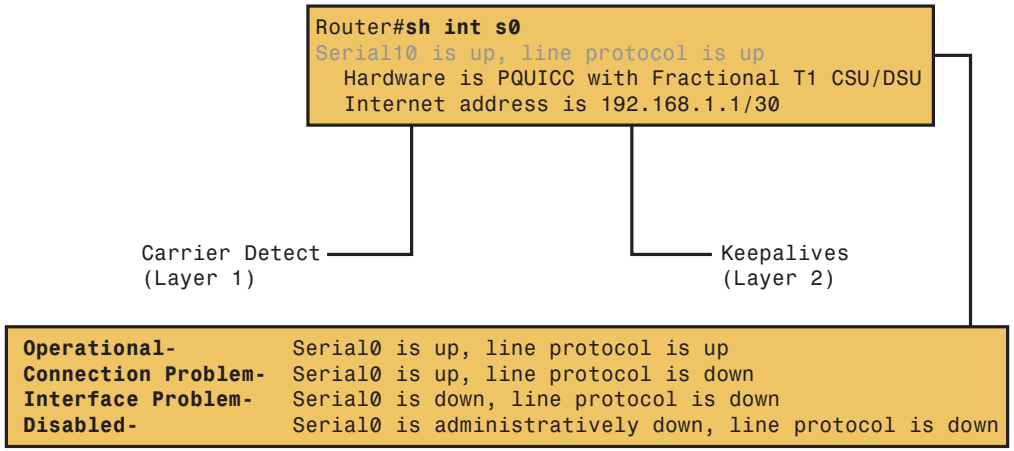
- Whether the interface is administratively down
- Whether the line protocol is up or down
- An Internet address (if one is configured)
- Maximum transmission unit (MTU) and bandwidth
- Traffic statistics on the interface
- Interface encapsulation type

One of the most important elements of the show interface command is the display of the line and data-link status.

Figure 9-4 shows the line and data-link status of a serial interface and describes how to interrupt the interface status.

 Please see page 311 for more details.

FIGURE 9-4
Displaying Interface Line and Data-Link Status

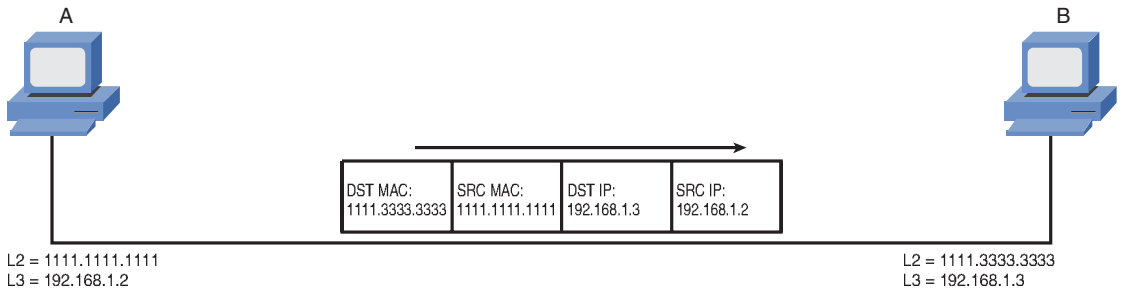


Exploring the Packet-Delivery Process

For hosts on an IP network to communicate with each other, they need a Layer 2 address (MAC address) and an IP address.

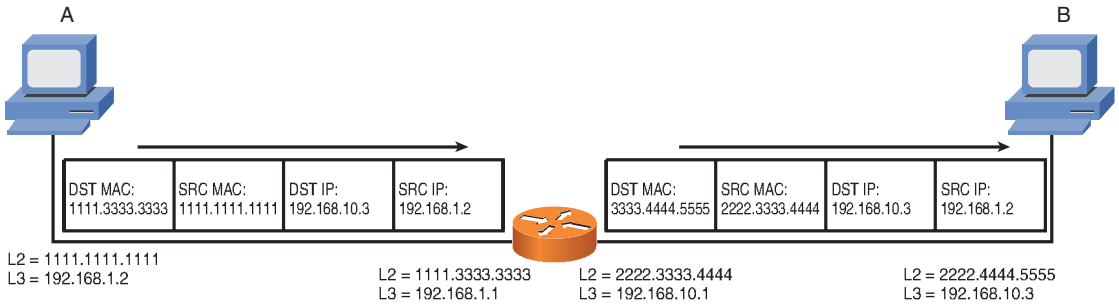
IP-enabled hosts use ARP to map the MAC address to the IP address when communicating with hosts on a local segment. Each host maintains an ARP table that contains the IP–to–MAC address mappings (see Figure 9-5).

FIGURE 9-5
Host-to-Host Packet Delivery



When an IP host wants to communicate with a host on a remote network, the local host will send an ARP request to find the MAC address of the host's default gateway. Because the remote host is on a remote network, the router will respond with its local MAC address and the IP address of the remote host. In Figure 9-6, host A wants to communicate with host B. Host A sends a packet with the destination MAC address of the router's Ethernet interface and the IP address of host B. The source MAC address and IP will be that of host A. When the router receives the packet, the router will take the packet, strip off the MAC address information, and rewrite the MAC address with the source MAC address of the router's exiting Ethernet interface and the destination MAC address of host B. The IP information does not change.

FIGURE 9-6
Host-to-Host Packet Delivery Through a Router



Using Common IOS Tools

You can verify connectivity using the ping command. The **ping** command also tells you the minimum, average, and maximum times for packets that make the round trip to the target system and back. You can assess the path's reliability using this command, as follows:

```
Router# ping 10.1.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

 Please see page 311 for more details.

You can use the **trace** command, as follows, to view the actual routes that packets take between devices:

```
Router# trace 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10

  1 10.1.1.10 4 msec 4 msec 4 msec
Router#
```

The **show ip arp** command displays the router's ARP cache.

Router Security

Configuring Router Passwords: Console and Telnet

The following example configures passwords on the console and vty lines of a router to homer and bart:

```
Router(config)# line console 0
Router(config-line)# login
Router(config-line)# password homer
Router(config)# line vty 0 4
Router(config-line)# login
Router(config-line)# password bart
```

The numbers 0 through 4 in the **line vty** command specify the number of Telnet sessions allowed in the router. You can also set up a different password for each line by using the **line vty** *port number* command.

 Please see page 311 for more details.

Configuring Router Passwords: Enable and Secret Passwords

NOTE
When the enable secret password is set, it is used instead of the enable password.

The following configures an enable password of apu and an enable secret password of flanders:

```
Router(config)# enable password apu
Router(config)# enable secret flanders
```

The **no enable password** command disables the privileged EXEC mode password.

The **no enable secret** command disables the encrypted password.

The console, Telnet, and enable passwords are displayed unencrypted. To encrypt them, use the service password-encryption global command, as follows:

```
Router(config)#service password-encryption
```

Configuring Login Banner and MOTD

The login banner is displayed before the username and password login prompts on a Cisco router. The login banner is configured using the **banner login** global command, as follows:

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#banner login #
Enter TEXT message.  End with the character '#'.
Notice! Only Authorized Personnel Are Allowed to Access This Device
#
```

The MOTD is displayed before the login banner. It is displayed to anyone connecting to the router through Telnet, console port, or auxiliary port. Use the **banner motd #** *text* **#** global configuration command to configure the MOTD, as follows:

```
Router(config)#banner motd #      <ENTER>
Enter TEXT message.  End with the character '#'.
Warning only authorized users many access this switch. <ENTER>
#
Router(config)#
```

 Please see page 311 for more details.

SSH Access

Cisco recommends using SSH to encrypt communication between the Cisco device and the host. Telnet is unsecure, and all communication between the Cisco device and host is sent in clear text. Use the following steps to configure SSH access:

Step 1. Create a local username and password on the device.

Step 2. Assign a domain name to the device.

Step 3. Generate a security key.

Step 4. Enable SSH.

Step 5. Configure vty ports to authenticate using SSH.

```
Router(config)#username eric password 0 ciscopress
Router(config)#ip domain-name cisco.com
Router(config)#crypto key generate rsa
The name for the keys will be: router.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
Router(config)#ip ssh ver 2
Router(config)#line vty 0 15
Router(config-line)#login local
Router(config-line)#transport input telnet ssh
```

 Please see page 311 for more details.

Securing vty Access

By default, after a vty password has been applied, any IP address can connect to vty ports. You should restrict access to vty ports to only specific IP address. This is done through standard access lists.

Standard access lists allow you to permit or deny traffic based on the source IP address. To restrict access to vty ports, you would create a standard access list that permits each authorized IP address to connect to vty and apply the access list to the vty ports.

At the end of each access list is an implicit deny any statement. So, if a host is not specifically permitted, it will be denied.

Wildcard Masks

Wildcard masks define the subset of the 32 bits in the IP address that must be matched.

Wildcards are used with access lists to specify a host, network, or part of a network.

In wildcard masks, when 0s are present, the octet address must match. Mask bits with a binary value of 1 are wildcards. For example, if you have an IP address of 172.16.0.0 with a wildcard mask of 0.0.255.255, the first two portions of the IP address must match 172.16, but the last two octets can be in the range of 1 to 255.

Configuring and Applying vty Access Lists

The command syntax to create a standard IP access list is as follows:

```
access-list access-list-number {permit| deny} source-address [wildcard-mask]
```

The *access-list-number* parameter is a number from 1 to 99 or 1300 to 1999.

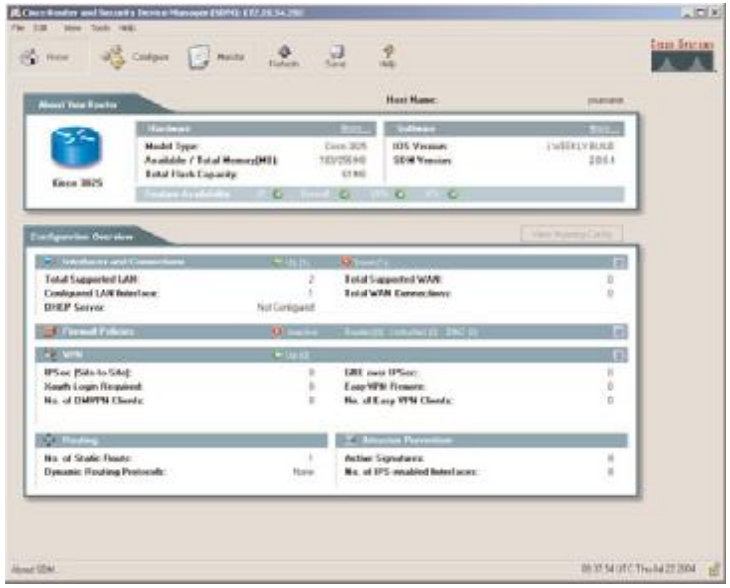
```
SwitchA(config)#access list 10 permit ip 192.168.10.0 0.0.0.255
Router(config)#line vty 0 15
Router(config-if)#access-class 10 in  This applies the access list to vty lines
```

 Please see page 311 for more details.

Cisco Router and Security Device Manager

The Cisco Security Device Manager (SDM) is a web-based tool that configures Cisco routers (see Figure 9-7). SDM helps simplify router deployments and troubleshoot complex network and Virtual Private Network (VPN) connectivity issues. SDM is supported on all Cisco routers and is a free tool that provides built-in wizards to help simply router configuration.

FIGURE 9-7
Cisco Security Device Manager



 Please see page 311 for more details.

SDM has the following features:

- Is an embedded web-based management tool
- Provides intelligent wizards to enable quicker and easier deployments and does not required Cisco IOS CLI knowledge
- Provides tools for advanced users such as
  - ACL editor
  - VPN crypto map editor
  - IOS CLI preview

Cisco SDM User Interface

To access SDM on your Cisco router, perform the following steps:

Step 1. Enable HTTP/HTTPS server on the router:

```
Router(config)#ip http server
Router(config)#ip http secure-server
Router(config)#ip http authentication local
```

Step 2. Create a user account with enable privileges:

```
Router(config)#username admin priviledge 15 password 0 password
```

Step 3. Configure SSH and Telnet for local login and privilege level 15:

```
Router(config)#line vty 0 4
Router(config-line)#privilege level 15
Router(config-line)#login local
Router(config-line)#transport input telnet
Router(config-line)#transport input telnet ssh
```

 Please see page 311 for more details.

After SDM is installed on a router, you can access it by typing in the IP address of the router's interface in a web browser.

For example, if the router's Fast Ethernet interface IP is 192.168.10.1, you would type **https://192.168.10.1.**

If you are configuring a router for the first time that has SDM installed, you need to connect to the router's Fast Ethernet interface through a crossover cable. After being connected, change the IP address of your computer to 10.10.10.2 255.255.255.248. Next, open your web browser, disable any pop-up blockers, and connected to SDM through web address http://10.10.10.1. The default username is cisco**,** and the password is cisco**.** After you connect, SDM will run and you will be guided through the SDM Express Setup Wizard to configure the router for the first time.

To download the latest version of SDM, go to the following URL:

http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm

SDM Wizards

SDM contains several wizards to simply router configuration tasks. Some of these wizards are as follows:

- **LAN Wizard:** Configures LAN interfaces and DHCP.
- **WAN Wizard:** Configures WAN interfaces.
- **Firewall Wizard:** Configures firewall policies on a router that has Cisco Security IOS Software.
- **VPN Wizard:** Configures site-to-site or remote VPN access.
- **Security Audit Wizard:** Audits the router and disables any unused or insecure service running on the router.
- **IPS Wizard:** Configures IPS policies. Requires the Advanced Security IOS Software.
- **QoS Wizard:** Configures quality of service.

 Please see page 311 for more details.

Configuring a Router as a DHCP Server

DHCP is a protocol that leases IP addresses to IP hosts. DHCP is built on a client-server model. The DHCP server hosts allocated network addresses and other IP configuration parameters. The DHCP client is a host that requests initialization parameters from a DHCP server.

DHCP supports the following three mechanisms for IP address allocation:

- **Automatic allocation:** Assigns a permanent IP address to a client
- **Dynamic allocation:** Assigns an IP address to a client for a set period of time
- **Manual allocation:** Assigns a specific IP address to a client as defined by the administrator using the client's MAC address

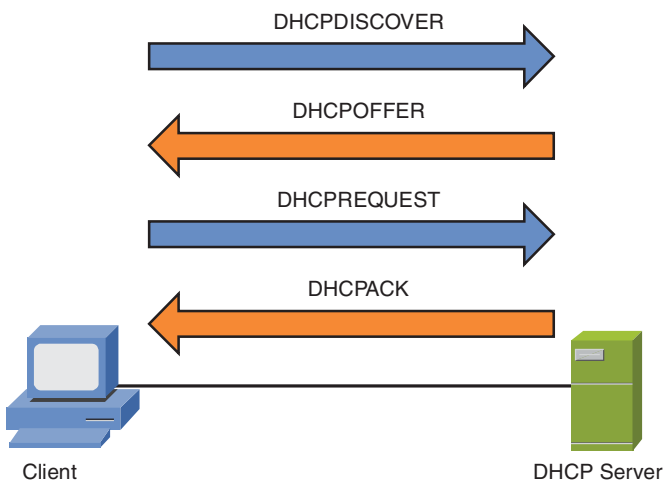
DHCP

Figure 9-8 shows the DHCP process as outlined here:

1. When a client boots up, it broadcasts a DHCPDISCOVER message on its local physical segment using IP address 255.255.255.255.
2. A DHCP server receives the DHCPDISCOVER message and responds with a DHCPOFFER message. This message contains IP configuration information such as DNS and default gateway.
3. After the client receives the DHCPOFFER, it responds with a DHCPREQUEST, indicating that it accepted the DHCPOFFER.
4. The server receives the DHCPREQUEST and sends a DHCPACK, acknowledging the process.

 Please see page 311 for more details.

FIGURE 9-8
DHCP Process



Using a Router as a DHCP Server

Cisco IOS Software includes a full DHCP server implementation that assigns IP addresses from specified address pools in the router and outer IP parameters such as DNS server and default router.

You have three ways to configure a Cisco router as a DHCP server: with the CLI, with the SDM Express Wizard, or in SDM after the router is configured.

If you are configuring a router for the first time using SDM, the SDM Express Wizard will run; one of the tasks the wizard allows you to do is configure the router as a DHCP server.

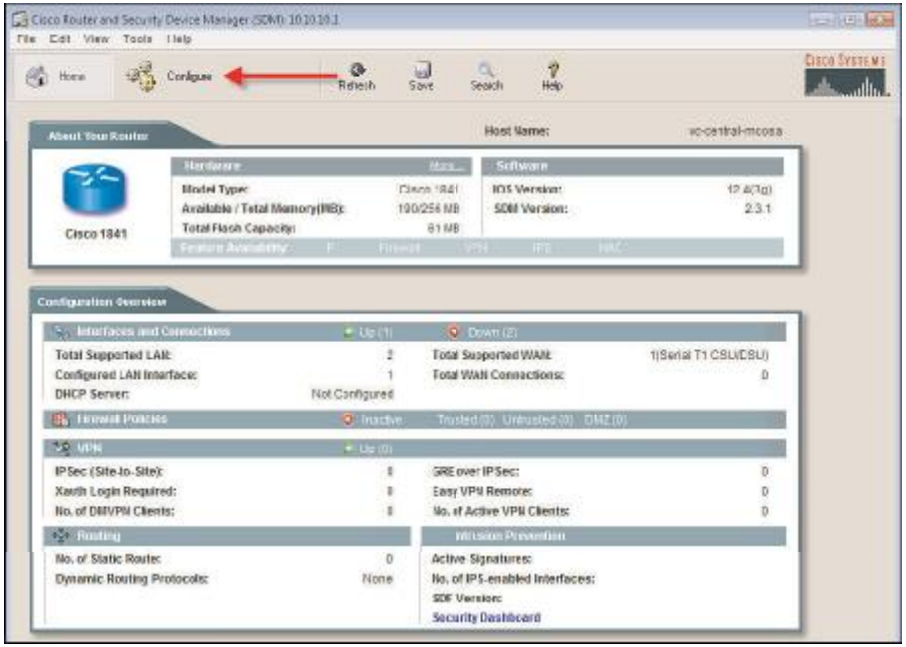
If a router is preconfigured and you want to configure it as DHCP server, follow these steps:

Step 1. Log on to the router using SDM.

Step 2. Click the **Configure** button, as shown in Figure 9-9.

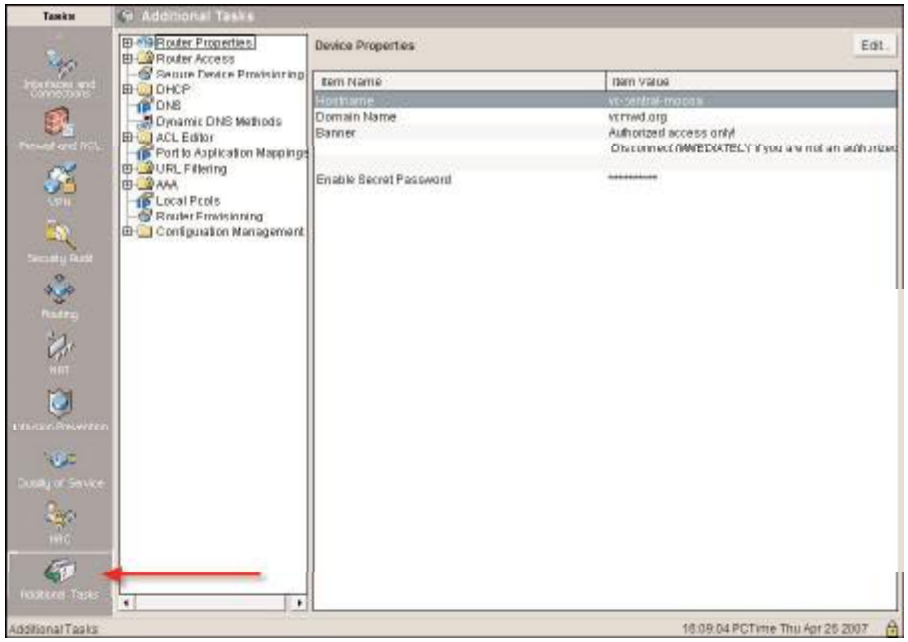
 Please see page 311 for more details.

FIGURE 9-9
Cisco SDM



Step 3. Click the **Additional Task** button, as shown in Figure 9-10.

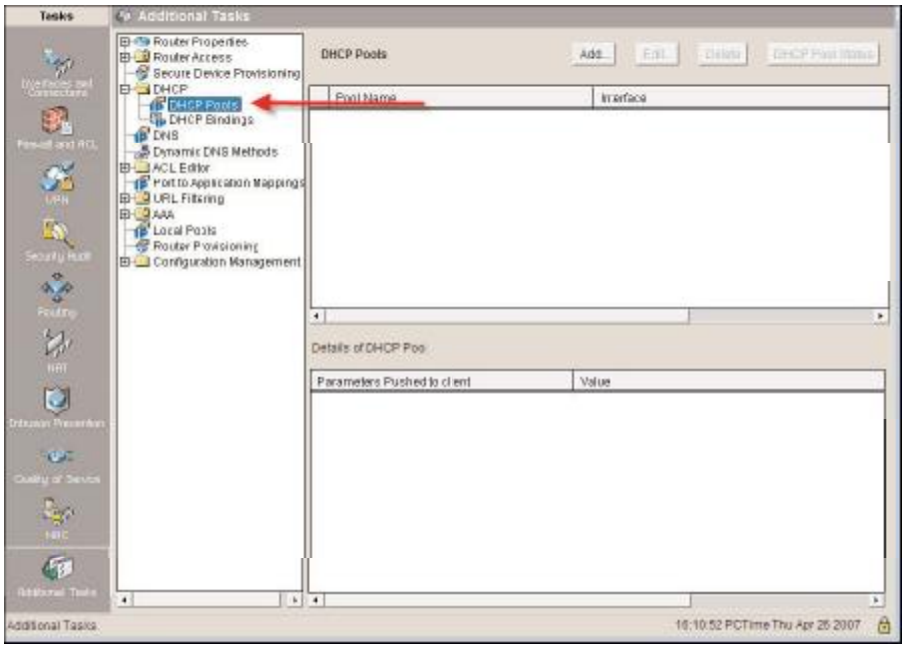
FIGURE 9-10
Configuring DHCP



Step 4. Expand the DHCP folder and select **DHCP Pools**, as shown in Figure 9-11. Click the **Add** button.

 Please see page 311 for more details.

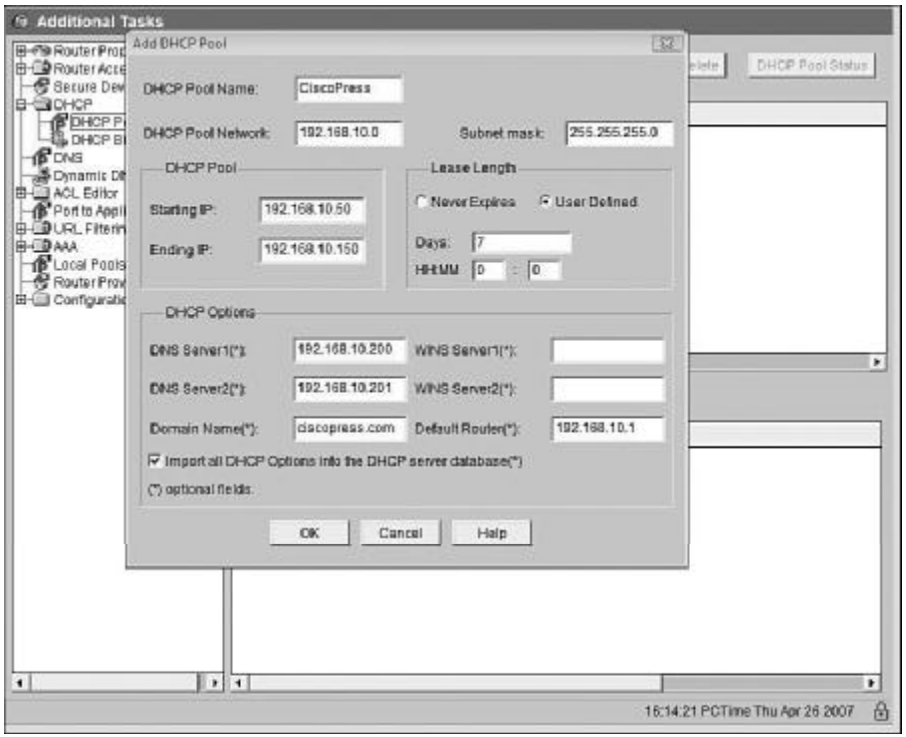
FIGURE 9-11
Configuring DHCP Pools



Step 5. Configure the DHCP Pool Name, DHCP Pool Network, DHCP Pool range, Lease Length, and DHCP Options, as shown in Figure 9-12. Click the **OK** button to save the configuration to the router. The IP address pool must be on the same subnet as the IP address of the LAN interface.

 Please see page 311 for more details.

FIGURE 9-12
Configure DHCP Options



DHCP/Bootp Relay Agent

When a DHCP-enabled client requests an IP address through a DHCPDISCOVER message, this message is broadcast to the local segment. By default, routers do not forward broadcasts. If the DHCP server is on a different segment than the DHCP client, the DHCP server will not see the DHCPDISCOVER messages from clients. The router needs to be configured to forward the DHCPDISCOVER broadcasts to the DHCP server. This is done through the following interface command:

```
ip helper-address [global] address
```

 Please see page 311 for more details.

The *address* parameter is the IP address of the DHCP server.

The **ip helper-address** command enables forwarding of UDP broadcasts received on the configured interface to a specific IP address, as follows:

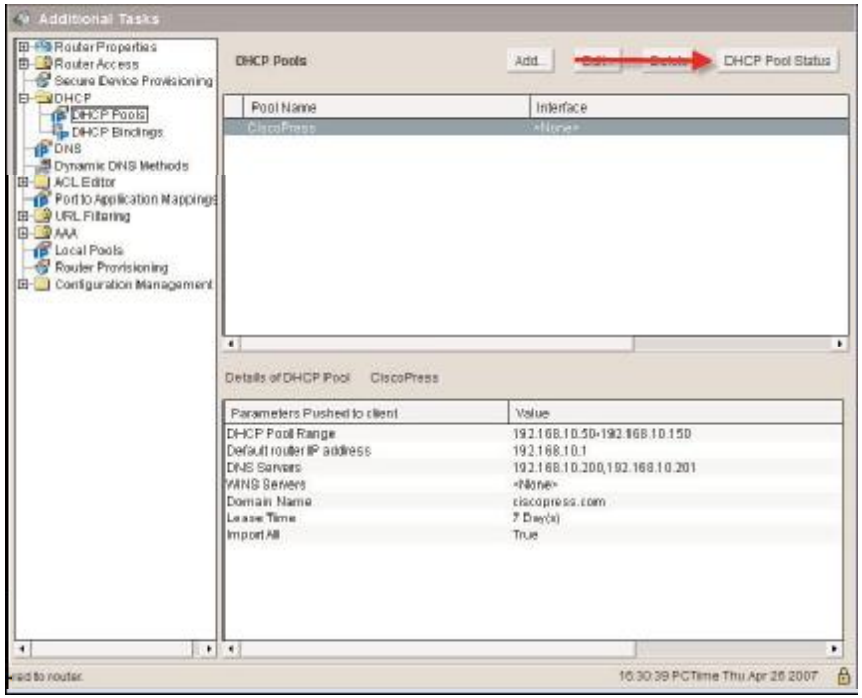
```
Router(config)#int f0/0
Router(config-if)# ip helper-address 192.168.11.200
```

Monitoring DHCP Server Function

The DHCP server on the router can be monitored through the SDM or CLI.

In Figure 9-13, the **DHCP Pool Status** button in SDM monitors the DHCP pool status in SDM.

FIGURE 9-13
SDM DHCP Pool Status



The **show ip dhcp conflicts** command displays any conflicts found by the DHCP server.

Accessing Remote Devices with Telnet or SSH

To establish a Telnet session, use the **telnet** command. Both the router's IP address and host name (when DNS or the host entry is present) can be used as an argument, as follows:

```
RouterA#telnet 10.2.2.2
```

To establish a SSH session, use the **ssh** command, as follows:

```
RouterA#ssh 10.2.2.2
```

The **show sessions** command displays a list of hosts to which you are connected. The **show ssh** command displays the list of hosts that are connected through SSH.

Pressing Ctrl-Shift-6 followed by X suspends the current session.

The **resume** command or pressing Enter resumes the last active session.

The **resume** *session-number* command reconnects to a specific session. Use the **show session** command to find the session number.

A Telnet or SSH session can be ended with the **exit**, **logout**, **disconnect,** and **clear** commands.

 Please see page 311 for more details.

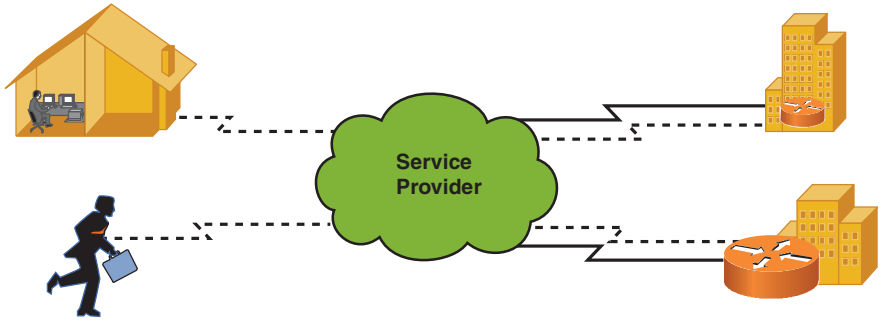
Section IV: Connecting Networks

Section 10
Understanding WAN Technologies

WAN Technologies Overview

WANs connect networks, users, and services across a broad geographic area. Figure 10-1 shows that companies use the WAN to connect company sites and mobile users for information exchange.

FIGURE 10-1
WAN Connections



WANs Versus LANs

LANs connect computers, peripherals, and other devices in a building or small geographic area. WANs connect LANs across a wide geographic area. LANs and all devices in the LAN are usually owned by the local organization. Outside service providers own the WAN and WAN devices.

 Please see page 311 for more details.

WAN Access and the OSI Model

WANs and their protocols function at Layers 1 and 2 of the OSI reference model.

The physical components of WANs define electrical, mechanical, and operational connections.

The data link layer defines WAN protocols that define how data is encapsulated for transmission across the WAN. Examples of these protocols are Frame Relay, ATM, High-Level Data Link Control (HDLC), and PPP.

WAN Devices

The following devices are used for WAN services:

- **Routers:** Connect the LAN to the WAN. Routers provide network layer services; they route data from one network to another.
- **Communication servers:** Concentrate dial-in and dial-out user communications.
- **Modems or DSU/CSUs:** In analog lines, modems convert analog to digital. Modems modulate and demodulate a signal, enabling data to be transmitted over telephone lines. In digital lines, data service units/channel service units (DSU/CSU) convert one form of digital format to another digital format.
- **WAN networking devices:** Used in the WAN network, they are multiport devices that switch Frame Relay, X.25, or ATM traffic. They operate at the data link layer of the OSI model.

Understanding Serial WAN Interfaces

WAN serial interfaces are either synchronous or asynchronous:

- **Synchronous links** have identical frequencies and contain individual characters encapsulated in control bits, called start/stop bits, which designate the beginning and end of each character. Synchronous links try to use the same speed as the other end of a serial link. Synchronous transmission occurs on V.35 and other interfaces, where one set of wires carries data and a separate set of wires carries clocking for that data.

 Please see page 311 for more details.

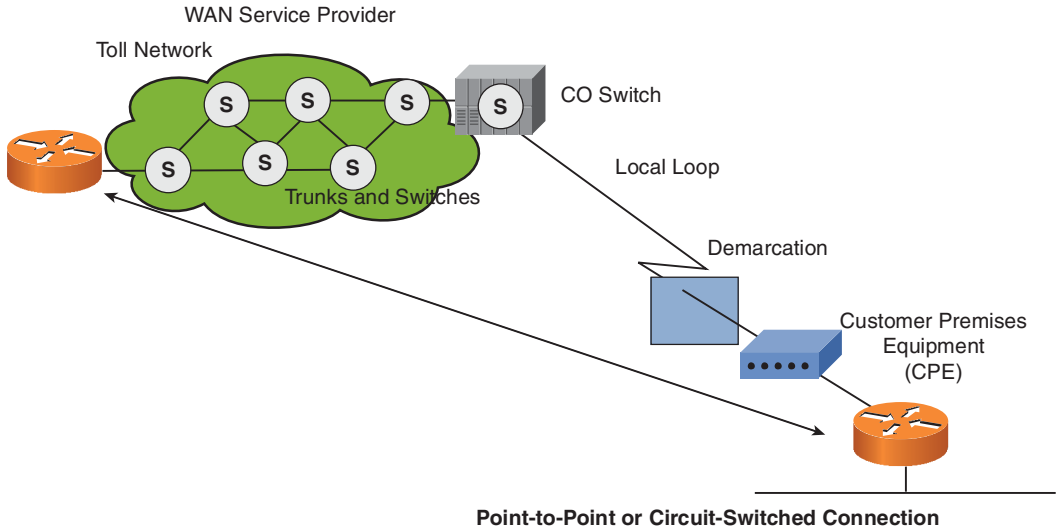
- **Asynchronous links** send digital signals without timing. Asynchronous links agree on the same speed, but there is no check or adjustment of the rates if they are slightly different. Only 1 byte per transfer is sent. Modems are asynchronous.

Serial interfaces are specified as DTE (data terminal equipment) or data communications equipment (DCE). DCE converts user data into the service provider's preferred format; in other words, DCEs provide clocking for the serial link. An example of a DCE is a CSU/DSU or a serial interface configured for clocking. The port configured as DTE requires external clocking from the CSU/DSU or other DCE device.

WAN Review

Figure 10-2 shows the typical WAN terminology and the list that follows provides more detailed definitions:

FIGURE 10-2
WAN Terminology



- **Customer premises equipment (CPE):** Located on the subscriber's premises and includes both equipment owned by the subscriber and devices leased by the service provider.
- **Demarcation (or demarc):** Marks the point where CPE ends and the local loop begins. It is usually located in the telecommunications closet.
- **Local loop (or last mile):** The cabling from the demarc into the WAN service provider's central office.
- **Central office (CO):** A switching facility that provides a point of presence for WAN service. The central office is the entry point to the WAN cloud, the exit point from the WAN for called devices, and a switching point for calls.
- **Toll network:** A collection of trunks inside the WAN cloud.

WAN Cabling

Several ways exist to carry traffic across the WAN. The implementation depends on distance, speed, and the type of service required. Connection speeds typically vary from 56 kbps to T1/E1 (1.544/2.048 Mbps, but can be as high as 10 Gbps). WANs use serial communication for long-distance communications.

Layer 2 Encapsulation Protocols

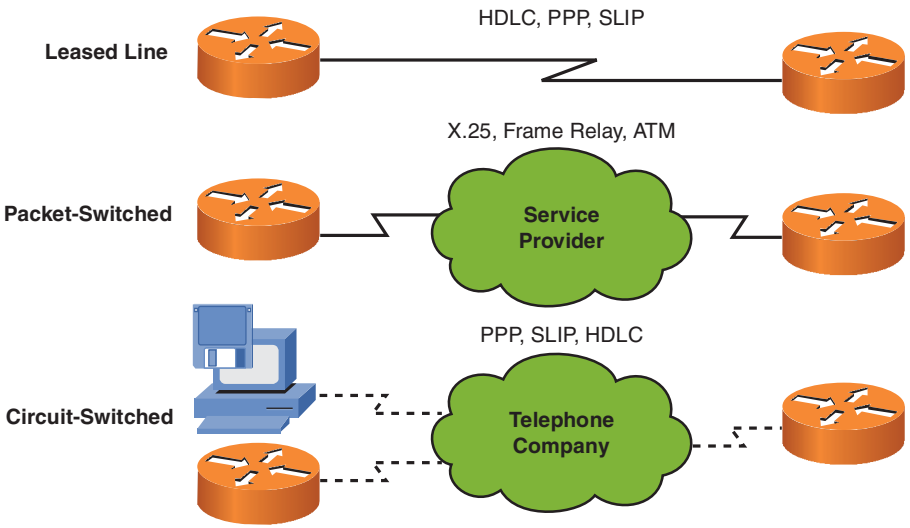
- **High-Level Data Link Control (HDLC):** The default encapsulation type for Cisco routers on point-to-point dedicated links and circuit-switched connections.
- **Point-to-Point Protocol (PPP):** Provides connections between devices over several types of physical interfaces, such as asynchronous serial, High-Speed Serial Interface (HSSI), ISDN, and synchronous. PPP works with many network layer protocols, including IP and IPX. PPP can use either Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) for authentication.
- **X.25/Link Access Procedure, Balanced (LAPB):** Defines connections between DTE and DCE for remote terminal access. LAPB is a data link layer protocol specified by X.25.

 Please see page 311 for more details.

- **Frame Relay:** Industry-standard switched data link layer protocol. Frame Relay (based on X.25) can handle multiple virtual circuits.
- **Asynchronous Transfer Mode (ATM):** International standard for cell relay using fixed-length (53-byte) cells for multiple service types. Fixed-length cells allow hardware processing, which greatly reduces transit delays. ATM takes advantage of high-speed transmission media such as E3, T3, and Synchronous Optical Network (SONET).

Figure 10-3 shows the typical WAN connections that each Layer 2 encapsulation protocol supports.

FIGURE 10-3
WAN Connections



Multiplexing

Multiplexing is the process of combining multiple signals over a single wire, fiber, or link. Four types of multiplexing operate at the physical layer:

- Time-division multiplexing (TDM)
- Frequency-division multiplexing (FDM)

 Please see page 311 for more details.

- Wave-division multiplexing (WDM) and dense WDM (DWDM)
- Statistical-division multiplexing

In TDM, each data channel is allocated bandwidth based on time slots, regardless of whether data is transferred; thus bandwidth is wasted when there is no data to transfer.

In FDM, information of each data channel is allocated bandwidth based on the signal frequency of the traffic. An example of this is FM radio.

In WDM and DWDM, each data channel is allocated bandwidth based on wavelength (inverse of frequency).

In statistical multiplexing, bandwidth is dynamically allocated to data channels.

WAN Communication Link Options

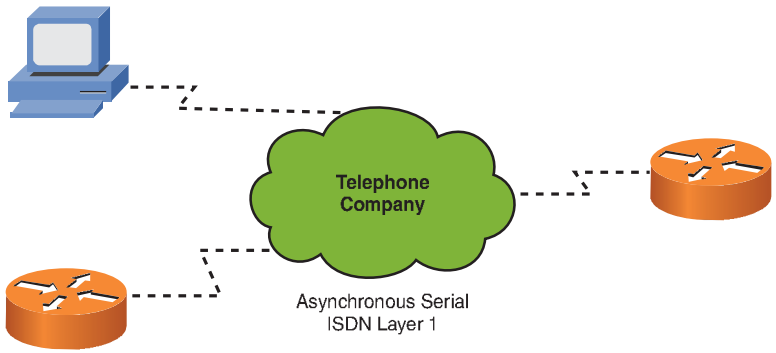
WAN services are generally leased from service providers on a subscription basis. The following three main types of WAN connections (services) exist:

- **Leased line:** A leased line (or point-to-point dedicated connection) provides a preestablished connection through the service provider's network (WAN) to a remote network. Leased lines provide a reserved connection for the client but are costly. Leased-line connections are typically synchronous serial connections. Figure 10-4 shows an example of a leased line WAN topology.

FIGURE 10-4
Leased-Line WAN

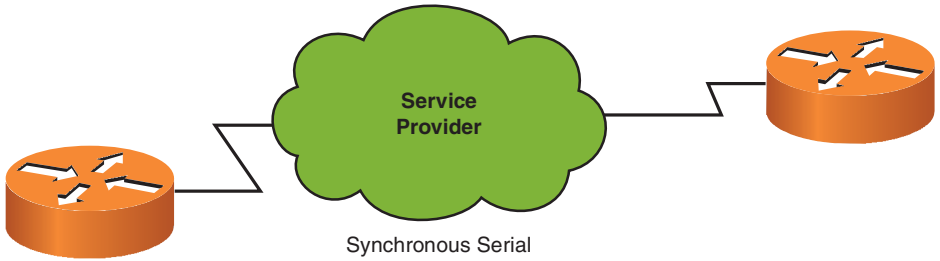
- **Circuit-switched:** Circuit switching provides a dedicated circuit path between sender and receiver for the duration of the call. Circuit switching is used for basic telephone service or Integrated Services Digital Network (ISDN). Figure 10-5 shows an example of a circuit-switched WAN topology.

FIGURE 10-5
Circuit-Switched WAN



- **Packet-switched:** With packet switching, devices transport packets using virtual circuits (VCs) that provide end-to-end connectivity. Programmed switching devices provide physical connections. Packet headers identify the destination. Packet switching offers leased line–type services over shared lines, but at a much lower cost. Figure 10-6 shows an example of a packet-switched WAN topology.

FIGURE 10-6
Packet-Switched WAN



Enabling the Internet Connection

Almost every business today connects to the Internet. It has become common for remote sites to connect to the central office through the Internet using VPNs. Usually, these remote sites connect to the Internet using digital subscriber line (DSL) or a packet-switching technology such as cable.

 Please see page 311 for more details.

Packet-Switched Communications

Packet-switched networks send data over different routes of a shared public network to reach the same destination. In other words, no dedicated path exists between the source and destination. Because packet-switched networks use different routes to send data, when the packets reach the destination, they might arrive out of order. It is the responsibility of the receiving protocol to assemble the packets in the correct order.

Digital Subscriber Line

DSL is a modem technology that uses the existing phone wires connected to virtually every home in most countries. The term xDSL refers to the different variations of DSL. DSL operates at Layer 1 of the OSI model and relies on higher-layer protocols for connection services and encapsulation.

DSL Types and Standards

Two types of DSL exist: asymmetric DSL (ADSL) and symmetric DSL (SDSL). ADSL's downlink speed is much greater than its uplink speed (thus the asymmetry). This is done because most users download much more from the Internet than they upload. SDSL is more useful for businesses because it gives equal bandwidth to the uplink and downlink.

DSL Equipment

The twisted-pair wires that provide phone service are ideal because the available frequency ranges on the wires far exceed those required to carry a voice conversation. DSL requires some specialized equipment to ensure that voice and data are kept separate and are routed to the right place:

- **Low-pass filters (LPF):** Placed on all phone jacks not used by a computer to prevent interference from high-frequency data signals
- **DSL modems:** The interface from the phone line to the computer
- **DSL access multiplexers (DSLAM):** Aggregate hundreds of signals from homes and are the access point to the Internet

 Please see page 311 for more details.

DSL Standards

Several international DSL standards exist, all of which are supported by DSL providers. They are listed in Table 10-1.

Table 10-1 DSL Standards

DSL Type	Speed	Distance Limit (ft)
Full-rate ADSL	384 kbps to 8 Mbps downlink and up to 1.024 Mbps uplink	18,000
G.lite	1.544 to 6 Mbps downlink and 640 kbps uplink	18,000
Very high data rate DSL (VDSL)	12.96 to 52.8 Mbps for both downlink and uplink	4,500
ISDN DSL (IDSL)	768 kbps for both downlink and uplink	22,000
High data rate DSL (HDSL)	1.544 to 2.048 Mbps for both downlink and uplink	12,000
G.SHDSL	192 kbps to 2.36 Mbps for both downlink and uplink	28,000

DSL Limitations and Advantages

Advantages:

- DSL offers speeds up to and exceeding T1 for a fraction of the cost.
- DSL supports data and voice.
- DSL is an always-on technology.
- DSL service providers can add circuits as needed.

Limitations:

- Availability.
- The telephone company must install DSL equipment.
- DSL has some distance limitations, and the signals cannot be amplified.

 Please see page 311 for more details.

Cable

Cable uses the same basic principles as DSL in that the bandwidth needed to accomplish the primary function (providing TV programming) is only a fraction of the available bandwidth on the wire or, in this case, cable.

Like DSL, cable modems provide always-on connectivity. This gives you the convenience of not having to dial up with every use, but it does make a system more vulnerable to hackers (which is why routers and firewalls should be installed behind a cable modem). Cable also offers speeds well over those of T1 (some claim up to six times T1 speed). Cable modems use quadrature amplitude modulation (QAM) to encode digital data into an analog signal to deliver 30 to 40 Mbps in one 6-MHz cable channel. A headend facility at the local cable office manages traffic flows and performs the following functions:

- Receives programming from networks
- Converts signals and places them on the proper channel frequency
- Combines all channels into one broadband analog channel
- Broadcasts the combined analog signal to subscribers

Cable Limitations and Advantages

Advantages:

- Cable offers very high speeds in both upstream and downstream directions.
- Cable is fairly widespread in the United States, so access is generally available.
- Many cable providers deploy hybrid-fiber coaxial (HFC) cable, which provides greater bandwidth and less noise than standard coaxial.

 Please see page 311 for more details.

Limitation:

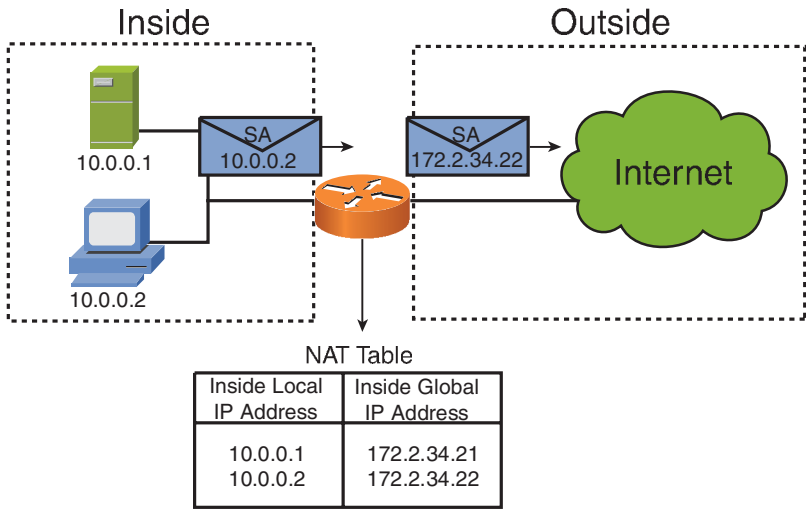
- Cable is a shared medium, so as more people use the system, each gets less bandwidth.

Introducing NAT and PAT

Network Address Translation (NAT) was initially developed as an answer to the diminishing number of IP addresses. When the IP address scheme was originally developed, it was believed that the address space would not run out. The combination of the PC explosion and the emergence of other network-ready devices quickly consumed many of the available addresses.

An additional (and equally important) benefit of NAT is that it hides private addresses from public networks, making communication more secure from hackers. Figure 10-7 shows how NAT translates the inside address of 10.0.0.1 to the outside address of 172.2.34.21.

FIGURE 10-7
Network Address Translation

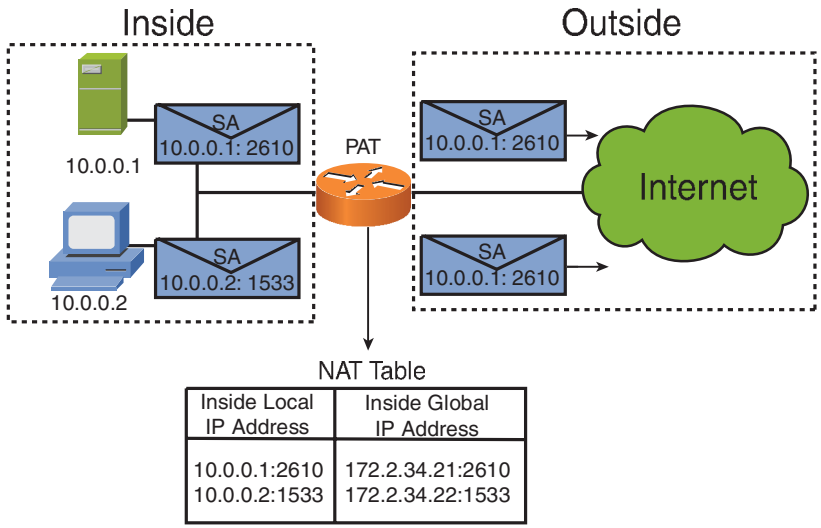


 Please see page 311 for more details.

- NAT is configured on a router, firewall, or other network device.
- Static NAT uses one-to-one private-to-public address translation.
- Dynamic NAT matches private addresses to a pool of public addresses on an as-needed basis. The address translation is still one-to-one.

Port Address Translation (PAT) is a form of dynamic address translation that uses many (private addresses) to few or one (public address). This is called overloading and is accomplished by assigning port numbers, as shown in Figure 10-8.

FIGURE 10-8
Port Address Translation



- Because the port number is 16 bits, PAT can theoretically map 65,536 sessions to a single public address.
- PAT continues to look for available port numbers. If one is not found, PAT increments the IP address (if available).

NAT Terminology

Table 10-2 lists the Cisco NAT terminology.

Table 10-2 NAT Terminology

Name	Description
Inside local address	The IP address assigned to a host on the inside, private network. Usually a private IP address.
Inside global address	A legal routable IP address that represents one or more inside local IP addresses to the outside world.
Outside local address	The IP address of an outside host as it appears to the inside, private network. This is usually a private IP address.
Outside global address	The IP address assigned to a host on the outside network by the host's owner. Usually a routable IP address.

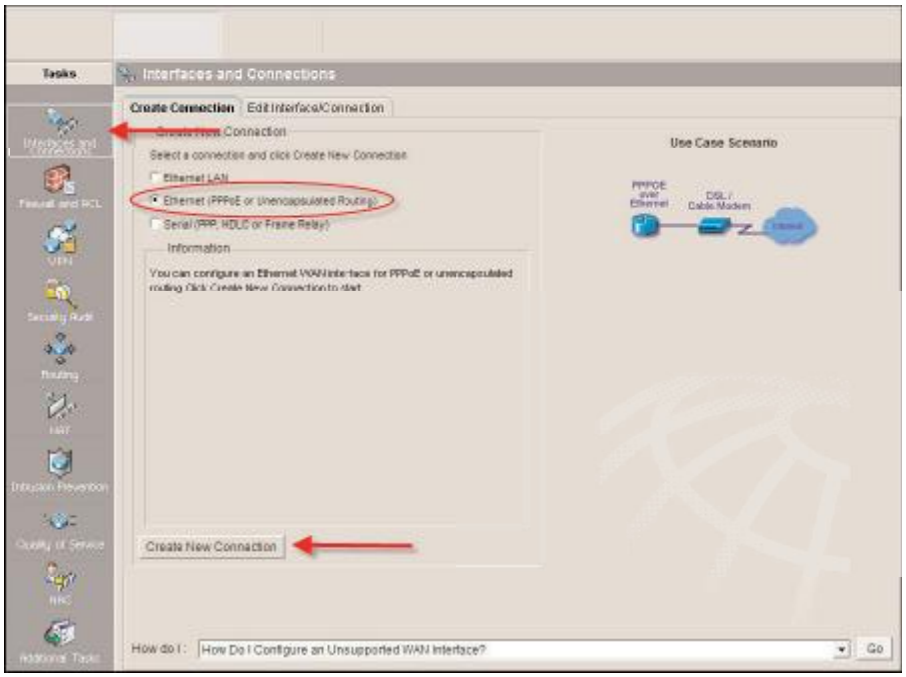
Configuring the DHCP Client and PAT Using SDM

To configure a router to be a DHCP client and accept an IP address from an ISP provider, use the following steps:

Step 1. Log on to the router using SDM. Click the **Configure** button, and then click the **Interfaces and Connections** button. Select the **Ethernet (PPPoE or Unencapsulated Routing)** option, and click the **Create New Connection** button, as shown in Figure 10-9.

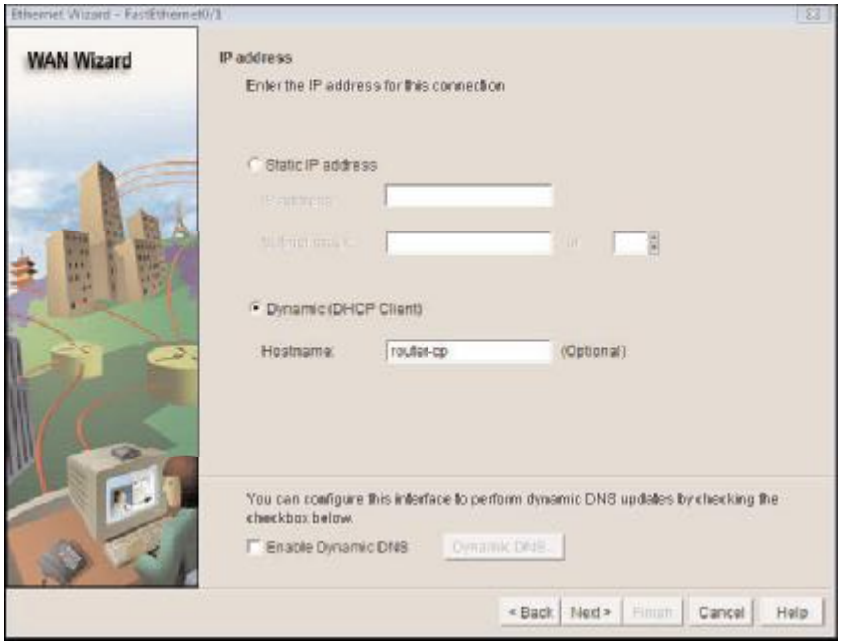
Step 2. The WAN Wizard appears. Click the **Next** button. If your ISP is using PPP over Ethernet (PPPoE), select the **Enable PPPoE** check box, and then click the **Next** button. Select the **Dynamic (DHCP Client)** option and enter the router's host name, as shown in Figure 10-10. Click the **Next** button.

FIGURE 10-9
SDM Router DHCP Client Configuration



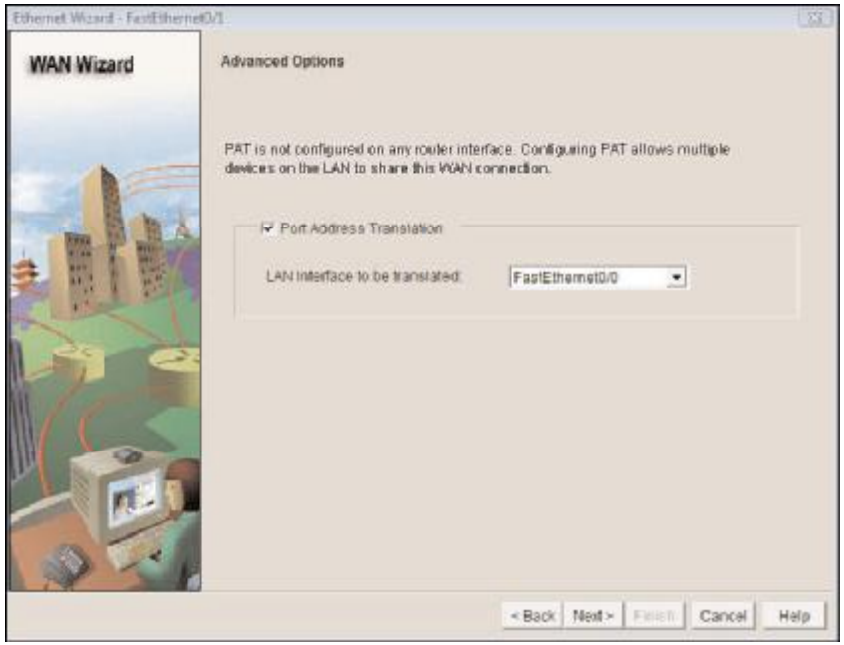
 Please see page 311 for more details.

FIGURE 10-10
SDM WAN Wizard



Step 3. Select the **Port Address Translation** check box and select the inside interface, as shown in Figure 10-11. Click the **Next** button.

FIGURE 10-11
SDM WAN Wizard
Advanced Options



Step 4. Verify the configuration and click the **Finish** button.

Verifying NAT and PAT Configuration

The **clear ip nat translation** * command clears all dynamic translation tables.

The **clear ip nat translation inside** *global-ip local-ip* command clears a specific entry from a dynamic inside translation table.

The **clear ip nat translation outside** *local-ip global-ip* command clears a specific outside translation address.

The **show ip nat translations** command lists all active translations.

The **show ip nat statistics** command shows all translation statistics.

 Please see page 311 for more details.

Configuring Serial Encapsulation

Configuring HDLC

HDLC is a data-link protocol used on synchronous serial data links. HDLC cannot support multiple protocols on a single link, because it lacks a mechanism to indicate which protocol it is carrying.

The Cisco version of HDLC uses a proprietary field that acts as a protocol field. This field makes it possible for a single serial link to accommodate multiple network-layer protocols. Cisco HDLC is a point-to-point protocol that can be used on leased lines between two Cisco devices. PPP should be used when communicating with non-Cisco devices. Figure 10-12 shows the frame format of HDLC.

FIGURE 10-12
HDLC Frame

Because HDLC is the default encapsulation type on serial links, you don't need to configure HDLC. However, if the encapsulation type has been changed to another protocol, the following command changes the serial interface encapsulation back to HDLC:

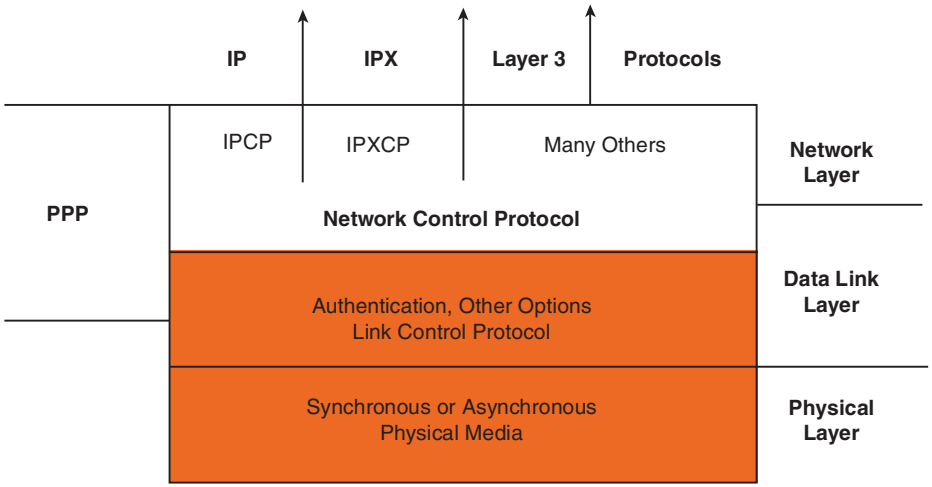
```
Router(config-if)#encapsulation hdlc
```

Configuring PPP

As shown in Figure 10-13, PPP uses a Network Control Protocol (NCP) component to encapsulate multiple protocols and the Link Control Protocol (LCP) to set up and negotiate control options on the data link.

 Please see page 311 for more details.

FIGURE 10-13
Point-to-Point Protocol



PPP Configuration Options

Cisco routers using PPP encapsulation include the LCP options shown in Table 10-3.

Table 10-3 PPP Configuration Options

Feature	How It Operates	Protocol
Authentication	Requires a password; performs challenge handshake	PAP, CHAP
Compression	Compresses data at source; reproduces data at destination	Stacker or Predictor
Error detection	Monitors data dropped on link; avoids frame looping	Magic Number
Multilink	Provides load balancing across multiple links	Multilink Protocol (MP)

Establishing a PPP Session

The three phases of PPP session establishment are described as follows:

1. **Link establishment:** Each PPP device sends LCP packets to configure and test the link (Layer 2).
2. **Authentication phase (optional):** If authentication is configured, either PAP or CHAP is used to authenticate the link. This must take place before the network layer protocol phase can begin (Layer 2).
3. **Network layer protocol phase:** PPP sends NCP packets to choose and configure one or more network layer protocols to be encapsulated and sent over the PPP data link (Layer 3).

Enabling PPP

To enable PPP encapsulation on a serial interface, enter the **encapsulation ppp** interface command, as follows:

```
RouterB(config-if)#encapsulation ppp
```

PPP Authentication Protocols

The two methods of authentication on PPP links are as follows:

- **Password Authentication Protocol (PAP):** The less-secure of the two methods; passwords are sent in clear text and are exchanged only upon initial link establishment.
- **Challenge Handshake Authentication Protocol (CHAP):** Used upon initial link establishment and periodically to make sure that the router is still communicating with the same host. CHAP passwords are exchanged as message digest algorithm 5 (MD5) hash values. CHAP uses a three-way handshake process to perform one-way authentication on a PPP serial interface.

 Please see page 311 for more details.

Configuring PPP Authentication

The three steps to enable PPP authentication on a Cisco router are as follows:

Step 1. Make sure that each router has a host name assigned to it using the **hostname** command.

Step 2. On each router, define the username of the remote router and the password that both routers will use with the **username** *remote-router-name* **password** *password* command.

Step 3. Configure PPP authentication with the **ppp authentication** {**chap | chap pap | pap chap | pap**} interface command. (If both PAP and CHAP are enabled, the first method you specify in the command is used. If the peer suggests the second method or refuses the first method, the second method is used.)

The following commands configure CHAP and PAP for authentication with the password of cisco. The remote router's host name is RouterA:

```
RouterB(config)#hostname RouterB
RouterB(config)#username RouterA password cisco
RouterB(config)#int s0
RouterB(config-if)#ppp authentication chap pap
```

Verifying the Serial Encapsulation Configuration

The **show interface** *interface-number* command shows the encapsulation type configured on the router's serial interface and the LCP and NCP states of an interface if PPP encryption is enabled:

```
RouterA#show int s0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10sec)
```

```
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
(text omitted)
```

The IOS **debug ppp authentication** command shows successful CHAP or PAP authentication.

The **debug ppp negotiation** command shows PPP-enabled routers performing negotiation.

Frame Relay

Frame Relay is a connection-oriented Layer 2 protocol that allows several data connections (virtual circuits) to be multiplexed onto a single physical link. Frame Relay relies on upper-layer protocols for error correction. Frame Relay specifies only the connection between a router and a service provider's local access switching equipment.

A connection identifier maps packets to outbound ports on the service provider's switch. When the switch receives a frame, a lookup table maps the frame to the correct outbound port. The entire path to the destination is determined before the frame is sent.

Frame Relay Terminology

- **VC (virtual circuit):** A logical circuit between two network devices. A VC can be permanent (PVC) or switched (SVC). PVCs save bandwidth (no circuit establishment or teardown) but can be expensive. SVCs are established on demand and are torn down when transmission is complete. VC status can be active, inactive, or deleted. Today, most Frame Relay circuits are PVCs.

 Please see page 311 for more details.

- **DLCI (data-link connection identifier):** Identifies the logical connection between two directly connected sets of devices. The DLCI is locally significant.
- **CIR (committed information rate):** The minimum guaranteed data transfer rate agreed to by the Frame Relay switch.
- **Inverse ARP:** Routers use inverse ARP to discover the network address of a device associated with a VC.
- **LMI (Local Management Interface):** A signaling standard that manages the connection between the router and the Frame Relay switch. LMIs track and manage keepalive mechanisms, multicast messages, and DLCI status. Routers autosense LMI types by sending a status request to the Frame Relay switch. The router configures itself to match the LMI type response. The three types of LMIs supported by Cisco Frame Relay switches are Cisco (developed by Cisco, StrataCom, Northern Telecom, and DEC), ANSI Annex D (ANSI standard T1.617), and Q933a (ITU-T Q.933 Annex A).
- **FECN (forward explicit congestion notification):** A message sent to a destination device when a Frame Relay switch senses congestion in the network.
- **BECN (backward explicit congestion notification):** A message sent to a source router when a Frame Relay switch recognizes congestion in the network. A BECN message requests a reduced data transmission rate.

ATM and Cell Switching

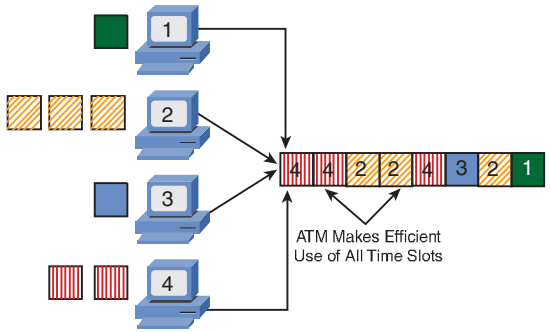
Asynchronous Transfer Mode (ATM) was originally developed as a high-speed public WAN transport for voice, video, and data. ATM was later modified by the ATM Forum to include transport over private networks.

ATM networks are composed of ATM switches interconnected by point-to-point ATM links. The links connecting the switches come in two forms: User-Network Interfaces (UNI), which connect ATM endpoints to ATM switches, and Network Node Interfaces (NNI), which connect ATM switches.

 Please see page 311 for more details.

The asynchronous part of ATM refers to the protocol's ability to use a more efficient version of time-division multiplexing (TDM). Multiplexing is a method of combining multiple data streams into a single physical or logical connection. Time division means that each data stream has an assigned slot in a repeating sequence. With synchronous TDM, each time slot is preassigned and is held open if the station assigned to it has no data to send. As shown in Figure 10-14, asynchronous transmission allows empty slots to be filled by stations that have data to send.

FIGURE 10-14
Asynchronous Transfer Mode



Section 11
RIP Routing

Dynamic Routing Protocol Overview

Routing protocols determine the best path packets take to reach a destination in a network. A routing protocol does this by defining rules to communicate with neighboring routings and then sending information about the router's learned routes to neighboring routers. Routing protocols are divided into two classes based on how they interact with other autonomous systems: exterior gateway protocols (EGP) and interior gateway protocols (IGP).

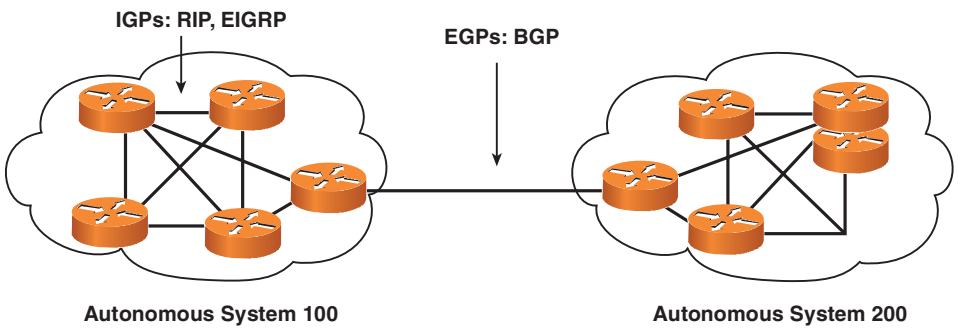
IGP and EGP

An autonomous system (AS) refers to a group of networks under a common administrative domain.

IGPs exchange information within an AS. Examples include RIP, EIGRP, OSPF, and IS-IS.

EGPs exchange information between autonomous systems. BGP is an example of an EGP.

FIGURE 11-1
IGPs and EGPs



Classes of Routing Protocols

As mentioned in Chapter 8, "Exploring the Functions of Routing," three classes or methods of routing protocols exist:

- Distance vector
- Link-state
- Advanced distance vector (also called balanced hybrid)

Routing Ranges with Administrative Distance

Several routing protocols can be used at the same time in the same network. When more than a single source of routing information exists for the same destination prefix, the source with the lowest administrative distance value is preferred.

Table 11-1 shows the default administrative distance of learned routes.

Table 11-1 AD

Route Source	Default Distance Values
Connected interface	0
Static route	1
EIGRP	5
BGP	20
Internal EIGRP	90
IGRP	100
IS-IS	115
RIP	120
EGP	140

continues

Table 11-1 AD *continued*

Route Source	Default Distance Values
ODR	160
External EIGRP	170
Internal BGP	200
Unknown	255

Classless Versus Classful Routing

Classless routing protocols include subnet mask information in routing advertisements and support variable-length subnet mask (VLSM). In classless routing, summarization is controlled manually. RIP v2, OSPF, IS-IS, and EIGRP are classless routing protocols.

Classful routing protocols do not include the subnet mask in routing advertisements. As a result, all subnetworks of the same major network must use the same subnet mask. Routers using classful routing protocols automatically perform route summarization across network boundaries. RIPv1 is an example of a classful routing protocol.

The **ip classless** command prevents a router from dropping packets for an unknown subnetwork of a directly attached network if a default route is configured. The **ip classless** command is enabled by default.

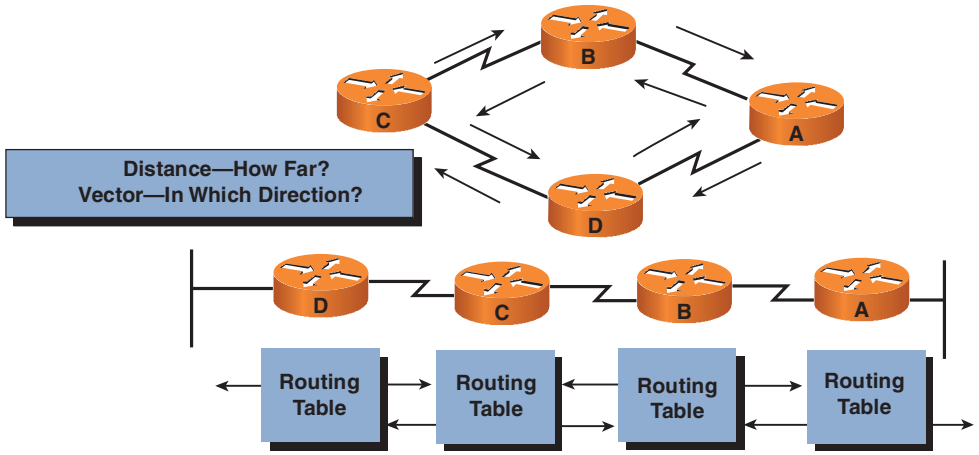
Distance Vector Route Selection

Routers using distance vector–based routing share routing table information with each other. This method of updating is called "routing by rumor." Each router receives updates from its direct neighbor. In Figure 11-2, Router B shares information with Routers A and C. Router C shares routing information with Routers B and D. In this case, the routing information

 Please see page 311 for more details.

is distance vector metrics (such as the number of hops). Each router increments the metrics as they are passed on (incrementing hop count, for example).

FIGURE 11-2
Distance Vector Routing Protocols

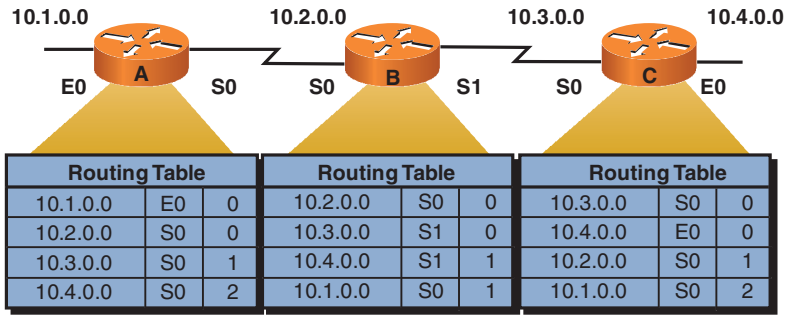


Distance accumulation keeps track of the routing distance between any two points in the network, but the routers do not know the exact topology of an internetwork.

How Information Is Discovered with Distance Vectors

Network discovery is the process of learning about nondirectly connected destinations. As the network discovery proceeds, routers accumulate metrics and learn the best paths to various destinations. In Figure 11-3, each directly connected network has a distance of 0. Router A learns about other networks based on information it receives from Router B. Router A increments the distance metric for any route learned by Router B. For example, Router B knows about the networks to Router C, which is directly connected. Router B then shares this information with Router A, which increments the distance to these networks by 1.

FIGURE 11-3
Distance Vector Route-Learning Process



Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

During updates, routing loops can occur if the network has inconsistent routing entries. Slow convergence on a new configuration is one cause of this phenomenon. The network is converged when all routers have consistent routing tables.

Routing Metrics

Routing protocols use their own rules and metrics to build and update routing tables automatically. Routing metrics are measures of path desirability. Different protocols use different metrics. Some common metrics are as follows:

- **Bandwidth:** The link's data capacity.
- **Delay:** The time required to move the packet from the current router to the destination. This depends on bandwidth, port delays, congestion, and distance.
- **Load:** The amount of activity on the interface.
- **Reliability:** The error rate of each network link.
- **Hop count:** The number of routers the packet must travel through before reaching the destination.
- **Cost:** An arbitrary value based on bandwidth, expense, and other metrics assigned by the administrator.

 Please see page 311 for more details.

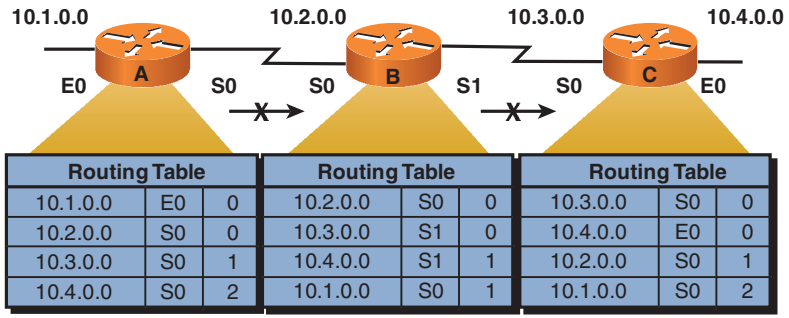
Techniques to Eliminate Routing Loops

A routing loop prevents some packets from being properly routed because of incorrect routing information circulating in the network. Routing loops usually occur when unreachable networks are incorrectly replaced by older routing information from other devices in the network. Routing protocols have some mechanisms to prevent routing loops.

Split Horizon

Split horizon is one way to eliminate routing loops and speed convergence. The idea behind split horizon is that it is never useful to send information about a route back in the direction from which the update came. If the router has no valid alternative path to the network, it is considered inaccessible. Split horizon also eliminates unnecessary routing updates, thus speeding convergence. In Figure 11-4, Router A, using split horizon, will not send route advertisements that contain routes learned on serial interface 0 out serial interface 0.

FIGURE 11-4
Split Horizon



Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

Hold-Down Timers

Hold-down timers dictate that when a route is invalid, no new route with the same or a worse metric will be accepted for the same destination for some period of time. This allows network updates to propagate throughout the network.

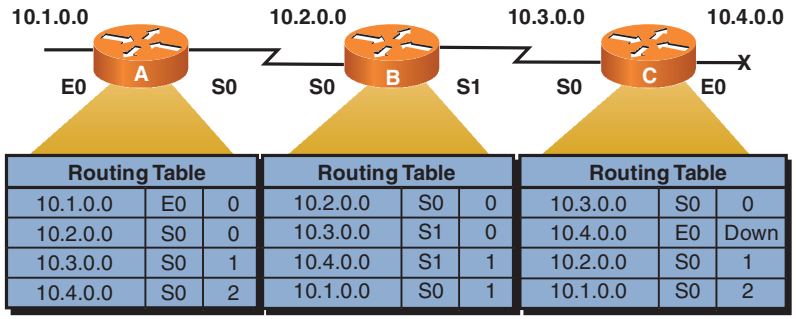
Route poisoning (part of split horizon) also eliminates routing loops caused by inconsistent updates. Route poisoning basically sets a route to "unreachable" and locks the table (using hold-down timers) until the network has converged.

Route Poisoning

In Figure 11-5, when network 10.4.0.0 goes down, Router C "poisons" its link to network 10.4.0.0 by sending an update for network 10.4.0.0 that indicates it has an infinite metric and a hop count of 16 (that is, it is unreachable). The router advertises the poisoned route to its neighbors.

Router C is no longer susceptible to incorrect updates about network 10.4.0.0 coming from neighboring routers that might claim to have a valid alternative path. After the hold-down timer expires (which is just longer than the time to convergence), Router C begins accepting updates again.

FIGURE 11-5
Routing Poisoning



Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

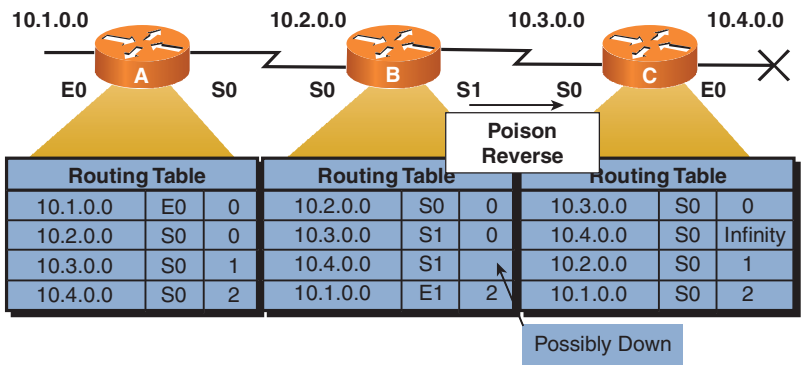
Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	Down
10.2.0.0	S0	1
10.1.0.0	S0	2

Poison Reverse

In Figure 11-6, when Router B sees the metric to 10.4.0.0 jump to infinity, it sends a return message (overriding split horizon) called a poison reverse back to Router C, stating that network 10.4.0.0 is inaccessible. This message ensures that all routers on that segment have received information about the poisoned route.

FIGURE 11-6
Poison Reverse



Triggered Updates

Also known as flash updates, triggered updates are routing updates sent immediately out a router's interface when it notices that a directly connected subnet has changed state.

RIP

RIP is a true distance vector routing protocol that sends its complete routing table out all active interfaces every 30 seconds. RIP is subject to the split horizon rule.

RIP uses a hop count as its metric to determine the best path to a remote network. The maximum allowable hop count is 15; thus a hop count of 16 is unreachable.

Two versions of RIP exist: version 1 and version 2.

RIP can load-balance over as many as 16 equal-cost paths; the default is 4.

RIPv1 and RIPv2 Comparisons

RIP version 1 is a classful protocol, meaning that it does not send its subnet mask in routing updates. As a result, RIPv1 does not support variable-length subnet mask.

RIP version 2 is a classless protocol that supports VLSM and sends its subnet mask in routing updates.

RIP version 2 also sends routing updates through multicast. RIP v1 broadcasts updates. RIP v2 also supports manual route summarization and authentication. RIP v1 does not.

RIP Timers

RIP uses four timers to regulate performance and route updates:

- **Route update timer:** The time between router updates. Default is 30 seconds.
- **Route invalid timer:** The time that must expire before a route becomes invalid. Default is 180 seconds.
- **Route hold-down timer:** If RIP receives an update with a hop count higher than the metric recording in the routing table, RIP goes into a hold-down for 180 seconds.
- **Route flush timer:** The time from when a route becomes invalid to when it is removed from the routing table. Default is 240 seconds.

Configuring and Verifying RIP

The commands to enable RIP on a Cisco router are as follows:

- **router rip** global command
- **network** *connected-network-address* configuration command

 Please see page 311 for more details.

For example, the following commands enable RIP and advertise routes for the locally connected networks 192.168.1.0 and 192.168.2.0:

```
RouterB(config)#router rip
RouterB(config-router)#network 192.168.1.0
RouterB(config-router)#network 192.168.2.0
```

The IOS command **show ip protocols**, as follows, displays values associated with routing timers, the administrative distance, and network information associated with the entire router:

```
RouterB#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 2 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface             Send  Recv   Key-chain
    Serial0               1     1 2
    Serial1               1     1 2
  Routing for Networks:
    192.168.1.0
    192.168.2.0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 120)
```

Displaying the Routing Table

The **show ip route** command, as follows, displays the Cisco routing table's contents:

```
RouterA#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 interarea
       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

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
R    192.168.0.0/24 [120/1] via 192.168.1.1, 00:00:21, Serial0
C    192.168.1.0/24 is directly connected, Serial0
C    192.168.2.0/24 is directly connected, Ethernet0
R*   0.0.0.0/0 [120/1] via 192.168.1.1, 00:00:21, Serial0
```

The [120/1] indicates that 120 is the AD and 1 is the number of hops to the remote network. R indicates that RIP has learned paths to networks 192.168.0.0/24 and 0.0.0.0/0.

Troubleshooting RIP

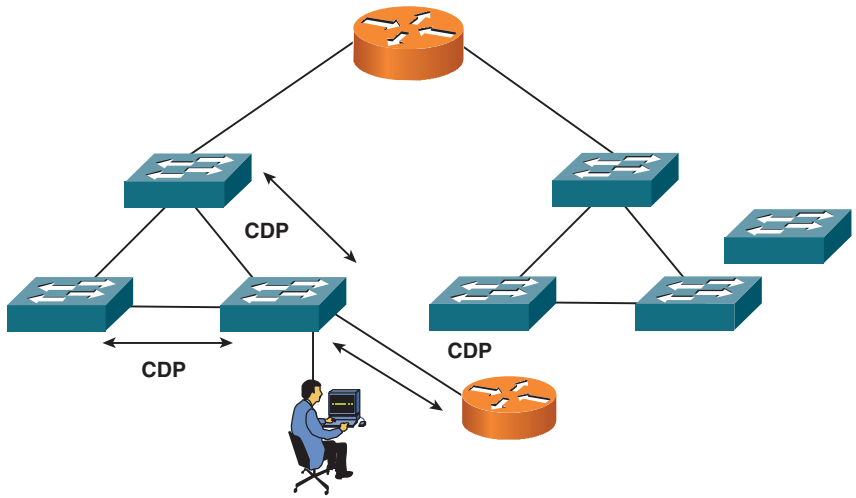
The **debug ip rip** command displays routing updates as they are sent and received, thus allowing you to troubleshoot RIP.

Section 12
Managing Your Network Environment

Discovering Neighbors on the Network with CDP

Cisco Discovery Protocol (CDP) is a proprietary tool that enables access to protocol and address information on directly connected devices. CDP runs over the data link layer, allowing devices running different network layer protocols to learn about each other. CDP summary information includes device identifiers, address lists, port identifiers, and platform.

FIGURE 12-1
CDP



CDP runs over all LANs, Frame Relay, ATM, and other WANs employing Subnetwork Access Protocol (SNAP) encapsulation. CDP starts by default on bootup and sends updates every 60 seconds.

 Please see page 311 for more details.

Implementation of CDP

- **cdp enable** enables CDP on an interface.
- **no cdp enable** disables CDP on an interface.
- **cdp run** allows other CDP devices to get information about your device.
- **no cdp run** disables CDP on a device.
- **show cdp** displays the CDP output.
- **show cdp neighbors** displays the CDP updates received on the local interfaces and information about CDP neighbors. For each CDP neighbor, the following is displayed:
  - Neighbor device ID
  - Local interface
  - Holdtime value in seconds
  - Neighbor device capability code (router, switch)
  - Neighbor hardware platform
  - Neighbor remote port ID
- **show cdp neighbors detail** displays updates received on the local interfaces. This command displays the same information as the **show cdp entry *** command. The **show cdp neighbors detail** command shows the same information as **sh cdp neighbors**, in addition to the network layer address of the CDP neighbor.

 Please see page 311 for more details.

- **show cdp entry** displays the following information about neighboring devices:
  - Neighbor device ID
  - Layer 3 protocol information
  - Device platform
  - Device capabilities
  - Local interface type and outgoing remote port ID
  - Holdtime value in seconds
  - Cisco IOS Software type and release
- **show cdp traffic** displays information about interface traffic.
- **show cdp interface** displays interface status and configuration information.

Managing Router Startup and Configuration

When a router is booted up, it goes through the following sequence:

1. The router checks its hardware with a power-on self test (POST).
2. The router loads a bootstrap code.
3. The Cisco IOS Software is located and loaded using the information in the bootstrap code.
4. The configuration is located and loaded.

 Please see page 311 for more details.

Router Components

The major router components are as follows:

- **RAM:** Random-access memory contains key software (IOS).
- **ROM:** Read-only memory contains startup microcode.
- **NVRAM:** Nonvolatile RAM stores the configuration.
- **Configuration register:** Controls the bootup method.
- **Interfaces:** The interface is the physical connection to the external devices. Physical connections can include Token Ring and FDDI.
- **Flash memory:** Flash contains the Cisco IOS Software image. Some routers run the IOS image directly from flash and do not need to transfer it to RAM.

ROM Functions

ROM contains the startup microcode and consists of the following four areas:

- **Bootstrap code:** Brings the router up during initialization. Reads the configuration register to determine how to boot.
- **POST:** Tests the basic function of the router hardware and determines the hardware present.
- **ROMMON:** A low-level operating system normally used for manufacturing, testing, troubleshooting, and password recovery.
- **Mini Cisco IOS Software file:** Loads a new Cisco IOS image into flash memory from a TFTP server.

 Please see page 311 for more details.

How a Cisco Device Locates and Loads IOS Images

The bootstrap code locates and loads the Cisco IOS image. It does this by first looking at the configuration register. The default value for the configuration register is 0x2102. Changing the configuration register changes the location of the IOS load.

If the configuration register's fourth character is from 0x2 to 0xF, the bootstrap parses the startup-config file in NVRAM from the **boot system** command that specifies the name and location of the Cisco IOS Software image to load.

After the IOS is loaded, the router must be configured. Configurations in NVRAM are executed. If one does not exist in NVRAM, the router initiates an auto-install or setup utility. The auto-install routine attempts to download a configuration file from a TFTP server.

The Configuration Register

The config register includes information that specifies where to locate the Cisco IOS Software image.

Before changing the configuration register, use the **show version** command to determine the current image. The last line contains the register value. Changing this value changes the location of the IOS load (and many other things). A **reload** command must be used for the new configuration to be set. The register value is checked only during the boot process.

Table 12-1 shows the configuration register values and meanings.

Table 12-1 Configuration Register Values

Configuration Register Boot Field Value	Meaning
0x0	Use ROM monitor mode (manually boot using the **boot** command)
0x1	Automatically boot from ROM (provides IOS subset)
0x2 to 0xF	Examine NVRAM for boot system commands (0x2 is the default if router has flash)

 Please see page 311 for more details.

The **show version** command verifies changes in the configuration register setting.

The **show flash** command displays contents in flash memory, including the image filenames and sizes.

The **show running-config** command shows the current running configuration in RAM.

The **show startup-config** command shows the configuration file saved in NVRAM. This is the configuration that will be used if the router is reloaded and the running-config is not saved.

Managing IOS Images

The Cisco IOS File System (IFS) feature provides an interface to the router file systems. The uniform resource locator (URL) convention allows you to specify files on network devices.

URL prefixes for Cisco network devices are as follows:

- **bootflash:** Boot flash memory
- **flash:** Available on all platforms
- **flh:** Flash load helper log files
- **ftp:** File Transfer Protocol (FTP) network server
- **nvram:** NVRAM
- **rcp:** Remote Copy Protocol (RCP) network server
- **slot0:** First PCMCIA flash memory card
- **slot1:** Second PCMCIA flash memory card
- **system:** Contains the system memory and the running configuration
- **tftp:** Trivial File Transfer Protocol (TFTP) network server

 Please see page 311 for more details.

Backing Up and Upgrading IOS Images

```
wg_ro_a# show flash
wg_ro_a# copy flash tftp
wg_ro_a# copy tftp flash
```

When using the **copy flash** command, you must enter the IP address of the remote host and the name of the source and destination system image file.

The router prompts you for the IP address of the remote host and the name of the source and destination system image file.

Cisco IOS copy Command

As shown in Figure 12-2, the **copy** commands are used to move configuration from one component or device to another. The syntax is as follows:

```
copy object source destination
```

For example:

```
copy running-config startup-config
```

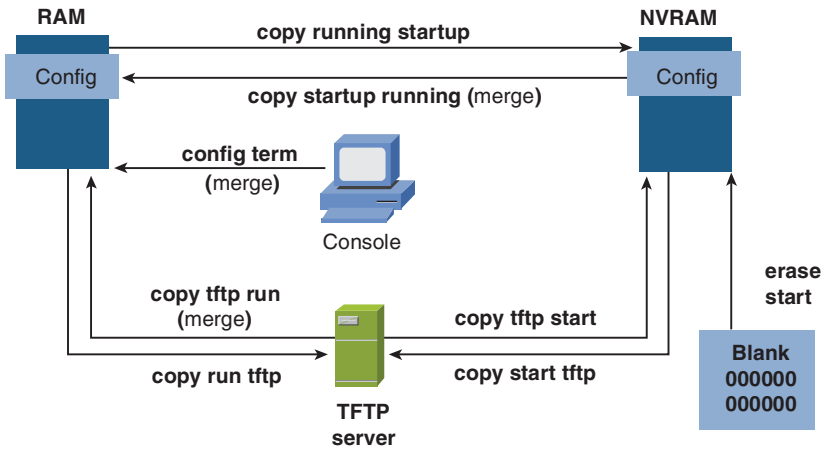


FIGURE 12-2
IOS **copy** Command

NOTE
When a configuration is copied into RAM, it merges with the existing configuration in RAM. It does not overwrite the existing configuration. In Cisco IOS Release 12.3T and later, the **configure replace** command allows you to overwrite the running configuration.

 Please see page 311 for more details.

The **show running-config** and **show startup-config** commands are useful troubleshooting aids. These commands allow you to view the current configuration in RAM or the startup configuration commands in NVRAM.

You know that you are looking at the startup config file when you see a message at the top telling you that NVRAM has been used to store the configuration.

You know that you are looking at the current config file when you see the words "Current configuration" at the top of the display.

Troubleshooting

Troubleshooting is aided with the **show** and **debug** commands. The following table details the differences between the two.

	show	debug
Characteristics	Static	Dynamic
Processing Load	Low overhead	High overhead
Primary Use	Gather facts	Observe processes

 Please see page 311 for more details.

ICND2

Part I: LAN Switching

Section 1
Implementing VLANS and Trunks

VLANs

The virtual LAN (VLAN) organizes physically separate users into the same broadcast domain. The use of VLANs improves performance, security, and flexibility. The use of VLANs also decreases the cost of arranging users, because no extra cabling is required.

VLAN Characteristics

VLANs allow logically defined user groups rather than user groups defined by their physical locations. For example, you can arrange user groups such as accounting, engineering, and finance, rather than everyone on the first floor, everyone on the second floor, and so on.

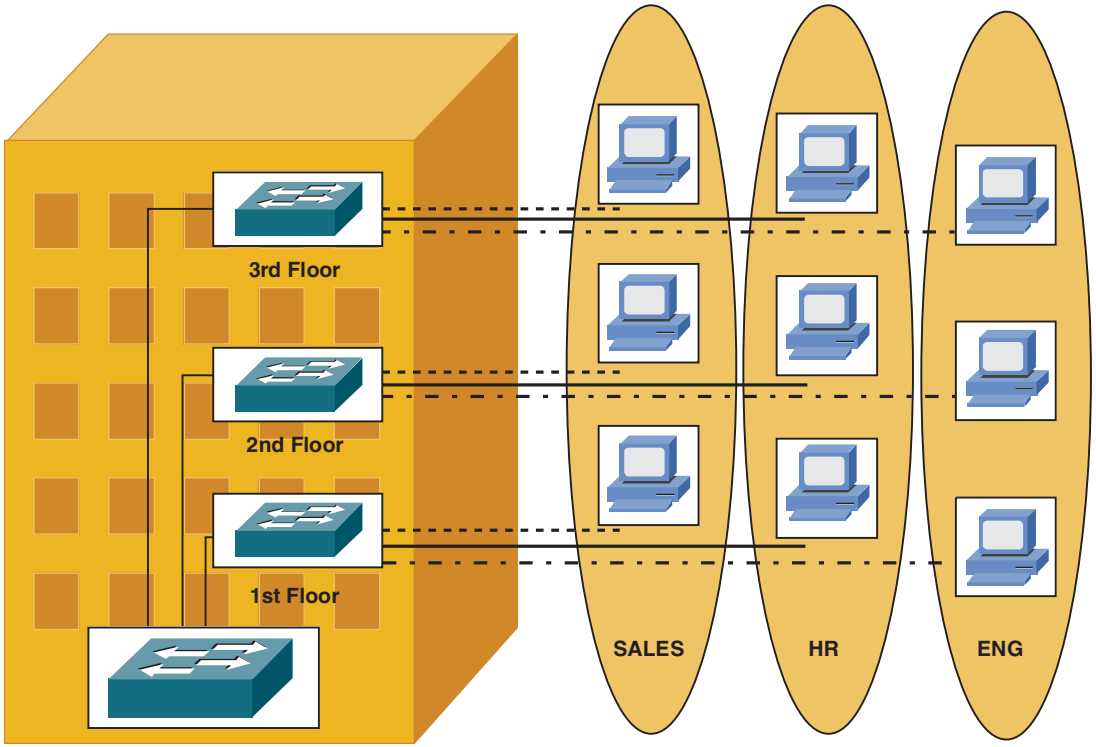
- VLANs define broadcast domains that can span multiple LAN segments.
- VLANs improve segmentation, flexibility, and security.
- VLAN segmentation is not bound by the physical location of users.

 Please see page 311 for more details.

- Each switch port can be assigned to an access VLAN, a voice VLAN, or a trunk.
- Ports assigned to the same VLAN share broadcasts and are in the same broadcast domain.
- A VLAN can exist on one or several switches.

Figure 1-1 shows a VLAN design. Note that VLANs are defined by user functions rather than locations.

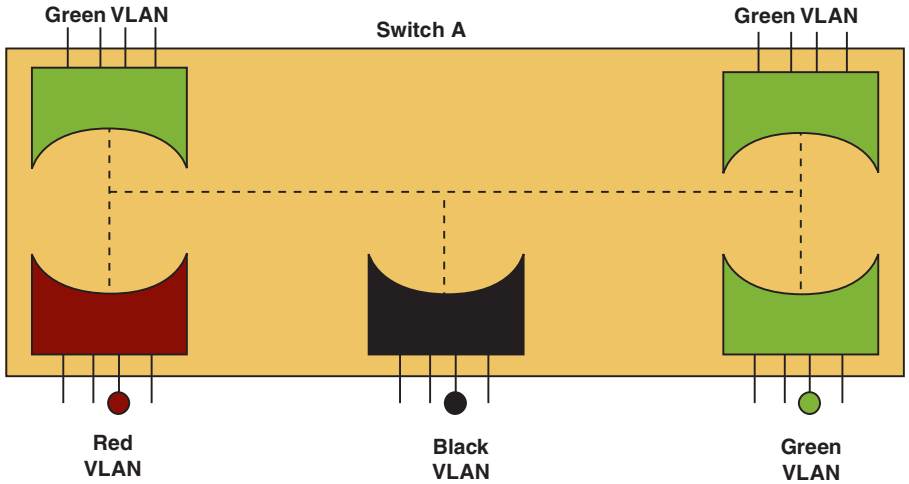
FIGURE 1-1
VLAN Design



VLAN Operation

Figure 1-2 shows that each VLAN on a switch behaves as if it were a separate physical bridge. The switch forwards packets (including unicasts, multicasts, and broadcasts) only to ports assigned to the same VLAN from which they originated. This drastically cuts down on network traffic.

FIGURE 1-2
VLAN Operation



VLANs require a trunk or a physical connection for each VLAN to span multiple switches. Each trunk can carry traffic for multiple VLANs.

Supported VLANs

The Catalyst 2960 supports VLANs in VLAN Trunking Protocol (VTP) client, server, and transparent mode. VLANs are identified by a number from 1 to 4094. VLAN IDs 1002 through 1005 are reserved. The switch supports up to 255 VLANs.

 Please see page 311 for more details.

VLAN Port Membership Modes

A port must be assigned (configured) to a VLAN by assigning a membership mode that specifies the kind of traffic the port carries:

- **Static access:** The port belongs to only one VLAN and is manually assigned.
- **Trunk (IEEE 802.1Q):** The port is a member of all VLANs.
- **Dynamic access:** The port belongs to one VLAN and is dynamically assigned by a VLAN Membership Policy Server (VMPS). Dynamic access ports cannot connect to another switch.
- **Voice VLAN:** The port is an access port attached to a Cisco IP phone that is configured to use one VLAN for voice traffic and another VLAN for data traffic from a device connected to the IP phone.

Trunking

The IEEE 802.1Q protocol defines VLAN topologies and connects multiple switches and routers. 802.1Q tagging provides a standard method of identifying frames that belong to a particular VLAN by using an internal process that modifies the existing Ethernet frame with the VLAN identification.

Cisco supports 802.1Q trunking over Fast Ethernet and Gigabit Ethernet links. 802.1Q defines how to carry traffic from multiple VLANs over a single point-to-point link.

VLAN Trunking Protocol

VLAN Trunking Protocol (VTP) is a Layer 2 messaging protocol that maintains VLAN configuration consistency throughout a common administrative domain by managing VLAN additions, deletions, and name changes across multiple switches. Without VTP, you would have to manually add VLAN information to each switch in the network.

 Please see page 311 for more details.

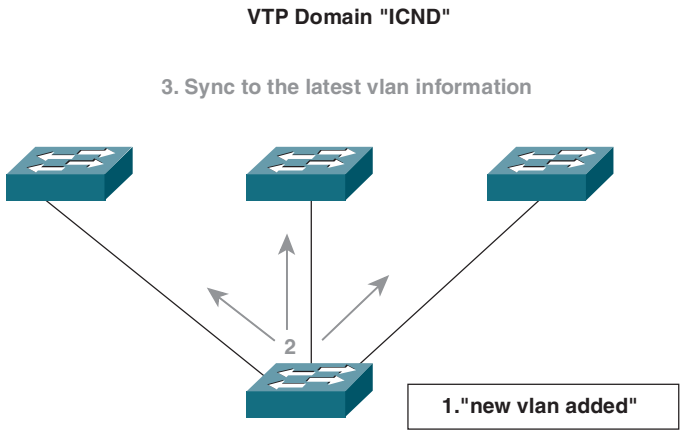
How VTP Works

Whenever a change occurs in the VLAN database, the VTP server increments its configuration revision number and then advertises the new revision throughout the VTP domain. A VTP domain is one or more interconnected switches that share the same VTP environment. When a switch receives the VTP advertisement, it overwrites its configuration with the new information if the new revision number is higher than the one it already has. If the revision number is the same, the switch ignores the advertisement. If the revision number is lower, the switch replies with the more up-to-date revision number. VTP cannot cross a Layer 3 boundary.

VTP Example

In Figure 1-3, the VTP server notifies all switches in its VTP domain that a new VLAN, named "ICND," has been added. The server advertises VLAN configuration information to maintain domain consistency.

FIGURE 1-3 Advertising VLAN Configuration Information



VTP Modes

A Catalyst switch can operate in three different modes: server, client, or transparent. The default mode is server mode. VLAN configurations are not advertised until a management domain name is specified or learned. Following are the VTP modes:

- **Server:** Switch can add, delete, and modify VLANs and other configuration parameters for the VTP domain.
- **Client:** Switch cannot create, delete, or modify VLANs. Transmits and receives VTP updates over trunk links.
- **Transparent:** Switch does not participate in the VTP domain. Switch can add, delete, and modify VLANs locally. In VTP version 2, transparent switches forward VTP advertisements they receive.

VLAN Database

VLAN information is stored in a file located in flash called vlan.dat. If this file is deleted, all switch VLAN information is deleted.

VTP Advertisements

VTP advertisements are only sent over trunk links. They are flooded over the native VLAN (VLAN1 by default) every five minutes or whenever a change occurs. VTP advertisements include

- VTP domain name
- VTP configuration revision number
- Update identity and update timestamp
- Message digest algorithm 5 (MD5) VLAN configuration
- Frame format
- VLAN ID, name, type, and state

 Please see page 311 for more details.

VTP Versions

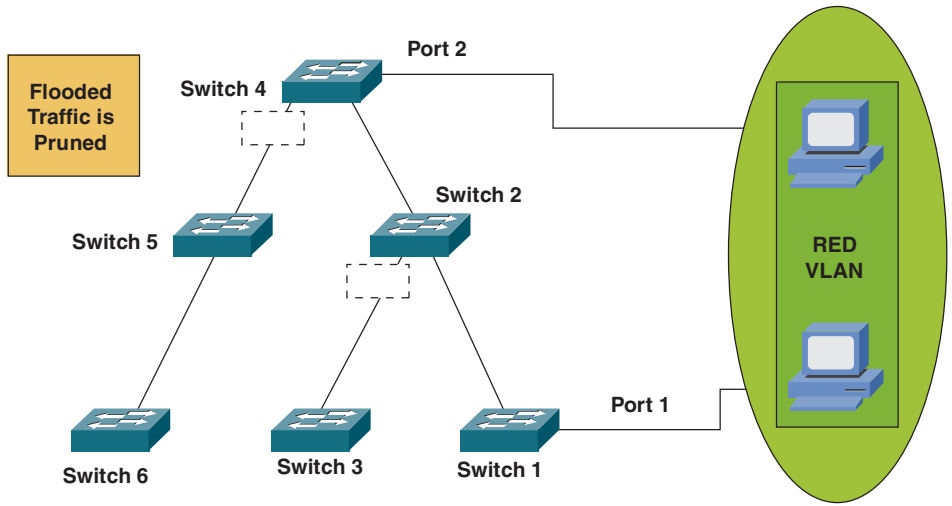
Two versions of VTP exist: version 1 and 2. VTP version 1 is the default VTP version. Version 2 includes the following additional features:

- Token Ring support
- Unrecognized type-length-value
- Version-dependent transparent mode (forwards VTP messages in transparent mode out all trunk links)
- Consistency checks

VTP Pruning

VTP pruning improves bandwidth by restricting broadcasts, multicasts, and unknown unicasts from flooding the entire domain. Figure 1-4 shows an example of VTP pruning.

FIGURE 1-4
VTP Pruning



By default, a trunk carries traffic for all VLANs in the VTP management domain. With VTP pruning enabled, update traffic from station A is not forwarded to switches 3, 5, and 6, because traffic for the red VLAN has been pruned on the links indicated on switches 2 and 4.

Default VTP Configuration

The default VTP configuration on a Catalyst 2960 switch is as follows:

- **VTP domain:** Null
- **VTP mode:** Server
- **VTP version:** Version 1
- **VTP password:** None
- **VTP pruning:** Disabled

Configuring VTP, VLANs, and Trunks

The steps to configure VLANs on a Catalyst 2960 switch are as follows:

Step 1. Configure VTP.

Step 2. Add VLANs and assign port membership modes.

Step 3. Define trunks.

 Please see page 311 for more details.

VTP Command

vtp [mode {server | client | transparent}] [domain *domain-name*] **[password** *password*] **[pruning {enable | disable}] [version {1 | 2}]**

- *domain-name*: Can be specified or learned (is case sensitive).
- *password*: Can be set for the VTP management domain. The password is case sensitive and must be the same for all the switches in the management domain.
- **pruning:** VTP pruning on a server propagates the changes throughout the entire VTP domain.
- **version:** Setting the version on a server propagates the changes throughout the entire VTP domain.

Configuring VTP on a 2960

```
Cat2960(config)#vtp mode server
Cat2960(config)#vtp domain CiscoPress
Changing VTP domain name from NULL to CiscoPress
Cat2960(config)#vtp password ICND
Setting device VLAN database password to ICND
Cat2960(config)#vtp version 2
Cat2960(config)#vtp pruning
Pruning switched on
Cat2960#show vtp status
Cat2960#show vtp counters
```

Adding, Modifying, and Deleting a VLAN on a 2960

```
Switch(config)#vlan 10
Switch(config-vlan)#name Accounting
```

 Please see page 311 for more details.

```
Switch(config)#vlan 10
Switch(config-vlan)#name Sales
Switch(config)#no vlan 10
Switch#show vlan brief
```

Configuring a Trunk Link

Cisco switches use DTP (Dynamic Trunking Protocol) to negotiate a trunk link. The **switchport trunk** command sets Fast Ethernet or Gigabit Ethernet ports to trunk mode.

```
switchport mode [dynamic {auto | desirable} | trunk]
```

- **mode dynamic auto** allows the interface to convert to a trunk link if the connecting neighbor interface is set to **trunk** or **desirable**.
- **mode dynamic desirable** allows the interface to actively attempt to convert the link to a trunk link. The link becomes a trunk if the neighbor interface is set to **trunk**, **desirable**, or **auto**. This is the recommended setting.
- **trunk** sets the interface to trunking on.

```
Cat2960(config)#interface g0/1
Cat2960(config-if)#switchport mode trunk
Cat2960(config-if)#interface g0/2
Cat2960(config-if)#switchport mode dynamic desirable
Cat2960#show interface trunk
```

Defining Allowed VLANs

By default, all VLANs (1–4094) are allowed to propagate on all trunk links. To limit a trunk to allow only specified VLANs, use the following command:

```
switchport trunk allowed vlan {add | all | except | remove} vlan-list
```

 Please see page 311 for more details.

The following command allows only VLANs 10–50 on a trunk link:

```
Cat2960(config-if)#switchport trunk allowed vlan 10-50
```

Assigning Ports to a VLAN on a 2960

Assigning a single port:

```
Cat2960(config)#interface fastethernet 0/1
Cat2960(config-if-range)#switchport mode access
Cat2960(config-if-range)#switchport access vlan 10
```

Assigning a range of ports:

```
Cat2960(config)#interface range fastethernet 0/1 - 12
Cat2960(config-if-range)#switchport mode access
Cat2960(config-if-range)#switchport access vlan 10
```

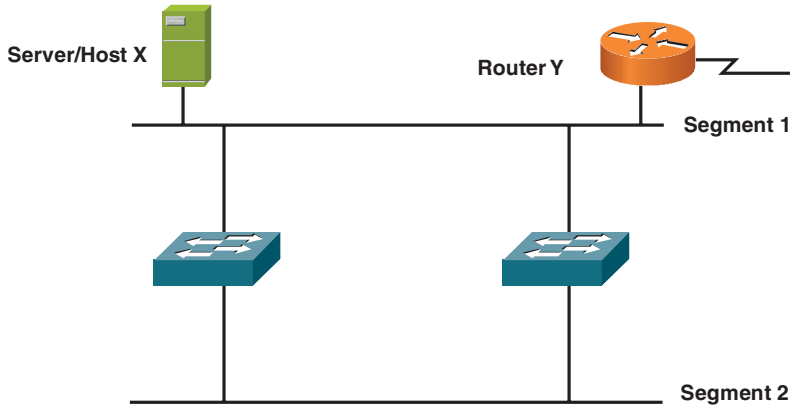
 Please see page 311 for more details.

Section 2
Redundant Switching and STP

Redundant Switched Topology Issues

A redundant topology has multiple connections to switches or other devices. Redundancy ensures that a single point of failure does not cause the entire switched network to fail. In the absence of the Spanning Tree Protocol (STP), Layer 2 redundancy can cause problems in a network, including broadcast storms, multiple copies of frames, multiple loops, and MAC address table instability. Figure 2-1 shows a redundant topology.

FIGURE 2-1
Redundant Switched Topology



Broadcast Storms

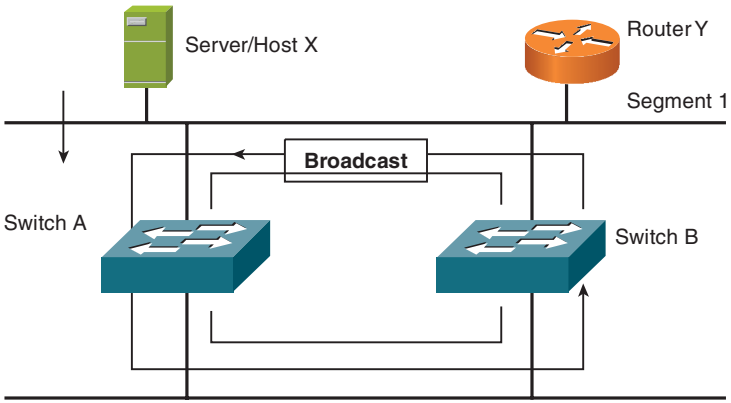
The flooding of broadcast frames can cause a broadcast storm (indefinite flooding of frames) unless a mechanism is in place to prevent it.

 Please see page 311 for more details.

An example of a broadcast storm is shown in Figure 2-2 and can be described as follows:

1. Host X sends a broadcast frame, which is received by switch A.
2. Switch A checks the destination and floods it to the bottom Ethernet link, segment 2.
3. Switch B receives the frame on the bottom port and transmits a copy to the top segment.
4. Because the original frame arrives at switch B through the top segment, switch B transmits the frame a second time. The frame travels continuously in both directions.

FIGURE 2-2
Broadcast Storm



Multiple Frame Transmission

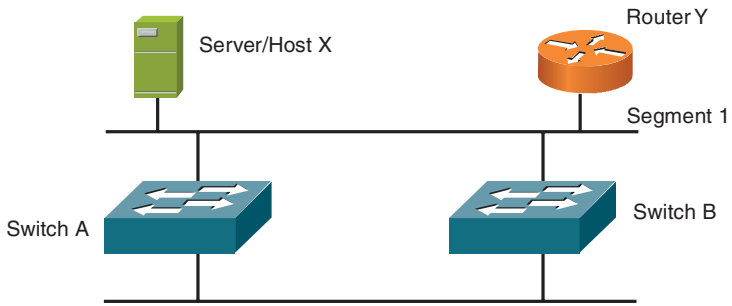
Some protocols cannot correctly handle duplicate transmissions. Protocols that use sequence numbering see that the sequence has recycled. Other protocols process the duplicate frame with unpredictable results. As depicted in Figure 2-3, multiple frame transmissions occur as follows:

 Please see page 311 for more details.

1. Host X sends a frame to Router Y. One copy is received over the direct Ethernet connection, segment 1. Switch A also receives a copy.
2. Switch A checks the destination address. If the switch does not find an entry in the MAC address table for Router Y, it floods the frame on all ports except the originating port.
3. Switch B receives the frame on segment 2 and forwards it to segment 1.

Note that Router Y has now received the same frame twice.

FIGURE 2-3
Multiple Frame Transmission



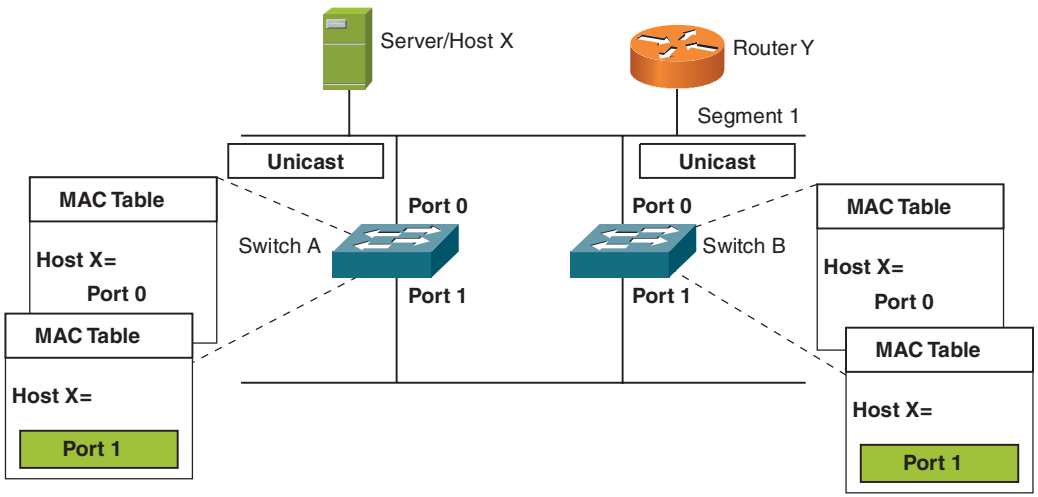
MAC Database Instability

Database instability occurs when a switch receives the same frame on different ports. Figure 2-4 shows how this occurs:

1. Host X sends a frame to Router Y. When the frame arrives at switches A and B, they both learn the MAC address for host X and associate it with port 0.
2. The frame is flooded out port 1 of each switch (assuming that Router Y's address is unknown).
3. Switches A and B receive the frame on port 1 and incorrectly associate host X's MAC address with that port.

This process repeats indefinitely.

FIGURE 2-4
MAC Database Instability

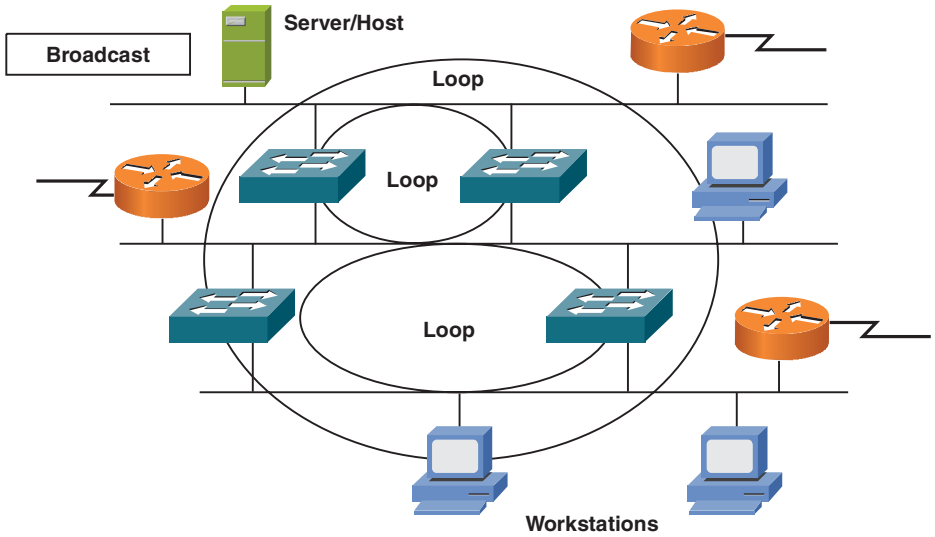


Multiple Loops

Multiple loops can occur in large switched networks. When multiple loops are present, a broadcast storm clogs the network with useless traffic. Packet switching is adversely affected in such a case and might not work. Unlike the time-to-live (TTL) mechanism in IP, Ethernet has no built-in mechanism to stop loops after they begin. Figure 2-5 shows an example of multiple loops occurring in a network.

 Please see page 311 for more details.

FIGURE 2-5
Network Experiencing Multiple Loops



Spanning Tree Protocol

Spanning Tree Protocol (STP) prevents looping traffic in a redundant switched network by blocking traffic on the redundant links. If the main link goes down, Spanning Tree activates the standby path. STP operation is transparent to end stations.

STP was developed by Digital Equipment Corp. (DEC) and was revised in the IEEE 802.1d specification. The two algorithms are incompatible. Catalyst switches use the IEEE 802.1d STP by default.

Spanning Tree Operation

STP assigns roles to switches and ports so that only one path is available through the switch network at any given time.

 Please see page 311 for more details.

This is accomplished by assigning a single root bridge, root ports for nonroot bridges, and a single designated port for each network segment. On the root bridge, all ports are designated ports. Assignment is made by cost. Table 2-1 shows the costs for switch interfaces.

Table 2-1 Spanning Tree Costs

Link Speed	Cost
10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100

On the root bridge, all ports are set to the forwarding state. For the nonroot bridge, only the root port is set to the forwarding state. The port with the lowest-cost path to the root bridge is chosen as the root port.

One designated port is assigned on each segment. The bridge with the lowest-cost path to the root bridge is the designated port. Figure 2-6 shows a root bridge, nonroot bridge, and port status.

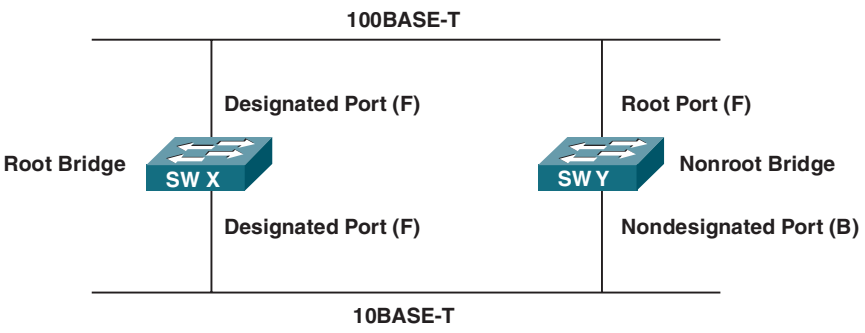


FIGURE 2-6 Root Bridge, Nonroot Bridge, and Port Status

 Please see page 311 for more details.

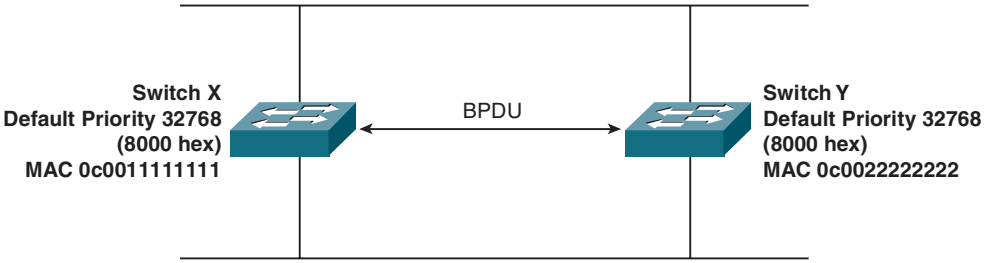
Spanning Tree must select the following:

- One root bridge
- One root port per nonroot bridge
- One designated port per network segment

Selecting the Root Bridge

Switches running STP exchange information at regular intervals using a frame called the bridge protocol data unit (BPDU). Each bridge has a unique bridge ID. The bridge ID contains the bridge MAC address and a priority number. The midrange value of 32768 is the default priority. The bridge with the lowest bridge ID is selected as the root bridge. When switches have the same priority, the one with the lowest MAC address is the root bridge. Figure 2-7 shows switch X as the root bridge.

FIGURE 2-7
Root Bridge Selection



Spanning Tree Election Criteria

Spanning Tree builds paths from the root bridge along the fastest links. It selects paths according to the following criteria:

1. Lowest path cost to the root bridge
2. Lowest sender bridge ID
3. Lowest sender port ID

 Please see page 311 for more details.

Port States

Frames take a finite amount of time to travel or propagate through the network. This delay is known as propagation delay. When a link goes down, Spanning Tree activates previously blocked links. This information is sent throughout the network, but not all switches receive it at the same time. To prevent temporary loops, switches wait until the entire network is updated before setting any ports to the forwarding state. Each switch port in a network running STP is in one of the following states listed in Table 2-2.

Table 2-2 Spanning Tree Port States

Port State	Timer	Actions
Blocking	Max Age (20 sec)	Receives BPDUs, discards frames, does not learn MAC addresses
Listening	Forward Delay (15 sec)	Receives BPDUs to determine its role in STP, discards frames and MAC addresses
Learning	Forward Delay	Receives and transmits BPDUs, does not learn MAC addresses, discards frames
Forwarding	—	Forwards frames, learns MAC addresses, receives and transmits BPDUs

The forward delay is the time it takes for a port to go to a higher state. It usually takes 50 seconds for a port to go from the blocking state to the forwarding state, but the timers can be adjusted.

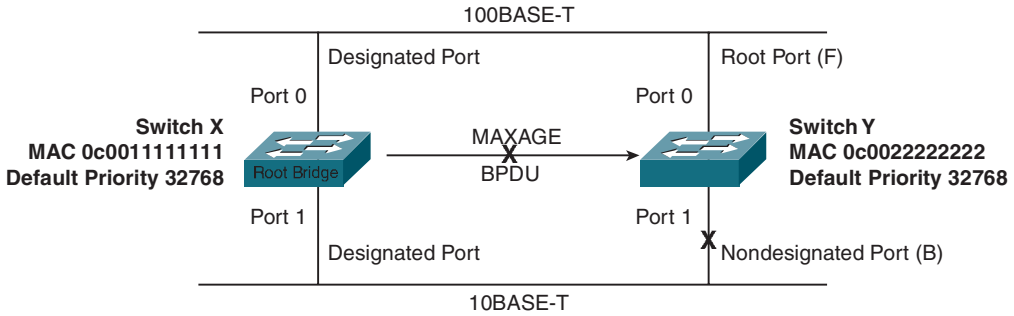
Spanning Tree Recalculation

When a link fails, the network topology must change. Connectivity is reestablished by placing key blocked ports in the forwarding state.

In Figure 2-8, if switch X fails, switch Y does not receive the BPDU. If the BPDU is not received before the MAXAGE timer expires, Spanning Tree begins recalculating the network. In the figure, switch Y is now the root bridge. If switch X comes back up, Spanning Tree recalculates the network, and switch X is once again the root bridge.

 Please see page 311 for more details.

FIGURE 2-8
Spanning Tree Recalculation



Time to Convergence

A network is said to have converged when all ports in a switched network are in either a blocking or forwarding state after a topology change.

PortFast

Spanning Tree PortFast is a Cisco feature that causes an access port on a switch to transition immediately from the blocking state to the forwarding state, thus bypassing the listening and learning states.

PortFast is used on access ports that are connected to a single workstation or server to allow these devices to connect to the network immedidately rather than waiting for STP to converge. PortFast is useful if a workstation is configured to acquire an IP address through Dynamic Host Configuration Protocol (DHCP). The workstation can fail to get an IP address because the switch port the workstation is connected to might not have transitioned to the forwarding state by the time DHCP times out.

 Please see page 311 for more details.

Configuring PortFast

PortFast is configured using the following interface command:

```
SwitchA(config-if)#spanning-tree portfast
```

PortFast can be configured globally on all nontrunking links using the following global command:

```
SwitchA(config-if)#spanning-tree portfast default
```

PortFast can be disabled using the **no spanning-tree portfast** interface command.

Per-VLAN STP+ (PVST+)

PVST+ creates a different spanning-tree instance for each VLAN on a switch. Each VLAN has its own root bridge, root port, designated port, and nondesignated port.

PVST+ is enabled by default on Cisco switches running 802.1D. In PVST+, the spanning-tree topology can be configured so that each VLAN has a different root bridge. Providing different STP root switches per VLAN creates a more redundant network.

PVST+ Extended Bridge ID

PVST+ requires a separate instance of Spanning Tree for each VLAN. STP requires that each switch have a unique bridge ID (BID). The original 802.1D standard BID consisted of the bridge priority and MAC address. Because PVST+ requires a separate instance of Spanning Tree for each VLAN, the BID field is required to carry VLAN ID (VID) information. This is accomplished by reusing a portion of the Priority field as the extended system ID to carry the VID. Therefore, in PVST+, the BID consists of the following:

- **Bridge priority:** A 4-bit field. The default is 32,768.
- **Extended system ID:** A 12-bit field carrying the VID.
- **MAC address:** A 6-byte field containing the MAC address of the switch.

 Please see page 311 for more details.

Rapid Spanning Tree Protocol (802.1w)

Rapid Spanning Tree Protocol (RSTP, 802.1w) significantly speeds the convergence process after a topology change occurs in a switched network. In 802.1D, a redundant port can take up to 50 seconds to transition from a blocking state to a forwarding state. RSTP works by designating an alternative port and a backup port. These ports are allowed to immediately enter the forwarding state rather than passively wait for the network to converge. Table 2-3 shows the new port states in RSTP and describes how they compare to 802.1D.

Table 2-3 Port State Comparison

Operational Status	STP Port State	RSTP Port State	Port Included in Active Topology?
Enabled	Blocking	Discarding	No
Enabled	Listening	Discarding	No
Enabled	Learning	Learning	Yes
Enabled	Forwarding	Forwarding	Yes
Disabled	Disabled	Disabled	No

Per-VLAN Rapid Spanning Tree Plus (PVRST+)

Like the original 802.1D standard, the 802.1w standard uses Common Spanning Tree (CST), which uses one spanning tree instance for the entire switched network. PVRST+ defines a spanning-tree protocol that has one instance of RSTP per VLAN.

Multiple Spanning Tree Protocol (MSTP)

MSTP (802.1Q-2003) allows switches running RSTP to group VLANs into one instance of Spanning Tree. Each VLAN group has a separate instance of Spanning Tree that is independent of other Spanning Tree instances.

 Please see page 311 for more details.

RSTP Port Roles

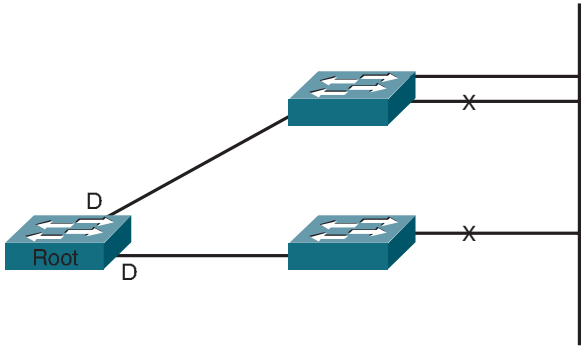
RSTP has new port roles. The root port and designated port roles are the same as they are in 802.1D. However, the blocking port in 802.1D is split into the backup and alternate port roles. Also, in RSTP, the Spanning Tree Algorithm determines the role of a port based on BPDUs. The port roles in RSTP are as follows:

- **Root port:** The port that received the best BPDU on a switch
- **Designated port:** The port that sends the best BPDU on the segment
- **Backup port:** A port that receives more useful BPDUs from the same switch it is on and is in a blocking state
- **Alternate port:** A port that receives more useful BPDUs from another switch and is in a blocking state

In RSTP, if the root port fails, the alternate port will become the new root port, and the backup port will become the new designated port.

Figure 2-9 shows the new port roles in RSTP.

FIGURE 2-9
RSTP Port Roles



R = Root Port
D = Designated Port
A = Alternate Port
B = Backup Port

New BPDU Format

RSTP uses a new BPDU format. Additionally, RSTP uses BPDUs as a keepalive mechanism. RSTP sends a BPDU every hello-time (2 seconds by default). If a port does not receive three consecutive BPDUs (6 seconds), the switch considers it has lost connectivity to its direct neighbor and begins to transition to the forwarding state.

Edge Port

An RSTP edge port is a port that is directly connected to end stations. Because directly connected end stations cannot create bridging loops in a switched network, the edge port directly transitions to the forwarding state.

Edge ports are configured using the **spanning-tree portfast** interface command.

Point-to-Point Link

A point-to-point link is a link in RSTP that directly connects two switches (an uplink) in full-duplex.

Link Type

In RSTP, a link can only rapidly transition to a forwarding state on edge port and on point-to-point links. The link type is automatically derived from the duplex mode of a port. Full-duplex is assumed to be point-to-point, and a half-duplex link is considered a shared point.

 Please see page 311 for more details.

Configuring RSTP

Cisco Catalyst switches support three types of STP:

- PVST+
- PVRST+
- MSTP

The default STP for Cisco Catalyst switches is PVST+, with a separate STP instance for each VLAN, one root bridge for all VLANs, and no load sharing. The Cisco version of PVST+ includes proprietary extensions such as BackboneFast, UplinkFast, and PortFast.

To configure PVRST+, perform the following steps:

Step 1. Enable PVRST+.

Step 2. Designate and configure a switch to be the root bridge.

Step 3. Designate and configure a switch to be the secondary (backup) root bridge.

Step 4. Verify the configuration.

Enabling PVRST+

The **spanning-tree mode rapid-pvst** global command, as follows, enables PVRST+ on a Cisco Catalyst switch:

```
SwitchA(config)#spanning-tree mode rapid-pvst
```

Configuring the Root and Backup Root Switch

In STP, the root switch is the switch with the lowest bridge ID (BID). The BID consists of the bridge priority and the switch MAC address. Because all Cisco switches have the same bridge priority (32768), the switch with the lowest MAC

 Please see page 311 for more details.

address will be the root bridge. In many cases, this is not desired. For example, an older (and potentially slower) switch will have a lower MAC address than a newer switch, and the older switch will be the root bridge.

To specify a switch to be the root switch, use the following global command:

```
spanning-tree vlan vlan-number root primary
```

For example, the following command configures the switch to be the root switch for only VLAN 1:

```
Cat2960(config)#spanning-tree vlan 1 root primary
```

The **spanning-tree root primary** command increases the switch priority (lowering the numerical value) so that the switch becomes the root bridge and forces Spanning Tree to perform a recalculation.

To configure the backup root switch, use the **spanning-tree vlan** *vlan-number* **root secondary** global command, as follows:

```
Cat2960(config)#spanning-tree vlan 1 root secondary
```

Verifying PVRST+

To verify whether RSTP is enabled on a switch, use the **show spanning-tree vlan** *vlan-number* command, as follows:

```
SwitchA#show spanning-tree vlan 1
VLAN0001
Spanning tree enabled protocol rstp
Root ID Priority 24606
Address 000d.65ac.5040
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 24606 (priority 24576 sys-id-ext 30)
Address 000d.65ac.5040
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

 Please see page 311 for more details.

```
Aging Time 300
Interface  Role  Sts  Cost  Prio.Nbr  Type
---------  ----  ---  ----  --------  ----
Gi0/1      Desg  FWD  4     128.1     P2p
Gi0/2      Desg  FWD  4     128.2     P2p
```

EtherChannel

EtherChannel is a Cisco feature that allows combining of up to eight physical links into one logical connection. This logical connection load-balances traffic between the physical links and is seen by Spanning Tree as one link. Thus with EtherChannel, instead of a redundant link not being used, all physical links are forwarding traffic.

EtherChannel provides an easy way to increase network bandwidth. Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet links can be configured for EtherChannel. If one of the physical links in the EtherChannel group fails, the other links still forward traffic.

Securing the Expanded Network

As also mentioned in ICND1, you must ensure that the network is secure from unauthorized activity. Ways to secure the network include

- Physical security
- Switch security (switch authentication)
- Port-based authentication

 Please see page 311 for more details.

Physical Security

Physical security prevents unauthorized physical access to switches. This means that switches are in a secure location (for example, a locked closet and rack), with only authorized personnel allowed to access the devices.

Switch Security

Switch security, also called switch-based authentication, prevents unauthorized users from accessing the switch remotely and viewing or changing the configuration of a switch. Switch-based authentication includes

- Setting privilege-level passwords
- Setting enable passwords
- Setting Telnet passwords
- Setting console passwords
- Setting username and password pairs with different levels of access
- Controlling switch access with a TACACS+ or RADIUS authentication server
- Configuring the switch to use Secure Shell (SSH) instead of Telnet
- Configuring HTTPS on the switch
- Disabling unneeded services, such as tcp-small-servers, udp-small-server, finger, and the service config
- Using warning banners
- Configuring switch logging

 Please see page 311 for more details.

Implementing and Verifying Port Security

Port security limits the number of MAC address allowed per port and can also limit which MAC addresses are allowed. Allowed MAC addresses can be manually configured or dynamically learned by the switch. The interface command to configure port security is as follows:

```
switchport port-security [mac-address mac-address | mac-address sticky [mac-address] | maximum value |
  violation {restrict | shutdown}
```

- **switchport port-security mac-address** *mac-address*: Manually configures the port to use a specific MAC address.
- **switchport port-security mac-address sticky:** Configures the switch to dynamically learn the MAC address of the device attached to the port.
- **switchport port-security maximum** *value*: Configures the maximum number of MAC addresses allowed on the port. The default value is 1.
- **switchport port-security violation {restrict | shutdown}:** Configures the action to be taken when the maximum number of MAC addresses is reached and when MAC addresses not associated with the port try to access the port. The **restrict** parameter tells the switch to restrict access to learned MAC addresses that are above the maximum defined addresses. The **shutdown** parameter tells the switch to shut down all access to the port if a violation occurs.

The following example demonstrates how to configure port security:

```
Cat2960(config)#int f0/1
Cat2960(config-if)#switchport mode access
Cat2960(config-if)#switchport port-security
Cat2960(config-if)#switchport port-security max 1
Cat2960(config-if)#switchport port-security mac-address sticky
Cat2960(config-if)#switchport port-sec violation restrict
```

 Please see page 311 for more details.

To verify port security, use the **show port-security** command, as follows:

```
Cat2960#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-------------------------------------------------------------------------
     Fa0/1             1            0                  0         Restrict
-------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8320
```

Securing Unused Ports

To secure unused ports, either disable the port or place the port in an unused VLAN.

A switch port is disabled by issuing the **shutdown** interface command.

Port-Based Authentication

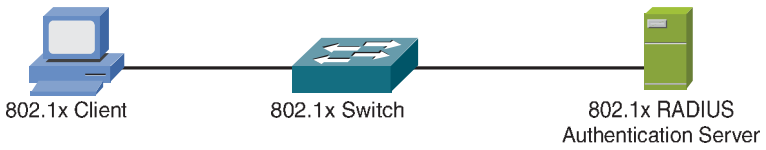
Port-based authentication prevents unauthorized devices from gaining access to the network. Based on 802.1x, port-based authentication requires a client to be authenticated to a server before it is allowed on the LAN.

802.1x is a standards-based method that defines client-server–based access control and has the following device roles, as displayed in Figure 2-10:

- **Client:** The device (workstation) that requests access to the LAN. Must be running 802.1x-compliant client software.
- **Authentication server:** Performs the authentication of the client, validating the identity of the client. Currently, a RADIUS server with Extensible Authentication Protocol (EAP) is the only supported authentication server.
- **Switch:** Controls the physical access to the network based on the authentication status of the client. Acts as a proxy between the client and authentication server.

 Please see page 311 for more details.

FIGURE 2-10
802.1x Device Roles



 Please see page 311 for more details.

Section 3
Troubleshooting Switched Networks

In a switched environment, typical issues include physical issues or hardware problems, Layer 2 issues, and configuration issues. Physical issues can include port failures, network interface card (NIC) failures, and port configuration issues.

Layer 2 issues can include links not properly trunking, CAM table inconsistencies (the CAM table is the table that stores all the MAC addresses and the ports associated with the MAC addresses), or spanning-tree issues.

Configuration issues can include these issues and inconsistencies in configuration such as VTP, VLANs, or Spanning Tree.

General Troubleshooting Suggestions

The following are three suggestions to general switch troubleshooting:

- Become familiar with normal switch operation.
- Have an accurate physical and logical map of the network.
- Do not assume a component is working without checking it first.

Troubleshooting Port Connectivity Problems

Common causes for port connectivity problems include hardware issues, configuration issues, and traffic issues.

 Please see page 311 for more details.

Hardware Issues

- Check the port status of the ports involved. Make sure that the ports are enabled and not shut down.
- Check the cable. Make sure that the cable is good and that the proper cable type is used.
- Check for loose connections.
- Make sure that the cable is plugged in to the correct port.

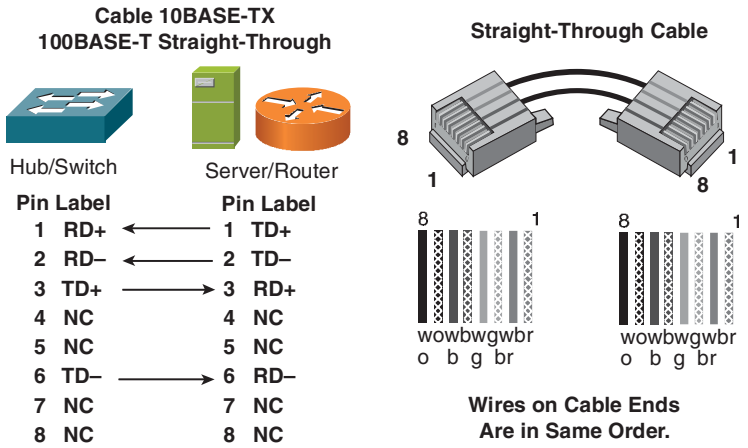
Cable Type

When using copper cabling, make sure you are using the correct cable type for the connection you are making.

Straight-through RJ-45 cables connect nonsimilar devices to each other: data terminal equipment (DTE) devices (end stations, routers, or servers) to a data communications equipment (DCE) device (switch or hub).

Crossover cables typically connect simialar devices, such as when connecting one switch to another. Figure 3-1 shows the pin-outs for a crossover cable.

FIGURE 3-1
Crossover Cable and Pin-Outs



 Please see page 311 for more details.

Verify Port Information

To view port information, such as port type, speed, duplex settings, or statistics and errors, use the **show interface** *interface-id* privileged EXEC command. The following command shows the information for interface g0/1. The highlighted areas are areas you should be familiar with.

```
SwitchA#show interface g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet Port, address is 000d.65ac.5040 (bia 000d.65ac.5040)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, link type is auto, media type is 1000BaseSX
  input flow-control is on, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:09, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 10000 bits/sec, 8 packets/sec
  5 minute output rate 10000 bits/sec, 7 packets/sec
     1476671 packets input, 363178961 bytes, 0 no buffer
     Received 20320 broadcasts (12683 multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     1680749 packets output, 880704302 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

 Please see page 311 for more details.

Port Errors

The following are reasons for common port errors:

- **"errDisable" message:** EtherChannel misconfiguration, duplex mismatch, BPDU port-guard has been enabled on the port, Unidirectional Link Detection (UDLD), native VLAN mismatch.
- **Excessive collisions:** Duplex mismatch, faulty port, oversaturated medium, or distance between the two switches exceeds the cable specifications.
- **Excessive runts:** Runts are frames smaller than 64 bytes with a bad frame check sequence (FCS). Bad cabling or inconsistent duplex settings cause runts.
- **Excessive giants:** Giants are frames greater than the Ethernet maximum transmission unit (MTU) of 1518 bytes. The cause is usually a faulty NIC.

Port Connectivity Problem Summary

- Become familiar with normal switch operation.
- Have an accurate physical and logical map of the network.
- Do not assume that a component is working without checking it first.
- Check port status of ports involved.

Troubleshooting VLANs

The first step in troubleshooting VLANs is to check the VLAN configuration. If hosts cannot communicate with each other, make sure that they are on the same VLAN. If hosts cannot communicate between VLANs, make sure that your routing is configured correctly.

 Please see page 311 for more details.

VLAN problems are classified into two categories: intraVLAN and interVLAN connectivity. Problems within each category are as follows:

- Slow collision domain connectivity
- Slow broadcast domain connectivity (slow VLAN)
- Slow broadcast domain interVLAN connectivity

Troubleshooting Collision Domain Issues

Causes for collision domain issues include the following:

- The segment is overloaded or oversubscribed.
- Bad cabling on the segment.
- NICs on the segment do not have compatible settings.
- Faulty NICs.

Troubleshooting Slow IntraVLANs

Cause for slowness between hosts on the same VLAN can be caused by

- Traffic loops
- Overloaded or oversubscribed VLAN
- Switch congestion
- Misconfiguration
- Hardware problems

 Please see page 311 for more details.

Troubleshooting InterVLAN Connectivity

Most interVLAN connectivity issues are caused by misconfiguration. InterVLAN routing was probably not properly configured and needs to be configured to route between the VLANs.

Troubleshooting Trunking

Most trunking problems occur because of misconfiguration on the trunking links. However, first verify that the interfaces are physically working. Here are some common trunking issues:

- Both sides of the links are not set to the correct trunking mode. For example, both sides of the link are set to auto.
- The same trunking encapsulation is not used on both sides.
- A native VLAN mismatch exists.

Troubleshooting VTP

VTP problems occur when a misconfiguration exists between the switches and VTP information is not propagating. A common indication that a switch is experiencing a VTP problem is when the switch is not receiving or updating its VLAN information.

The following are common things to check when troubleshooting VTP problems:

- Make sure that trunking is configured between the switches. VTP information is sent over trunk links.
- Make sure that the domain name matches on both switches. The domain name is case sensitive.
- If using a VTP password, make sure that the password is the same on both switches. The password is case sensitive.
- Verify that the switch is in the proper mode: server, client, or transparent.

 Please see page 311 for more details.

Adding a New Switch to a VTP Domain

By default, all Cisco switches are VTP servers. If a new switch is added to the network, its revision number might be higher than the revision number of the actual VTP server. If this is the cause, the new switch will overwrite all VLAN information in the VTP domain, resulting in lost VLANs. To prevent this from occurring, reset the revision number on the new switch to 0 by changing its VTP domain name on the switch, change the VTP domain name back to the proper VTP domain name, and add the switch to the network.

Troubleshooting Spanning Tree

Spanning Tree's primary function is to prevent loops from occurring in a redundant switched network. STP works at Layer 2 of the OSI model. A failure in Spanning Tree usually leads to a bridging loop. Use the following commands to view Spanning Tree information and see whether a loop exists in the network:

- **show spanning-tree:** Displays the root ID, bridge ID, and priority time for all VLANs in STP.
- **show spanning-tree vlan** *vlan-id***:** Displays STP information for a specific VLAN.
- **debug spanning-tree:** Verifies receipt of BPDUs and troubleshoots other Spanning Tree errors.

To identify a bridging loop, check the port utilization on your devices and look for abnormal values. If a bridging loop is found, disable the redundant ports to break the loop.

 Please see page 311 for more details.

Part II: Routing

Section 4
Routing Operations and VLSM

Routing Overview

Routing is the process of getting packets and messages from one location to another.

A router needs the following key information, as displayed in Figure 4-1:

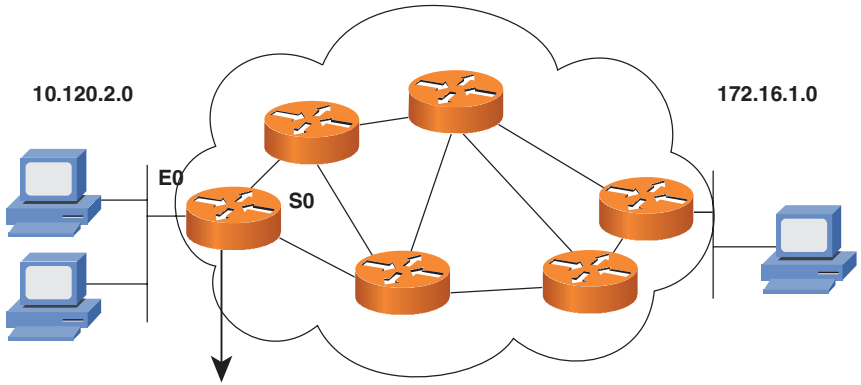
- **Destination address:** The destination (typically an IP address) of the information being sent. This includes the subnet address.
- **Possible routes:** Likely routes to get from source to destination.
- **Best route:** The best path to the intended destination.
- **Status of routes:** Known paths to destinations.

A router is constantly learning about routes in the network and storing this information in its routing table. The router uses its table to make forwarding decisions. The router learns about routes in one of two ways:

- Manually (routing information entered by the network administrator)
- Dynamically (a routing process running in the network)

 Please see page 311 for more details.

FIGURE 4-1
Information Needed by Router for Routing



Network Protocol	Destination Network	Exit Interface
Connected	10.120.2.0	E0
Learned	172.16.1.0	S0

Routed Protocol: IP

Dynamic Routing Overview

Routing protocols determine paths between routers and maintain routing tables. Dynamic routing uses routing protocols to disseminate knowledge throughout the network. A routing protocol defines communication rules and interprets network layer address information. Routing protocols describe the following:

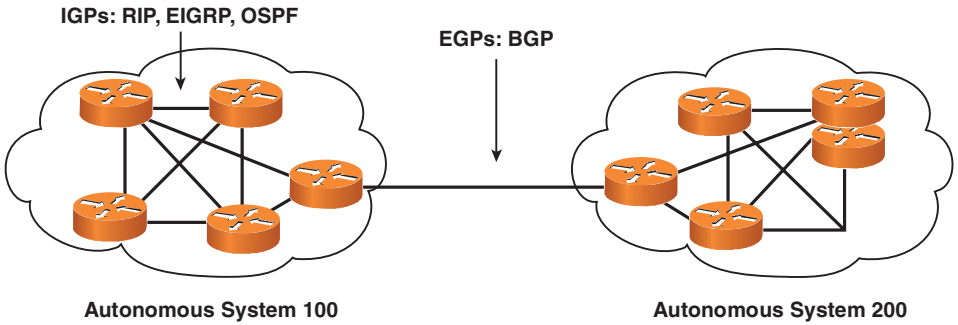
- Routing update methods
- Information contained in updates
- When updates are sent
- Paths to other routers

 Please see page 311 for more details.

Autonomous Systems

An autonomous system refers to a group of networks under a common administrative domain. Interior gateway protocols (IGP), such as Routing Information Protocol (RIP) and Enhanced IGRP (EIGRP), exchange routing information within an autonomous system. Exterior gateway protocols (EGP) connect between autonomous systems. A Border Gateway Protocol (BGP) is an example of an EGP. Figure 4-2 shows autonomous systems and where IGPs and EGPs are used.

FIGURE 4-2
Autonomous Systems



Administrative Distance

Several routing protocols can be used at the same time in the same network. When more than a single source of routing information exists, the router uses an administrative distance (AD) value to rate the trustworthiness of each routing information source. The administrative distance metric is an integer from 0 to 255. In general, a route with a lower number is considered more trustworthy and is more likely to be used. Figure 4-3 shows that Router A has two paths to network E learned from RIP and EIGRP. Because Interior Gateway Routing Protocol (IGRP) has a lower AD than RIP, Router A will pick the path advertised by IGRP.

FIGURE 4-3
Administrative Distance Determines Path

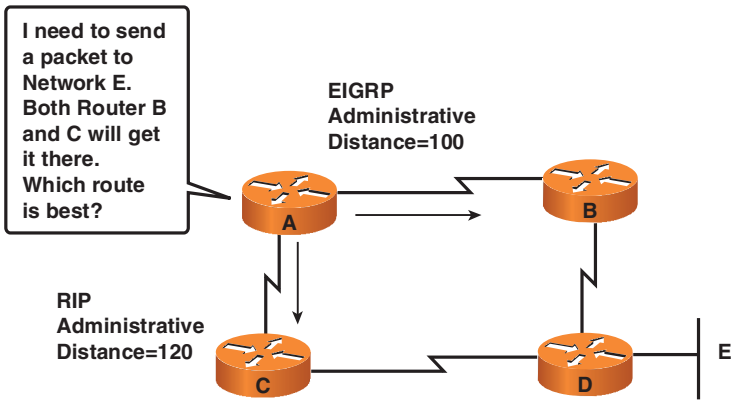


Table 4-1 shows the default administrative distance values.

Table 4-1 Default Administrative Distance Values

Route Source	Default Distance
Connected interface	0
Static route	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
External EIGRP	170
Unknown	255

 Please see page 311 for more details.

Routing Protocol Classes

The following three basic routing protocol classes exist:

- **Distance vector:** Uses the direction (vector) and distance to other routers as metrics. RIPv2 is a distance vector protocol.
- **Link-state:** Also called shortest path first, this protocol re-creates the topology of the entire network. Open Shortest Path First (OSPF) and Intermediate System–to–Intermediate System (IS-IS) are link-state protocols.
- **Balance hybrid:** Combines the link-state and distance vector algorithms. EIGRP is a balanced hybrid protocol.

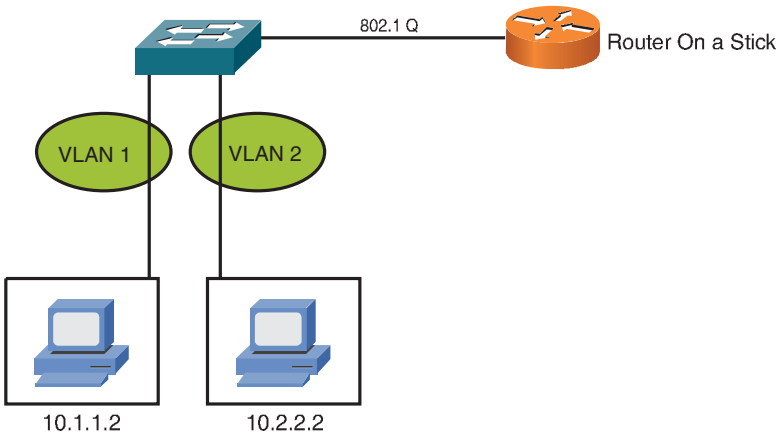
InterVLAN Routing

VLANs create a logical segmentation of Layer 3, performed at Layer 2. End stations in different segments (broadcast domains) cannot communicate with each other without the use of a Layer 3 device such as a router. InterVLAN routing is handled by either a router or a Layer 3 switch. For interVLAN routing with a router, each VLAN must have a separate physical connection on the router, or trunking must be enabled on a single physical connection for interVLAN routing to work.

Figure 4-4 shows a router attached to a switch. The end stations in the two VLANs communicate with each other by sending packets to the router, which forwards them to the other VLAN. This setup is called “router on a stick.”

 Please see page 311 for more details.

FIGURE 4-4
Router on a Stick

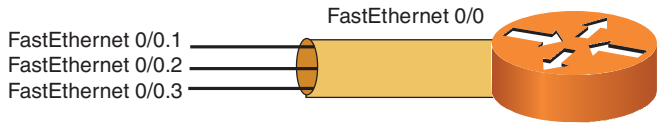


Dividing Physical Interfaces into Subinterfaces

InterVLAN routing using router on a stick requires the use of subinterfaces. A subinterface is a logical, addressable interface on the router's physical port. A single port can have many subinterfaces. Router on a stick requires a Fast Ethernet (or Gigabit Ethernet) port, with one subinterface configured per VLAN.

In Figure 4-5, the FastEthernet 0/0 interface is divided into multiple subinterfaces (FastEthernet 0.1, FastEthernet 0.2, and so on).

FIGURE 4-5
Using Subinterfaces



 Please see page 311 for more details.

Configuring Subinterfaces for InterVLAN Routing

To configure interVLAN routing on a router, first create a subinterface and then configure the subinterface with the **encapsulation dot1q** *vlan-id* command, where the *vlan-id* is the VLAN number of the associated VLAN. The following example enables interVLAN routing for VLANs 1, 10, and 20:

```
RouterB(config)#int f0/0
RouterB(config-if)#ip address 192.168.1.1 255.255.255.0
RouterB(config-if)#int f0/0.10
RouterB(config-if)#ip address 192.168.10.1 255.255.255.0
RouterB(config-if)#encapsulation dot1q 10
RouterB(config-if)#int f0/0.20
RouterB(config-if)#ip address 192.168.20.1 255.255.255.0
RouterB(config-if)#encapsulation dot1q 20
```

Remember that in 802.1Q, the native VLAN is not encapsulated. In the previous example, the physical interface f0/0 is in the native VLAN because the **encapsulation dot1q** command is not configured. VLAN 1 is the default native VLAN if not otherwise specified with the **dot1q** *vlan-id* **native** command. The subinterfaces f0/0.10 and f0/0.20 were configured for 802.1Q tagging and are therefore in VLANs 10 and 20, respectively.

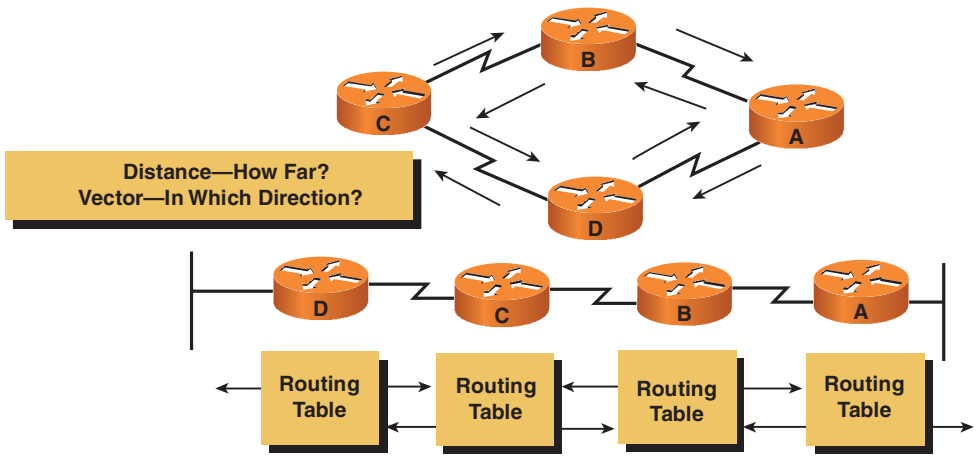
By using subinterfaces for interVLAN communication, all traffic must go through the router's interface. For large networks, this can cause a bottleneck. To prevent a bottleneck, use a Layer 3 switch to perform interVLAN routing.

Distance Vector Routing

Routers using distance vector–based routing share routing table information with each other. This method of updating is called "routing by rumor." Each router receives updates from its direct neighbor. In Figure 4-6, Router B shares information with Routers A and C. Router C shares routing information with Routers B and D. In this case, the routing information is distance vector metrics (such as the number of hops). Each router increments the metrics as they are passed on (incrementing hop count, for example).

 Please see page 311 for more details.

FIGURE 4-6
Distance Vector Route Information



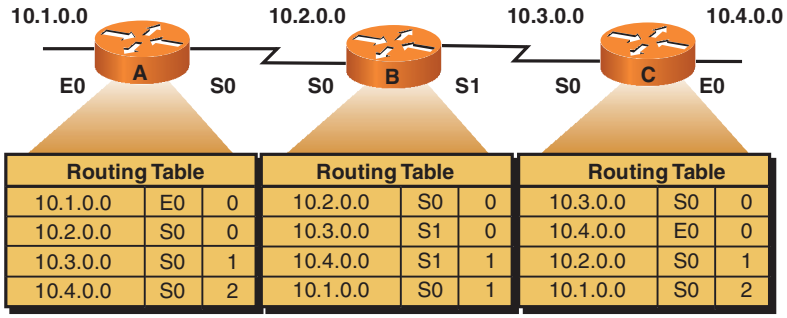
Distance accumulation keeps track of the routing distance between any two points in the network, but the routers do not know the exact topology of an internetwork.

How Information Is Discovered with Distance Vectors

Network discovery is the process of learning about nondirectly connected destinations. As the network discovery proceeds, routers accumulate metrics and learn the best paths to various destinations. In Figure 4-7, each directly connected network has a distance of 0. Router A learns about other networks based on information it receives from Router B. Router A increments the distance metric for any route learned by Router B. For example, Router B knows about the networks to Router C, which is directly connected. Router B increments its distance metrics by 1 and sends them to Router A.

 Please see page 311 for more details.

FIGURE 4-7
Network Discovery for Distance Vector



Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

Examining Distance Vector Routing Metrics

Distance vector routing protocols use routing algorithms to determine the best route. These algorithms generate a metric value for each path through the network. The lower the metric, the better the path. Metrics can be calculated based on one or more characteristics of a path. Commonly used metrics are as follows:

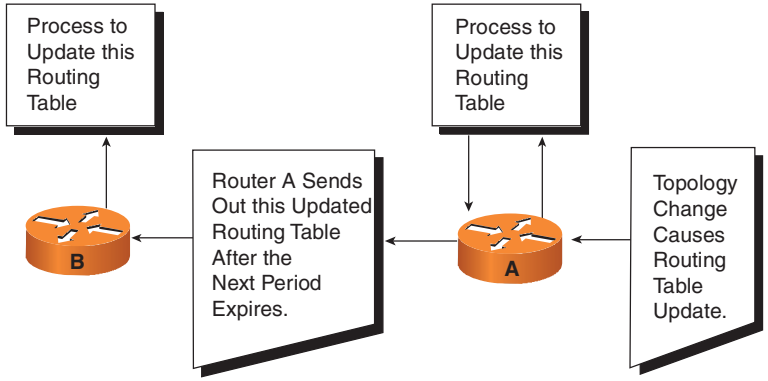
- **Cost:** An arbitrary value based on a network administrator–determined value. Usually based on bandwidth.
- **Bandwidth:** An administrative value that usually reflects the link speed of an interface. This is not based on the actual link speed of an interface. For example, the default value of serial links is 1544 kbps, even if the link speed is greater than 1544 kbps.
- **Delay:** A fixed attribute based on interface type.
- **Load:** The amount of activity on a network resource, such as a router or link.
- **Reliability:** The bit-error rate of each network link.
- **MTU (maximum transmission unit):** The maximum frame size allowed on the link.

 Please see page 311 for more details.

Updating Routing Tables

A router compares the information contained in the update to its current table. If the update contains information about a better (lower-metric) route to a destination, the router updates its own routing table. During updates, the router sends its entire routing table to each of its adjacent neighbors. The table includes the total path cost (defined by its metric) and the logical address of the first router on the path to each destination network. In Figure 4-8, Router B is one unit of cost from Router A. Therefore, it adds 1 to all costs reported by Router A.

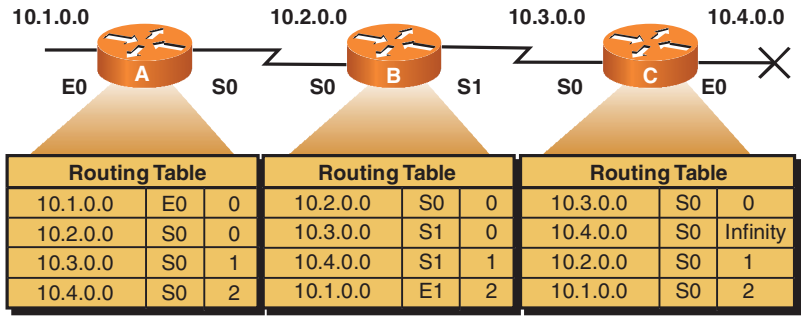
FIGURE 4-8
Routing Table Updates



How Routing Loops Occur in Distance Vector Protocols

During updates, routing loops can occur if the network has inconsistent routing entries. Slow convergence on a new configuration is one cause of this phenomenon. The network is converged when all routers have consistent routing tables. Figure 4-9 illustrates how a routing loop occurs. Before a network failure, all routers have correct tables. Figure 4-9 uses hop count as a cost metric, so the cost of each link is 1. Router C is directly connected to network 10.4.0.0, with a distance of 0. Router A's path to network 10.4.0.0 is through Router B, with a hop count of 2.

FIGURE 4-9
Hop Count as a Cost Metric



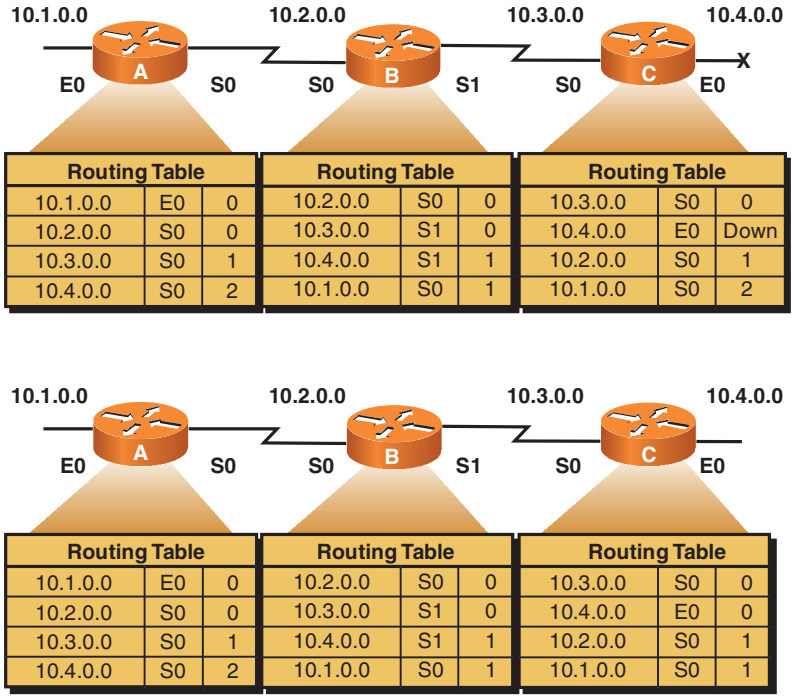
Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	E1	2

Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	Infinity
10.2.0.0	S0	1
10.1.0.0	S0	2

In Figure 4-10, network 10.4.0.0 fails, and Router C detects the failure and stops routing packets to that network. At this point, Routers A and B still do not know of the failure. Router A's table still shows a valid path to 10.4.0.0 through Router B. If Router B sends out its normal update to Routers A and C, Router C sees a valid path to 10.4.0.0 through Router B and updates its routing table to reflect a path to network 10.4.0.0 with a hop count of 2 (remember, B has incremented the hop count for A). Now Router C sends an update back to Router B, which then updates Router A. Router A detects the modified distance vector to network 10.4.0.0 as 4. With each update, the incorrect information continues to bounce between the routers. Without some mechanism to prevent this, the updates continue. This condition, called counting to infinity, continuously loops packets around the network.

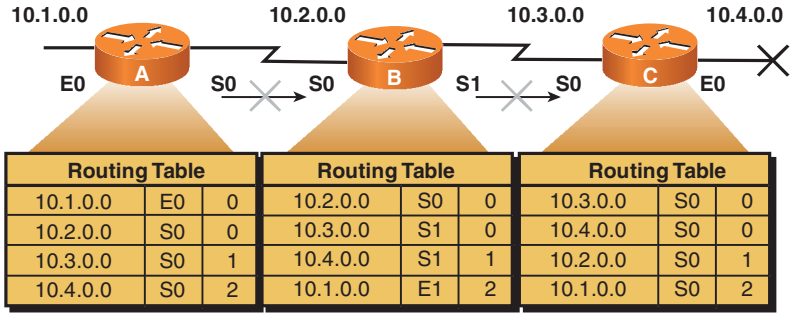
FIGURE 4-10
Counting to Infinity



Split Horizon

Split horizon is one way to eliminate routing loops and speed convergence. The idea behind split horizon is that it is never useful to send information about a route back in the direction from which the update came. If the router has no valid alternative path to the network, it is considered inaccessible. Split horizon also eliminates unnecessary routing updates, thus speeding convergence. Figure 4-11 shows the same network. Routers A and B do not advertise the failed route 10.1.4.0 out of the interfaces they originally learned the route. In this case, this is interface Serial 0 for Router A and interface Serial 1 for Router B.

FIGURE 4-11
Split Horizon Eliminates Routing Loops



Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	E1	2

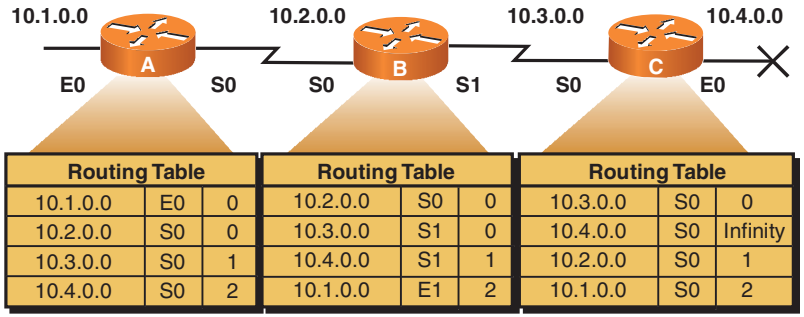
Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

Route Poisoning

Route poisoning (part of split horizon) also eliminates routing loops caused by inconsistent updates. Route poisoning sets a route to "unreachable." By poisoning a route, the router is not susceptible to incorrect updates about the poisoned network from other routers that claim to have a valid alternate path.

Figure 4-12 shows an example of route poisoning. When network 10.4.0.0 goes down, Router C "poisons" its link to network 10.4.0.0 with an infinite metric (marked as unreachable, seen as a hop count of 16 in RIP).

FIGURE 4-12
Route Poisoning Eliminates Routing Loops



Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	E1	2

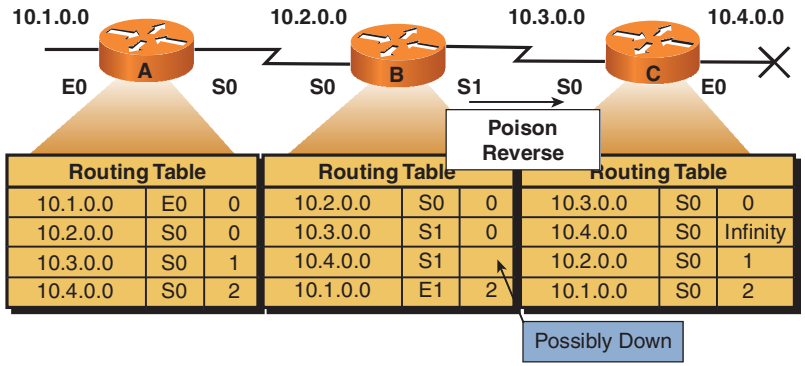
Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	Infinity
10.2.0.0	S0	1
10.1.0.0	S0	2

When Router B sees the metric of 10.4.0.0 jump to infinity, Router B sends a poison reverse back to Router C. The poison reverse states that network 10.4.0.0 is inaccessible. Poison reverse is a specific circumstance that overrides split horizon. Router C is no longer susceptible to incorrect updates about network 10.4.0.0.

Poison Reverse

In Figure 4-13, when Router B sees the metric to 10.4.0.0 jump to infinity, it sends a return message (overriding split horizon) called a poison reverse back to Router C, stating that network 10.4.0.0 is inaccessible. This message ensures that all routers on that segment have received information about the poisoned route.

FIGURE 4-13
Using Poison Reverse to Broadcast Information About a Failed Route



Triggered Updates

A triggered update is sent immediately in response to a change in the network. The router detecting the change immediately sends an update message to adjacent routers, which then generate their own triggered updates. This continues until the network converges. The following two problems exist with triggered updates:

- The update message can be dropped or corrupted.
- The updates do not happen instantly. A router can issue a regular update before receiving the triggered update. If this happens, the bad route can be reinserted into a router that received the triggered update.

 Please see page 311 for more details.

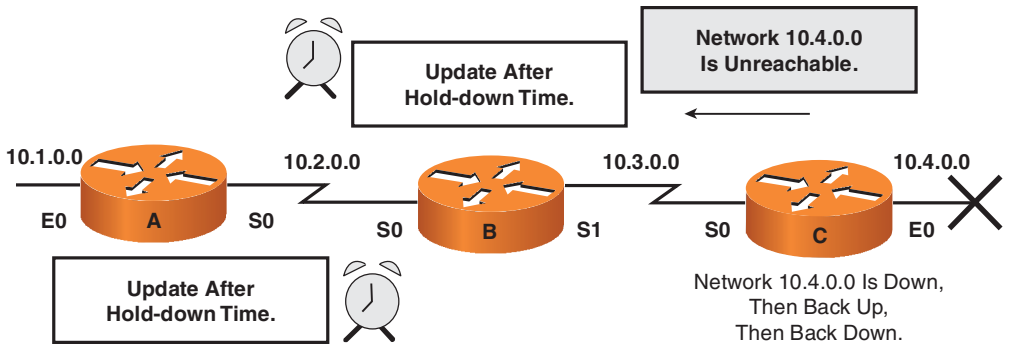
Solution: Hold-down timers dictate that when a route is invalid, no new route with the same or a worse metric will be accepted for the same destination for a period of time. This allows the triggered update to propagate throughout the network.

Hold-Down Timers

Hold-down timers prevent regular update messages from inappropriately reinstating a route that might have gone bad. They force routers to hold any changes for a period of time.

Figure 4-14 shows the hold-down implementation process, which is described in the following list:

FIGURE 4-14
Hold-Down Timer Process



1. When a router receives an update that a network is down, it marks the route as inaccessible and starts a hold-down timer.
2. If an update is received from a neighboring router with a better metric, the router removes the timer and uses the new metric.

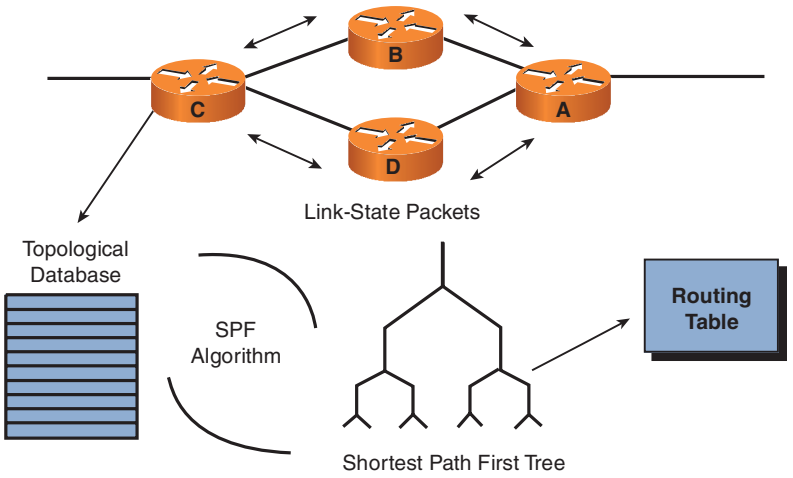
 Please see page 311 for more details.

3. If an update is received (before the hold-down timer expires) with a poorer metric, the update is ignored.
4. During the hold-down period, routes appear in the routing table as "possibly down."

Link-State Routing

The link-state-based routing algorithm (also known as shortest path first [SPF]) maintains a database of topology information. Unlike the distance vector algorithm, link-state routing maintains full knowledge of distant routers and how they interconnect. Network information is shared in the form of link-state advertisements (LSA). See Figure 4-15.

FIGURE 4-15
Link-State Routing



With link-state routing protocols, each router has a full map of the network topology. As such, a router can independently make a decision based on its map of the network.

Each link-state router must keep a record of the following:

- Immediate neighbor routers
- All other routers in the network
- The best paths to each destination

Link-state routing provides better scaling than distance vector routing for the following reasons:

- Link-state sends only topology changes (called triggered updates). Distance vector sends complete routing tables.
- Link-state updates are sent less often than distance vector updates.
- Link-state uses a hierarchy by dividing large routing domains into smaller routing domains called areas. Areas limit the scope of route changes.
- Link-state supports classless addressing and summarization.
- Link-state routing converges fast and is robust against routing loops, but it requires a great deal of memory and strict network designs.

Advanced Distance Vector Routing

Advanced distance vector (also called balanced hybrid) routing combines aspects of both distance vector and link-state protocols. Advanced distance vector routing uses distance vectors with more accurate metrics, but unlike distance vector routing protocols, it updates only when a topology change occurs. Balanced hybrid routing provides faster convergence while limiting the use of resources such as bandwidth, memory, and processor overhead. Cisco Enhanced IGRP is an example of an advanced distance vector protocol.

 Please see page 311 for more details.

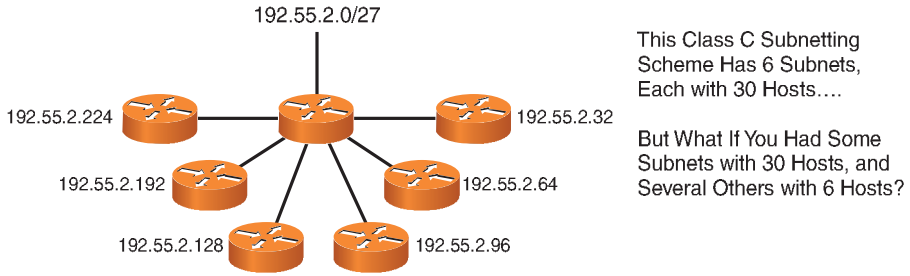
Variable-Length Subnet Mask (VLSM)

VLSMs were developed to allow multiple levels of subnetting in an IP network. This allows network administrators to overcome the limitations of fixed-sized subnets within a network and, in effect, subnet a subnet. VLSMs are not available in RIPv1.

The primary benefit of VLSMs is more efficient use of IP addresses.

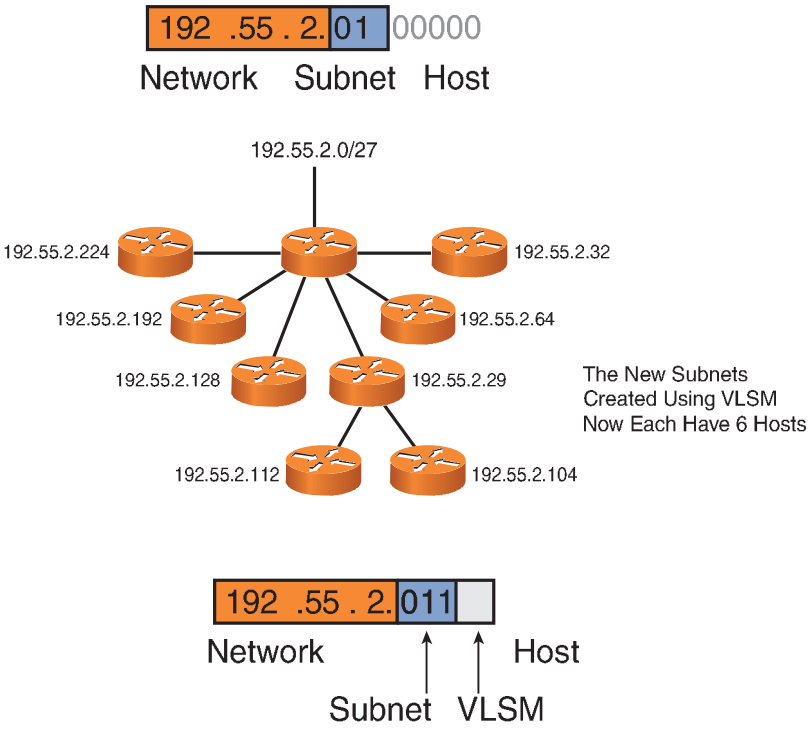
Figure 4-16 shows that without VLSMs, you are confined to a fixed number of subnets, each with a fixed number of hosts.

FIGURE 4-16
Subnets/Hosts Fixed Without VLSMs



With VLSMs, you can have multiple subnets, with a varying number of hosts. Adding subnets works the same way as normal subnets. Figure 4-17 shows the same network, and VLSM uses bits from the subnet portion of the address.

FIGURE 4-17
VLSMs Increase the Number of Subnet/Host Possibilities



Summarizing Routes

In large networks, it is impractical for a router to maintain tables with hundreds of thousands of routes. Route summarization (also called route aggregation or supernetting) reduces the number of routes that a router must maintain by representing a series of network numbers in a single summary address.

Router summarization is most effective within a subnetted environment when the network addresses are in contiguous blocks in powers of 2.

 Please see page 311 for more details.

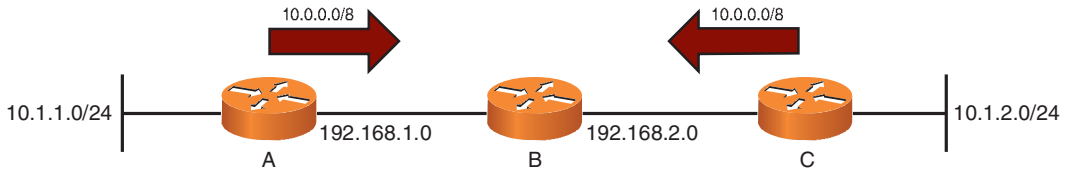
Route summarization can also isolate topology changes, because the routing changes are propagated only to the router that accesses the rest of the network. All other routers use a summary address.

Classless routing schemes, such as RIPv2, IS-IS, EIGRP, and OSPF, support route summarization using subnets and VLSMs. RIP and EIGRP automatically perform route summarization to the classful network boundary when routing updates cross between two major networks. OSPF must be configured to manually perform summarization.

Summarizing Routes in Discontinuous Networks

RIP and EIGRP automatically perform route summarization to the classful network boundary when routing updates cross between two major networks. This works fine if the network is continuous; however, this automatic summarization causes problems if the network is discontinuous. Figure 4-18 shows Routers A and C are connected to networks 10.1.1.0/24 and 10.1.2.0/24. Because the network is discontinuous, Routers A and C automatically summarize that they are connected to network 10.0.0.0/8. As a result, Router B thinks it has two routes to network 10.0.0.0/8.

FIGURE 4-18
Autosummarization in a Discontinuous Network



 Please see page 311 for more details.

Section 5
Implementing OSPF in a Single Area

OSPF is an interior gateway protocol based on link state rather than distance vectors. OSPF uses Dijkstra's shortest path first (SPF) algorithm to determine the best path to each network. OSPF was developed in the 1980s as an answer to RIP's inability to scale well in large IP networks.

OSPF is an open-standard, classless protocol that converges quickly and uses costs as a metric. Cisco IOS automatically calculates cost based on the interface bandwidth.

When a router is configured for OSPF, the first thing the router does is create a topology table of the network. OSPF does this by sending Hellos out each OSPF interface, while listening for Hellos from other routers. If the routers share a common data link and agree on certain parameters set in their Hello packets, they become neighbors. If these parameters are different, they do not become neighbors and communication stops. OSPF routers can form adjacencies with certain neighbor routers. The routers that OSPF routers build adjacencies with are determined by the data link media type.

After adjacencies have been formed, each router sends link-state advertisements (LSA) to all adjacent routers. These LSAs describe the state of each of the router's links. Because of the varying types of link-state information, OSPF defines multiple LSA types.

Finally, routers receiving an LSA from neighbors record the LSA in a link-state database and flood a copy of the LSA to all other neighbors. When all databases are complete, each router uses the SPF algorithm to calculate a loop-free, best-path topology and builds its routing table based on this topology.

 Please see page 311 for more details.

OSPF Terminology

When learning about OSPF, you might encounter different terminology for the OSPF tables. Following is list of common terminology used in OSPF:

- OSPF neighbor table = Adjacency database
- OSPF topology table = OSPF topology database (link-state database [LSDB])
- Routing table = Forwarding database

Router ID

For OSPF to initialize, it must be able to define a router ID for the entire OSPF process. A router can receive its router ID from several sources. First, it can be assigned manually through the **router-id** command. Second, it is the numerically highest IP address set on a loopback interface. The loopback interface is a logical interface that never goes down. If no loopback address is defined, an OSPF enabled router will select the numerically highest IP address on any of its OSPF-configured interfaces as its router ID.

The router ID is chosen when OSPF is initialized. Initialization occurs when a router loads its OSPF configuration, whether at startup or when OSPF is first configured or reloaded. If other interfaces later come online that have a higher IP address, the OSPF router ID does not change until the OSPF process is restarted.

Hello Packet

The Hello protocol ensures that communication between OSPF routers is bidirectional. It is the means by which neighbors are discovered and acts as keepalives between neighbors. It also establishes and maintains neighbor relationships and elects the designated router (DR) and the backup designated router (BDR) to represent the segment on broadcast and nonbroadcast multiaccess (NBMA) networks.

 Please see page 311 for more details.

Each Hello packets contains the following:

- Router ID of the originating router
- Area ID of the originating router interface
- Address mask of the originating router interface
- Authentication type and information of the originating router interface
- HelloInterval
- RouterDeadInterval
- Router priority
- DR and BDR
- 5 flag bits for optional capabilities
- Router IDs of the originating router's neighbors

Hello packets are periodically sent out each interface using IP multicast address 224.0.0.5 (AllSPFRouters). The HelloInterval each router uses to send out the Hello protocol is based on the media type. The default HelloInterval of broadcast, point-to-point, and point-to-multipoint networks is 10 seconds. On NBMA networks the default HelloInterval is 30 seconds.

For OSPF-enabled routers to become neighbors, certain parameters in the Hello packet must match. These parameters are as follows:

- Subnet mask used on the subnet
- Subnet number

 Please see page 311 for more details.

- HelloInterval
- DeadInterval
- OSPF area ID

LSAs

After OSPF-enabled routers form full adjacencies, the next step is for routers to exchange link-state information. This is done through LSAs. LSAs report the state of routers' links. LSAs are also packets that OSPF uses to advertise changes in the condition of links to other OSPF routers in the form of a link-state update.

LSAs have the following characteristics:

- LSAs are reliable.
- LSAs are flooded throughout the OSPF area.
- LSAs have a sequence number and a timer. The sequence number and timer ensure that each router has the most current LSA.
- LSAs are refreshed every 30 minutes.

Eleven different and distinct link-state packet formats are used in OSPF, and each is used for a different purpose. The ICND exam will only test you on two LSA types, Type 1 and Type 2.

Type 1 LSAs are router LSAs and are generated by each router for each area to which it belongs. These LSAs describe the states of the router's links to the area and are flooded within a single area.

Type 2 LSAs are network LSAs and are generated by the DR and BDR. They describe the set of routers attached to a particular network. They are flooded within a single area.

 Please see page 311 for more details.

OSPF Network Types

OSPF defines the following five network types:

- Broadcast networks
- Nonbroadcast multiaccess (NBMA) networks
- Point-to-point networks
- Point-to-multipoint networks
- Virtual links

Examples of broadcast networks are Ethernet and Token Ring. OSPF routers on broadcast networks elect a designated router (DR) and backup designated router (BDR). All routers on the broadcast segment form adjacencies with the DR and BDR. On broadcast networks, all LSA packets are multicast to the DR and BDR address of 224.0.0.6; Hellos are still multicast to the all OSPF routers address of 224.0.0.5. The router with the highest OSPF interface priority is elected the DR, and the router with the second-highest OSPF interface priority is the BDR. The OSPF interface priority defaults to 1 but should be administratively configured to manually define the DR and BDR. If the default priority value of 1 is left on all router interfaces, the DR/BDR election relies on the router ID (RID): The highest RID on the segment becomes the DR, and the second-highest becomes the BDR.

NBMA networks include Frame Relay, X.25, and ATM; they are capable of connecting more than two routers but have no broadcast capability. NBMA networks elect a DR and BDR, and all OSPF packets are unicast.

Point-to-point networks, such as a T1, connect a single pair of routers that always become adjacent. No DR/BDR elections take place.

Point-to-multipoint networks are a special configuration of NBMA networks in which networks are treated as a collection of point-to-point links. Routers on these networks do not elect a DR or BDR, and because all links are seen as point-to-point, all OSPF packets are multicast.

 Please see page 311 for more details.

Virtual links are a special configuration that is interpreted by the router as unnumbered point-to-point networks. Virtual links are created by the administrator.

Configuring OSPF

The **router ospf** *process-id* command enables the OSPF process, and the **network** *address wildcard-mask* **area** *area-id* command assigns networks to a specific OSPF area. For example, the following configuration enables OSPF process 10 and activates OSPF on all interfaces that have interface addresses that match the address and mask combination for area 0. For example, if a router has two interfaces configured with IP addresses 192.168.10.1/27 and 192.168.10.33/27 each, OSPF will be enabled on both interfaces. Notice that you must specify the wildcard mask instead of the subnet mask:

```
RouterA(config)#router ospf 10
RouterA(config-router)#network 192.168.10.0 0.0.0.255 area 0
```

The process ID is locally significant to the router and is used to differentiate between different OSPF processes running on the router; this value (unlike the autonomous system value in EIGRP) does not need to match between routers.

Verifying OSPF

The **show ip protocols** command verifies that OSPF is configured.

The **show ip route** command displays all known routes.

The **show ip ospf interface** command lists the area in which the router interface resides and the neighbors of the interface. Additionally, it lists the interface state, process ID, router ID, network type, cost, priority, DR and BDR, timer intervals, and authentication if it is configured. Here is an example of the **show ip ospf interface** command:

```
RouterB# show ip ospf interface ethernet 0
Ethernet0 is up, line protocol is up
  Internet Address 10.1.1.1/24, Area 0
  Process ID 1, Router ID 172.16.0.2, Network Type BROADCAST, Cost: 10
```

 Please see page 311 for more details.

```
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 172.16.0.1, Interface address 10.1.1.2
Backup Designated router (ID) 172.16.0.2, Interface address 10.1.1.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:06
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 2, maximum is 2
Last flood scan time is 0 msec, maximum is 4 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 172.16.0.1  (Designated Router)
Suppress hello for 0 neighbor(s)
```

To analyze the OSPF events, use the **debug ip ospf events** command.

Load Balancing with OSPF

Load balancing is a function of Cisco IOS router software and is supported for static routes, RIP, RIPv2, IGRP, EIGRP, OSPF, IS-IS, and BGP.

When a router has multiple paths with the same AD and cost to a destination, packets are load-balanced across the paths. OSPF only supports equal-cost load balancing. EIGRP also supports unequal-cost load balancing.

Per-Destination and Per-Packet Load Balancing

In per-destination load balancing, the router distributes packets based on the destination address.

In per-packet load balancing, the router sends one packet for one destination over the first path, and the second packet for the same destination over the second path.

 Please see page 311 for more details.

Load Balancing with Different Costs

OSPF does not support unequal-cost load balancing. If OSPF has two unequal links to a destination, only the lowest-cost path is used. The other path remains idle. To use the other link for load balancing, you need to manually change the cost of the interface.

Because OSPF's metric is based on cost, to load-balance between two links with different costs, you have to manually configure each interface with the same cost. The **ip ospf cost** *interface-cost* interface command sets the OSPF cost of an interface. In the example that follows, you would enter the following commands to make both interfaces have the same cost:

```
RouterA(config)#interface serial 0/0
RouterA(config-if)#ip ospf cost 10
RouterA(config-if)#interface serial 0/1
RouterA(config-if)#ip ospf cost 10
```

Authentication with OSPF

OSPF authentication prevents unauthorized routers from forming adjacencies with OSPF-enabled routers.

OSPF supports three types of authentication:

- Null authentication
- Plain-text authentication
- MD5 authentication

 Please see page 311 for more details.

Configuring Plain-Text Authentication

The following steps configure OSPF plain-text authentication:

Step 1. Assign a password to be used with the **ip ospf authentication-key** *password* interface command.

Step 2. Specify the authentication type with the **ip ospf authentication** interface command.

Step 3. Configure authentication under the OSPF area using the **area** *area-id* **authentication** command.

The following enables plain-text authentication using the password of cisco on interface serial 0/0:

```
RouterA(config)#interface serial 0/0
RouterA(config-if)#ip ospf authentication-key cisco
RouterA(config-if)#ip ospf authentication
RouterA(config-if)#!
RouterA(config)#router ospf 1
RouterA(config-if)#area 0 authentication
```

Verifying Plain-Text Authentication

The **show ip ospf interface** command shows whether OSPF authentication is enabled. The highlighted item in the following example shows that plain-text authentication is enabled:

```
RouterA# show ip ospf interface serial0
Serial0 is up, line protocol is up
  Internet Address 192.16.0.1/24, Area 0
  Process ID 10, Router ID 172.16.0.1, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
```

```
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 4 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Simple password authentication enabled
```

Configuring MD5 Authentication

Configuring MD5 authentication between two OSPF routers is similar to configuring plain-text authentication, except you need to have a key ID and a password.

The **ip ospf message-digest-key** *key-id* **md5** *password* interface command sets the password between the two routers. The **area** *area-id* **authentication message-digest** command enables MD5 for the OSPF area. The following commands enable MD5 authentication for key 1 with the password of cisco:

NOTE
The *key-id* and *password* parameters must be the same between neighboring devices.

```
RouterA(config)#interface serial 0/0
RouterA(config-if)#ip ospf message-digest-key 1 md5 cisco
RouterA(config-if)#ip ospf authentication message-digest
RouterA(config-if)#
RouterA(config)#router ospf 1
RouterA(config-router)#area 0 authentication message-digest
```

Verifying MD5 Authentication

The **show ip ospf interface** command shows whether OSPF authentication is enabled. The highlighted item in the following example shows that MD5 authentication is enabled:

```
RouterA# show ip ospf interface serial0
Serial0 is up, line protocol is up
  Internet Address 192.16.0.1/24, Area 0
  Process ID 10, Router ID 172.16.0.1, Network Type POINT_TO_POINT, Cost: 64
```

 Please see page 311 for more details.

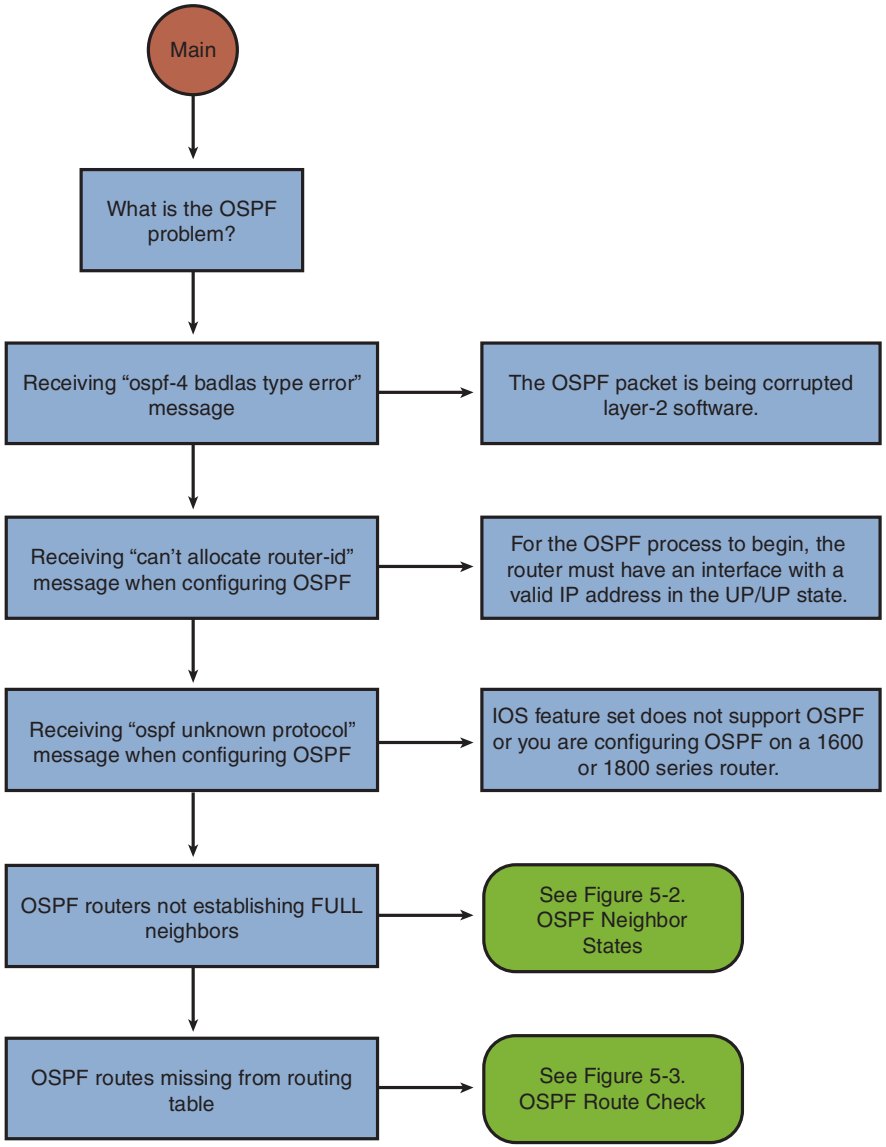
```
Transmit Delay is 1 sec, State POINT_TO_POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:04
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 4 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
  Youngest key id is 1
```

Troubleshooting OSPF

Troubleshooting OSPF can be complex. Figure 5-1 shows a basic flow chart to begin the troubleshooting process in OSPF.

 Please see page 311 for more details.

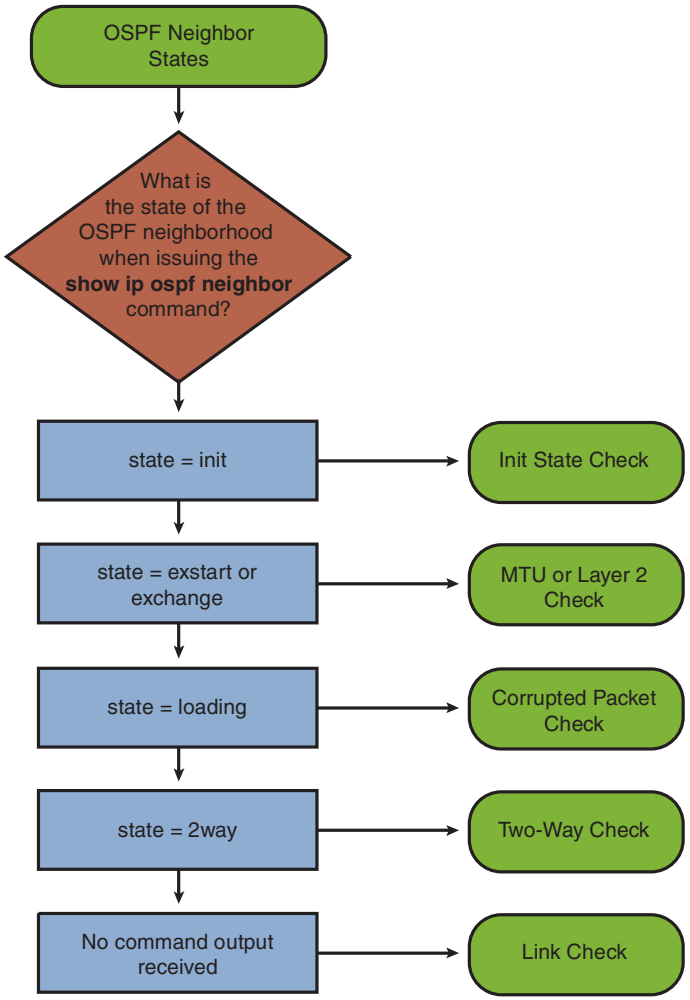
FIGURE 5-1
OSPF
Troubleshooting
Flow Chart



Troubleshooting Neighbor States

Figure 5-2 displays some of the most common neighbor states and describes steps to resolve the received neighbor states.

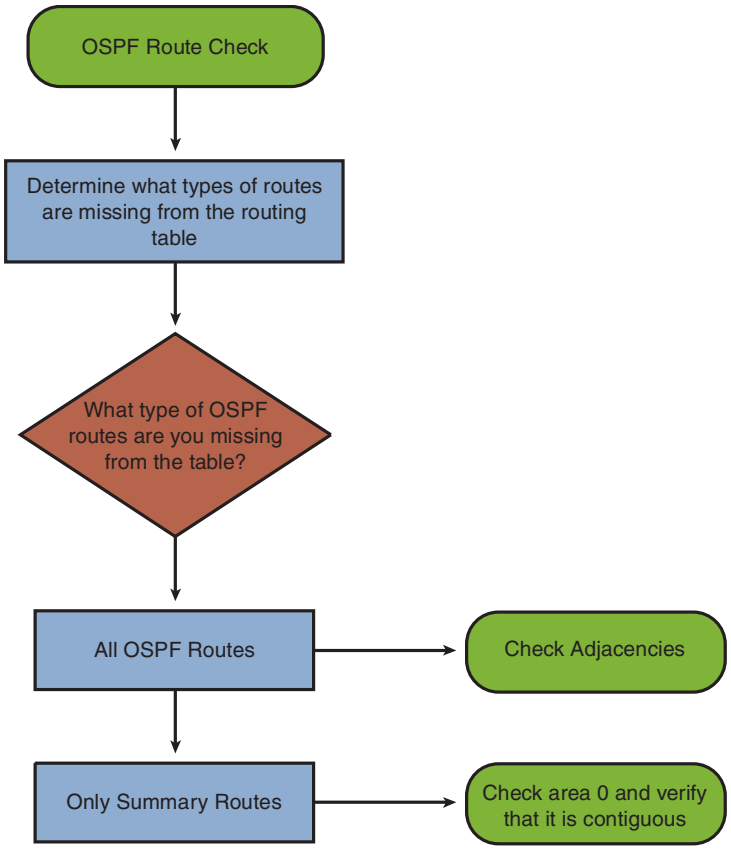
FIGURE 5-2
Troubleshooting Neighbor States



Troubleshooting Routing Table

Figure 5-3 shows a flow chart to troubleshoot OSPF routing table issues.

FIGURE 5-3
OSPF Routing Table Troubleshooting Flow Chart



 Please see page 311 for more details.

Troubleshooting Commands

- **show ip ospf interface:** Lists the area in which the interface belongs, and neighbors adjacent on the interface.
- **show ip ospf neighbor:** Lists neighbors and current neighbor status.
- **debug ip ospf events:** Shows messages for each OSPF packet.
- **debug ip ospf packet:** Shows log messages that describe the contents of all OSPF packets.
- **debug ip ospf hello:** Shows messages describing Hello packets and Hello failures.
- **debug ip ospf adj:** Shows the authentication process if OSPF authentication is configured.

The **debug ip ospf adj** command is an important command for troubleshooting OSPF adjacencies. OSPF routers exchange Hello packets to create neighbor adjacencies. For an OSPF adjacency to occur, the following four items in an OSPF Hello packet must match:

- Area ID
- Hello/dead intervals
- Authentication password
- Stub area flag

To determine whether any of these Hello packet options do not match, use the **debug ip ospf adj** command. The following output shows a successful adjacency on the serial 0 interface:

```
RouterA# debug ip ospf adj
00:50:57: %LINK-3-UPDOWN: Interface Serial0, changed state to down
00:50:57: OSPF: Interface Serial0 going Down
00:50:57: OSPF: 172.16.10.36 address 192.16.64.1 on Serial0 is dead,
  state DOWN
```

 Please see page 311 for more details.

```
00:50:57: OSPF: 70.70.70.70 address 192.16.64.2 on Serial0 is dead,
  state DOWN
00:50:57: %OSPF-5-ADJCHG: Process 10, Nbr 70.70.70.70 on Serial0 from
  FULL to DOWN, Neighbor Down: Interface down or detached
00:50:58: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
  seq 0x80000009
00:50:58: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
  changed state to down
00:51:03: %LINK-3-UPDOWN: Interface Serial0, changed state to up
00:51:03: OSPF: Interface Serial0 going Up
00:51:04: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
  seq 0x8000000A
00:51:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
  changed state to up
00:51:13: OSPF: 2 Way Communication to 70.70.70.70 on Serial0,
  state 2WAY
00:51:13: OSPF: Send DBD to 70.70.70.70 on Serial0 seq 0x2486 opt 0x42
  flag 0x7 len 32
00:51:13: OSPF: Rcv DBD from 70.70.70.70 on Serial0 seq 0x19A4 opt 0x42
  flag 0x7 len 32 mtu 1500 state EXSTART
00:51:13: OSPF: First DBD and we are not SLAVE
00:51:13: OSPF: Rcv DBD from 70.70.70.70 on Serial0 seq 0x2486 opt 0x42
  flag 0x2 len 72 mtu 1500 state EXSTART
00:51:13: OSPF: NBR Negotiation Done. We are the MASTER
00:51:13: OSPF: Send DBD to 70.70.70.70 on Serial0 seq 0x2487 opt 0x42
  flag 0x3 len 72
00:51:13: OSPF: Database request to 70.70.70.70
00:51:13: OSPF: sent LS REQ packet to 192.16.64.2, length 12
```

 Please see page 311 for more details.

```
00:51:13: OSPF: Rcv DBD from 70.70.70.70 on Serial0 seq 0x2487 opt 0x42
  flag 0x0 len 32 mtu 1500 state EXCHANGE
00:51:13: OSPF: Send DBD to 70.70.70.70 on Serial0 seq 0x2488 opt 0x42
  flag 0x1 len 32
00:51:13: OSPF: Rcv DBD from 70.70.70.70 on Serial0 seq 0x2488 opt 0x42
  flag 0x0 len 32 mtu 1500 state EXCHANGE
00:51:13: OSPF: Exchange Done with 70.70.70.70 on Serial0
00:51:13: OSPF: Synchronized with 70.70.70.70 on Serial0, state FULL
00:51:13: %OSPF-5-ADJCHG: Process 10, Nbr 70.70.70.70 on Serial0 from LOADING
  to FULL, Loading Done
00:51:14: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
  seq 0x8000000B
```

 Please see page 311 for more details.

Section 6
Implementing EIGRP

Enhanced IGRP (EIGRP) is a Cisco-proprietary routing protocol. EIGRP is a classless routing protocol, meaning that it sends the subnet mask of its interfaces in routing updates, which use a complex metric based on bandwidth and delay.

EIRGP is an advanced distance vector protocol with some link-state features. As such, EIGRP is classified as a balanced hybrid protocol.

EIGRP Features

- **Protocol-independent modules:** EIGRP supports IP, IPv6, Internetwork Packet Exchange (IPX), and AppleTalk.
- **Reliable Transport Protocol:** RTP controls sending, tracking, and acknowledging updates and EIGRP messages.
- **Neighbor discovery/recovery:** EIGRP discovers neighboring devices using periodic Hello messages.
- **Diffusing Update Algorithm (DUAL):** EIGRP uses DUAL to calculate and maintain loop-free paths and provide fast convergence.
- **Partial updates:** EIGRP sends partial triggered updates instead of periodic updates.

EIGRP Terminology

- **Neighbor table:** Lists all adjacent routers. Includes the neighbor's address and the interface through which it can be reached. EIGRP routers keep a neighbor table for each routed Layer 3 protocol (IP, IPX, AppleTalk).
- **Topology table:** Contains all learned routes to a destination. The topology table holds all successor and feasible successor routes in its table.
- **Routing table:** Holds the best routes (the successor routes) to each destination.

 Please see page 311 for more details.

EIGRP Path Calculation

DUAL uses distance information (metric) to select the best, loop-free path to a destination. It does this by selecting a successor with the best feasible distance. A backup route, called the feasible successor, is selected if the advertised distance is less than the feasible distance. The following is a list of the terminology DUAL uses to select a route:

- **Successor:** The primary route used to reach a destination. The successor route is kept in the routing table.
- **Feasible successor:** The backup route. Must have an AD less than the FD of the current successor route.
- **Advertised distance (AD):** The lowest-cost route between the next-hop router and the destination.
- **Feasible distance (FD):** The sum of the AD plus the cost between the local router and the next-hop router.

Configuring and Verifying EIGRP

The **router eigrp** *process-id* command enables EIGRP on the router. This is followed by the **network** command to enable EIGRP on the specified interfaces. The following commands enable EIGRP using AS 100 and then enable EIGRP on all router interfaces with IP addresses in the networks 192.168.3.0 and 192.168.4.0:

```
RouterA(config)#router eigrp 100 (100 is the process-id)
RouterA(config-router)#network 192.168.3.0
RouterA(config-router)#network 192.168.4.0
```

- **show ip eigrp neighbors:** Displays EIGRP adjacencies and directly connected neighbors.
- **show ip route eigrp:** Displays all EIGRP routes in the routing table.
- **show ip eigrp topology:** Displays the EIGRP topology table, including successors and feasible successors.
- **debug eigrp neighbors:** Displays neighbors discovered by EIGRP and the contents of Hello packets.

 Please see page 311 for more details.

Load Balancing with EIGRP

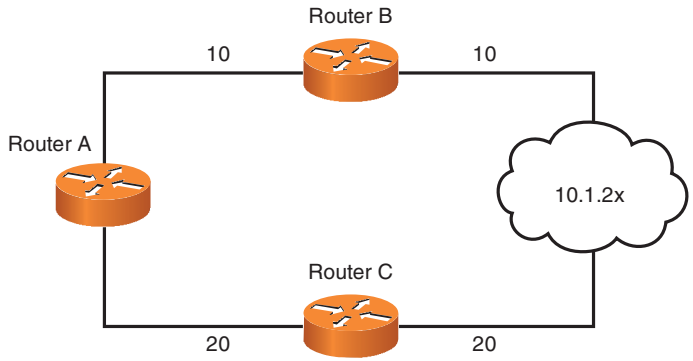
Load balancing is a router's ability to balance traffic over all its network's ports that are the same metric from the destination address.

EIGRP uses a complex metric based on bandwidth, delay, load, reliability, and MTU to select the best path to a destination. By default, EIGRP only uses bandwidth and delay to calculate its metric.

By default, EIGRP can automatically load-balance up to 4 equal-cost routes (16 routes being the maximum); this is called equal-cost load balancing.

Unequal-cost load balancing is when a router can load-balance traffic to a destination through links of different cost or speeds. In Figure 6-1, Router A has two unequal paths to network 10.1.2.x.

FIGURE 6-1
EIGRP Unequal-Cost Load Balancing



Because the path through Router B has a lower cost than the path through Router C, Router A will route all traffic to network 10.1.2.x through Router B.

To configure Router A to perform unequal-cost load balancing, you need to use the **variance** *multiplier* command on Router A. The multiplier is a variance value between 1 and 128, with the default set to 1.

To determine the variance, divide the metric of the cost between Router C by the cost of Router B. In this case, it would be 40/20, which equals 2. So the variance to perform unequal-cost load balancing to network 10.1.2.x is 2. The following configuration sets the variance on Router A to 2:

```
RouterA(config)#router eigrp 100
RouterA(config-router)#variance 2
```

EIGRP Authentication

EIGRP supports MD5 route authentication. The following steps enable authentication on a Cisco router:

Step 1. Enter the interface you want to configure authentication on.

Step 2. Enable MD5 authentication using the **ip authentication mode eigrp** *process-id* **md5** interface command.

Step 3. Create an authentication key using the **ip authentication key-chain eigrp** *process-id key-chain* command. The *key-chain* parameter is the name of the key you want to create.

Step 4. Exit interface configuration mode.

Step 5. Identify the key chain you configured in Step 3 using the **key chain** *name-of-key-chain* command.

Step 6. Create a key number: **key** *number.*

Step 7. Identify the key string using the **key-string** *text* command.

The following example configures MD5 authentication with cisco as the key:

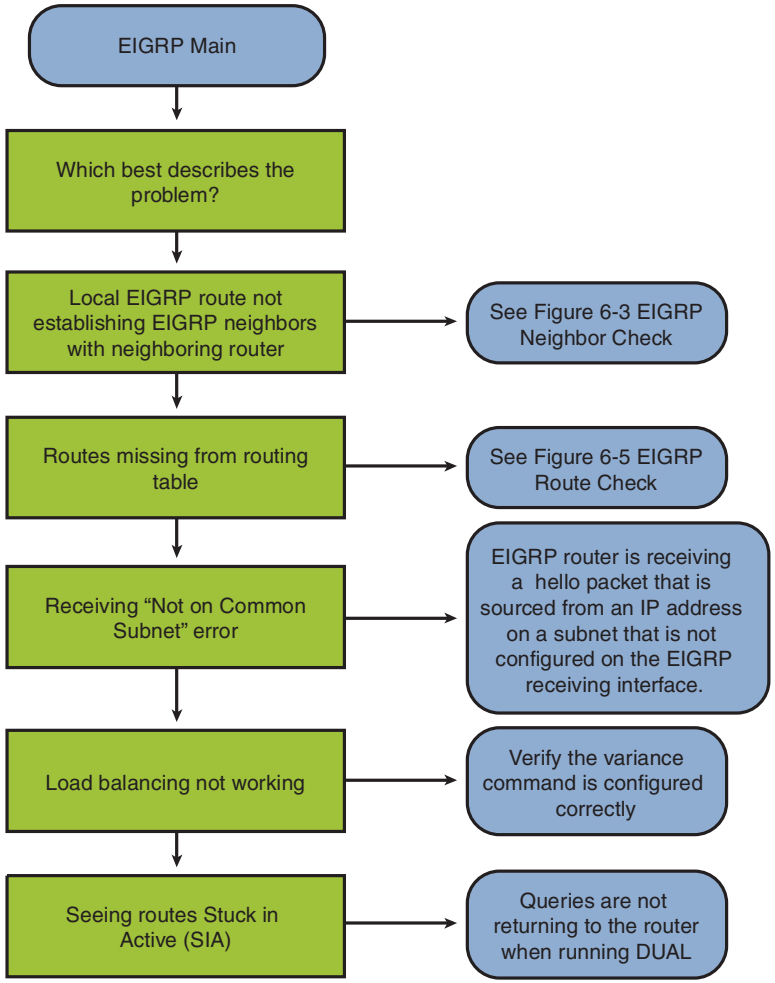
```
RouterA(config)#interface serial 0/0
RouterA(config-if)#ip authentication mode eigrp 100 md5
RouterA(config-if)#ip authentication key-chain eigrp 100 cisco
RouterA(config-if)#!
RouterA(config)#key chain cisco
RouterA(config-keychain-key)#key 1
RouterA(config-keychain-key)#key-string firstkey
```

 Please see page 311 for more details.

Troubleshooting EIGRP

Figure 6-2 shows a basic flow chart with the steps to take to approach EIGRP troubleshooting.

FIGURE 6-2
EIGRP Troubleshooting Flow Chart



 Please see page 311 for more details.

EIGRP Neighbor Troubleshooting

When EIGRP is not forming neighbor relationships with other EIGRP routers, use the flow charts from Cisco.com in Figures 6-3 and 6-4 to troubleshoot the issue.

FIGURE 6-3
EIGRP Neighbor Check: Part I

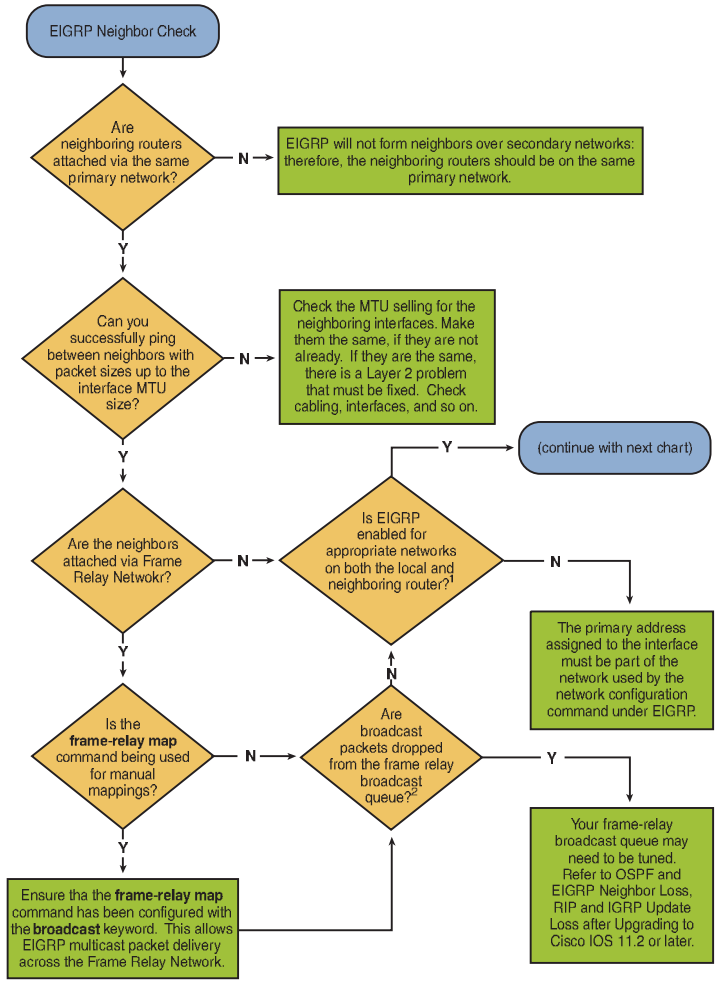
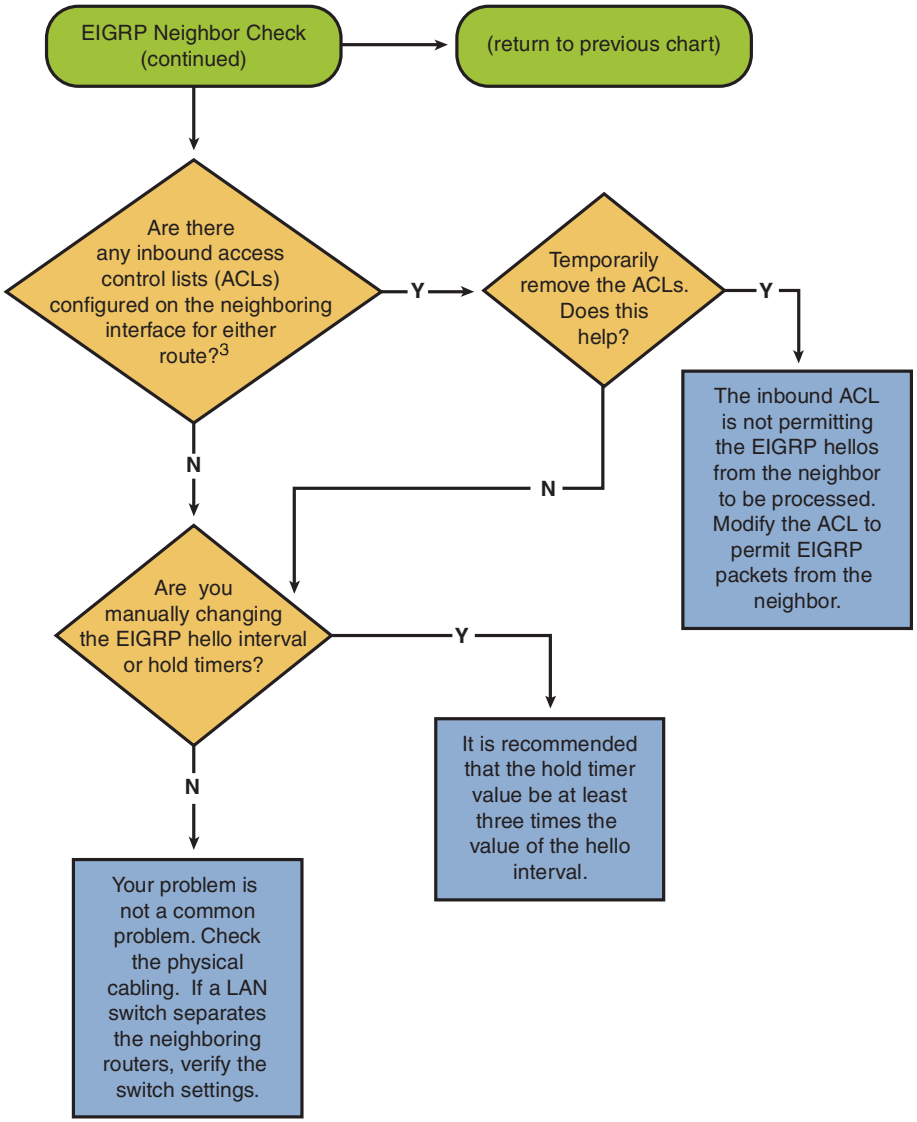


FIGURE 6-4
EIGRP Neighbor Check: Part II



EIGRP Route Troubleshooting

If EIGRP is not populating the routing table, Figures 6-5 and 6-6 outline some common steps for troubleshooting the error.

FIGURE 6-5
EIGRP Route Check: Part I

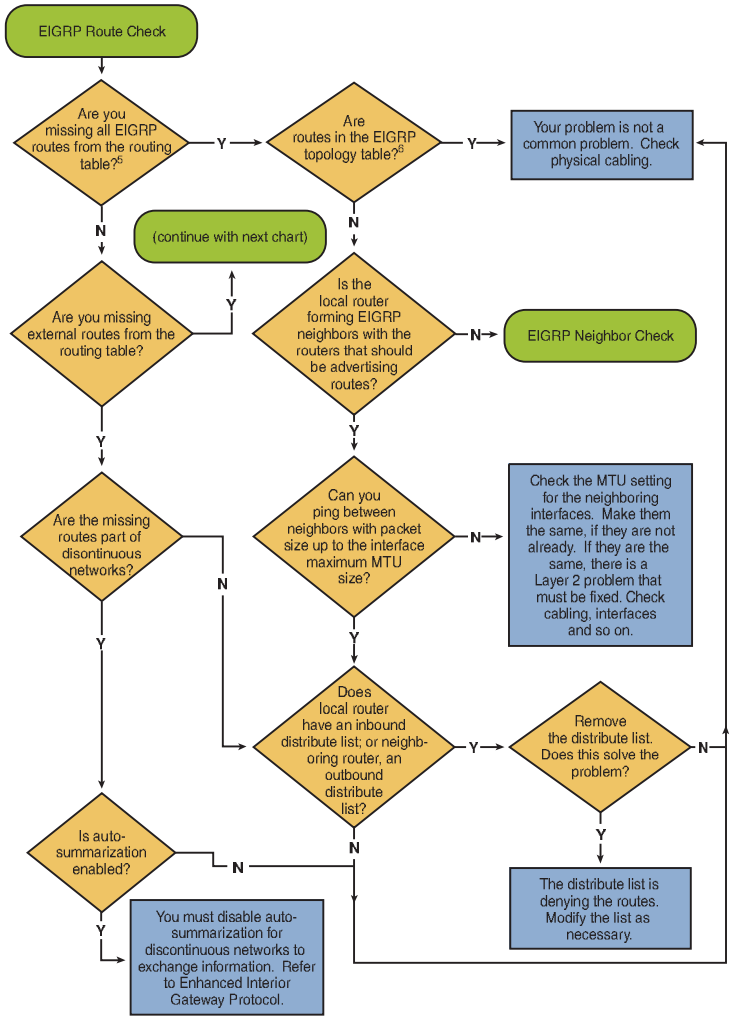
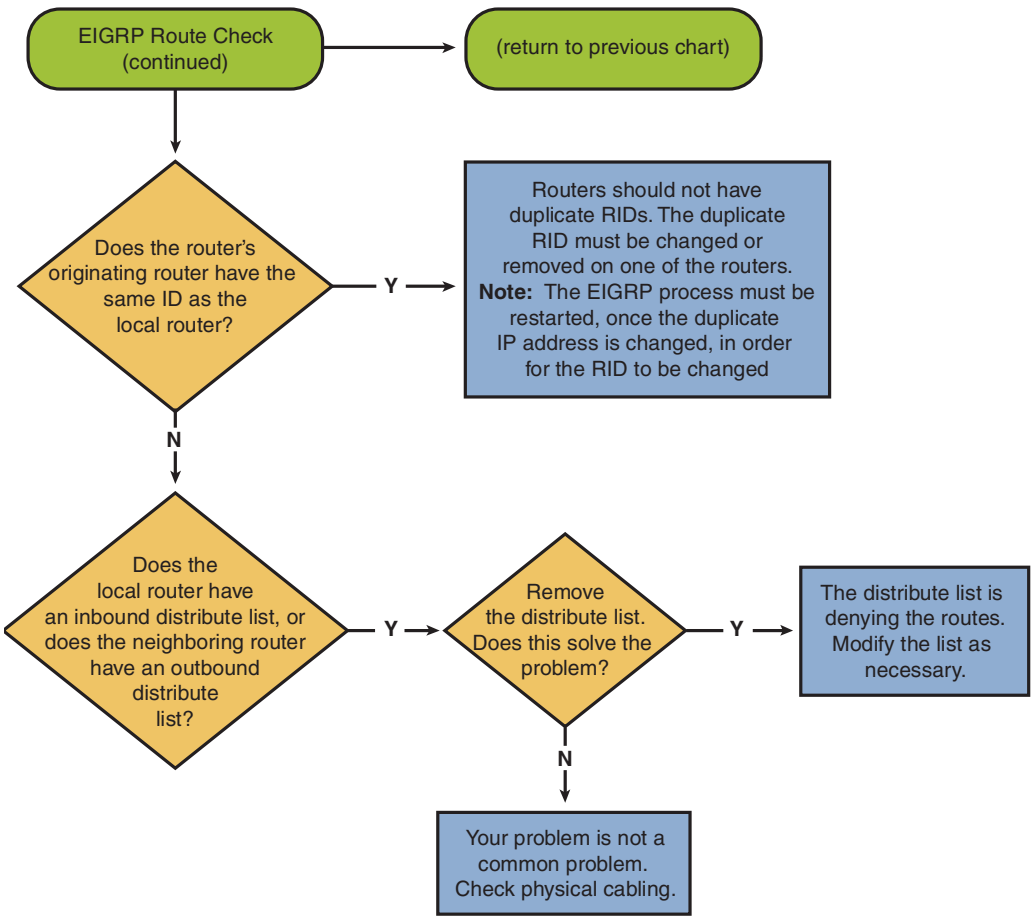


FIGURE 6-6
EIGRP Route Check: Part II



Troubleshooting MD5 Authentication

The **debug eigrp packets** command allows you to troubleshot EIGRP MD5 authentication problems. In the following example, Router A is receiving EIGRP packets with MD5 authentication and a key string different from what it is expecting. The result is an authentication mismatch, and the neighbor relationship is declared down:

```
RouterA#debug eigrp packets
EIGRP Packets debugging is on
(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)
R2#
*Apr 21 16:50:18.749: EIGRP: pkt key id = 2, authentication mismatch
*Apr 21 16:50:18.749: EIGRP: Serial0/0/1: ignored packet from 192.168.1.101, opcode = 5
(invalid authentication)
*Apr 21 16:50:18.749: EIGRP: Dropping peer, invalid authentication
*Apr 21 16:50:18.749: EIGRP: Sending HELLO on Serial0/0/1
*Apr 21 16:50:18.749: AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
*Apr 21 16:50:18.753: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.1.101
  (Serial0/0/1) is down: Auth failure
```

 Please see page 311 for more details.

Part III: Access Lists and Managing Address Spaces

Section 7
Managing Traffic with ACLs

As a network grows, it becomes more important to manage the increased traffic going across the network. Access lists help limit traffic by filtering based on packet characteristics. Access lists define a set of rules that routers use to identify particular types of traffic. Access lists can be used to filter both incoming and outgoing traffic on a router's interface. An access list applied to a router specifies only rules for traffic going through the router. Traffic originating from a router is not affected by that router's access lists. (It is subject to access lists within other routers as it passes through them.)

Access lists are used for many reasons. Cisco security devices like firewalls and VPN concentrators use access lists to define access to the network. Access lists are used to define the traffic that a firewall or VPN concentrator will encrypt. Cisco routers also use access lists for quality of service (QoS), route filters, Network Address Translation, and packet prioritization.

Packet Filtering

Access lists can be configured to permit or deny incoming and outgoing packets on an interface. By following a set of conventions, the network administrator can exercise greater control over network traffic by restricting network use by certain users or devices.

 Please see page 311 for more details.

Types of Access Lists

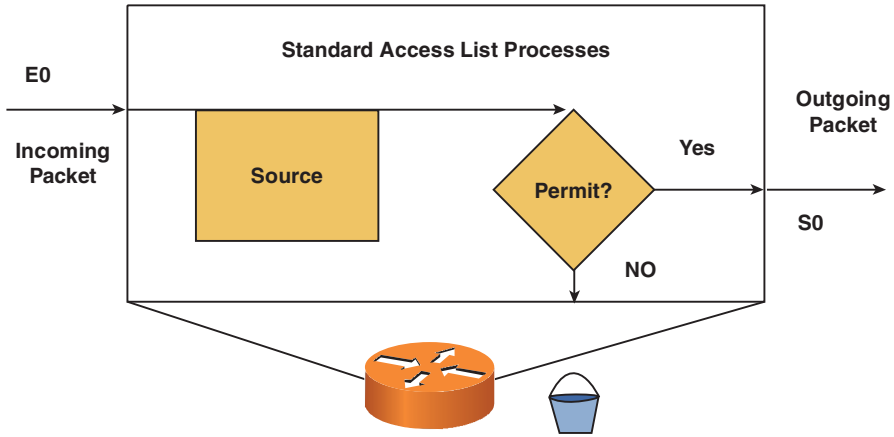
The following two methods identify access control lists (ACL):

- **Numbered ACLs:** Use a number for identification
- **Named ACLs:** Use a descriptive name or number for identification

Numbered and named ACLs can be categorized further into the following types of ACLs:

- **Standard access lists** check packets' source addresses. Standard IP access lists permit or deny output for an entire protocol suite based on the source network/subnet/host IP address. Standard ACLs should be placed as close to the destination as possible. Figure 7-1 shows the standard access list processes.

FIGURE 7-1
Standard Access List Processes



- **Extended access lists** check both source and destination packet addresses. Extended lists specify protocols, port numbers, and other parameters, allowing admins more flexibility and control. Extended ACLs should be placed as close to the source as possible.

 Please see page 311 for more details.

Table 7-1 shows the difference between standard and extended access lists.

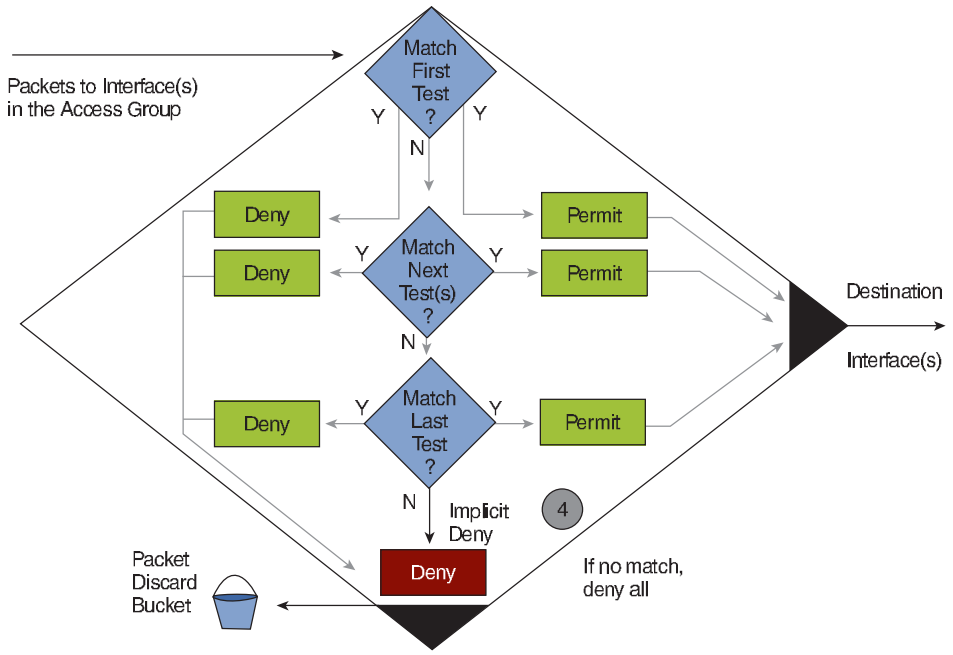
TABLE 7-1 Types of Access Lists

Standard	Extended
Filter based on source	Filter based on source and destination
Permit or deny the entire TCP/IP protocol suite	Specify a specific IP protocol and port number
Range: 1 to 99, 1300 to 1999	Range: 100 to 199, 2000 to 2699

Access List Operations

Access list statements are operated on one at a time from top to bottom. Figure 7-2 shows the process of ACLs.

FIGURE 7-2
ACL Process



As soon as a packet header match is found, the packet is operated on (permitted or denied), and the rest of the statements are skipped.

If no match is found, the packet is tested against the next statement until a match is found or the end of the list is reached. An implicit deny statement is present at the end of the list (all remaining packets are dropped). Unless at least one permit statement exists in an access list, all traffic is blocked.

Access List Process Options

- **Inbound access lists:** Incoming packets are processed before they are sent to the outbound interface. If the packet is to be discarded, this method reduces overhead (no routing table lookups). If the packet is permitted, it is processed in the normal way.
- **Outbound access lists:** Outgoing packets are processed by the router first and then are tested against the access list criteria.

Protocol Access List Identifiers

The access list number entered by the administrator determines how the router handles the access list. The arguments in the statement follow the number. The types of conditions allowed depend on the type of list (defined by the access list number). Conditions for an access list vary by protocol. You can have several different access lists for any given protocol, but only one protocol, per direction, per interface is allowed on any access list.

Testing Against Access List Statements

For TCP/IP packets, access lists check the packet and upper-layer headers for different items (depending on the type of access list [standard or extended]).

 Please see page 311 for more details.

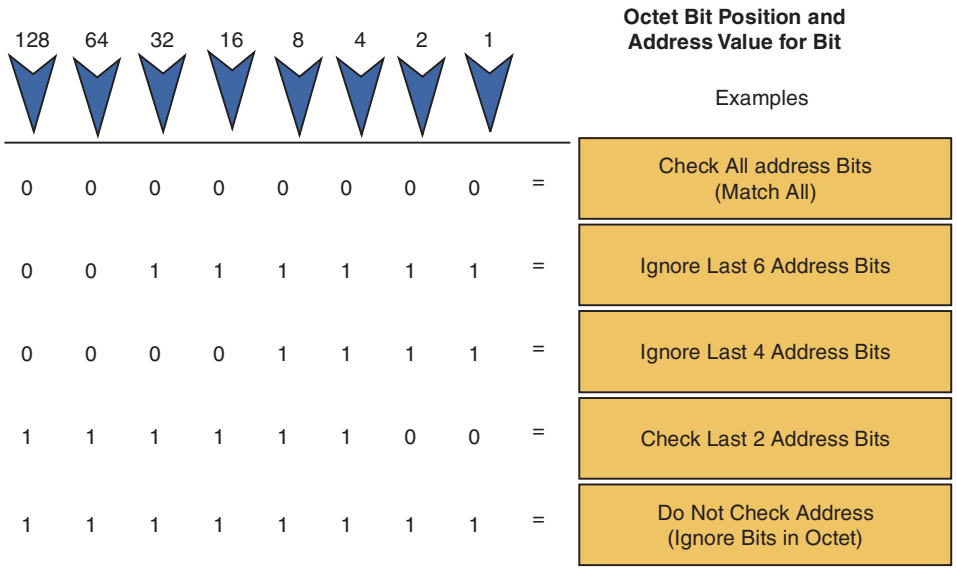
Standard IP access lists are assigned the range of numbers 1 to 99 and 1300 to 1999. Extended IP access lists use the range 100 to 199 and 2000 to 2699. After a packet is checked for a match with the access list statement, it is either permitted through an interface or discarded.

Wildcard Masking

It is not always necessary to check every bit within an address. Wildcard masking identifies which bits should be checked or ignored (see Figure 7-3). Administrators can use this tool to select one or more IP addresses for filtering. Wildcard mask bits are defined as follows:

- A wildcard mask bit of 0 means to check the corresponding bit value.
- A wildcard mask bit of 1 means do not check (ignore) that corresponding bit value.

FIGURE 7-3
Wildcard Masking



To specify an IP host address within a permit or deny statement, enter the full address followed by a mask of all 0s (0.0.0.0).

To specify that all destination addresses are permitted in an access list, enter 0.0.0.0 as the address, followed by a mask of all 1s (255.255.255.255).

A shortcut to find the wildcard mask is to subtract the subnet mask from 255.255.255.255. For example, 172.16.0.0/22 has the following subnet mask: 255.255.252.0. If you subtract this subnet mask from 255.255.255.255 you get the wildcard mask to use:

```
  255.255.255.255
– 255.255.252.0
    0.  0.  3.255
```

Abbreviations can be used instead of entering an entire wildcard mask.

- **Check all addresses:** To match a specific address, use the word *host*: 172.30.16.29 0.0.0.0 can be written as **host 172.30.16.29**.
- **Ignore all addresses:** Use the word *any* to specify all addresses: 0.0.0.0 255.255.255.255 can be written as **any**.

IP Access List Entry Sequence Numbering

IP access list entry sequence numbering allows you to edit the order of ACL statements using sequence numbers. Prior to IP access list entry sequence numbering, if you wanted to edit one line in an access list, the entire access list had to be removed and replaced with the new updated access list.

IP access list entry sequence numbering requires Cisco IOS Software Release 12.3 and allows you to add access-list entry sequence numbers to the beginning standard and extended access-list rules to allow you to make additions and changes to individual rules in the access list.

 Please see page 311 for more details.

Guidelines for Placing Access Lists

Extended IP access lists can block traffic from leaving the source and should be as close as possible to the source of the traffic to be denied.

Standard IP access lists block traffic at the destination and should be as close as possible to the destination of the traffic to be denied.

Additional Types of ACLs

Standard and extended ACLs can become the basis for other types of ACLs that provide additional functionality. These other types of ACLS include the following:

- Dynamic ACLs (lock-and-key)
- Reflective ACLs
- Time-based ACLs

Dynamic ACLs

Dynamic ACLs (lock-and-key) dynamically create access-list entries on the router to allow a user that has authenticated to the router through Telnet to access resources that are blocked behind the router.

Dynamic ACLs depend on the user authenticating to the router and an extended access list. Considered lock-and-key, the configuration starts with an extended ACL that blocks traffic through the router. A user who wants to traverse through the router is blocked by the extended ACL until he authenticates to the router through Telnet with a username and password. After being authenticated, the Telnet connection is dropped and a single-entry dynamic ACL entry is added to the extended ACL to permit the user to traverse through the router.

 Please see page 311 for more details.

Reflective ACLs

Reflective ACLs allow IP packets to be filtered based on upper-layer session information. They are used to allow outbound traffic, and they limit inbound traffic in response to sessions that originate from a network inside the router.

Reflective ACLs contain only temporary entries that are created when a new IP session begins and are removed when the session ends. Reflective ACLs are *not* applied directly to an interface, but are "nested" within an extended named IP ACL that is applied to an interface.

Time-Based ACLs

Time-based ACLs are similar to extended access lists, except they control access based on time.

Configuring IP Access Lists

Access lists are processed from top to bottom, making statement ordering critical to efficient operation. Always place specific and frequent statements at the beginning of an access list. Named access lists and ACLs using extended sequence entries allow the removal and changes of individual statements. Remember that all access lists end with an implicit deny any statement.

Guidelines for Implementing Access Lists

- Be sure to use the correct numbers for the type of list and protocols you want filtered.
- You can use only one access list per protocol, per direction, per interface. A single interface can have one access list per protocol.
- Put more-specific statements before more-general ones. Frequently occurring conditions should be placed before less-frequent conditions.

 Please see page 311 for more details.

- Additions are always added to the end of the access list. You cannot selectively add or remove statements in the middle of standard or extended access lists unless you are using named ACLs or extended sequence entries (IOS 12.3).
- Without an explicit permit, the implicit deny at the end of every list causes all packets to be denied. Every access list should include at least one permit statement.
- An interface with an empty access list applied to it allows (permits) all traffic. Create your statements before applying the list to an interface.
- Access lists filter only traffic going through the router.

Configuring Standard IP Access Lists

The command syntax to create a standard IP access list is as follows:

```
access-list access-list-number {permit | deny} source-address [wildcard-mask]
```

where *access-list-number* is a number from 1 to 99 or 1300 to 1999.

For example, the following command creates access list number 10, which denies any IP address between 192.168.0.1 and 192.168.255.255:

```
RouterA(config)#access-list 10 deny 192.168.0.0 0.0.255.255
RouterA(config)#access-list 10 permit any any
```

Configuring Extended IP Access Lists

The Cisco IOS command syntax to create an extended access list is as follows:

```
access-list access-list-number {permit | deny} protocol source-address
  source-wildcard [operator port] destination-address destination-wildcard
  [operator port]
```

 Please see page 311 for more details.

where:

- *protocol* examples include IP, TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), generic routing encapsulation (GRE), and IGRP.
- *operator port* can be **lt** (less than), **gt** (greater than), **eq** (equal to), or **neq** (not equal to) and a protocol port number.

The following example creates an extended access list that blocks FTP traffic from network 172.16.4.0/24 to network 172.16.3.0/24 and applies the ACL to interface Ethernet 0:

```
RouterA>enable
RouterA#config term
RouterA(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255  172.16.3.0 0.0.0.255 eq 21
RouterA(config)#access-list 101 permit ip any any
RouterA(config)#interface ethernet 0
RouterA(config-if)#access group 101 in
```

Using IP Access List Entry Sequence Numbers

To use entry sequence numbers, you first create the access list. Then you add the access list rules by first defining the entry sequence where you want the rule to be added in the access list. The following example creates an extended ACL, using entry sequence numbers, that permits HTTP and FTP traffic from network 192.168.1.0/24 to network 172.16.0.0/16:

```
RouterA(config)#ip access list extended 100
RouterA(config-ext-nacl)#1 permit tcp 192.168.1.0 0.0.0.255 172.16.0.0 0.0.255.255 eq http
RouterA(config-ext-nacl)#10 permit tcp 192.168.1.0 0.0.0.255 172.16.0.0 0.0.255.255 eq ftp
```

In the preceding example, if you want to add a rule in between rule 1 and 10, you give it a sequence number between 1 and 10. If you want to edit only one line in the ACL, you would enter the ACL you want to edit and then use the sequence number to identify which line you want to edit.

Configuring Named Access Lists

When you create a named access list, you use the **ip access-list extended** *name* global command, where *name* is the name of the access list. Issuing this command places you in named IP access list subcommand mode, which then allows you to enter the access list parameters.

The following creates a named access list that blocks ping from networks 172.160.0.0/22 to host 192.168.0.101:

```
RouterA(config)#ip access-list extended block-ping
RouterA(config-ext-nacl)#deny icmp 172.16.0.0 0.0.3.255 host 192.168.0.101 echo
RouterA(config-ext-nacl)#permit ip any any
```

Applying Access Lists

To apply an access list to an interface on a Cisco router, use the **ip access-group** interface command, as follows:

```
ip access-group access-list-number {in | out}
```

For example, the following applies access list 10 to serial interface 0 as an inbound access list:

```
RouterA(config)#int s0
RouterA(config-if)#ip access-group 10 in
```

To remove an access list from a router, first remove it from the interface by entering the **no ip access-group** *access-list-number direction* command. Then remove the access list by entering the **no access-list** *access-list-number* global command.

 Please see page 311 for more details.

Creating Dynamic Access Lists

Follow these steps to create a dynamic ACL:

Step 1. Create a user authentication method on the router. This can either be local or remote using a AAA or RADIUS server.

The following example enables local authentication on the router:

```
RouterA(config)#username remote password 0 cisco
RouterA(config)#username remote autocommand access-enable host timeout 10
```

This creates a user named remote with a password of cisco and configures the router to time out after 10 minutes of idle traffic.

Step 2. Define an extended ACL to permit vty access but block all other traffic. For example:

```
RouterA(config)#access-list 101 permit tcp any host 192.168.1.1 eq telnet
RouterA(config)#interface s0
RouterA(config-if)#ip access-group 101 in
```

Step 3. Create a dynamic ACL that applies to the extended ACL you created after it is authenticated. For example, the following command creates the dynamic ACL that is applied to ACL 101:

```
RouterA(config)#access-list 101 dynamic remoteaccess timeout 15 permit ip 192.168.1.0 0.0.0.255
 10.1.1.0 0.0.0.255
```

Because this example is using local authentication, the router needs to be configured to locally authenticate when a user tries to connect to the vty ports:

```
RouterA(config)#line vty 0 4
RouterA(config-line)#login local
```

 Please see page 311 for more details.

Verifying Access List Configuration

The **show ip interface** *interface-type interface-number* command displays whether an IP access list is applied to an interface.

The **show running-config** and **show access-list** commands display all access lists configured on a router.

Virtual Terminal (vty) Access Lists

In addition to physical ports, devices also have virtual ports (called virtual terminal lines). Most current Cisco devices support 16 virtual terminal lines, numbered vty 0 through vty 15. Standard and extended access lists applied to physical interfaces do not prevent router-initiated Telnet sessions.

Virtual terminal access lists can block vty access to the router or block access to other routers on allowed vty sessions. Restrictions on vty access should include all virtual ports, because users can connect through any vty port. The syntax for a vty access list is as follows:

```
line vty {vty# | vty-range}
access-class {IP access list #} in
```

After the vty statements are added, they are assigned to the router with the following command:

```
access-class access-list-number {in | out}
```

Specifying **in** prevents incoming Telnet connections, and **out** prevents Telnet connections to other routers from the vty ports.

Troubleshooting Access Lists

Access lists are processed from the top down. Most access list errors are due to an incorrect statement entry that denies traffic.

To troubleshoot access lists, verify that the statements are correct and applied to the proper interface and direction. Also, remember that at the end of each access list is an implicit deny any statement.

 Please see page 311 for more details.

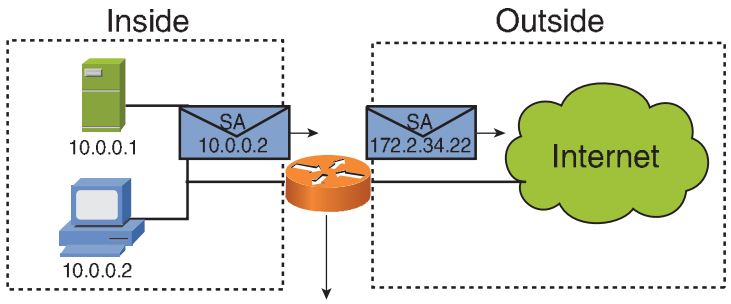
Section 8
Managing Address Space with NAT and IPv6

Network Address Translation (NAT) was initially developed as an answer to the diminishing number of IP addresses. When the IP address scheme was originally developed, it was believed that the address space would not run out. The combination of the PC explosion and the emergence of other network-ready devices quickly consumed many of the available addresses.

An additional (and equally important) benefit of NAT is that it hides private addresses from public networks, making communication more secure from hackers. Figure 8-1 shows how NAT translates the inside address of 10.0.0.1 to the outside address 172.2.34.21. Properties of NAT are as follows:

- NAT is configured on a router, firewall, or other network device.
- Static NAT uses one-to-one private-to-public address translation.
- Dynamic NAT matches private addresses to a pool of public addresses on an as-needed basis. The address translation is still one-to-one.

FIGURE 8-1
NAT

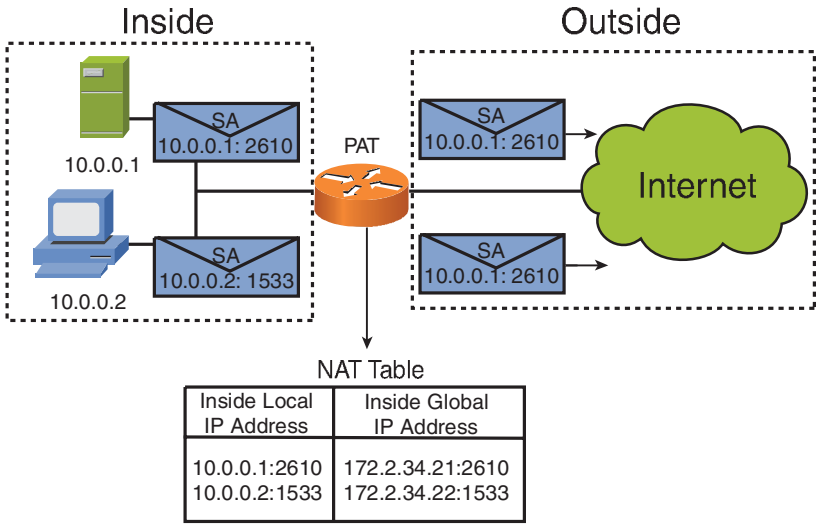


 Please see page 311 for more details.

Port Address Translation (PAT) is a form of dynamic address translation that uses many (private addresses) to few or one (public address). This is called overloading and is accomplished by assigning port numbers, as shown in Figure 8-2. Details of PAT are as follows:

- Because the port number is 16 bits, PAT can theoretically map 65,536 sessions to a single public address.
- PAT continues to look for available port numbers. If one is not found, PAT increments the IP address (if available).

FIGURE 8-2
PAT



 Please see page 311 for more details.

NAT Terminology

Table 8-1 lists the Cisco NAT terminology.

TABLE 8-1 NAT Terminology

Name	Description
Inside local address	The IP address assigned to a host on the inside, private network. Usually a private IP address.
Inside global address	A legal routable IP address that represents one or more inside local IP addresses to the outside world.
Outside local address	The IP address of an outside host as it appears to the inside, private network. This is usually is a private IP address.
Outside global address	The IP address assigned to a host on the outside network by the host's owner. Usually a routable IP address.

Configuring Static NAT

To configure static NAT, you must first create the static mapping table and then define which interfaces on your router connect to the inside network and the outside network. The following example creates the static mapping and defines interface s0 as connecting to the outside network and interface e0 as connecting to the inside network:

```
RouterB(config)#ip nat inside source static 192.168.10.5 216.1.1.3
RouterB(config)#int s0
RouterB(config-if)#ip nat outside
RouterB(config-if)#int e0
RouterB(config-if)#ip nat inside
```

 Please see page 311 for more details.

Configuring Dynamic NAT

To configure dynamic NAT, you first have to create a NAT pool of external IP addresses that internal hosts can draw from. Then create an access list that defines the internal hosts to be translated. Finally, enable the translation to occur. As with static NAT, you have to define which interface is internal and which interface is external:

```
RouterB(config)#ip nat pool cisco 216.1.1.1 216.1.1.14 netmask 255.255.255.240 (creates a NAT pool called cisco)
RouterB(config)#access-list 10 permit 192.168.10.0 0.0.0.255 (defines the IP addresses that will be translated)
RouterB(config)#ip nat inside source list 10 pool cisco (establishes dynamic translation of access list 10
  with the NAT pool named cisco)
```

Configuring PAT

To configure PAT, you first define an access list that permits the internal hosts to be translated. You then use the **ip nat inside source list** *access-list-number* **interface** *interface-type* **overload** global command, as follows:

```
RouterA>enable
RouterA#config term
RouterA(config)#acess-list 99 permit 10.0.0.1
RouterA(config)#ip nat inside source list 99 interface fa0/1 overload
RouterA(config)#interface ethernet 0
RouterA(config-if)#ip nat inside
RouterA(config-if)#exit
RouterA(config)#interface fa 0/1
RouterA(config-if)#ip nat ouside
RouterA(config-if)#exit
RouterA(config)#exit
```

 Please see page 311 for more details.

Verifying NAT and Resolving Translation Table Issues

The **clear ip nat translation *** command clears all dynamic translation tables.

The **clear ip nat translation inside global-ip local-ip** command clears a specific entry from a dynamic translation table.

The **clear ip nat translation outside local-ip global-ip** command clears a specific outside translation address.

The **show ip nat translations** command lists all active translations.

The **show ip nat statistics** command shows all translation statistics.

Transitioning to IPv6

IPv6 is an updated version of IP with the following features:

- Larger address space (128 bits)
- Simplified header
- Autoconfiguration
- Security with mandatory IPsec for all IPv6 devices
- Mobility
- Enhanced multicast support
- Extensions headers
- Flow labels

 Please see page 311 for more details.

- Improved address allocation
- Address aggregation

Although IPv6 has many advanced features, the primary reason for the move to IPv6 is because of the depletion of IPv4 addresses.

Format of IPv6 Addresses

IPv6 addresses are 128 bits long and are represented in eight 16-bit hexadecimal segments. An example of an IPv6 address is as follows:

2001:0D02:0000:0000:0000:C003:0001:F00D

Figure 8-3 shows the IPv6 address structure.

FIGURE 8-3
IPv6 Address Structure

Two rules for reducing the size of written IPv6 address are as follows:

- **Rule 1:** The leading 0s in any segment do not have to be written. If any segment has fewer than four hexadecimal digits, it is assumed that the missing digits are leading 0s. For example,

  2001:0D02:0000:0000:0000:C003:0001:F00D

  can be written as

  2001:D02:0:0:0:C003:1:F00D

 Please see page 311 for more details.

- **Rule 2:** Any single, consecutive fields of all 0s can be represented with a double colon (::). For example, 2001:D02:0:0:0:C003:1:F00D can be further reduced to

  2001:D02::C003:1:F00D

The double colon can only be used once.

Types of IPv6 Addresses

The three types of IPv6 addresses are as follows:

- **Unicast:** A global unicast address is an address that is globally unique and can be routed globally. Link-local unicast addresses are addresses that are confined to a single link.
- **Anycast:** An address that represents a service instead of a device. Features one-to-nearest mapping.
- **Multicast:** An address that identifies a set of devices. Features one-to-many mapping. Replicates IPv4 broadcast addresses.

Assigning IPv6 Addresses

IPv6 addresses can be assigned in one of the following ways:

- Statically
- Stateless autoconfiguration
- DHCPv6

In static assignment, the network administrator assigns an IPv6 address to a host.

 Please see page 311 for more details.

Hosts use stateless autoconfiguration by waiting for a router to advertise the local prefix. If the end system has a 64-bit MAC address, the host joins the prefix and its MAC address to form an IPv6 address. If the end system has a 48-bit MAC address, the host flips the global/local bit and inserts 0XFFEE in the middle of the MAC address. This is called the EUI-64 address, and it is joined to the prefix to form the IPv6 address.

DHCPv6 works that same way that DHCPv4 works.

Routing with IPv6

IPv6 supports the following routing protocols:

- Static
- RIPng
- OSPFv3
- EIGRP for IPv6
- IS-IS for IPv6
- MP-BGP

Static Routing

Static routing with IPv6 is configured the same way as with IPv4. However, IPv6 has one specific requirement: The router must be able to determine the link-local address of each neighboring router. In other words, do not use a global unicast address as a next-hop address when configuring IPv6 static routes.

 Please see page 311 for more details.

RIPng

RIPng is the IPv6 of RIP, a distance vector protocol. RIPng is defined in RFC 2080 and is based on RIPv2. RIPng uses hop count as its metric and has a maximum hop count of 15. However, some changes to RIPng include the following:

- Uses IPv6 for transport.
- Uses multicast group FF02::09 to advertise routes every 30 seconds.
- Updates are sent on UDP port 521.

OSPFv3

OSPFv3 is based on the current version of OSPF, which is version 2. Like version 2, OSPFv3 sends Hellos to neighbors, and exchanges LSAs and database descriptors (DBD). However, OSPFv3 runs directly over IPv6 and advertises using multicast groups FF02::5 and FF02::06, but uses its link-local address as the source address of its advertisements.

FF02::5 is the "all OSPF routers" address, and FF02::06 is the "all OSPF DRs" address.

OSPFv3 does not include authentication because authentication in IPv6 is handled through IPsec.

EIGRP for IPv6

EIGRP for IPv6 is the same EIGRP protocol as used with IPv4. It uses the same metric but includes a protocol-dependent module for IPv4 and IPv6.

Strategies for Implementing IPv6

Several strategies exist for migrating from IPv4 to IPv6. These strategies are called transition mechanisms, and they allow IPv4 hosts to communicate with IPv6 hosts. Three current IPv6 transition mechanisms are as follows:

 Please see page 311 for more details.

- **Dual stack:** A network interface that is configured with an IPv4 address and an IPv6 address
- **Tunneling:** Consists of encapsulating IPv6 packets within IPv4 packets
- **Proxying and translation:** A device that can translate IPv6 addresses to IPv4 addresses to communicate with IPv4 servers.

Configuring IPv6

IPv6 is not enabled by default on Cisco routers. The **ipv6 unicast-routing** global command enables IPv6 on the router.

The following are steps for configuring IPv6:

Step 1. Obtain IPv6 prefixes.

Step 2. Allocate IPv6 addresses to devices.

Step 3. Configure router interfaces.

Step 4. Configure tunnels (if communicating over an IPv4 network).

Step 5. Configure routing (static, RIPng, OSPF, EIGRP).

Step 6. Configure name servers.

The following example configures a router with IPv6, assigns an IPv6 address, configures a tunnel, enables RIPng, and configures a name server:

```
RouterA#config term
RouterA(config)#ipv6 unicast-routing
RouterA(config)#interface ethernet 0
RouterA(config-if)#ipv6 address 2001:0d02::2:0100/64
RouterA(config-if)#interface tunnel 0       (create the tunnel interface)
```

 Please see page 311 for more details.

```
RouterA(config-if)#ipv6 unnumbered ethernet 0    (identify the tunnel)
RouterA(config-if)#tunnel source ethernet 0       (configure tunnel source as e0)
RouterA(config-if)#tunnel desitnation 192.168.10.2    (the IPv4 address the tunnel terminates)
RouterA(config-if)#tunnel mode ipv6ip            (configure the tunnel mode as IPv6)
RouterA(config-if)#exit
RouterA(config)#ipv6 router rip cisco    (enable rip with the process called cisco)
RouterA(config-rtr)#interface s0
RouterA(config-if)#ipv6 rip cisco enable       (enable rip for the interface)
RouterA(config-if)#ip name-server 2001:d02::c003:1::f00d (enable name servers)
```

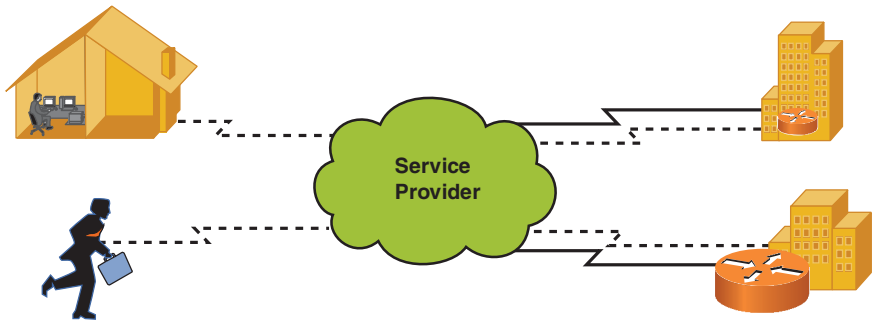
 Please see page 311 for more details.

Part IV: Extending the Network into the WAN

Section 9
Establishing Serial Point-to-Point Connections

WANs connect networks, users, and services across a broad geographic area. Companies use the WAN to connect company sites for information exchange (see Figure 9-1).

FIGURE 9-1
WAN Connections



Understanding Serial WAN Interfaces

WAN serial interfaces, defined as follows, are either synchronous or asynchronous:

- **Synchronous links** have identical frequencies and contain individual characters encapsulated in control bits, called start/stop bits, which designate the beginning and end of each character. Synchronous links try to use the same speed as the other end of a serial link. Synchronous transmission occurs on V.35 and other interfaces, where one set of wires carries data and a separate set of wires carries clocking for that data.

 Please see page 311 for more details.

- **Asynchronous links** send digital signals without timing. Asynchronous links agree on the same speed, but no check or adjustment of the rates occurs if they are slightly different. Only 1 byte per transfer is sent. Modems are asynchronous.

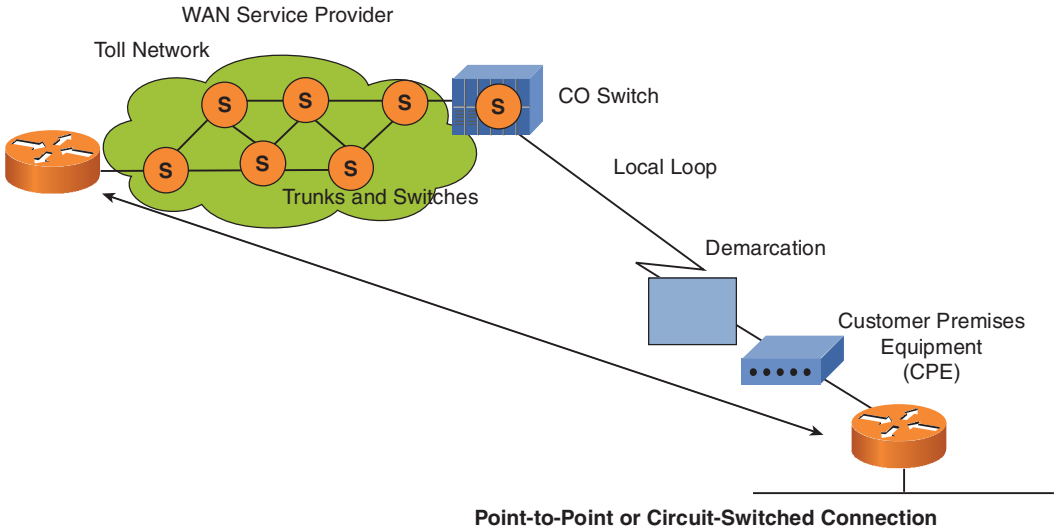
Serial interfaces are specified as DTE (data terminal equipment) or data communications equipment (DCE). DCE converts user data into the service provider's preferred format; in other words, DCEs provide clocking for the serial link. An example of a DCE is a channel service unit/data service unit (CSU/DSU) or a serial interface configured for clocking. The port configured as DTE requires external clocking from the CSU/DSU or other DCE device.

WAN Review

Figure 9-2 shows the typical WAN topology with explanations as follows:

- **Customer premises equipment (CPE):** Located on the subscriber's premises and includes both equipment owned by the subscriber and devices leased by the service provider.

FIGURE 9-2
Typical WAN Topology



 Please see page 311 for more details.

- **Demarcation (or demarc):** Marks the point where CPE ends and the local loop begins. Usually it is located in the telecommunications closet.
- **Local loop (or last mile):** The cabling from the demarc into the WAN service provider's central office.
- **Central office (CO):** A switching facility that provides a point of presence for WAN service. The central office is the entry point to the WAN cloud, the exit point from the WAN for called devices, and a switching point for calls.
- **Toll network:** A collection of trunks inside the WAN cloud.

WAN Connection Types

WAN services are generally leased from service providers on a subscription basis. The following three main types of WAN connections (services) exist:

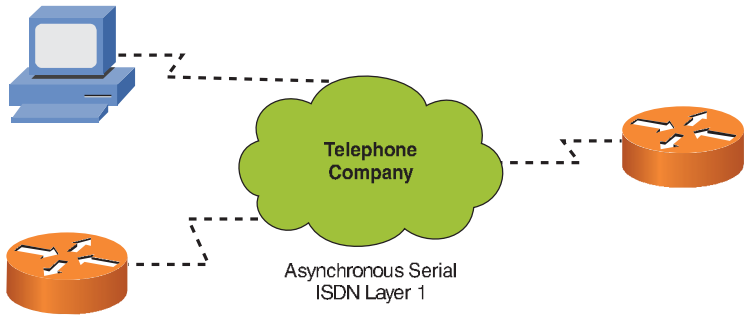
- **Leased-line:** A leased line (or point-to-point dedicated connection) provides a preestablished connection through the service provider's network (WAN) to a remote network. Leased lines provide a reserved connection for the client but are costly. Leased-line connections typically are synchronous serial connections.

FIGURE 9-3
Leased-Line WAN

- **Circuit-switched:** Circuit switching provides a dedicated circuit path between sender and receiver for the duration of the call. Circuit switching is used for basic telephone service or ISDN.

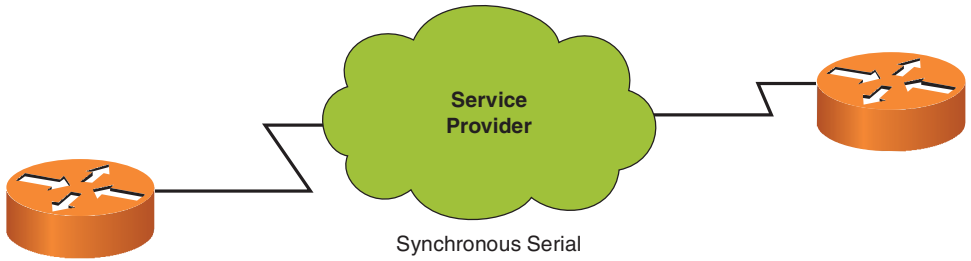
 Please see page 311 for more details.

FIGURE 9-4
Circuit-Switched WAN



- **Packet-switched:** With packet switching, devices transport packets using virtual circuits (VC) that provide end-to-end connectivity. Programmed switching devices provide physical connections. Packet headers identify the destination. Packet switching offers leased line–type services over shared lines, but at a much lower cost.

FIGURE 9-5
Packet-Switched WAN



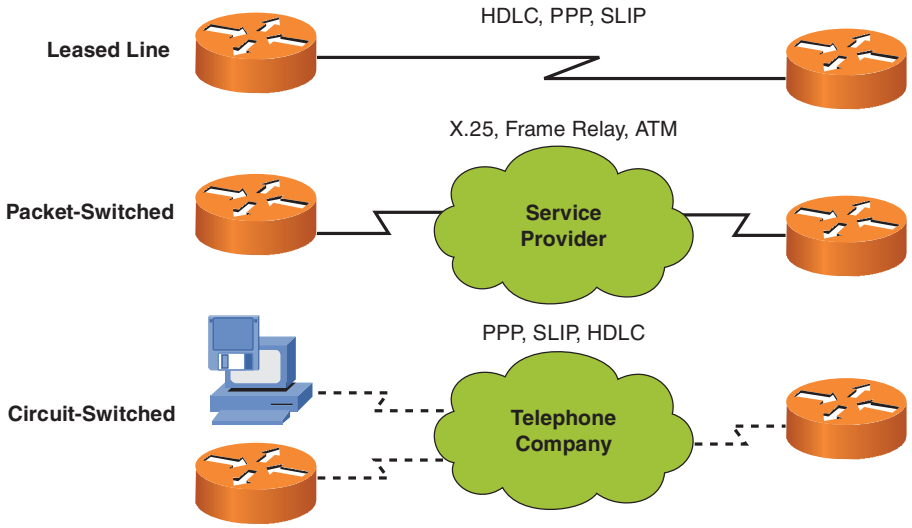
Layer 2 Encapsulation Protocols

- **High-Level Data Link Control (HDLC):** The default encapsulation type on point-to-point dedicated links and circuit-switched connections.

- **Point-to-Point Protocol (PPP):** Provides connections between devices over several types of physical interfaces, such as asynchronous serial, High-Speed Serial Interface (HSSI), ISDN, and synchronous. PPP works with many network layer protocols, including IP and IPX. PPP uses Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) for basic security.
- **Frame Relay:** Industry-standard switched data link layer protocol. Frame Relay (based on X.25) can handle multiple virtual circuits.
- **Asynchronous Transfer Mode (ATM):** International standard for cell relay using fixed-length (53-byte) cells for multiple service types. Fixed-length cells allow hardware processing, which greatly reduces transit delays. ATM takes advantage of high-speed transmission media such as E3, T3, and Synchronous Optical Network (SONET).

Figure 9-6 shows the typical WAN connections that each Layer 2 encapsulation protocol supports.

FIGURE 9-6
WAN Connection Support by Layer 2 Encapsulation Protocols



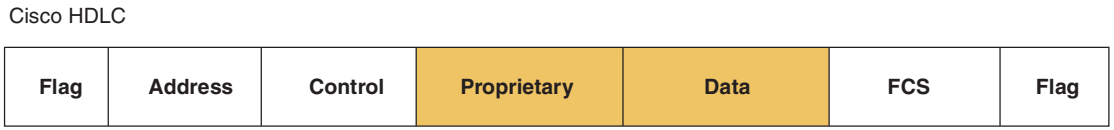
Configuring Serial Point-to-Point Encapsulation

Configuring HDLC

HDLC is a data-link protocol used on synchronous serial data links. HDLC cannot support multiple protocols on a single link, because it lacks a mechanism to indicate which protocol it is carrying.

The Cisco version of HDLC uses a proprietary field that acts as a protocol field. This field makes it possible for a single serial link to accommodate multiple network-layer protocols. Cisco HDLC is a point-to-point protocol that can be used on leased lines between two Cisco devices. PPP should be used when communicating with non-Cisco devices. Figure 9-7 shows the frame format of HDLC.

FIGURE 9-7
HDLC Frame Format



Because HDLC is the default encapsulation type on serial links, you don't need to configure HDLC. However, if the encapsulation type has been changed to another protocol, the following command changes the serial interface encapsulation back to HDLC:

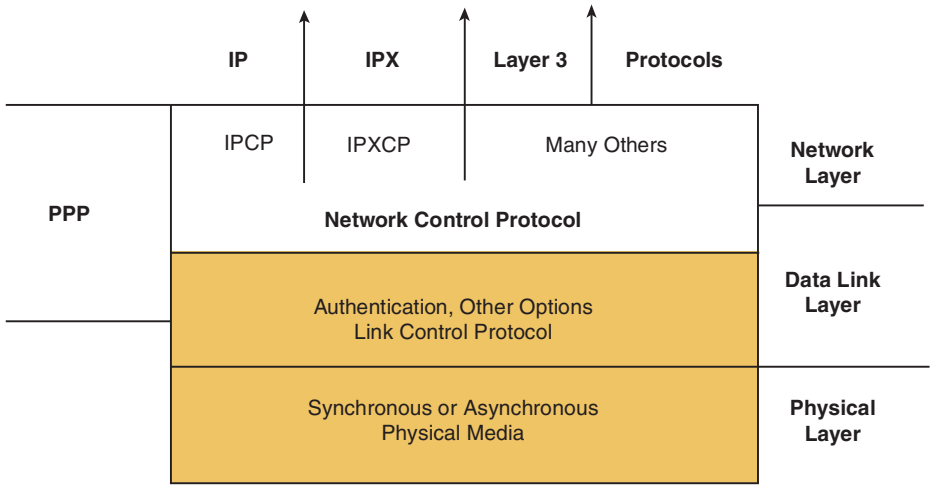
```
Router(config-if)#encapsulation hdlc
```

Configuring PPP

As shown in Figure 9-8, PPP uses a Network Control Protocol (NCP) component to encapsulate multiple protocols and the Link Control Protocol (LCP) to set up and negotiate control options on the data link.

 Please see page 311 for more details.

FIGURE 9-8
Point-to-Point Protocol



PPP Configuration Options

Cisco routers using PPP encapsulation include the LCP options shown in Table 9-1.

Table 9-1 PPP Configuration Options

Feature	How It Operates	Protocol
Authentication	Requires a password; performs challenge handshake	PAP, CHAP
Compression	Compresses data at the source; reproduces data at the destination	Stacker or Predictor
Error detection	Monitors data dropped on a link; avoids frame looping	Magic Number
Multilink	Load balancing across multiple links	Multilink Protocol (MP)

 Please see page 311 for more details.

Establishing a PPP Session

The three phases of PPP session establishment are link establishment, authentication, and the network protocol phase:

Step 1. **Link establishment:** Each PPP device sends LCP packets to configure and test the link (Layer 2).

Step 2. **Authentication phase (optional):** If authentication is configured, either PAP or CHAP is used to authenticate the link. This must take place before the network layer protocol phase can begin (Layer 2).

Step 3. **Network layer protocol phase:** PPP sends NCP packets to choose and configure one or more network layer protocols to be encapsulated and sent over the PPP data link (Layer 3).

Enabling PPP

To enable PPP encapsulation on a serial interface, enter the **encapsulation ppp** interface command, as follows:

```
RouterB(config-if)#encapsulation ppp
```

PPP Authentication Protocols

The two methods of authentication on PPP links are as follows:

- **Password Authentication Protocol (PAP):** The less-secure of the two methods. Passwords are sent in clear text and are exchanged only upon initial link establishment.
- **Challenge Handshake Authentication Protocol (CHAP):** Used upon initial link establishment and periodically to make sure that the router is still communicating with the same host. CHAP passwords are exchanged as MD5 hash values. CHAP uses a three-way handshake process to perform one-way authentication on a PPP serial interface.

 Please see page 311 for more details.

Configuring PPP Authentication

The three steps to enable PPP authentication on a Cisco router are as follows:

Step 1. Make sure that each router has a host name assigned to it using the **hostname** command.

Step 2. On each router, define the username of the remote router and password that both routers will use with the **username** *remote-router-name* **password** *password* command.

Step 3. Configure PPP authentication with the **ppp authentication** {**chap | chap pap | pap chap | pap**} interface command. (If both PAP and CHAP are enabled, the first method you specify in the command is used. If the peer suggests the second method or refuses the first method, the second method is used.)

The following commands configure CHAP and PAP for authentication with the password of cisco. The remote router's host name is RouterA:

```
RouterB(config)#hostname RouterB
RouterB(config)#username RouterA password cisco
RouterB(config)#int s0
RouterB(config-if)#ppp authentication chap pap
```

Verifying the Serial Encapsulation Configuration

The **show interface** *interface-number* command, as follows, shows the encapsulation type configured on the router's serial interface and the LCP and NCP states of an interface if PPP encryption is enabled:

```
RouterA#show int s0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

 Please see page 311 for more details.

```
 Encapsulation PPP, loopback not set, keepalive set (10sec)
 LCP Open
 Open: IPCP, CDPCP
 Last input 00:00:02, output 00:00:02, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0 (size/max/drops); Total output drops: 0
(text omitted)
```

 Please see page 311 for more details.

Section 10
Establishing Frame Relay Connections

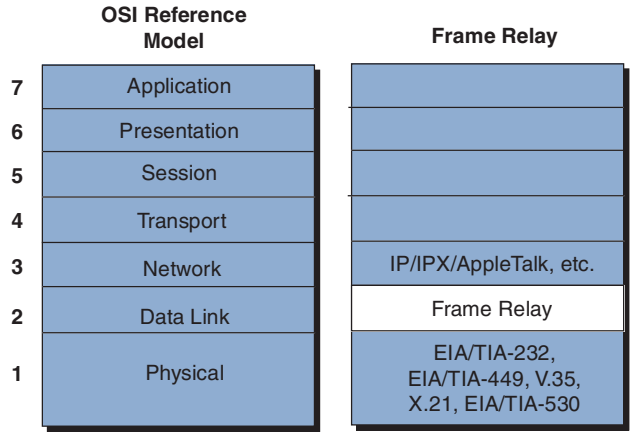
Frame Relay is a connection-oriented Layer 2 protocol that allows several data connections (virtual circuits) to be multiplexed onto a single physical link. Frame Relay relies on upper-layer protocols for error correction. Frame Relay specifies only the connection between a router and a service provider's local access switching equipment.

A connection identifier maps packets to outbound ports on the service provider's switch. When the switch receives a frame, a lookup table maps the frame to the correct outbound port. The entire path to the destination is determined before the frame is sent.

Frame Relay Stack

As Figure 10-1 shows, the bulk of Frame Relay functions exist at the lower two layers of the OSI reference model. Frame Relay is supported on the same physical serial connections that support point-to-point connections. Cisco routers support the EIA/TIA-232, EIA/TIA-449, V.35, X.21, and EIA/TIA-530 serial connections. Upper-layer information (such as IP data) is encapsulated by Frame Relay and is transmitted over the link.

FIGURE 10-1
Frame Relay Functions at Layer 1 and 2 of the OSI Reference Model



 Please see page 311 for more details.

Frame Relay Terminology

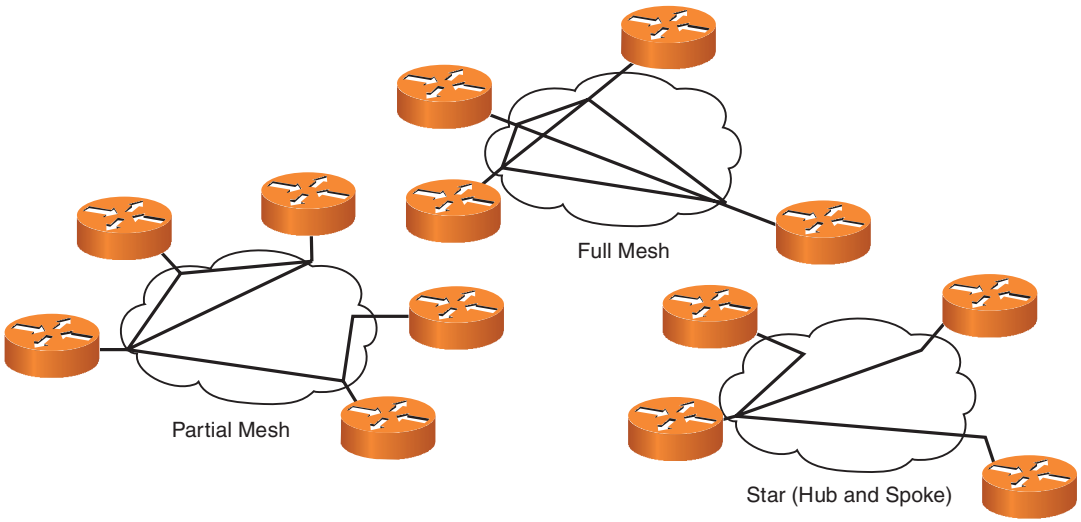
- **VC (virtual circuit):** A logical circuit between two network devices. A VC can be a permanent virtual circuit (PVC) or a switched virtual circuit (SVC). PVCs save bandwidth (no circuit establishment or teardown) but can be expensive. SVCs are established on demand and are torn down when transmission is complete. VC status can be active, inactive, or deleted. Today, most Frame Relay circuits are PVCs.
- **DLCI (data-link connection identifier):** Identifies the logical connection between two directly connected sets of devices. The DLCI is locally significant.
- **CIR (committed information rate):** The minimum guaranteed data transfer rate agreed to by the Frame Relay switch.
- **Inverse ARP (Inverse Address Resolution Protocol):** Routers use Inverse ARP to discover the network address of a device associated with a VC.
- **LMI (Local Management Interface):** A signaling standard that manages the connection between the router and the Frame Relay switch. LMIs track and manage keepalive mechanisms, multicast messages, and status. LMI is configurable (in Cisco IOS Software Release 11.2 and later), but routers can autosense LMI types by sending a status request to the Frame Relay switch. The router configures itself to match the LMI type response. The three types of LMIs supported by Cisco Frame Relay switches are Cisco (developed by Cisco, StrataCom, Northern Telecom, and DEC), ANSI Annex D (ANSI standard T1.617), and q933a (ITU-T Q.933 Annex A).
- **FECN (forward explicit congestion notification):** A message sent to a destination device when a Frame Relay switch senses congestion in the network.
- **BECN (backward explicit congestion notification):** A message sent to a source router when a Frame Relay switch recognizes congestion in the network. A BECN message requests a reduced data transmission rate.

 Please see page 311 for more details.

Frame Relay Topologies

Frame Relay networks can be designed using star, full-mesh, and partial-mesh topologies. Figure 10-2 shows the three topologies in Frame Relay.

FIGURE 10-2
Frame Relay Topologies



A star topology, also known as a hub-and-spoke configuration, is the common network topology. Remote sites are connected to a central site, which usually provides services. Star topologies require the fewest PVCs, making them relatively inexpensive. The hub router provides a multipoint connection using a single interface to interconnect multiple PVCs.

In a full-mesh topology, all routers have virtual circuits to all other destinations. Although it is expensive, this method provides redundancy, because all sites are connected to all other sites. Full-mesh networks become very expensive as the number of nodes increases. The number of links required in a full-mesh topology that has n nodes is $[n * (n - 1)]/2$.

 Please see page 311 for more details.

In a partial-mesh topology, not all sites have direct access to all other sites. Connections usually depend on the traffic patterns within the network.

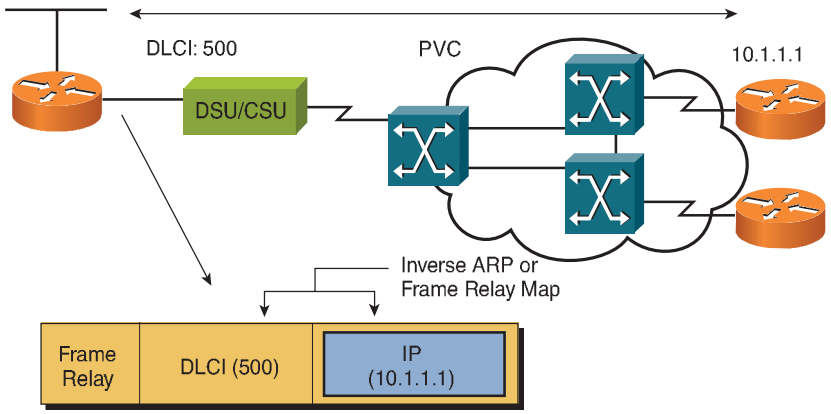
By default, a Frame Relay network provides nonbroadcast multiaccess (NBMA) connectivity between remote sites. An NBMA environment is treated like other broadcast media environments, such as Ethernet, where all the routers are on the same subnet.

However, to reduce costs, NBMA clouds are usually built in a hub-and-spoke topology. With this topology, the physical network does not provide the multiaccess capabilities that Ethernet does, so each router might not have a separate PVC to reach the other remote routers on the same subnet. When running Frame Relay with multiple PVCs over a single interface, you can encounter split horizon when running a routing protocol.

Frame Relay Address Mapping

Because Frame Relay is an NBMA, it needs to have a way to map Layer 2 information with Layer 3. In typical multiaccess networks, broadcasts perform this functionality. Because Frame Relay is nonbroadcast, another mechanism is needed. To correctly route packets, each DLCI must be mapped to a next-hop address. These addresses can be manually configured or dynamically mapped using Inverse ARP. After the address is mapped, it is stored in the router's Frame Relay map table. Figure 10-3 shows how Inverse ARP maps a DLCI to an IP address.

FIGURE 10-3
Inverse ARP Maps DLCIs to IP Addresses



 Please see page 311 for more details.

LMI Signaling Process

1. The router connects to a Frame Relay switch through a channel service unit/data service unit (CSU/DSU).
2. The router sends a VC status inquiry to the Frame Relay switch.
3. The switch responds with a status message that includes DLCI information for the usable PVCs.
4. The router advertises itself by sending an Inverse ARP to each active DLCI.
5. The routers create map entries with the local DLCI and network layer address of the remote routers. Static maps must be configured if Inverse ARP is not supported.
6. Inverse ARP messages are sent every 60 seconds.
7. LMI information is exchanged every 10 seconds.

How Service Providers Map Frame Relay DLCIs

DLCIs are numbers that identify the logical connection between the router and the Frame Relay switch. The DLCI is the Frame Relay Layer 2 address, and it is locally significant. DLCIs are usually assigned by the Frame Relay service provider. A Frame Relay router learns about a remote router's DLCI by either Inverse ARP (which is automatically enabled on Cisco routers) or by static mappings.

Configuring Frame Relay

The three commands used to configure basic Frame Relay on a router select the Frame Relay encapsulation type, establish the LMI connection, and enable Inverse ARP. The commands used are as follows:

```
encapsulation frame-relay [cisco | ietf]
frame-relay lmi-type {ansi | cisco | q933i}
frame-relay inverse-arp [protocol] [dlci]
```

 Please see page 311 for more details.

Configuring Basic Frame Relay

```
RouterA>enable
RouterA#config term
RouterA(config)#int ser 1
RouterA(config-if)#ip address 10.16.0.1  255.255.255.
RouterA(config-if)#encapsulation frame-relay cisco
RouterA(config-if)#frame-relay lmi-type   cisco
RouterA(config-if)#bandwidth 64
RouterA(config-if)#frame-relay inverse-arp ip 16
RouterA(config-if)#exit
RouterA(config)#exit
RouterA#
```

Configuring a Static Frame Relay Map

A router's address-to-DLCI table can be defined statically when Inverse ARP is not supported. These static maps can also be used to control broadcasts. To statically configure the map table, use the following command:

frame-relay *map protocol protocol-address dlci* **[broadcast] [ietf | cisco | payload-compress packet-by-packet]**

where:

- *protocol* specifies bridging or logical link control.
- **broadcast** is an optional parameter that controls broadcasts and multicasts over the VC.
- **payload-compress** is an optional Cisco-proprietary compression method.

The **frame interface** *dlci* command also statically maps a local DLCI to a configured Layer 3 protocol on a subinterface. The difference is that map statements are used in multipoint Frame Relay configurations and the **frame interface** *dlci* command is used in point-to-point subinterface configurations.

 Please see page 311 for more details.

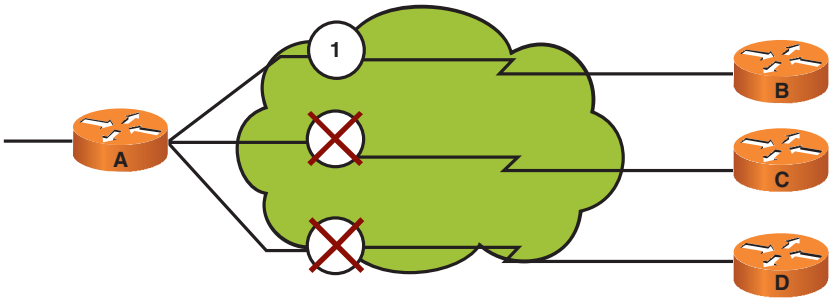
Resolving Reachability Issues in Frame Relay

In any Frame Relay topology, when a single interface must be used to interconnect multiple sites, you can have reachability issues because of the NBMA nature of Frame Relay.

Two problems that the Frame Relay NBMA topology can cause are routing update problems because of split horizon and broadcast replications issues.

In Figure 10-4, Router A receives a routing update from Router B. Because Router A received the update on its serial interface, and because of the split horizon rule, Router A cannot send the updated route information to Routers C and D, causing Routers C and D to not learn about Router B.

FIGURE 10-4
Frame Relay Reachability Issues



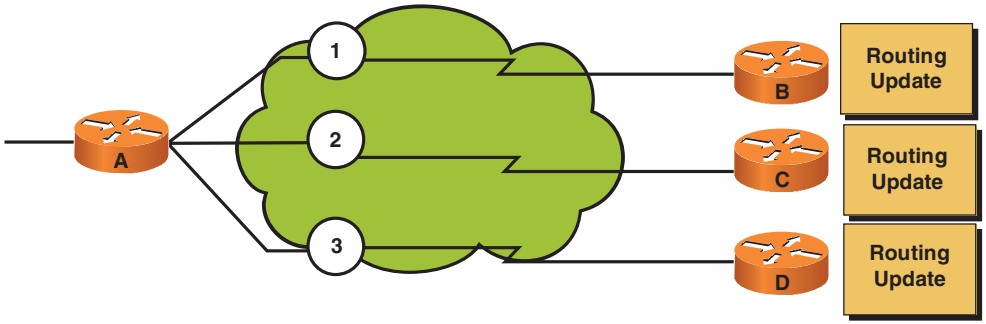
These reachability issues can be solved by disabling split horizon or configuring subinterfaces on the router.

Disabling split horizon increase the chances of routing loops in a network. The best option is to configure subinterfaces. These logically assigned interfaces let the router forward broadcast updates in a Frame Relay network.

 Please see page 311 for more details.

As Figure 10-5 shows, subinterfaces are logical subdivisions of a physical interface. Routing updates received on one subinterface can be sent out another subinterface without violating split horizon rules. By configuring virtual circuits as point-to-point connections, the subinterface acts similar to a leased line. It is also possible (and sometimes recommended) to turn off split horizon to solve this problem.

FIGURE 10-5
Subinterface Example



Configuring Subinterfaces

To enable Frame Relay on a subinterface, you must remove the IP address from the primary interface with the **no ip address** *ip-address subnet-mask* interface command, enable Frame Relay encapsulation on the serial interface, and then configure each subinterface with the IP address.

Subinterfaces can be configured as either point-to-point or multipoint.

With point-to-point configuration, one PVC connection is established with another physical interface or subinterface on a remote router using a single subinterface. In other words, each point-to-point subinterface is a different subnet.

With multipoint configuration, multiple PVC connections are established with multiple physical interfaces or subinterfaces on remote routers on a single subinterface. All interfaces involved use the same subnet, and each interface has its own local DLCI.

 Please see page 311 for more details.

To select a subinterface, use the following command:

```
interface serial-number.subinterface-number {multipoint | point-to-point}
```

To configure a subinterface, use the following command:

```
frame-relay interface-dlci dlci-number
```

The range of subinterface numbers is 1 to 4,294,967,293. The number that precedes the period (.) must match the physical interface number to which this subinterface belongs.

The *dlci-number* option binds the local DLCI to the Layer 3 protocol configured on the subinterface, as evidenced by the **show frame-relay map** command. This is the only way to link an LMI-derived PVC to a subinterface (LMI does not know about subinterfaces).

Configuring Point-to-Point Subinterfaces

To configure point-to-point subinterfaces, enter the following sample commands:

```
West-SD(config-if)#no ip address 192.168.1.5 255.255.255.0
West-SD(config-if)#encap frame-relay
West-SD(config-if)#int s0.1 point-to-point
West-SD(config-if)#ip address 192.168.1.5 255.255.255.0
West-SD(config-if)#frame-relay interface-dlci 10
West-SD(config-if)#int s0.2 point-to-point
West-SD(config-if)#ip address 192.168.2.5 255.255.255.0
West-SD(config-if)#frame-relay interface-dlci 20
```

Configuring Multipoint Subinterfaces

To configure multipoint subinterfaces, enter the following sample commands:

```
West-SD(config-if)#no ip address 192.168.1.5 255.255.255.0
```

 Please see page 311 for more details.

```
West-SD(config-if)#encap frame-relay
West-SD(config-if)#int s0.1 multipoint
West-SD(config-if)#ip address 192.168.1.5 255.255.255.0
West-SD(config-if)#frame-relay interface-dlci 10
```

Verifying Frame Relay

You can use the following commands to verify and display Frame Relay information:

- **show interface:** Displays Layer 1 and Layer 2 status, DLCI information, and the LMI DLCIs used for the local management interface.
- **show frame-relay lmi:** Displays LMI traffic statistics (LMI type, status messages sent, and invalid LMI messages).
- **show frame-relay pvc:** Displays the status of all configured connections, traffic statistics, and BECN and FECN packets received by the router.
- **show frame-relay map:** Displays the current map entries for static and dynamic routes. The **frame-relay-inarp** command clears all dynamic entries.

Troubleshooting Frame Relay

The **show interface** command provides a wealth of information for troubleshooting Frame Relay. What follows are different examples of output from the **show interface** command and possible reasons for the Frame Relay link failures:

```
RouterA#show int s0
Serial0 is down, line protocol is down
  Hardware is HD64570
  Internet address is 192.168.1.2/24
```

 Please see page 311 for more details.

If the **show interface** command shows that the interface is down and the line protocol is down, the error is at the physical layer. This means that the problem is with the cable, the CSU/DSU, or the serial line. To troubleshoot the problem, perform the following:

- Check the cable to make sure that it is a DTE serial cable and that the cables are securely attached.
- If the cable is correct, try a different serial port.
- If the cable does not work on the second port, try replacing the cable. If replacing the cable does not work, the problem lies with your carrier.

```
RouterA#show int s0
Serial0 is up, line protocol is down
  Hardware is HD64570
  Internet address is 192.168.1.2/24
```

In the preceding example, the line is up but the line protocol is down. This means that the router is getting carrier signal from the CSU/DSU, and the problem is with the data link layer. Causes for the line protocol being down include the following:

- Frame Relay provider not activating its port
- LMI mismatch
- Encapsulation mismatch
- DLCI is inactive or has been deleted

 Please see page 311 for more details.

Section 11
Introducing VPN Solutions

What Is a VPN?

Virtual Private Networks (VPN) provide an Internet-based WAN infrastructure of connecting branch offices, home offices, and telecommuters to the network. In other words, VPNs allow office locations and remote users to interconnect with each other, securely through the Internet. After they are connected through the secure VPN connection, the interconnected networks become part of the network as if they were connected through a leased line such as a classic WAN link.

Benefits of VPNs

VPNs provide the following benefits:

- **Cost savings:** VPNs enable organizations to use the Internet to interconnect offices.
- **Security:** VPNs use advanced encryption and authentication protocols to protect data from unauthorized access.
- **Scalability:** Because VPNs use the Internet, adding new users or organizations is easily done without changing the organization's network infrastructure.

Types of VPNs

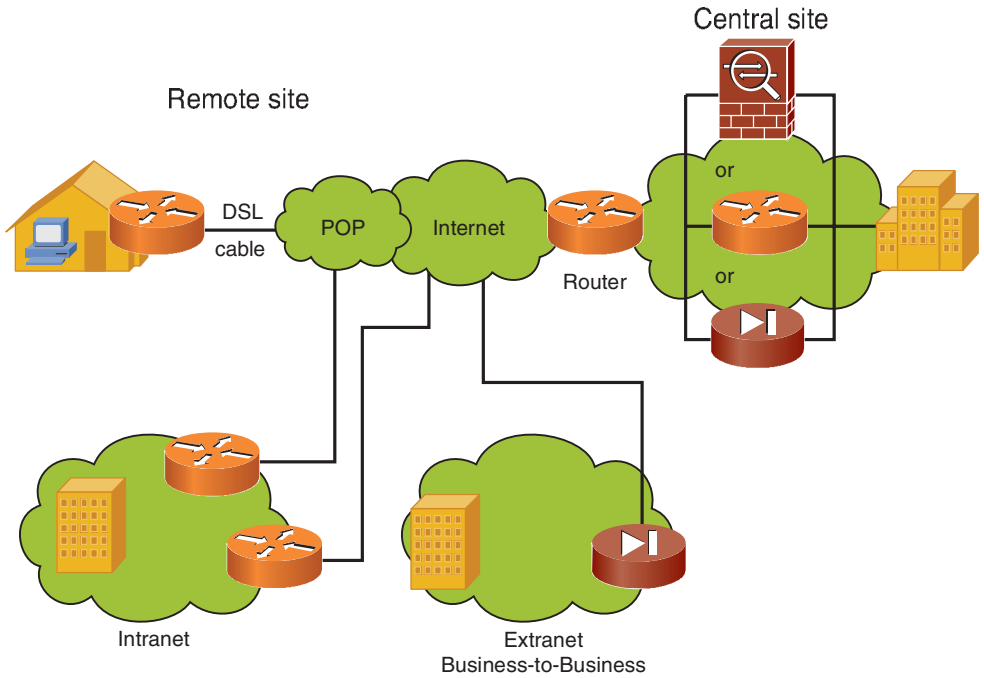
The following two types of VPN networks exist:

- Site-to-site
- Remote access

 Please see page 311 for more details.

Site-to-site VPNs are an extension of a classic WAN network. They connect entire networks to each other. All traffic is sent and received through a VPN "gateway." The VPN gateway is responsible for encapsulating and encrypting outbound traffic for all traffic from a particular site to the destination site. The destination VPN gateway decrypts the traffic and forwards it to the private network. A VPN gateway can be a router, a firewall, a VPN concentrator, or a Cisco ASA series adaptive security appliance. Figure 11-1 shows an example of a site-to-site VPN.

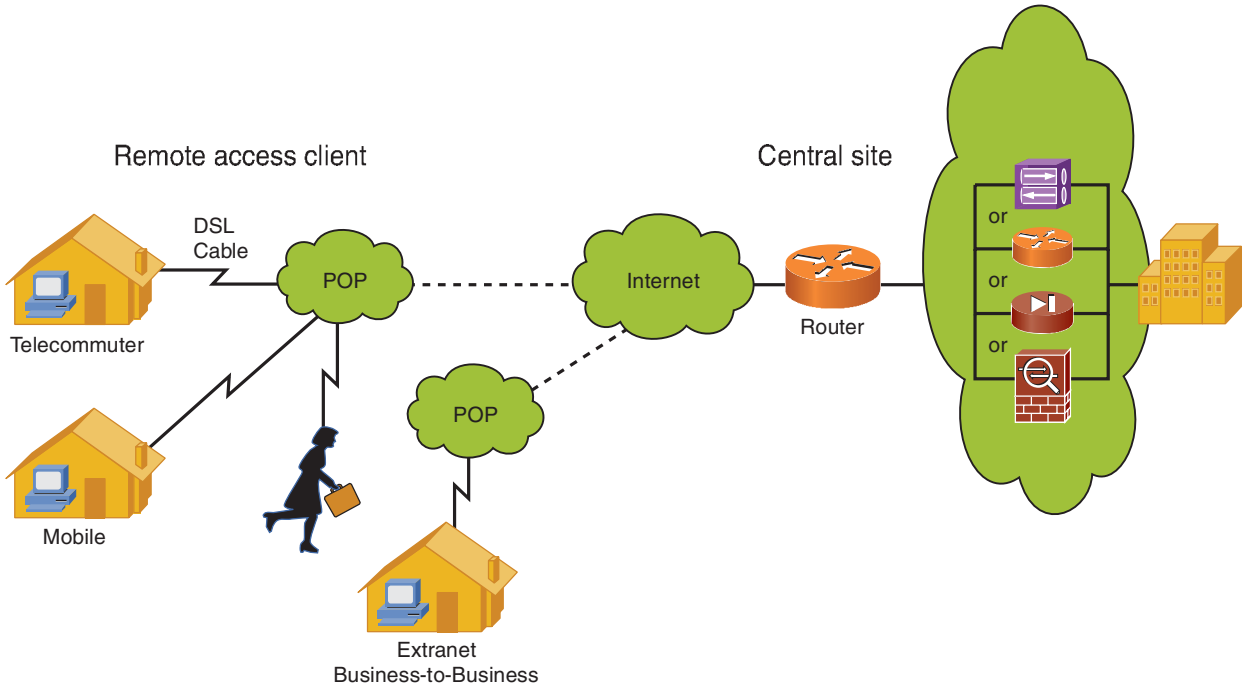
FIGURE 11-1
Site-to-Site VPN



Remote-access VPNs are used for telecommuters, mobile users, and extranet traffic. They connect individual hosts' security to the company private network. Remote VPNs can use any Internet-based medium to connect to the VPN, and each host connects through VPN client software. Figure 11-2 shows an example of remote-access VPNs.

 Please see page 311 for more details.

FIGURE 11-2
Remote-Access VPNs



Cisco Easy VPN

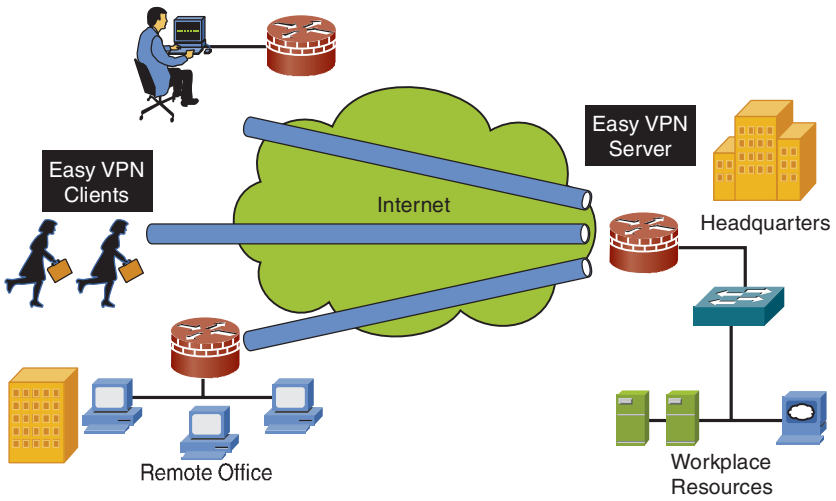
Cisco Easy VPN is a cost-effective solution for deploying VPNs that is ideal for remote offices that have little IT support.

As shown in Figure 11-3, two components of Cisco Easy VPN exist:

- Cisco Easy VPN Server
- Cisco Easy VPN Remote

 Please see page 311 for more details.

FIGURE 11-3
Cisco Easy VPN Components



The VPN server is a dedicated VPN gateway like a Cisco VPN concentrator, Cisco PIX firewall, Cisco ASA adaptive security appliance, or a Cisco IOS router. The VPN server can terminate VPN tunnels initiated by mobile and remote workers running Cisco VPN client software. It also terminates VPN tunnels in site-to-site VPNs.

The Cisco VPN remote enables Cisco IOS routers, PIX firewalls, Cisco ASA appliances, and Cisco VPN hardware clients to receive security polices from a Cisco Easy VPN server to minimize VPN configuration requirements at remote locations.

Cisco IOS IPsec/SSL VPNs

Cisco IOS IPsec/SSL–based VPNs, or WebVPNs, provide remote-access connectivity from almost any Internet-enabled location using a web browser and its native SSL encryption. A WebVPN does not require client software to be installed on the endpoint host.

Because no client software is needed, WebVPNs allow an organization to extend secure remote access to almost any Internet-enabled host.

 Please see page 311 for more details.

VPN Components

The hardware and software components that usually make up a VPN are as follows:

- Cisco VPN-enabled IOS routers
- Cisco ASA adaptive security appliances
- VPN clients

Introducing IPsec

IPsec is an industry-standard protocol that acts at the network layer, protecting and authenticating IP packets between IPsec peers (devices). IPsec secures a path between a pair of gateways, a pair of hosts, or a gateway and a host.

IPsec is not bound to any specific encryption or authentication algorithm, keying or technology, or security algorithms, thus allowing IPsec to support newer and better algorithms.

IPsec provides the following four functions:

- **Confidentiality (encryption):** Packets are encrypted before being transmitting across a network.
- **Data integrity:** The receiver can verify that the transmitted data was not altered or changed. This is done through checksums.
- **Authentication:** Ensures that the connection is made with the desired communication partner.
- **Antirelay protection:** Verifies that each packet is unique and not duplicated. This is done by comparing the sequence number of the received packets with a sliding window to the destination host or gateway.

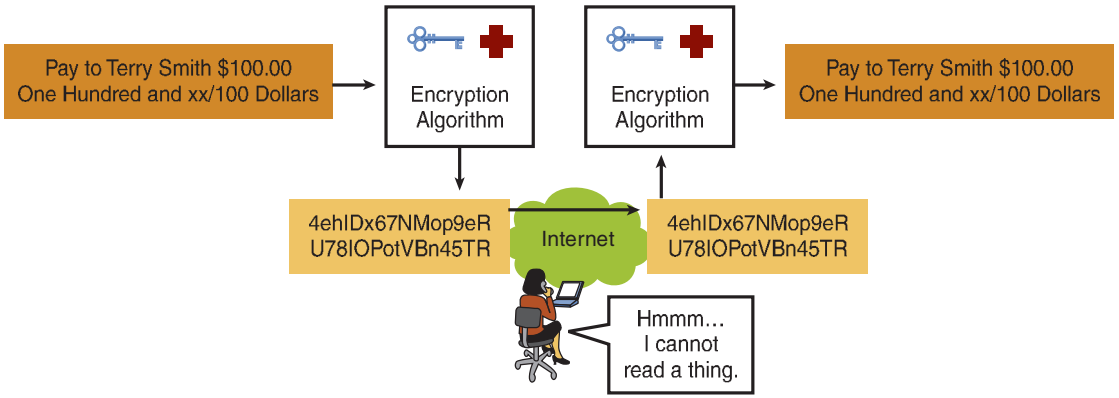
 Please see page 311 for more details.

Confidentiality

IPsec provides confidentiality by encrypting the data. The data is digitally scrambled, rendering it unreadable.

As shown in Figure 11-4, for encryption to work, both the sender and receiver must know the rules to transform the original message into its coded form. These rules are based on an algorithm.

FIGURE 11-4
Encryption Confidentiality



Encryption Algorithms

Encryption rules are based on an algorithm and key. The degree of security depends on the length of the key of the encryption algorithm; the shorter the key, the easier it is to break. IPsec supports the following encryption algorithms:

- **Data Encryption Standard (DES):** Uses a 56-bit key that ensures high-performance encryption. Uses a symmetric key cryptosystem.
- **Triple DES (3DES):** A variant of DES that breaks data into 64-bit blocks. 3DES then processes each block three times, each time with an independent 56-bit key, thus providing signification encryption strength over DES. Uses a symmetric key cryptosystem.

 Please see page 311 for more details.

- **Advanced Encryption Standard (AES):** Provides stronger encryption than DES and is more efficient than 3DES. Key lengths can be 128-, 192-, and 256-bit keys.

Diffie-Hellman Key Exchange

Encryption algorithms such as DES and 3DES require a symmetric shared secret key to perform encryption and decryption. The Diffie-Hellman (DH) Key Exchange is a public key exchange that exchanges symmetric shared secret keys used for encryption and decryption over an insecure channel.

Data Integrity

To ensure data integrity, IPsec uses a data integrity algorithm that adds a hash to the message. The hash guarantees the integrity of the original message. If the transmitted hash matches the received hash, the message has not been tampered with.

The data integrity algorithm is called the Hash-based Message Authentication Code (HMAC). HMAC is a type of message authentication code that uses a cryptographic hash function in combination with a secret key. Two common HMAC algorithms used by IPsec are as follows:

- **HMAC - Message Digest Algorithm 5 (MD5):** Uses a 128-bit shared secret key. The message and 128-bit shared secret key are combined and run through the MD5 hash algorithm, producing a 128-bit hash. This hash is added to the original message and forwarded to the remote host.
- **HMAC - Secure Hash Algorithm-1 (SHA-1):** Uses a 160-bit secret key. The message and 160-bit shared secret key are combined and run through the SHA-1 hash algorithm, producing a 160-bit hash. This hash is added to the original message and forwarded to the remote host.

 Please see page 311 for more details.

Authentication

In a VPN, before a communication path is considered secure, the end devices must be authenticated. The two peer authentication methods are as follows:

- **Pre-Shared Keys (PSK):** Pre-Shared Keys are a secret key value entered into each peer manually that authenticates the peer.
- **Rivest, Shamir, and Adelman (RSA) signatures:** RSA signatures use the exchange of digital certifications to authenticate the peers.

IPsec Protocol Framework

IPsec is a framework of open standards that spells out the rules for secure communications. To do this, IPsec relies on existing algorithms to implement encryption, authentication, and key exchange. As shown in Figure 11-5, the two main IPsec framework protocols are as follows:

- **Authentication Header (AH):** AH provides authentication and data integrity for IPsec using the authentication and data integrity algorithms. AH does not encrypt packets and, used alone, provides weak protection. As such, AH can be used with ESP to provide data encryption and tamper-aware security features.
- **Encapsulation Security Protocol (ESP):** ESP provides encryption, authentication, and integrity. ESP encrypts the IP packet and the ESP header, thus concealing the data payload and the identities of the source and destination.

 Please see page 311 for more details.

FIGURE 11-5
IPsec Framework Protocols

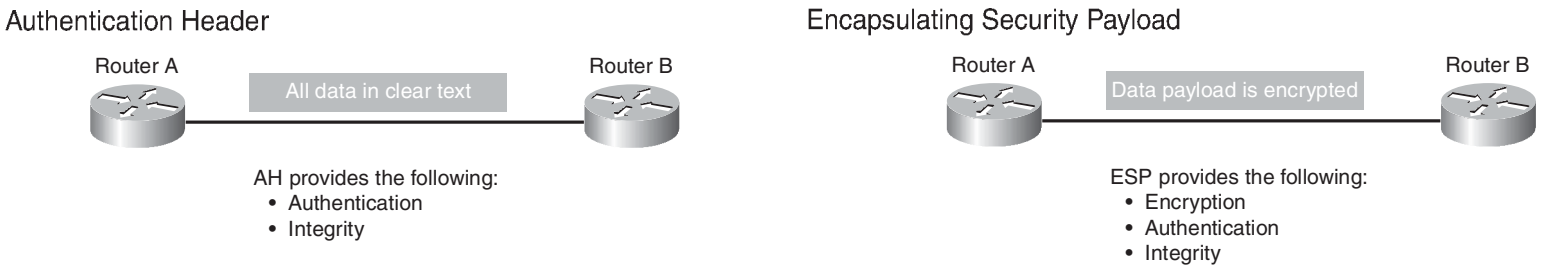
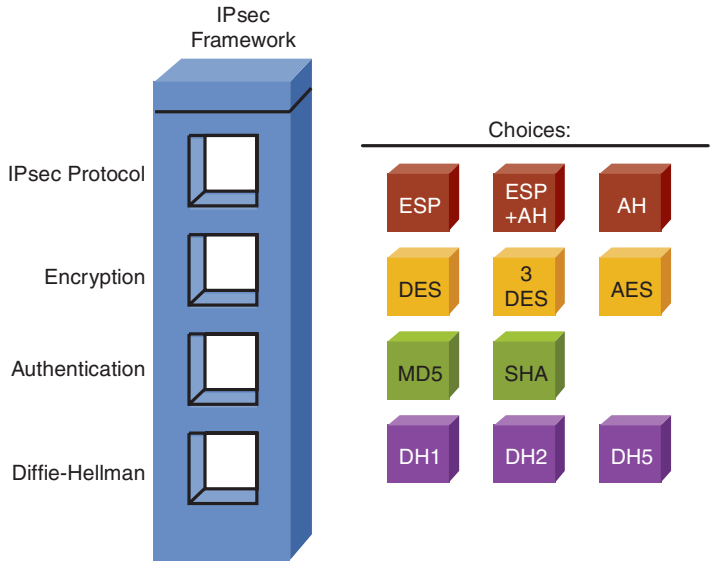


Figure 11-6 shows the standard algorithms that IPsec uses.

FIGURE 11-6
IPsec Framework and Authentication Protocols



CCNA Quick Reference Sheets

Eric Rivard
Jim Doherty

Published by:
Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240 USA

First Digital Edition July 2007

ISBN-10: 1-58705-460-4

ISBN-13: 978-1-58705-460-0

Warning and Disclaimer

This digital Short Cut is designed to provide information about the CCNA exam. Every effort has been made to make this digital Short Cut as complete and accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this digital Short Cut.

The opinions expressed in this digital Short Cut belong to the authors and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this digital Short Cut that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this digital Short Cut should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical Short Cuts of the highest quality and value. Each Short Cut is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members of the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments on how we could improve the quality of this digital Short Cut, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@cisco-press.com. Please be sure to include the digital Short Cut title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

The publisher offers excellent discounts on this digital Short Cut when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com.

For sales outside the United States please contact: **International Sales** international@pearsoned.com

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.