

# CCNA Notes

## Introduction







Cisco offers two options for obtaining the CCNA certification:





- Pass Exam 640-802 OR
- Pass Exam 640-822 AND Exam 640-816

While you can use these notes to prepare for either exam, the notes are geared towards passing the single exam. I recommend you study all of the material and take the single exam option rather than taking two exams.

### **Cisco Device Icons**

- The following table lists the specific icons Cisco uses to represent network devices and connections.

Icon	Represents
	Hub
	Bridge
	Switch
	Router
	Access point
	Network cloud

	Ethernet connection
	Serial Line connection
	Wireless connection
	Virtual Circuit

## The OSI Model

As you study this section, answer the following questions:

- What is the OSI model and why is it important in understanding networking?
- How does the third OSI model layer relate to administering routers?
- Which OSI model layer is concerned with MAC addresses?
- What protocols correspond to the Presentation and Session layers?
- What is the difference between the TCP and UDP protocols?
- What is the EIA/TIA 232 protocol concerned with?

This section covers the following exam objectives:

- 103. Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network
- 105. Describe the purpose and basic operation of the protocols in the OSI and TCP models
- 110. Identify and correct common network problems at layers 1, 2, 3 and 7 using a layered model approach

### **OSI Model Facts**

The OSI model classifies and organizes the tasks that hosts perform to prepare data for transport across the network. You should be familiar with the OSI model because it is the most widely used method for understanding and talking about network communications. However, remember that it is only a theoretical model that defines standards for programmers and network administrators, not a model of actual physical layers.

Using the OSI model to discuss networking concepts has the following advantages:

- Provides a common language or reference point between network professionals
- Divides networking tasks into logical layers for easier comprehension
- Allows specialization of features at different levels
- Aids in troubleshooting
- Promotes standards interoperability between networks and devices
- Provides modularity in networking features (developers can change features without changing the entire approach)

However, you must remember the following limitations of the OSI model.

- OSI layers are theoretical and do not actually perform real functions.
- Industry implementations rarely have a layer-to-layer correspondence with the OSI layers.
- Different protocols within the stack perform different functions that help send or receive the overall message.
- A particular protocol implementation may not represent every OSI layer (or may spread across multiple layers).

To help remember the layer names of the OSI model, try the following mnemonic devices:

Layer	Name	Mnemonic (Bottom to top)	Mnemonic (Top to bottom)
<b>Layer 7</b>	Application	Away	All
<b>Layer 6</b>	Presentation	Pizza	People
<b>Layer 5</b>	Session	Sausage	Seem

<b>Layer 4</b>	Transport	Throw	To
<b>Layer 3</b>	Network	Not	Need
<b>Layer 2</b>	Data Link	Do	Data
<b>Layer 1</b>	Physical	Please	Processing

Have some fun and come up with your own mnemonic for the OSI model, but stick to just one so you don't get confused.

### Lower OSI Layer Facts

The following table summarizes basic characteristics of the lower OSI model layers.

Layer	Description
Physical	<p>The Physical layer of the OSI model sets standards for sending and receiving electrical signals between devices. It describes how digital data (bits) are converted to electric pulses, radio waves, or pulses of lights.</p> <p>Devices that operate at the physical layer send and receive a stream of bits.</p>
Media Access Control (MAC)	<p>The Media Access Control (MAC) layer defines specifications for controlling access to the media. The MAC sublayer is responsible for:</p> <ul style="list-style-type: none"> <li>• Adding frame start and stop information to the packet</li> <li>• Adding Cyclical Redundancy Check (CRC) for error checking</li> <li>• Converting frames into bits to be sent across the network</li> <li>• Identifying network devices and network topologies in preparation for media transmission</li> <li>• Defining an address (such as the MAC address) for each physical device on the network</li> <li>• Controlling access to the transmission medium</li> </ul>
Data Link	<p>The Logical Link Control (LLC) layer provides an interface between the MAC layer and upper-layer protocols. LLC protocols are defined by the IEEE 802.2 committee. The LLC sublayer is responsible for:</p> <ul style="list-style-type: none"> <li>• Maintaining orderly delivery of frames through sequencing</li> <li>• Controlling the flow or rate of transmissions using the following: <ul style="list-style-type: none"> <li>○ <a href="#">Acknowledgements</a></li> <li>○ <a href="#">Buffering</a></li> <li>○ <a href="#">Windowing</a></li> </ul> </li> <li>• Ensuring error-free reception of messages by retransmitting</li> <li>• Converting data into an acceptable form for the upper layers</li> <li>• Removing framing information from the packet and forwarding the message to the Network layer</li> <li>• Provide a way for upper layers of the OSI model to use any MAC layer protocol</li> <li>• Defining Service Access Points (SAPs) by tracking and managing different protocols</li> </ul>
Network	<p>The Network layer describes how data is routed across networks and on to the destination. Network layer functions include:</p> <ul style="list-style-type: none"> <li>• Maintaining addresses of neighboring routers.</li> <li>• Maintaining a list of known networks.</li> </ul>

	<ul style="list-style-type: none"> <li>• Determining the next network point to which data should be sent. Routers use a routing protocol to take into account various factors such as the number of hops in the path, link speed, and link reliability to select the optimal path for data.</li> </ul> <p>Packets forwarded from the Transport to the Network layer become datagrams and network-specific (routing) information is added. Network layer protocols then ensure that the data arrives at the intended destinations.</p>
Transport	<p>The Transport layer provides a transition between the upper and lower layers of the OSI model, making the upper and lower layers transparent from each other.</p> <ul style="list-style-type: none"> <li>• Upper layers format and process data without regard for delivery</li> <li>• Lower layers prepare the data for delivery by fragmenting and attaching transport required information</li> </ul> <p>Transport layer uses the following:</p> <ul style="list-style-type: none"> <li>• Port (or socket) numbers are used to identify distinct applications running on the same system. This allows each host to provide multiple services.</li> <li>• The Transport layer receives large packets of information from higher layers and breaks them into smaller packets called <i>segments</i>. Segmentation is necessary to enable the data to meet network size and format restrictions.</li> <li>• The receiving Transport layer uses packet sequence numbers to reassemble segments into the original message.</li> <li>• Connection-oriented protocols perform error detection and correction and identify lost packets for retransmission. A connection-oriented protocol is a good choice where: <ul style="list-style-type: none"> <li>○ Reliable, error-free communications are more important than speed</li> <li>○ Larger chunks of data are being sent</li> </ul> </li> <li>• Connectionless services assume an existing link between devices and allow transmission without extensive session establishment. Connectionless communications use no error checking, session establishment, or acknowledgements. Connectionless protocols allow quick, efficient communication at the risk of data errors and packet loss. Connectionless protocols are a good choice where: <ul style="list-style-type: none"> <li>○ Speed is important</li> <li>○ Smaller chunks of data are being sent</li> </ul> </li> </ul>

### Upper OSI Model Layer Facts

The following table summarizes basic characteristics of the upper OSI model layers.

Layer	Description
Application	<p>The Application layer integrates network functionality into the host operating system, and enables network services. The Application layer does not include specific applications that provide services, but rather provides the capability for services to operate on the network. These services include:</p> <ul style="list-style-type: none"> <li>• File services--transferring, storing, and updating shared data</li> <li>• Print services--enabling network printers to be shared by multiple users</li> <li>• Message services--transferring data in many formats (text, audio, video) from one location to another, or from one user to another</li> </ul>

	<ul style="list-style-type: none"> <li>• Application services--sharing application processing throughout the network and enabling specialized network servers to perform processing tasks</li> <li>• Database services--storing, retrieving, and coordinating database information throughout the network</li> </ul> <p>The Application layer specifies many important network services that are used on the Internet. These include:</p> <ul style="list-style-type: none"> <li>• HTTP</li> <li>• Telnet</li> <li>• FTP</li> <li>• TFTP</li> <li>• SNMP</li> </ul> <p><b>Note:</b> Most Application layer protocols operate at multiple layers down to the Session and even Transport layers. However, they are classified as Application layer protocols because they start at the Application layer (the Application layer is the highest layer where they operate).</p>
Presentation	<p>The Presentation layer formats or "presents" data into a compatible form for receipt by the Application layer or the destination system. Specifically, the Presentation layer ensures:</p> <ul style="list-style-type: none"> <li>• Formatting and translation of data between systems</li> <li>• Negotiation of data transfer syntax between systems, through converting character sets to the correct format.</li> <li>• Compatibility with the host</li> <li>• Encapsulation of data into message envelopes by encryption and compression</li> <li>• Restoration of data by decryption and decompression</li> </ul> <p>The Presentation layer formats data for the Application layer. Therefore, it also sets standards for multimedia and other file formats. These include standard file formats such as:</p> <ul style="list-style-type: none"> <li>• JPEG, BMP, TIFF, PICT</li> <li>• MPEG, WMV, AVI</li> <li>• ASCII, EBCDIC</li> <li>• MIDI, WAV</li> </ul>
Session	<p>The Session layer's primary function is managing the sessions in which data is transferred. Functions at this layer may include:</p> <ul style="list-style-type: none"> <li>• Establishment and maintenance of communication sessions between the network hosts, ensuring that data is transported.</li> <li>• Management of multiple sessions (each client connection is called a <i>session</i>). A server can concurrently maintain thousands of sessions.</li> <li>• Assignment of the session ID number to each session, which is then used by the Transport layer to properly route the messages.</li> <li>• Dialog control--specifying how the network devices coordinate with each other (simplex, half-duplex, and full-duplex).</li> <li>• Termination of communication sessions between network hosts upon completion of the data transfer.</li> </ul> <p>The Session layer protocols and interfaces coordinate requests and responses between different hosts using the same application. These protocols and interfaces include:</p>

	<ul style="list-style-type: none"> <li>• Network File System (NFS)</li> <li>• Apple Session Protocol (ASP)</li> <li>• Structured Query Language (SQL)</li> <li>• Remote procedure call (RPC)</li> <li>• X Window</li> </ul>
--	---

## OSI Layer Review

The following table compares the functions performed at each OSI model layer.

Layer	Description and Keywords	Protocols	Devices	Encapsulation
Application	<ul style="list-style-type: none"> <li>• Provides an interface for a service to operate</li> <li>• Communication partner identification</li> </ul>	<ul style="list-style-type: none"> <li>• HTTP</li> <li>• Telnet</li> <li>• FTP</li> <li>• TFTP</li> <li>• SNMP</li> </ul>		User information and data
Presentation	<ul style="list-style-type: none"> <li>• Data format (file formats)</li> <li>• Encryption, translation, and compression</li> <li>• Data format and exchange</li> </ul>	<ul style="list-style-type: none"> <li>• JPEG, BMP, TIFF, PICT</li> <li>• MPEG, WMV, AVI</li> <li>• ASCII, EBCDIC</li> <li>• MIDI, WAV</li> </ul>		Data
Session	<ul style="list-style-type: none"> <li>• Keeps data streams separate (session identification)</li> <li>• Set up, maintain, and tear down communication sessions</li> </ul>	<ul style="list-style-type: none"> <li>• SQL</li> <li>• NFS</li> <li>• ASP</li> <li>• RPC</li> <li>• X window</li> </ul>		Data
Transport	<ul style="list-style-type: none"> <li>• Reliable (connection-oriented) and unreliable (connectionless) communications</li> <li>• End-to-end flow control</li> <li>• Port and socket numbers</li> <li>• Segmentation, sequencing, and combination</li> </ul>	<ul style="list-style-type: none"> <li>• TCP (connection-oriented)</li> <li>• UDP (connectionless)</li> </ul>		Segments
Network	<ul style="list-style-type: none"> <li>• Logical addresses</li> <li>• Path determination (identification and selection)</li> <li>• Routing packets</li> </ul>	<ul style="list-style-type: none"> <li>• IP</li> <li>• IPX</li> <li>• AppleTalk</li> <li>• DECNET</li> </ul>	<ul style="list-style-type: none"> <li>• Routers</li> <li>• Layer 3 switches</li> </ul>	Packets

Data Link	Logical Link Control (LLC)	<ul style="list-style-type: none"> <li>Convert bits into bytes and bytes into frames</li> <li>MAC address, hardware address</li> <li>Logical network topology</li> <li>Media access</li> <li>Flow control <ul style="list-style-type: none"> <li>Acknowledgements</li> <li>Buffering</li> <li>Windowing</li> </ul> </li> <li>Parity and CRC</li> </ul>	<ul style="list-style-type: none"> <li>LAN protocols : 802.2 (LLC), 802.3 (Ethernet), 802.5 (Token Ring), 802.11 (Wireless)</li> <li>WAN protocols : HDLC, PPP, Frame Relay, ISDN, ATM</li> </ul>	<ul style="list-style-type: none"> <li>Network Interface Card (NIC) transceivers</li> <li>Switch</li> <li>Bridge</li> </ul>	Frames
	Media Access Control (MAC)				
Physical		<ul style="list-style-type: none"> <li>Move bits across media</li> <li>Cables, connectors, pin positions</li> <li>Electrical signals (voltage, bit synchronization)</li> <li>Physical topology (network layout)</li> </ul>	<ul style="list-style-type: none"> <li>EIA/TIA 232 (serial signaling)</li> <li>V.35 (modem signaling)</li> <li>Cat5</li> <li>RJ45</li> </ul>	<ul style="list-style-type: none"> <li>Transmission media (cable and wires)</li> <li>Media connectors</li> <li>Transceivers (including transceivers built into NICs)</li> <li>Modems</li> <li>Repeaters</li> <li>Hubs</li> <li>Multiplexers</li> <li>CSUs/DSUs</li> <li>Wireless Access Points</li> </ul>	Bits



## TCP/IP

As you study this section, answer the following questions:

- How does the DOD model correspond to the OSI model?
- Which TCP/IP protocols allow for copying and moving files?
- What does the Telnet protocol allow you to do?
- Which protocol includes a set of messages that controls how data moves through a network?
- What is the role of the subnet mask?
- What is the default address class of the IP address 132.11.166.5?
- What three address ranges are used for private IP addresses?
- What is the broadcast address of network 132.11.0.0?

This section covers the following exam objectives:

- 103. Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network
- 104. Describe common networked applications including web applications
- 105. Describe the purpose and basic operation of the protocols in the OSI and TCP models
- 106. Describe the impact of applications (Voice Over IP and Video Over IP) on a network
- 301. Describe the operation and benefits of using private and public IP addressing

### **TCP/IP Protocol Suite Facts**

Groups of protocols (called *protocol suites* or *protocol stacks*) are designed to interact and be used together. The TCP/IP protocol suite is used on the Internet and on most networks. Nearly all computers today use TCP/IP protocols for communication because it is highly scalable and routable. When learning about TCP/IP protocols, it is common to use a theoretical layered model called the TCP/IP model (also known as the Department of Defense (DoD) model). The layers of the DoD model are as follows:

- The Application layer (also called the Process layer) corresponds to the Session, Presentation, and Application layers of the OSI model.
- The Host-to-host layer is comparable to the Transport layer of the OSI model and is responsible for error checking and reliable packet delivery. Here, the data stream is broken into segments that must be assigned sequence numbers so that the segments can be reassembled correctly on the remote side after they are transported.
- The Internet layer is comparable to the Network layer of the OSI model. It is responsible for moving packets through a network. This involves addressing of hosts and making routing decisions to identify how the packet transverses the network.
- The Network Access layer corresponds to the functions of the Physical and Data Link layers of the OSI model. It is responsible for describing the physical layout of the network and how messages are formatted on the transmission medium. Sometimes this layer is divided into the Network Access and the Physical layer.

**Note:** The TCP/IP model focuses specifically on the functions in the Internet layer and the Host-to-Host layer. All other functions of the traditional OSI model are encompassed in the first and fourth layers.

The following table lists several protocols in the TCP/IP protocol suite.

<b>Protocol</b>	<b>Description</b>	<b>OSI Model Layer(s)</b>	<b>DoD Model Layer</b>
File Transfer Protocol (FTP)	File Transfer Protocol (FTP) provides a generic method of transferring files. It	Application, Presentation,	Application/Process

	can include file security through usernames and passwords, and it allows file transfer between dissimilar computer systems.	Session	
Trivial File Transfer Protocol (TFTP)	Trivial File Transfer Protocol (TFTP) is similar to FTP. It lets you transfer files between a host and an FTP server. However, it provides no user authentication and uses UDP instead of TCP as the transport protocol.	Application, Presentation, Session	Application/Process
Hypertext Transfer Protocol (HTTP)	The Hypertext Transfer Protocol (HTTP) is used by Web browsers and Web servers to exchange files (such as Web pages) through the World Wide Web and intranets. HTTP can be described as an information requesting and responding protocol. It is typically used to request and send Web documents, but is also used as the protocol for communication between agents using different TCP/IP protocols.	Application, Presentation, Session	Application/Process
Simple Mail Transfer Protocol (SMTP)	Simple Mail Transfer Protocol (SMTP) is used to route electronic mail through the internetwork. E-mail applications provide the interface to communicate with SMTP or mail servers.	Application, Presentation, Session	Application/Process
Simple Network Management Protocol (SNMP)	Simple Network Management Protocol (SNMP) is a protocol designed for managing complex networks. SNMP lets network hosts exchange configuration and status information. This information can be gathered by management software and used to monitor and manage the network.	Application, Presentation, Session	Application/Process
Telnet	Remote Terminal Emulation (Telnet) allows an attached computer to act as a dumb terminal, with data processing taking place on the TCP/IP host computer. It is still widely used to provide connectivity between dissimilar systems.	Application, Presentation, Session	Application/Process
Network File System (NFS)	Network File System (NFS) was initially developed by Sun Microsystems. It consists of several protocols that enable users on various platforms to seamlessly access files from remote file systems.	Application, Presentation, Session	Application/Process
Voice Over Internet Protocol (VoIP)	Voice over Internet Protocol (VoIP) is a protocol optimized for the transmission of voice through the Internet or other packet switched networks. Voice over IP protocols carry telephony signals as digital audio encapsulated in a data packet stream over IP.	Application, Presentation, Session	Application/Process

Transmission Control Protocol (TCP)	Transmission Control Protocol (TCP) operates at the Transport layer. It provides connection-oriented services and performs segment sequencing and service addressing. It also performs important error-checking functions and is considered a host-to-host protocol.	Transport	Host-to-Host (Transport)
User Datagram Protocol (UDP)	User Datagram Protocol (UDP) is considered a host-to-host protocol like TCP. It also performs functions at the Transport layer. However, it is not connection-oriented like TCP. Because of less overhead, it transfers data faster, but is not as reliable.	Transport	Host-to-Host (Transport)
Domain Name System (DNS)	Domain Name System (DNS) is a system that is distributed throughout the internetwork to provide address/name resolution. For example, the name "www.testout.com" would be identified with a specific IP address.	Transport	Host-to-Host (Transport)
Internet Protocol (IP)	Internet Protocol (IP) is the main TCP/IP protocol. It is a connectionless protocol that makes routing path decisions, based on the information it receives from ARP. It also handles logical addressing issues through the use of IP addresses.	Network	Internet
Internet Control Message Protocol (ICMP)	Internet Control Message Protocol (ICMP) works closely with IP in providing error and control information that helps move data packets through the internetwork.	Network	Internet
Internet Group Membership Protocol (IGMP)	Internet Group Membership Protocol (IGMP) is a protocol for defining host groups. All group members can receive broadcast messages intended for the group (called multicasts). Multicast groups can be composed of devices within the same network or across networks (connected with a router).	Network	Internet
Address Resolution Protocol (ARP)	Address Resolution Protocol (ARP) is used to get the MAC address of a host from a known IP address. ARP is used within a subnet to get the MAC address of a device on the same subnet as the requesting device.	Network	Internet
Reverse Address Resolution Protocol (RARP)	Both BOOTP (Bootstrap Protocol) and RARP (Reverse Address Resolution Protocol) are used to discover the IP address of a device with a known MAC address. BOOTP is an enhancement to RARP, and is more commonly implemented than RARP. As its name implies, BOOTP is used by computers as they boot to receive an IP address from a	Network	Internet
Bootstrap Protocol (BOOTP)		Network	Internet

	BOOTP server. The BOOTP address request packet sent by the host is answered by the server.		
Dynamic Host Configuration Protocol (DHCP)	<p>The Dynamic Host Configuration Protocol (DHCP) simplifies address administration. DHCP servers maintain a list of available and assigned addresses, and communicate configuration information to requesting hosts. DHCP has the following two components.</p> <ul style="list-style-type: none"> <li>• A protocol for delivering IP configuration parameters from a DHCP server to a host</li> <li>• A protocol specifying how IP addresses are assigned</li> </ul>	Network	Internet
Open Shortest Path First (OSPF)	Open Shortest Path First (OSPF) is a route discovery protocol that uses the link-state method. It is more efficient than RIP in updating routing tables, especially on large networks.	Network	Internet
Routing Information Protocol (RIP)	Routing Information Protocol (RIP) is a route discovery protocol that uses the distance-vector method. If the network is large and complex, OSPF should be used instead of RIP.	Network	Internet

The TCP/IP protocol suite was developed to work independently of the Physical layer implementation. You can use a wide variety of architectures with the TCP/IP protocol suite.

### IP Address and Class Facts

IP addresses allow hosts to participate on IP based networks. An IP address:

- Is a 32-bit binary number represented as four octets (four 8-bit values). Each octet is separated by a period.
- IP addresses can be represented in one of two ways:
  - Decimal (for example 131.107.2.200). In decimal notation, each octet must be between 0 and 255.
  - Binary (for example 1000011.01101011.00000010.11001000). In binary notation, each octet is an 8-digit number.
- The IP address includes both the network and the host address.
- Each IP address has an implied address class that can be used to infer the network portion of the address.
- The subnet mask is a 32-bit number that is associated with each IP address that identifies the network portion of the address. In binary form, the subnet mask is always a series of 1's followed by a series of 0's (1's and 0's are never mixed in sequence in the mask). A simple mask might be 255.255.255.0.

IP addresses have a default *class*. The address class identifies the range of IP addresses and a default subnet mask used for the range. The following table shows the default address class for each IP address range.

Class	Address Range	First Octet Range	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	1-126 (00000001--01111110 binary)	255.0.0.0
B	128.0.0.0 to 191.255.255.255	128-191 (10000000--10111111 binary)	255.255.0.0
C	192.0.0.0 to 223.255.255.255	192-223 (11000000--11011111 binary)	255.255.255.0
D	224.0.0.0 to 239.255.255.255	224-239 (11100000--11101111 binary)	n/a
E	240.0.0.0 to 255.255.255.255	240-255 (11110000--11111111 binary)	n/a

When using the default subnet mask for an IP address, you have the following number of subnet addresses and hosts per subnet:

- There are only 126 Class A network IDs (most of these addresses are already assigned). Each class A address gives you 16,777,214 hosts per network.
- There are 16,384 Class B network IDs. Each class B address gives you 65,534 hosts per network.
- There are 2,097,152 Class C network IDs. Each class C address gives you 254 hosts per network.
- Class D addresses are used for multicast groups rather than network and host IDs.
- Class E addresses are reserved for experimental use.

### Special Address Facts

You should understand the following special addresses:

Address	Consideration
Network	<p>The first octet(s) in an address range is used to identify the network itself. For the network address, the host portion of the address contains all 0's. For example:</p> <ul style="list-style-type: none"> <li>• Class A network address: 115.0.0.0</li> <li>• Class B network address: 154.90.0.0</li> <li>• Class C network address: 221.65.244.0</li> </ul> <p>0.0.0.0 is the network address used by routers to specify the "default" route. Using a generic value reduces the number of routing table entries. Some older routers use this address as a broadcast address.</p>
Host	<p>The range of IP addresses available to be assigned to network hosts is identified by the subnet mask and/or the address class. For example:</p> <ul style="list-style-type: none"> <li>• For the class A network address 115.0.0.0, the host range is 115.0.0.1 to 115.255.255.254.</li> <li>• For the class B network address 154.90.0.0, the host range is 154.90.0.1 to 154.90.255.254.</li> <li>• For the class C network address 221.65.244.0, the host range is 221.65.244.1 to 221.65.244.254.</li> </ul> <p><b>Note:</b> A special way to identify a host on a network is by setting the network portion of the address to all 0's. For example, the address 0.0.64.128 means "host 64.128 on this network."</p>
Broadcast	The last address in the range is used as the broadcast address and is used to send

	<p>messages to all hosts on the network. In binary form, the broadcast address has all 1's in the host portion of the address. For example, assuming the default subnet masks are used:</p> <ul style="list-style-type: none"> <li>• 115.255.255.255 is the broadcast address for network 115.0.0.0</li> <li>• 154.90.255.255 is the broadcast address for network 154.90.0.0</li> <li>• 221.65.244.255 is the broadcast address for network 221.65.244.0</li> </ul> <p>Two other formats you might see for the broadcast address:</p> <ul style="list-style-type: none"> <li>• The broadcast address might also be designated by setting each of the network address bits to 0. For example, 0.0.255.255 is the broadcast address of a Class B address. This designation means "the broadcast address for this network."</li> <li>• 255.255.255.255 indicates a broadcast message intended for all hosts on this network.</li> </ul>
Local host	<p>Addresses in the 127.0.0.0 range are reserved for the local host (in other words "this" host or the host you're currently working at). The most commonly-used address is 127.0.0.1 which is the loopback address.</p>
Private use	<p>The following address ranges have been reserved for private use:</p> <ul style="list-style-type: none"> <li>• 10.0.0.0 to 10.255.255.255</li> <li>• 172.16.0.0 to 172.31.255.255</li> <li>• 192.168.0.0 to 192.168.255.255</li> </ul> <p>Use addresses in these ranges for your private networks. Routers connected to the Internet typically filter messages within these ranges and prevent them from being propagated to the Internet.</p>

## Device Communication

As you study this section, answer the following questions:

- Which OSI model layer uses service data units called *frames*?
- When moving from top to bottom through the OSI model layers, which comes first, packets or segments?
- What gets added to the service data unit at the Network layer? At the Data Link layer?

This section covers the following exam objectives:

- 103. Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network

### **Data Encapsulation Facts**

*Encapsulation* is the process of breaking a message into packets, adding control and other information, and transmitting the message through the transmission media. You need to know the following five-step data encapsulation process:

1. Upper layers prepare the *data* to be sent through the network.
2. The Transport layer breaks the data into pieces called *segments*, adding sequencing and control information.
3. The Network layer converts the segments into *packets*, adding logical network and device addresses.
4. The Data Link layer converts the packets into *frames*, adding physical device addressing information.
5. The Physical layer converts the frames into *bits* for transmission across the transmission media.

The following short descriptions can help you remember the steps of the data encapsulation process:

1. Upper layers--*data*
2. Transport layer--*segments*
3. Network layer--*packets* containing *logical* addresses
4. Data Link layer--*framing* that adds *physical* addresses
5. Physical layer--*bits*

## Ethernet

As you study this section, answer the following questions:

- What is the purpose of the jam signal and the back off in Ethernet communications?
- What is the maximum cable length allowed for 100BaseTX?
- What is the physical device address used on Ethernet networks?
- Two devices are using full-duplex communications with the 1000BaseT standards. What is the amount of bandwidth available?
- Under what conditions can you disable collision detection on an Ethernet network?

This section covers the following exam objectives:

- 109. Describe the components required for network and Internet communications
- 201. Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts
- 202. Explain the technology and media access control method for Ethernet networks
- 403. Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts

### **Ethernet Architecture Facts**

The following table shows specifics of the Ethernet architecture.

Specification	Description
Topology	<p>The <i>physical</i> topology is the mapping of the nodes of a network and the physical connections between them, such as the layout of wiring, cables, the locations of nodes, and the interconnections between the nodes and the cabling or wiring system. The <i>logical</i> topology is the way messages are sent through the network connections. Ethernet supports the following topologies:</p> <p><a href="#">Physical bus, logical bus</a> <a href="#">Physical star, logical bus</a> <a href="#">Physical star, logical star</a></p>
Media access	<p>Ethernet uses Carrier Sense, Multiple Access/Collision Detection (CSMA/CD) to control access to the transmission medium. Devices use the following process to send data:</p> <ol style="list-style-type: none"><li>1. Because all devices have equal access to the transmission media (multiple access), a device with data to send first listens to the transmission medium to determine if it is free (carrier sense).</li><li>2. If it is not free, the device waits a random time and listens again to the transmission medium. When it is free, the device transmits its message.</li><li>3. If two devices transmit at the same time, a collision occurs. The sending devices detect the collision (collision detection) and send a jam signal.</li><li>4. Both devices wait a random length of time before attempting to resend the original message (called a <i>backoff</i>).</li></ol>
Transmission media	<p>Ethernet supports the following cable types:</p> <ul style="list-style-type: none"><li>• Unshielded twisted-pair cables (UTP) with RJ-45 connectors. This is the most common transmission medium used for Ethernet. Each cable consists of eight wires, twisted into four pairs. UTP cables are classified by categories:<ul style="list-style-type: none"><li>○ Cat3, rated up to 10 Mbps</li><li>○ Cat4, rated up to 16 Mbps</li></ul></li></ul>



	<ul style="list-style-type: none"> <li>○ Cat5, rated up to 100 Mbps</li> <li>○ Cat5e, rated up to 1,000 Mbps (gigabit)</li> <li>• Fiber optic, most commonly used in high-speed applications such as servers or streaming media. Fiber optic cables have ST, SC, LC, and MT-RJ connectors.</li> <li>• Coaxial for older Ethernet implementations (often called <i>thinnet</i> or <i>thicknet</i> networks). Coaxial cables have F-Type and BNC connectors.</li> </ul>
Frame type	<p>The Ethernet frame size is 64 to 1518 bytes (this is the same for all Ethernet standards). Four frame types are supported:</p> <ul style="list-style-type: none"> <li>• Ethernet 802.3 is the original Ethernet frame type.</li> <li>• Ethernet 802.2 is the frame type that accommodates standards set by the IEEE 802.2 committee related to the logical link control (LLC) sublayer. It is a more current frame type than 802.3.</li> <li>• Ethernet II is a frame type that provides the ability to use TCP/IP as a transport/network layer protocol. Other Ethernet frame types operate strictly with IPX/SPX as a transport/network layer protocol.</li> <li>• Ethernet SNAP (SubNetwork Address Protocol) is an enhanced version of Ethernet 802.2 that allows for greater compatibility with other network architectures such as Token Ring. This frame type also supports TCP/IP.</li> </ul>
Physical address	<p>The MAC address (also called the burned-in address) is the Data Link layer physical device address.</p> <ul style="list-style-type: none"> <li>• The MAC address is a 12-digit hexadecimal number (each number ranges from 0-9 or A-F).</li> <li>• The address is often written as 00-B0-D0-06-BC-AC or 00B0.D006.BCAC, although dashes, periods, and colons can be used to divide the MAC address parts.</li> <li>• The MAC address is guaranteed unique through design. The first half (first 6 digits) of the MAC address is assigned to each manufacturer. The manufacturer determines the rest of the address, assigning a unique value which identifies the host address. A manufacturer that uses all the addresses in the original assignment can apply for a new MAC address assignment.</li> </ul> <p><b>Note:</b> Some network cards allow you to change (logically assigned address) the MAC address through jumpers, switches, or software. However, there is little practical reason for doing so.</p>

## Ethernet Standards

The following table compares the characteristics of various Ethernet implementations.

Category	Standard	Bandwidth	Cable Type	Maximum Segment Length
Ethernet	10Base5	10 Mbps	Coaxial (thicknet)	500 meters
	10Base2	10 Mbps	Coaxial (thinnet)	185 meters
	10BaseT	10 Mbps (half duplex) 20 Mbps (full duplex)	Twisted pair (Cat3, 4, or 5)	100 meters

Fast Ethernet	100BaseTX	100 Mbps (half duplex) 200 Mbps (full duplex)	Twisted pair (Cat5)	100 meters
	100BaseT4	100 Mbps (half duplex) 200 Mbps (full duplex)	Twisted pair (Cat5)	100 meters
	100BaseFX	100 Mbps (half duplex) 200 Mbps (full duplex)	Fiber optic	412 meters (half duplex multimode cable) 2,000 meters (full duplex singlemode cable)
Gigabit Ethernet	1000BaseSX (short)	1,000 Mbps (half duplex) 2,000 Mbps (full duplex)	Fiber optic	220 to 550 meters depending on cable quality
	1000BaseLX (long)	1,000 Mbps (half duplex) 2,000 Mbps (full duplex)	Fiber optic	550 to 5,000 meters depending on cable quality
	1000BaseCX (short copper)	1,000 Mbps (half duplex) 2,000 Mbps (full duplex)	Special copper	25 meters, used within wiring closets
	1000BaseT	1,000 Mbps (half duplex) 2,000 Mbps (full duplex)	Twisted pair (Cat5e)	100 meters

Fast Ethernet was designed to be as compatible with 10BaseT Ethernet as possible. This provides an easy migration path from 10BaseT to 100BaseT/100BaseT4 (and even to Gigabit Ethernet).

- Most new networking devices that are Fast or Gigabit Ethernet capable also support 10BaseT standards. Devices autosense the specifics of the network configuration and set themselves to use the fastest communication method possible.
- If your network uses 10BaseT and has Cat5 cable, you can slowly migrate from 10BaseT to FastEthernet (remember that FastEthernet uses Cat5 cable). As you replace components such as NICs and hubs with FastEthernet devices, portions of the network will begin operating at FastEthernet speeds.
- You can begin your upgrade with:
  - Critical components, such as hubs, switches, and server NICs
  - Segments that service mission-critical applications
  - Workstations that have heavy bandwidth requirements

### Half- and Full-Duplex

With the original Ethernet standards, all devices shared the same cable. This caused two problems:

- Collisions occur when two devices transmit at the same time. Devices needed to be able to detect and recover from collisions.
- Each device could either transmit or receive data at any given time. This meant that the device was either receiving data or listening for incoming data. Devices were not able to both send and receive at the same time (much like using a one-lane road for traffic in two different directions).

These two problems were solved in the following ways:

- Using twisted pair cable, multiple strands of wires are combined into a single cable. Devices can use different wires to send and receive data (allowing them to do both simultaneously).
- Using switches, devices are given a dedicated communication path. With a single device connected to a switch port, collisions are eliminated.

With these problems solved, you can turn off collision detection. Devices can transmit and receive data simultaneously, and can begin transmitting data as soon as they have data to send.

Devices with collision detection turned on operate in *half-duplex* mode; devices with collision detection turned off operate in *full-duplex* mode.

Mode	Description	Bandwidth
Half-duplex	<ul style="list-style-type: none"><li>• Collision detection is turned on</li><li>• The device can only send or receive at any given time</li><li>• Devices connected to a hub must use half-duplex communication</li></ul>	Up to the rated bandwidth (10 Mbps for 10BaseT, 100 Mbps for 100BaseT, etc.)
Full-duplex	<ul style="list-style-type: none"><li>• Collision detection is turned off</li><li>• The device can send and receive at the same time</li><li>• Requires full-duplex capable NICs</li><li>• Requires switches with dedicated switch ports (a single device per port)</li></ul>	Double the rated bandwidth (20 Mbps for 10BaseT, 200 Mbps for 100BaseT, etc.)

## Bridging and Switching

As you study this section, answer the following questions:

- What is the difference between a bridge and a switch?
- What is the 80/20 rule of network segmentation with bridges?
- How do bridges and switches learn MAC addresses?
- What is the difference between the store-and-forward and the fragment-free switching methods?
- Which switching method is the fastest?

This section covers the following exam objectives:

- 101. Describe the purpose and functions of various network devices
- 102. Select the components required to meet a network specification
- 103. Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network
- 108. Determine the path between two hosts across a network
- 109. Describe the components required for network and Internet communications
- 204. Explain basic switching concepts and the operation of Cisco switches

### **Bridge Facts**

A *bridge* is a data forwarding device that provides data transfer. You should understand the following concepts relating to the operation of bridges.

- Bridges connect two media segments that use the same protocol.
- Bridges examine the source address to determine the media segment of network devices.
- Bridges operate at the Data Link layer of the OSI model.
- Bridges maintain a table of device addresses and their corresponding segments.
- Each segment connected by a bridge can have the same network address.
- Messages within a media segment are prevented from crossing over to another segment.

Bridges offer the following advantages:

- Bridges prevent wasted bandwidth by eliminating unnecessary traffic between segments.
- Bridges increase the maximum network length.
- Bridges forward packets for multiple upper-layer protocols.
- Bridges can link segments with dissimilar transmission media and media access methods.

Bridges have the following limitations:

- Bridges cannot link multiple architectures because different frame types are used.
- Bridges cannot translate upper-layer protocols.
- Bridges cannot forward packets to different networks based on the network address.
- Bridges do not filter broadcast packets.

Use bridges to isolate traffic to a segment, or to prevent unwanted traffic from crossing over to other segments, or to slow WAN links. When designing the placement of bridges on the network, follow the 80/20 rule.

- At least 80% of network traffic should stay within a segment.
- No more than 20% of network traffic should pass through the bridge to another segment.

### **Switch Facts**

A *switch* is a multiport bridge. It provides the same functionality, but with a higher port density. In addition, switches provide features that cannot be found in bridges.

- Switches are associated with the Data Link layer of the OSI Model.
- Switches build a forwarding database in a manner similar to bridges. Switches examine the source and destination Data Link address in each packet to build the database and make forwarding decisions.
- Switches connect multiple segments or devices and forward packets to only one specific port.
- You can connect a single device to a switch port or multiple devices to a switch port by using a hub.

Switches offer the following advantages over a non-switched network.

- Switches create separate collision domains.
- Switches provide guaranteed bandwidth between devices, if dedicated ports are used.
- Switches can be used to provide collision-free networking, if only one device is connected to each switch port.
- Switches enable full-duplex communication.
- Switches induce less latency than other segmentation solutions.
- Switches can simultaneously switch multiple messages.
- Switches can mix 10 Mbps- and 100 Mbps-capable devices, if the switch is a 100 Mbps switch.
- Ethernet switches can be implemented without re-cabling.

Switches have replaced bridges in most network applications.

### **Bridge and Switch Forwarding Facts**

Both bridges and switches build a forwarding database. The database is a list of Data Link (MAC) addresses and the port used to reach the device. Bridges and switches can automatically learn about devices to build the forwarding database. A network administrator can also program the device database manually. Bridges and switches use the following process to dynamically build the forwarding database:

- The process begins by examining the source address of an incoming packet. If the source address is not in the forwarding database, an entry for the address is made in the database. The port it came in on is also recorded.
- The destination address is then examined.
  - If the destination address is in the database, the packet is forwarded to the appropriate port if the port is different than the one on which it was received.
  - If the destination address is not in the database, the packet is sent out all ports except for the one on which it was received. This is known as *flooding*.
  - A broadcast packet is forwarded (*flooded*) to all ports except the one on which it was received.

Transparent bridges forward packets only if the following conditions are met.

- The frame contains data from the layers above the Data Link layer.
- The frame's integrity has been verified through a valid Cyclic Redundancy Check (CRC).
- The frame is not addressed to the bridge.

How switches forward packets depends on the switch type. The following table compares the different methods the switch uses to forward packets (some Cisco switches support all three methods).

Method	Characteristics
Store-and-forward	Store-and-forward switches: <ul style="list-style-type: none"> <li>• Receive the entire frame.</li> <li>• Verify the frame's integrity (check the CRC). Frames with errors are not forwarded.</li> <li>• Forward the frame to the destination device.</li> <li>• Introduce more latency (delay) than cut-through switches.</li> </ul>
Cut-through	Cut-through switches: <ul style="list-style-type: none"> <li>• Read the destination device address.</li> <li>• Forward the packet without verifying frame integrity.</li> <li>• Are faster than store-and-forward switches (less latency).</li> </ul>
Fragment-free	Fragment-free switches: <ul style="list-style-type: none"> <li>• Read the first 64 bytes of a frame.</li> <li>• Verify that the packet is not a fragment.</li> <li>• Forward non-fragmented frames.</li> <li>• Introduce some latency, but not as great as store-and-forward switching.</li> </ul>

**Note:** Newer switches can monitor each port and determine which switching method to use. They can automatically change to store-and-forward if the number of errors on a port exceeds a configurable threshold.

## Routing

As you study this section, answer the following questions:

- What type of information is stored in the routing table?
- What is *convergence*?
- What is the function of a routing protocol?
- A computer needs to send a message to another computer on the same network. What MAC address would go into the destination portion of the frame?
- A computer needs to send a message to another computer on a different network. What MAC address would go into the destination portion of the frame?
- As a packet moves from device to device through an internetwork, do the Network layer addresses change or remain the same?

This section covers the following exam objectives:

- 101. Describe the purpose and functions of various network devices
- 103. Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network
- 108. Determine the path between two hosts across a network
- 109. Describe the components required for network and Internet communications
- 401. Describe basic routing concepts (including: packet forwarding, router lookup process)

### **Routing Facts**

A *router* is a device that sends packets from one network to another network. Routers receive packets, read their headers to find addressing information, and send them on to their correct destination on the network or Internet. Routers can forward packets through an internetwork by maintaining routing information in a database called a *routing table*. The routing table typically contains the address of all known networks and routing information about that network such as:

- Interface
- Routing Path
- Next Hop
- Route Metric (Cost)
- Route Timeout

Routers build and maintain their routing database by periodically sharing information with other routers. The exact format of these exchanges is based on the routing protocol. The routing protocol determines:

- The information contained in the routing table
- How messages are routed from one network to another
- How topology changes (i.e. updates to the routing table) are communicated between routers

Regardless of the method used, changes in routing information take some time to be propagated to all routers on the network. The term *convergence* is used to describe the condition when all routers have the same (or correct) routing information.

### **Message Routing Facts**

To send a message from one host to another on a different network, the following process is used:

1. The sending host prepares a packet to be sent. It uses its own IP address for the source Network layer address, and the IP address of the final receiving device as the destination Network layer address.

2. The sending host creates a frame by adding its own MAC address as the source Physical layer address. For the destination Physical layer address, it uses the MAC address of the default gateway router.
3. The sending host transmits the frame.
4. The next hop router reads the destination MAC address in the frame. Because the frame is addressed to that router, it processes the frame.
5. The router strips off the frame header and examines the packet destination address. It uses a routing protocol to identify the next hop router in the path.
6. The router repackages the packet into a new frame. It uses its own MAC address as the source Physical layer address. It uses the MAC address of the next hop router for the destination Physical layer address.
7. The router transmits the frame.
8. The next hop router repeats steps 4 through 7 as necessary, until the frame arrives at the last router in the path.
9. The last router in the path receives the frame and checks the destination IP address contained in the packet.
10. Because the destination device is on a directly connected network, the router creates a frame using its own MAC address as the source address, and the MAC address of the destination device as the destination physical address.
11. The router transmits the frame.
12. The destination device receives the frame. Inside the packet it finds the destination address matching its own IP address, with the source IP address being that of the original sending device.

Be aware of the following:

- On an Ethernet network, the Data Link layer address is the MAC address. On an IP network, the Network layer address is the IP address.
- Both Data Link physical addresses and Network logical addresses are used to send packets between hosts.
- The Data Link address identifies the physical interface. The Network address contains both a logical network address and a logical device address.
- IP (Network layer) addresses are contained in the IP header; MAC (Data Link) addresses are contained in the Ethernet frame header.
- Both the source and destination Network and Data Link addresses are typically contained in the packet.
- Data Link addresses in the packet change as the packet is delivered from hop to hop. At any point in the process, the Data Link destination address indicates the physical address of the next hop on the route. The Data Link source address is the physical address of the device sending the frame.
- Network addresses remain constant as the packet is delivered from hop to hop. The Network addresses indicate the logical address of the original sending device and the address of the final destination device.
- A router uses the logical network address specified at the Network layer to forward messages to the appropriate network segment.



## Connecting Cisco Devices

As you study this section, answer the following questions:

- What HyperTerminal settings should you use to connect to the router console for the first time?
- What are the requirements for using a VTY (virtual terminal) connection to a Cisco device?
- What type of cable do you use to connect a PC to a router console port?

After finishing this section, you should be able to complete the following tasks:

- Use HyperTerminal to connect to a Cisco device console.
- Use Telnet to create a virtual terminal connection to a Cisco device.

This section covers the following exam objectives:


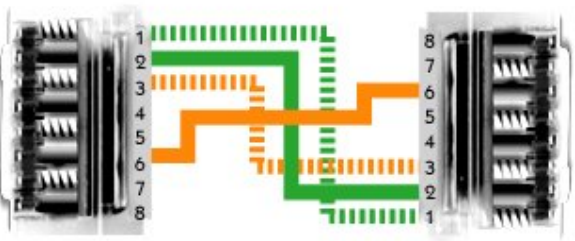
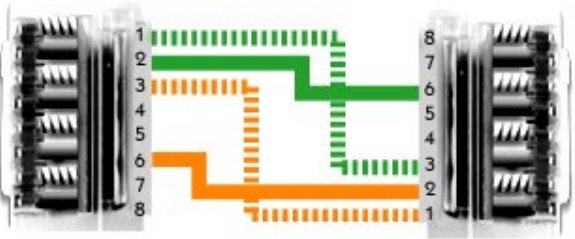
- 205. Perform and verify initial switch configuration tasks including remote access management
- 405. Access and utilize the router to set basic parameters

### Device Connection Facts

Cisco routers and switches do not have monitors, and you cannot connect a keyboard or a mouse directly to the device. To manage the device, you connect to the router or switch through either a dedicated terminal or a PC. There are several options you can use to manage a Cisco device. These include:

Connection Type	Description
Console	<p>A console connection allows for a direct connection through a PC to the console port on the device. The PC will need a terminal emulation program (such as HyperTerminal and PuTTY) to connect to the device's command line interface. In the terminal emulation program, use the following settings:</p> <ul style="list-style-type: none"><li>• 9600 baud (or a rate supported by your router)</li><li>• Data bits = 8 (default)</li><li>• Parity = None (default)</li><li>• Stop bits = 1 (default)</li><li>• Flow control = None</li></ul>
Virtual Terminal (VTY)	<p>A VTY connection connects through a LAN or WAN interface configured on the device. Use a program such as Telnet or SSH to open the command line interface. The Cisco device must be configured with an IP address before a VTY connection can be made.</p>
Security Device Manager (SDM)	<p>The Cisco SDM allows a Web browser connection to the device. Once connected, the SDM allows you to manage the security features and network connections through a Web-based graphical user interface. Be aware of the following SDM settings:</p> <ul style="list-style-type: none"><li>• 10.10.10.1 is the default IP address of the SDM</li><li>• The default value for both the username and password is <b>cisco</b></li></ul> <p><b>Note:</b> A new router may not be completely configured for an SDM connection, so you may need to make a console connection first.</p>

Use the following cable types to make the initial connection to the switch or the router for device management:

Cable Type	Pin-outs	Use
 <p data-bbox="418 569 605 600">Rollover Cable</p>	<p data-bbox="824 281 911 552">           1 --&gt; 8            2 --&gt; 7            3 --&gt; 6            4 --&gt; 5            5 --&gt; 4            6 --&gt; 3            7 --&gt; 2            8 --&gt; 1         </p>	<p data-bbox="943 296 1373 464">           Use a rollover Ethernet cable to connect the device's console port to the serial port on a PC. Connect the RJ-45 end to the console port, and connect the serial end to the PC.         </p>
 <p data-bbox="321 947 708 978">Straight-through Ethernet Cable</p>	<p data-bbox="824 730 911 863">           1 --&gt; 1            2 --&gt; 2            3 --&gt; 3            6 --&gt; 6         </p>	<p data-bbox="943 625 1403 831">           Use a straight-through Ethernet cable to connect an Ethernet port on a router to an Ethernet port on a hub or switch. You can then access the router from another PC connected to the same network using a VTY connection.         </p> <p data-bbox="943 867 1403 968"> <b>Note:</b> If the router has an AUI port, connect one end to an AUI transceiver before connecting to the router.         </p>
 <p data-bbox="358 1331 670 1362">Crossover Ethernet Cable</p>	<p data-bbox="824 1115 911 1247">           1 --&gt; 3            2 --&gt; 6            3 --&gt; 1            6 --&gt; 2         </p>	<p data-bbox="943 1024 1403 1192">           Use a crossover Ethernet cable to connect an Ethernet port on a router directly to the NIC in a PC. Establish a VTY session from the PC to connect to the device.         </p> <p data-bbox="943 1234 1403 1335"> <b>Note:</b> If the router has an AUI port, connect one end to an AUI transceiver before connecting to the router.         </p>

## System Startup

As you study this section, answer the following questions:

- If the router can't find an IOS image in flash, where will it look next?
- What happens if the router can't find a configuration file at startup?
- What is the role of the configuration register?
- What configuration register value tells the router to skip the startup-config file?

After finishing this section, you should be able to complete the following tasks:

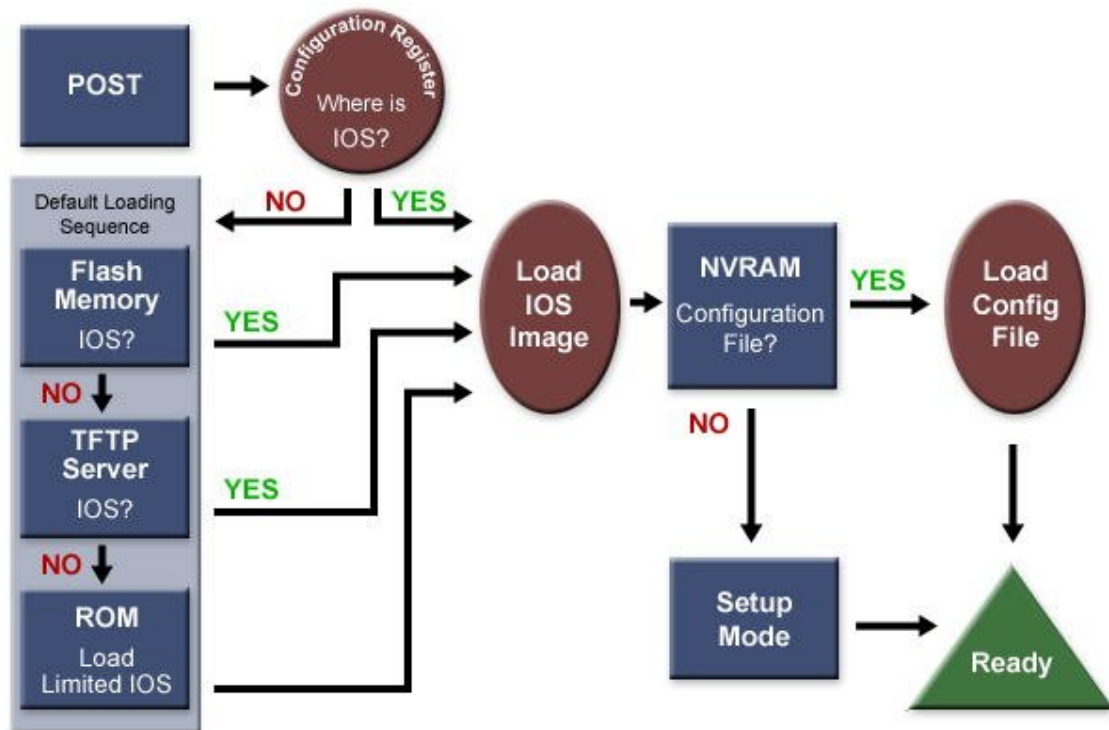
- Use setup mode to complete an initial configuration of a Cisco device.
- Use the Express setup to configure a Cisco device.

This section covers the following exam objectives:

- 205. Perform and verify initial switch configuration tasks including remote access management
- 402. Describe the operation of Cisco routers (including: router bootup process, POST, router components)

### Startup Facts

The following graphic details the process used to boot the device.



When you turn the router on, it runs through the following boot process.

1. The Power-On Self Test (POST) checks the router's hardware. When the POST completes successfully, the System OK LED indicator comes on.
2. The router checks the [configuration register](#) to identify where to load the IOS image from. A setting of 0x2102 means that the router will use information in the startup-config file to

locate the IOS image. If the startup-config file is missing or does not specify a location, it will check the following locations for the IOS image:

1. Flash (the default location)
  2. TFTP server
  3. ROM (used if no other source is found)
3. The router loads the configuration file into RAM (which configures the router). The router can load a configuration file from:
1. NVRAM (startup-configuration file)
  2. TFTP server
  3. If a configuration file is not found, the router starts in setup mode.

## Setup Mode Facts

If the router is brand new, it has no startup-config file. Therefore, when it boots, it immediately enters Setup mode. Setup mode is a special, guided routine that asks you a series of questions and uses your responses to make basic configuration entries.

There are two ways to enter setup mode:

- Boot the router without the startup-config file. This happens when you erase the current startup-config file, or when you boot a new router.
- Use the **setup** command from privileged mode.

You can exit setup mode without answering all the questions by pressing **Ctrl + C**. The information you've entered to that point will not be saved.

Cisco routers and switches come with the following defaults:

- No set passwords. During setup mode, passwords are created.
- All router interfaces are in shutdown mode until they are enabled.
- All switch interfaces are enabled and ready to forward packets.

**Note:** Some Cisco switches allow you to enter an express setup mode. Be aware of the following express setup details:

- The device must be enabled as a DHCP server.
- The device must be power cycled while pressing the Mode button and while your PC is connected to an Ethernet interface.
- Use a Web browser to enter the express setup mode by going to 10.10.10.1.

## Command Line Interface (CLI)

As you study this section, answer the following questions:

- What router mode is indicated by the # prompt?
- How can you get a list of allowed keywords for a command?
- You use help to get a list of keywords for a command. In the list of options you see: A.B.C.D. What should you type to complete the command?
- How can you move the cursor backwards one word?
- How do you turn off console configuration messages?

After finishing this section, you should be able to complete the following tasks:

- Use help to identify possible commands, keywords, and parameters.
- Use advanced editing features to efficiently enter commands at the console.
- Turn on and access commands in the history buffer.

This section covers the following exam objectives:

- 205. Perform and verify initial switch configuration tasks including remote access management
- 405. Access and utilize the router to set basic parameters
- **Command Mode Prompts and Commands**
- The following table summarizes basic command mode prompts and other commands.

Mode	Prompt	To Enter	To Exit
User EXEC	Router>	Press <enter>, then log in	exit logout disconnect
Privileged EXEC	Router#	enable	disable (exit disconnects)
Global Configuration	Router(config)#	config terminal	exit, ^Z*
Line	Router(config-line)#	line <type> <number>	exit, ^Z*
Interface	Router(config-if)#	interface <type> <number>	exit, ^Z*
Subinterface	Router(config-subif)#	interface <type> <number>.<subnumber>	exit, ^Z*
Router	Router(config-router)#	router <type>	exit, ^Z*
Setup	None, interactive dialog	setup erase startup-config+reload	^C
ROM Monitor	rommon>	ROM Monitor mode lets you configure your router if the router can't find a valid system image, or if the boot sequence is interrupted when you start the router. It is an emergency command-line access to the router. To go to EXEC mode from this mode, type <b>continue</b> at the prompt.	
RXBoot	<boot>	RXBoot mode lets a router boot with a limited version of the IOS when it cannot	

		find a valid IOS image in Flash. You enter RXBoot mode by modifying the configuration register before rebooting the router.	
--	--	---	--

- \***^Z (Ctrl + Z)** exits all configuration modes to privileged EXEC mode. **exit** "backs up" one configuration mode.
- **Command Help Facts**
- Help is available in all device modes. It is context sensitive, so the information you see depends on what you are doing. Cisco bases this on the mode you are in and the words or partial words you type with the ?.

To...	Use...
Show list of all commands available in the current mode	?
Show commands that begin with specific letter(s)	xx? (no space between the letter and ?)
Show keywords for a command	command ? (space between command and ?)
Get the full command from a partial command	partial command + <tab> (no space)

- **Note:** Typing ? acts as a return, and repeats the last command you entered after the Help information displays. You do not need to retype the command after you ask for help on it.
- When you use Help to display the possible keywords for a command, you will see the following types of items.

When you see...	Supply...
WORD (in caps)	Type a one-word response
LINE (in caps)	Type a multiple-word response
<0-4567>	Enter a number within the range in brackets
<0-FFFFFF>	Enter a hexadecimal number within the range in brackets
<cr>	The command is complete as typed, press Enter to execute the command
A.B.C.D	Enter an IP address

### Editing Features Facts

The following lists summarize the advanced editing features of the CLI.

Use this ...	To ...
Ctrl + A	Move to the beginning of the line
Ctrl + E	Move to the end of the line
Ctrl + B Left arrow	Go back one character
Ctrl + F Right arrow	Go forward one character
Esc, then B (press and release Esc, before pressing B)	Go back one word
Esc, then F (press and release Esc, before pressing F)	Move forward one word

Ctrl + Z	Quit a configuration mode
terminal editing	Turn advanced editing on
terminal no editing	Turn advanced editing off

When you are in advanced editing mode, the \$ indicator appears after the prompt. As you type, commands longer than the command line appear to scroll under the prompt.

**Note:** The editing feature uses the same keystrokes as UNIX emacs editing.

### Command History Command List

By default, the IOS automatically saves the last 10 commands in the command history buffer. The command history is specific to the configuration mode you are in.

Use ...	To ...
Ctrl + P or Up arrow	Show the previous command
Ctrl + N or Down arrow	Show the next command
terminal history	Turn the command history on
terminal no history	Turn the command history off
terminal history size <0-256>	Set the size of the history buffer
show history	Show all the commands in the history buffer

### Controlling Screen Output

As you work with the device at the console and make configuration changes, response messages are often displayed on the screen. The following table describes various ways to control the response messages shown.

Problem	Solution
When making configuration changes, the following message is constantly displayed (sometimes as you are typing): %SYS-5-CONFIG_1: Configured from console by console	Use: no logging console to turn these messages off.
When working with the device through a Telnet session, when you use a debug command, output will not be shown.	Use: terminal monitor to send debug output to the telnet session.
When viewing debug information, you want to review previous information, or debug information is shown too quickly for you to examine it.	Use: logging buffered to send logging information to RAM, then use: show log to view information one screen at a time.

## Managing System Files

As you study this section, answer the following questions:

- Where is the startup-config file stored? Where is the running-config file stored?
- What is stored in ROM?
- What is the generic syntax for loading a configuration file into RAM?
- What does the **boot system** command do?

After finishing this section, you should be able to complete the following tasks:

- Save your configuration changes.
- Load an IOS image from an alternate location.
- Upgrade the IOS image.

This section covers the following exam objectives:

- 405. Access and utilize the router to set basic parameters
- 409. Manage IOS configuration files (including: save, edit, upgrade, restore)
- 410. Manage Cisco IOS
- **Router Memory**
- Be sure you understand the difference between the following types of router storage.

Memory Type	Characteristics
ROM (Read-Only Memory)	Preprogrammed, non-writable memory containing the bootstrap startup program, an older, smaller-scale version of the operating system (IOS) software, and the Power-on Self-Test (POST) program
Flash	Non-volatile but programmable memory containing the proprietary Cisco operating system (IOS) images <b>Note:</b> Older routers don't have flash memory
RAM (Random Access Memory)	Volatile memory containing the running operating system and current (unsaved) configuration information
NVRAM (Non-Volatile RAM)	Non-volatile but persistent memory that contains the backup copy of the startup configuration (startup-config) file and virtual configuration register <b>Note:</b> On some routers, NVRAM holds the IOS image

- The contents of non-volatile memory (such as ROM, flash, and NVRAM) remain when the router is powered off. The contents of volatile memory (RAM) are lost when the router is powered down.

### Copy Command List

The device can load a configuration file from:

- NVRAM (startup-configuration file by default value 0x2102)
- TFTP server

Changes to the configuration are stored in RAM in the running-config file. To save your configuration changes permanently, and to load different versions of the configuration files from various locations, use the `copy` command in privileged EXEC mode.

Use ...	To ...
<code>Router#copy run start</code>	Save the contents of the running-config file to NVRAM



Router#copy start run	Copy the startup-config file into RAM
Router#copy run tftp	Save the contents of the running-config file to a TFTP server
Router#copy start tftp	Save the contents of the startup-config file to a TFTP server
Router#copy tftp start	Copy a configuration file from the TFTP server into NVRAM
Router#copy tftp run	Copy a configuration file from the TFTP server into RAM
Router(config)#tftp-server flash <filename>	Configure a Cisco router as a TFTP server. When using this command, you must specify the location (flash or rom) of the IOS image file as well as the IOS image file name.

You can also use the **erase** command to delete the configuration files--but be very careful not to erase files you need!

Use ...	To ...
Router#erase flash	Delete the contents of Flash memory (deletes the IOS image)
Router#erase start	Erase the contents of the startup-config file
Router#erase nvram	Delete the contents of NVRAM (which also erases startup-config)
Router#reload	Restarts the router

You can also use the following commands to manage system files:

Use ...	To ...
show version	Display information about hardware and firmware including the configuration register value
configure memory or copy startup-config running-config	Copy configuration information from another source (like NVRAM)
configure terminal	Configure information into the RAM of a router

## IOS Boot and Upgrade Location Command List

The router can load an IOS image from the following locations:

- Flash
- TFTP server
- ROM (limited version of the IOS software)

Use the `boot system` command in global configuration mode to identify alternate locations for the IOS image. Use the `copy` command to archive, upgrade, or replace an IOS image.

Use ...	To ...
Router(config)#boot system flash <IOSfilename>	Identify an IOS image file in flash to use at boot.
Router(config)#boot system tftp <IOSfilename> <tftp_address>	Identify an IOS image file on a TFTP server to use at boot.

Router(config)#boot system rom (IOS versions 11.2 and below) Router(config)#boot system flash bootflash: (IOS versions 12.0 and above	Specify to use the limited IOS version stored in ROM at boot.
Router#copy flash tftp	Back up (copy) the IOS image from Flash to the TFTP server.
Router#copy tftp flash	Restore the IOS image from backup on the TFTP server to Flash.

**Note:** When you use the boot system command, you are not making backup copies of the IOS image, nor are you replacing the default IOS search order. You are directing the router where to look for the IOS image on boot-up. It tries each location in turn, until it finds a valid IOS image. If one is not found, it returns to the default load sequence.

## Using Show Commands

After finishing this section, you should be able to complete the following tasks:

- Use **show** commands to find information about the device configuration.

This section covers the following exam objectives:

- 215. Interpret the output of various show and debug commands to verify the operational status of a Cisco switched network
- 416. Verify router hardware and software operation using SHOW & DEBUG commands
- **Show Command List (Basic)**
- The following list summarizes common information you can display using common show commands.

Use this command...	To...
<code>show version</code>	View hardware configuration, running IOS version, ROM bootstrap version, and RAM and processor information
<code>show running-config</code>	View the currently running configuration file
<code>show startup-config</code> or <code>show config</code>	View the startup configuration file stored in NVRAM (the saved copy of the configuration file)
<code>show flash</code>	View the size of the configuration files and the available flash memory View information for all IOS image files stored on the router
<code>show history</code>	View the commands in the command history list
<code>show protocols</code> or <code>show interfaces</code> or <code>show ip interfaces</code>	View the IP addresses assigned to a specific interface
<code>show protocols</code> or <code>show interfaces</code>	View the status of all interfaces

## Hostname and Descriptions

As you study this section, answer the following questions:

- When is the Slot/Sub-slot/Port numbering used?
- How do fixed ports and WIC slots affect the numbering scheme for a device?
- What changes in the prompt after you set a hostname?

After finishing this section, you should be able to complete the following tasks:

- Change the device host name.
- Configure descriptions on device interfaces.

This section covers the following exam objectives:

- 205. Perform and verify initial switch configuration tasks including remote access management
- 405. Access and utilize the router to set basic parameters
- 406. Connect, configure, and verify operation status of a device interface

### Interface Numbering Facts

The switch interface numbering scheme includes the bank number and port number:

Portion	Details	Examples
Bank number	<ul style="list-style-type: none"><li>• Switches that have one fixed bank are assigned 0.</li><li>• Switches that have multiple banks start with 0 and are assigned from bottom to top. For example, if a switch had 5 banks, it would have bank numbers 0-4.</li></ul>	<b>FastEthernet 2/1</b> (3rd bank/1st port) <b>FastEthernet 1/5</b> (2nd bank/5th port)
Port number	<ul style="list-style-type: none"><li>• Port numbers are assigned starting with 1.</li><li>• Switches that have 1 row of ports on a bank are assigned from left to right.</li><li>• Switches that have 2 rows of ports on a bank are assigned from top to bottom and left to right.</li></ul>	<b>FastEthernet 0/7</b> (fixed bank or 1st bank/7th port) <b>FastEthernet 5/1</b> (6th bank/1st port)

Router interface numbering includes the following types of schemes:

Scheme	Details	Examples
Fixed ports	<p>Older Cisco routers, such as the Cisco 2500, use a fixed port numbering scheme. In the fixed port numbering scheme:</p> <ul style="list-style-type: none"><li>• Each built-in port was hard-wired with a port number.</li><li>• Numbering starts with 0, and is assigned from right to left.</li></ul>	<b>Serial0</b> (1st serial port) <b>Serial1</b> (2nd serial port) <b>Ethernet0</b> (1st Ethernet port)
Slot/Port numbering	Newer Cisco routers, such as the Cisco 2600, support WAN Interface Cards (WIC) and Network Modules (NM) with various ports. Some Network Modules include slots	<b>FastEthernet3/4</b> (3rd NM slot/5th FastEthernet port)

	<p>for WAN Interface Cards. In the Slot/Port numbering scheme:</p> <ul style="list-style-type: none"> <li>• The slot number scheme includes: <ul style="list-style-type: none"> <li>◦ Built-in ports and built-in WIC slots are given NM slot number 0. The remaining NM slots are assigned from right to left and bottom to top.</li> <li>◦ If the device does not have built-in ports or built-in WIC slots, the NM slot numbering is assigned from right to left and bottom to top, starting with 0.</li> </ul> <p><b>Note:</b> When learning about the router's NM slots, discover whether or not the router has built-in ports and built-in WIC slots.</p> </li> <li>• The port numbers start with 0 and are assigned from right to left and bottom to top for each NM slot.</li> </ul>	<p><b>FastEthernet0/3</b> (built-in/4th FastEthernet port)</p> <p><b>Serial2/3</b> (2nd NM slot/4th serial port)</p> <p><b>Serial1/5</b> (1st NM slot/6th serial port)</p> <p><b>Serial0/2</b> (built-in or 1st WIC slot/3rd serial port)</p>
Slot/Sub-slot/Port numbering	<p>The newest Cisco routers, such as the Cisco 1800/2800/3800, use an enhanced slot/port numbering scheme to identify the <i>WIC sub-slot</i>. In the Slot/Sub-slot/Port numbering scheme:</p> <ul style="list-style-type: none"> <li>• Built-in WIC ports are numbered using a slot of 0 and a sub-slot that is the WIC slot number.</li> <li>• WIC ports on a NM slot are numbered using the NM slot number and the WIC's sub-slot number on the NM.</li> <li>• Ports (<i>other than those of a WIC</i>) use the slot/port numbering scheme.</li> </ul>	<p><b>FastEthernet2/1/0</b> (2nd NM slot/2nd WIC sub-slot/1st FastEthernet port)</p> <p><b>FastEthernet0/0/0</b> (built-in/1st WIC sub-slot/1st FastEthernet port)</p> <p><b>FastEthernet0/1/3</b> (built-in/2nd WIC sub-slot/4th FastEthernet port)</p> <p><b>Serial4/1/1</b> (4th NM slot/2nd WIC sub-slot/2nd Serial port)</p> <p><b>Serial0/1/0</b> (built-in/2nd WIC sub-slot/1st Serial port)</p> <p><b>Ethernet1/0</b> (1st NM slot/1st Ethernet port)</p> <p><b>FastEthernet0/1</b> (built-in/2nd FastEthernet port)</p>

### Hostname and Description Command List

During initial setup, you can configure a host name for your device (i.e. router or switch). This is the name that appears in the EXEC prompt. Unlike the device itself, interfaces do not have specific names that change the prompt. However, you can add a description to the configuration file that helps you identify the interface.

Use ...	To ...
Router(config)#hostname <name>	Change the host name of the router
Router(config)#int serial 0/0 Router(config)#int s0/0	Go to interface configuration mode for the first serial interface. You can use abbreviations for the

<pre>Router(config)#int Ethernet 0 Router(config)#int ether0 Router(config)#int FastEthernet 0/1 Router(config)#int Fa0/1 Router(config)#int Gigabit 0/1 Router(config)#int gi0/1</pre>	<p>interface type, such as:</p> <ul style="list-style-type: none"> <li>• fa = FastEthernet</li> <li>• gi = Gigabit</li> <li>• s = Serial</li> <li>• e = Ethernet</li> </ul>
<pre>Router(config-if)#description &lt;description text&gt;</pre>	<p>Set a description for a specific interface</p>

### Examples

The following set of commands sets the hostname of the router to ATL1:

```
Router#config t
Router(config)#hostname ATL1
ATL1(config)#
```

The following set of commands adds a description of **ATL to NYC** for the first serial interface on the router:

```
Router(config)#int ser 0
Router(config-if)#description ATL to NYC
```

**Note:** To undo any configuration change, use the same command preceded by the **no** keyword followed by the command. For example, to remove a description from an interface, use the following command:

```
Router(config-if)#no description
```

Notice that in many cases you can leave off additional parameters when using the **no** command.

## System Passwords

As you study this section, answer the following questions:

- What is the difference between the **enable** and the **enable secret** passwords? Which one is more secure?
- How would you require a password when logging on through the console?
- You have configured the VTY lines on a router with a password but you did not use the **login** command. Will VTY login be allowed? Will a password be required?
- What must you do to disable VTY login?

After finishing this section, you should be able to complete the following tasks:

- Configure router passwords including: enable, console, and VTY.
- Restrict console and VTY access to a Cisco device.
- Recover device passwords.

This section covers the following exam objectives:

- 205. Perform and verify initial switch configuration tasks including remote access management
- 405. Access and utilize the router to set basic parameters
- 417. Implement basic router security

### Device Password Facts

The following table lists three of the most common passwords that you can configure on your device:

Password Type	Description
Console	Controls the ability to log on to the router through a console connection
VTY	Controls the ability to log on to the router using a virtual terminal (VTY) connection
EXEC mode	Controls the ability to switch to configuration modes. There are two different passwords that might be used: <ul style="list-style-type: none"><li>• The <b>enable</b> password is stored in clear text in the configuration file.</li><li>• The <b>enable secret</b> password is stored encrypted in the configuration file.</li></ul> <b>Note:</b> The router always uses the enable secret password if it exists.

Be aware of the following recommendations for configuring router passwords:

- Passwords are case-sensitive.
- For security reasons, you should not use the same password for both your enable and enable secret passwords.
- You can set the enable, enable secret, and line passwords in setup mode.
- Cisco routers support Terminal Access Controller Access Control System (TACACS) and Remote Authentication Dial-In User Service (RADIUS) to centrally validate users attempting to gain access to the router.

The following table summarizes basic password commands.

Use ...	To ...
Router(config)#enable secret <password>	Set the encrypted password used for privileged mode access. The enable secret is always used if it exists.  This command uses the Message-Digest 5 (MD5) hashing algorithm to encrypt the password.
Router(config)#enable password <password>	Set the unencrypted password for privileged mode access. This password is used if the enable secret is not set.
Router(config)#line con 0	Switch to the line configuration mode for the console.
Router(config)#line vty <0-197> <1-197>	Switch to the line configuration mode for the virtual terminal. Specify one line number or a range of line numbers, for example: <b>line vty 0 4</b>
Router(config-line)#password	Set the line password (for either console or VTY access).
Router(config-line)#login	Require the password for line access.
Router(config)#no enable secret Router(config)#no enable password Router(config-line)#no login Router(config-line)#no password	Remove the password. The <b>no login</b> command disables password checking.
Router(config)#service password-encryption	Encrypt all passwords as a type 7 password. Encrypted type 7 passwords are not secure and can be easily broken; however, the encrypted values do provide some level of protection from someone looking over your shoulder after having issued the <b>show run</b> command. Rather than relying on this encryption, make sure to use the <b>enable secret</b> command for better encryption.

**Note:** If you do not use the **login** command in line mode, a password will *not* be required for access, even though one is set.

Access to the console through a Telnet session is controlled by the **login** and the **password** entries. To prevent VTY access, there must be a login entry *without* a password set. Access is allowed based on the following conditions:

- no login, no password = access is allowed without a password
- login, no password = access is denied (the error message indicates that a password is required but none is set)
- no login, password = access is allowed without a password
- login, password = access is allowed only with correct password

### Password Recovery Facts

Password recovery is the process of discovering or resetting forgotten router passwords. The exact process you use to recover lost passwords depends on the switch model. Listed below are the general steps you would take for the 2960 switch:

1. Establish a console connection to the switch.
2. Unplug the power cable.
3. Hold down the mode button while reconnecting the power cable to the switch. Release the mode button when the SYST LED blinks amber and then turns solid green. When you release the mode button, the SYST LED blinks green.
4. Type the **flash\_init** command.



5. Type the **load\_helper** command.
6. Type the **dir flash:** command. **Note:** make sure to include the colon (:).
7. Type **rename flash:config.text flash:config.old** to rename the configuration file.
8. Type the **boot** command to restart the system.
9. Enter **yes** to terminate autoinstall.
10. Enter **n** at the prompt to abort the initial configuration dialog.
11. Type **enable** to enter enable mode.
  - o To save the previous settings and configurations of the switch, type **rename flash:config.old flash:config.text**
  - o To overwrite the settings and configurations of the switch, type **copy flash:config.text system:running-config** to copy the configuration file into memory.
 

**Note:** the configuration file is now reloaded.
12. Enter configuration mode to change the passwords.
13. In global EXEC mode, type **copy run start** to save the changes.

To recover passwords on most routers, you need to modify the [configuration register](#) to bypass the startup-config file and boot the router with a limited IOS version. You can then load the existing startup-config file and view or modify the current password settings. The exact process you use to recover lost passwords depends on the router model. Listed below are the general steps you would take for the 1800 series routers:

1. Establish a console connection to the router.
2. At the prompt, type **show version**. Record the value for the configuration register (usually 0x2102).
3. Turn the router off and on.
4. Within 60 seconds, use the keyboard to send a break sequence to the router. For a Windows system, the break sequence is typically one of the following:
  - o Break + F5
  - o Shift + F5
  - o ^\$B (Shift + 6, Shift + 4, Shift + b)
5. Type **confreg 0x2142** to change the configuration register setting.
6. Type **reset** or **i** to reboot. With the configuration register changed, the router reboots bypassing the startup-config file.
7. The router will automatically enter Setup mode. At this point you can:
  - o Use Setup mode to configure the router (including the passwords).
  - o Quit Setup mode (using Ctrl + C) and change only the existing passwords.
    1. Type **enable** to enter privileged EXEC mode.
    2. Type **copy start run** to load the startup-config file.
    3. Enter configuration mode to change the passwords.
    4. Type **config-register 0x2102** to change the configuration register back to the default.
    5. Exit configuration mode and use **copy run start** to save the changes to the passwords.
8. Use the **reload** command to restart the router normally.

## Banners

As you study this section, answer the following questions:

- When do each of the banners display?
- What banner do you configure if you use the **banner** command without specifying the banner type?
- What is the role of the delimiting character?
- You type the following command at the router: **banner exec this is it**. What will show following a successful login?

After finishing this section, you should be able to complete the following tasks:

- Configure, modify, and delete router banners.

This section covers the following exam objectives:

- 205. Perform and verify initial switch configuration tasks including remote access management
- 405. Access and utilize the router to set basic parameters
- 417. Implement basic router security

### **Banner Command List**

Banners display messages that anyone logging into the device can see. The following four types of banners display at various times during the login or startup sequence.

<b>Use . . .</b>	<b>To . . .</b>
Router (config) #banner Router (config) #banner motd	Set the Message-of-the-day (MOTD) banner. The MOTD banner displays immediately after a connection is made.
Router (config) #banner login	Set the login banner. The login banner displays after the MOTD banner and before the login prompt.
Router (config) #banner exec	Set the EXEC banner. The exec banner displays after a successful login.
Router (config) #banner incoming	Set the incoming banner. The incoming banner displays for a reverse telnet session.
Router (config) #no banner <type>	Removes the specified banner

**Note:** The **banner** command without a keyword defaults to set the MOTD banner.

Follow the banner command with a delimiting character. The delimiter encloses the banner text, and helps the router identify the beginning and ending of the banner. This allows you to construct multiple-line banners.

### **Example**

The following commands set the MOTD, login, and EXEC banners, using # as the delimiting character and inserting a hard return between each banner:

```
Router(config)#banner motd # This is the Message-of-the-day banner!  
#  
Router(config)#banner login # This is the Login banner!  
#  
Router(config)#banner exec # This is the Exec banner!
```

#

## Cisco Discovery Protocol (CDP)

As you study this section, answer the following questions:

- What are the requirements for using CDP?
- You have not yet configured an IP address on a Cisco router, but the interface is up. Will the router be able to use CDP to discover neighboring device information?
- You want to view information about a router that is two hops away? How can you view this information?
- How do you turn off CDP advertisements for a single interface? How do you disable CDP on a router?

After finishing this section, you should be able to complete the following tasks:

- Use CDP to view information about neighboring devices.
- Enable and disable CDP on devices and specific interfaces.
- Configure CDP timers.

This section covers the following exam objectives:

- 205. Perform and verify initial switch configuration tasks including remote access management
- 405. Access and utilize the router to set basic parameters
- 406. Connect, configure, and verify operation status of a device interface

### CDP Command List

The Cisco Discovery Protocol (CDP) is a protocol that Cisco devices use to learn and share information about each other. Cisco devices, such as routers and switches, can discover neighboring Cisco devices through CDP.

- By default, CDP is enabled on all interfaces.
- CDP only shares information with directly connected (neighboring) devices.
- CDP works when there is a valid Data Link layer connection.
- CDP works regardless of the Network layer and other protocols used. It can discover information on LANs, Frame Relay, and other network architectures.

Use the following commands to customize and view CDP information.

Use ...	To ...
Router(config)#cdp holdtime <10-255>	Specify the amount of time that information in a packet is still valid (default = 180 seconds) Use the <b>no cdp holdtime</b> command to reset the value to its default.
Router(config)#cdp timer <5-900>	Specify how often CDP packets are exchanged (default = 60 seconds) Use the <b>no cdp timer</b> command to reset the value to its default.
Router(config)#cdp run	Enable CDP on the router
Router(config)#no cdp run	Disable CDP on a router, to prevent the router from exchanging CDP packets
Router(config-if)#cdp enable	Turns CDP for an interface on

Router(config-if)#no cdp enable	Turns CDP for an interface off
Router#show cdp	View CDP information
Router#show cdp interface	Show information about neighbors accessed through an interface Show CDP configuration information for the router including the holdtime, encapsulation, and CDP exchange interval
Router#show cdp neighbors	Show information about all neighboring Cisco devices including: <ul style="list-style-type: none"> <li>• Device ID</li> <li>• Local interface</li> <li>• Holdtime</li> <li>• Capability</li> <li>• Platform</li> <li>• Port ID</li> </ul>
Router#show cdp neighbors detail	Shows all information for the <b>show cdp neighbors</b> command and adds: <ul style="list-style-type: none"> <li>• Network address (such as the IP address)</li> <li>• Enabled protocols</li> <li>• Software version</li> </ul>
Router#show cdp entry *	Show the same information as <b>show cdp neighbors detail</b>
Router#show cdp entry <name of the neighbor>	Show the same information as <b>show cdp neighbors detail</b> , but only for the named neighbor
Router#show cdp traffic	Show the number of CDP advertisements sent and received

### Examples

The following commands turn on CDP for the router and configures it to send CDP packets every 90 seconds.

```
Router(config)#cdp run
Router(config)#cdp timer 90
```

The following commands turn off CDP on the router's first Ethernet interface.

```
Router(config)#int eth 0
Router(config-if)#no cdp enable
```

## Connecting Devices

As you study this section, answer the following questions:

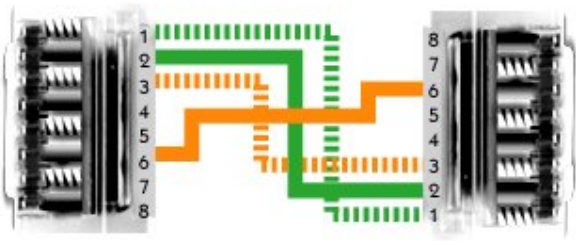
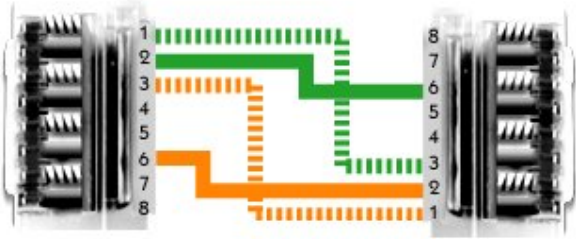
- When would you use a crossover cable when connecting to a Cisco device?
- What type of cable do you use to connect two switches?
- What is the SFP slot on a switch used for?
- How does Auto-MDI/MDIX affect cable selection when connecting devices?

This section covers the following exam objectives:

- 201. Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts
- 403. Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts

### LAN Connection Facts

When connecting devices in a LAN, you will need to use different types of Ethernet cables. You will need to know the pin positions of the cable types to differentiate them from each other. The types of Ethernet cables used for LAN connections include the following:

Type	Pin Position	Uses
 <p>Straight-through Ethernet Cable</p>	1 --> 1 2 --> 2 3 --> 3 6 --> 6	Use a straight-through Ethernet cable when connecting the following devices: <ul style="list-style-type: none"><li>• Workstation to hub</li><li>• Workstation to switch</li><li>• Router to hub</li><li>• Router to switch</li></ul>
 <p>Crossover Ethernet Cable</p>	1 --> 3 2 --> 6 3 --> 1 6 --> 2	Use a crossover Ethernet cable when connecting the following devices: <ul style="list-style-type: none"><li>• Switch to switch</li><li>• Switch to hub</li><li>• Hub to hub</li><li>• Workstation to router</li><li>• Workstation to workstation</li><li>• Router to router</li></ul>

Be aware of the following when making LAN connections:

- Through Auto-MDI/MDIX, newer switches can determine what type of Ethernet cable is needed and will internally change the sending/receiving pin positions if needed.
- Some Cisco routers provide a generic Attachment Unit Interface (AUI) port. The AUI port is designed to connect to an external transceiver for conversion to a specific media type, such as coaxial or fiber optic.

- To support LAN distances above twisted pair Ethernet limits (>100 meters), use the switch's SFP slot (a Gigabit uplink port) and fiber optic media.

## Switch Configuration

As you study this section, answer the following questions:

- What configuration modes are unique to switches?
- How do you identify ports which are administratively shut down?
- What information does the SYST LED provide?

After finishing this section, you should be able to complete the following tasks:

- Configure basic switch port parameters.
- View port statuses.

This section covers the following exam objectives:

- 205. Perform and verify initial switch configuration tasks including remote access management
- 207. Identify, prescribe, and resolve common switched network media issues, configuration issues, auto negotiation, and switch hardware failures
- 215. Interpret the output of various show and debug commands to verify the operational status of a Cisco switched network.

### Switch Activity Facts

In this course, you will learn how to configure the Catalyst 2960 series switch. The 2960 series switch has various status lights (or LEDs) which provide information about the switch's activity.

Light	Meaning
SYST (System)	<p>A single system light gives you information about the overall switch status.</p> <ul style="list-style-type: none"><li>• Solid green = System is operational</li><li>• Solid amber = System is receiving power but is not functioning properly</li><li>• Off = System is not powered on</li></ul>
RPS (Redundant Power Supply)	<p>A single RPS light shows the status of the redundant power supply.</p> <ul style="list-style-type: none"><li>• Solid green = RPS is present and ready to provide back-up power</li><li>• Flashing green = RPS is connected, but is unavailable because it is providing power to another device</li><li>• Solid amber = RPS is in standby mode or in a fault condition</li><li>• Off = RPS is off or not properly connected</li></ul>
Port	<p>Each port has a light that indicates the status of the port. By pressing the <b>Mode</b> button, you can view three different types of information for each port.</p>
	<p>When the <b>Mode</b> button selects Stat:</p> <ul style="list-style-type: none"><li>• Solid green = Link present and is operational</li><li>• Flashing green = Link activity (port is sending or receiving data)</li><li>• Alternating green-amber = Link fault (Error frames can affect connectivity, and errors such as excessive collisions, cyclic redundancy check (CRC) errors, and alignment and jabber errors are monitored for a link-fault indication)</li><li>• Solid amber = Port is blocked by Spanning Tree Protocol (STP) and <i>is not</i> forwarding data</li></ul>



	<ul style="list-style-type: none"> <li>Flashing amber = Port is blocked by STP and <i>is</i> sending or receiving packets</li> <li>Off = No link, or port was administratively shut down (if viewing the port status with the GUI, a brown color indicates a shut down port)</li> </ul>
Duplex (Port duplex mode)	<p>When the <b>Mode</b> button selects Duplex:</p> <ul style="list-style-type: none"> <li>Solid green = Full duplex</li> <li>Off = Half duplex, or no link present (if viewing the port duplex with the GUI, a blue color indicates half duplex)</li> </ul>
Speed (Port speed)	<p>When the <b>Mode</b> button selects Speed:</p> <ul style="list-style-type: none"> <li>Flashing green = 1000 Mbps (1 Gbps)</li> <li>Solid green = 100 Mbps</li> <li>Off = 10 Mbps, or no link present (if viewing the port speed with the GUI, a blue color indicates 10 Mbps)</li> </ul>

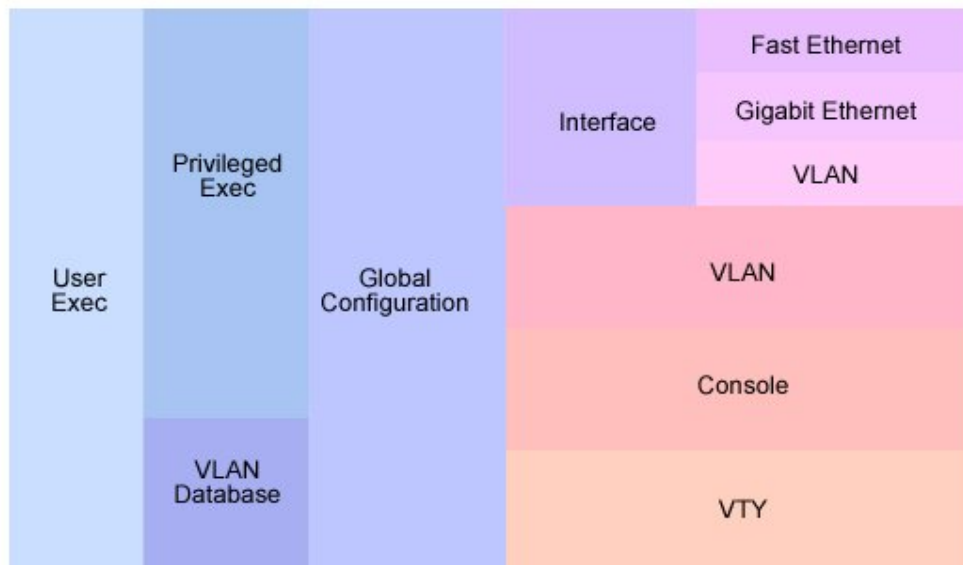
On a simple LAN, you can connect the switch to the network, connect devices, and it will automatically begin switching traffic to the correct ports. The switch comes preconfigured to work out-of-the-box without configuration. To customize the switch configuration, connect to the switch in one of the following ways:

- Console connection
- Telnet session
- Web management software (connect through the LAN through a Web browser)

**Note:** You must configure an IP address for the switch to manage it through a Telnet or Web session.

### Switch Configuration Modes

The following graphic illustrates some of the configuration modes of the switch.



The following table describes some of the configuration modes of the switch:

Mode	Details	CLI Mode Prompt
Interface configuration	<p>The switch has multiple interface modes depending on the physical (or logical) interface type. For this course, you should be familiar with the following switch interface modes:</p> <ul style="list-style-type: none"> <li>• Ethernet (10 Mbps Ethernet)</li> <li>• FastEthernet (100 Mbps Ethernet)</li> <li>• GigabitEthernet (1 GB Ethernet)</li> <li>• VLAN</li> </ul> <p><b>Note:</b> The VLAN interface configuration mode is used to configure the switch IP address and other management functions. It is a logical management interface configuration mode, instead of a physical interface configuration mode as used for the FastEthernet and GigabitEthernet ports.</p>	Switch(config-if)#
Config-vlan	<p>Details of the config-vlan mode include the following:</p> <ul style="list-style-type: none"> <li>• You can use the config-vlan mode to perform all VLAN configuration tasks.</li> <li>• Changes made in vlan mode take place immediately.</li> </ul> <p><b>Note:</b> Do not confuse the config-vlan mode with the VLAN interface configuration mode.</p>	Switch(config-vlan)#
VLAN configuration	<p>Details of the VLAN configuration mode include the following:</p> <ul style="list-style-type: none"> <li>• The vlan configuration mode allows you to only configure a subset of VLAN features.</li> <li>• Changes made in the VLAN configuration mode do not take effect until you save the changes, either before or while exiting the configuration mode.</li> <li>• Changes made in the VLAN configuration mode are not stored in the regular switch configuration file.</li> </ul> <p><b>Note:</b> The 2960 switch recommends that you configure VLAN parameters from config-vlan mode, because VLAN configuration mode is being deprecated (phased out).</p>	Switch(vlan)#
Line configuration	Use this mode to configure parameters for the terminal line, such as the console, Telnet, and SSH lines.	Switch(config-line)#

### Switch Configuration Command List

The following table lists common switch configuration commands:

Task	Command
Move to interface configuration mode	<pre>switch(config)#interface FastEthernet 0/14 switch(config)#interface GigabitEthernet 0/1</pre>
Move to configuration mode for a range of interfaces	<pre>switch(config)#interface range fastethernet 0/14 - 24 switch(config)#interface range gigabitethernet 0/1 - 4</pre>

	switch(config)#interface range fa 0/1 - 4 , 7 - 10 switch(config)#interface range fa 0/8 - 9 , gi 0/1 - 2
Set the port speed on the interface	switch(config-if)#speed 10 switch(config-if)#speed 100 switch(config-if)#speed 1000 switch(config-if)#speed auto
Set the duplex mode on the interface	switch(config-if)#duplex half switch(config-if)#duplex full switch(config-if)#duplex auto
Enable or disable the interface	switch(config-if)#no shutdown switch(config-if)#shutdown
Show interface status of all ports	switch#show interface status
Show line and protocol status of all ports	switch#show ip interface brief

Be aware of the following switch configuration details:

- All switch ports are enabled (no shutdown) by default.
- Port numbering on some switches begins at 1, not 0. For example, **FastEthernet 0/1** is the first FastEthernet port on a 2960 switch.
- Through auto-negotiation, the 10/100/1000 ports configure themselves to operate at the speed of attached devices. If the attached ports do not support auto-negotiation, you can explicitly set the speed and duplex parameters.
- If the speed and duplex settings are set to **auto**, the switch will use auto-MDIX to sense the cable type (crossover or straight-through) connected to the port and will automatically adapt itself to the cable type used. When you manually configure the speed or duplex setting, it disables auto-MDIX so you will need to be sure to use the correct cable.
- The 2960 switch always uses the store-and-forward switching method. On other switch models, you might be able to configure the switching method.

### Switch Interface Status Facts

You can use the interface status to understand connectivity problems and quickly see whether the link between the device and the network is operational. Use the following commands to view the interface status:

Use...	To...
switch#show interfaces	List a large set of information about each interface.
switch#show interface status	View summary information about the interface status.
switch#show ip interfaces	View a small set of information about each IP interface.
switch#show ip interfaces brief	View a single line of information about each IP interface.

The following table summarizes some possible conditions indicated by the interface status for Ethernet interfaces:

Line status	Protocol status	Interface status	Indicates...
administratively down	down	disabled	The interface is administratively disabled with the <b>shutdown</b> command.

down	down	notconnect	<p>There is a hardware or network connection problem (Physical layer), such as:</p> <ul style="list-style-type: none"> <li>• No cable is connected.</li> <li>• The cable is connected but is improperly wired (or broken) so that signals cannot be sent or received correctly.</li> <li>• The device on the other end of the cable is powered off or the other interface is administratively shut down.</li> </ul>
down	down	err-disabled	Port security has disabled the switch port.
up	up	connected	The interface is working correctly and a live connection is present.

## TCP/IP Configuration

As you study this section, answer the following questions:

- What is the minimum amount of information a workstation needs to communicate on a single subnet? What additional configuration values are required for inter-network communications?
- What address range indicates an APIPA address assignment?
- What are the drawbacks to using manual IP address assignments?
- Why does a switch have an IP address? Which interface is assigned the IP address?

After finishing this section, you should be able to complete the following tasks:

- Configure workstation TCP/IP settings.
- Configure an IP address and default gateway on a switch.
- Configure a router interface with an IP address.

This section covers the following exam objectives:

- 205. Perform and verify initial switch configuration tasks including remote access management
- 304. Implement static and dynamic addressing services for hosts in a LAN environment
- 405. Connect, configure, and verify operation status of a device interface

### TCP/IP Configuration Facts

The following table summarizes many of the configuration settings for a TCP/IP network.

Parameter	Purpose
IP address	Identifies both the logical host and logical network addresses. Two devices on the same network must have IP addresses with the same network portion of the address.
Subnet mask	Identifies which portion of the IP address is the network address. Two devices on the same network must be configured with the same subnet mask.
Default gateway	Identifies the router to which packets for remote networks are sent. The default gateway address is the IP address of the router interface on the same subnet as the local host. Without a default gateway set, most clients will be unable to communicate with hosts outside of the local subnet.
Host name	Identifies the logical name of the local system.
DNS server	Identifies the DNS server that is used to resolve host names to IP addresses.
MAC address	Identifies the physical address. On an Ethernet network, this address is burned in to the network adapter hardware.

**Note:** A host requires an IP address and subnet mask to communicate on a single subnet. A default gateway address is required to enable inter-subnet communications. At least one DNS server address is required for the host to use hostnames when contacting other hosts.

Several of the TCP/IP configuration settings can be assigned through the following methods:

Method	Description
Dynamic Host Configuration Protocol (DHCP)	<p>A DHCP server is a special server configured to pass out IP address and other IP configuration information to network clients.</p> <ul style="list-style-type: none"><li>• The DHCP server is configured with a range of IP addresses it can</li></ul>

	<p>assign to hosts.</p> <ul style="list-style-type: none"> <li>• The DHCP server can also be configured to pass out other IP configuration such as the default gateway and DNS server addresses.</li> <li>• The DHCP server ensures that each client has a unique IP address.</li> <li>• DHCP is a TCP/IP protocol. Any client configured to use DHCP can get an IP address from any server configured for DHCP, regardless of the operating system.</li> </ul> <p>DHCP requires a DHCP server and minimal configuration.</p>
Automatic Private IP Addressing (APIPA)	<p>APIPA is a Microsoft implementation of automatic IP address assignment without a DHCP server. Using APIPA, hosts assign themselves an IP address on the 169.254.0.0 network (mask of 255.255.0.0). With APIPA:</p> <ul style="list-style-type: none"> <li>• The host is configured to obtain IP information from a DHCP server (this is the default configuration).</li> <li>• If a DHCP server can't be contacted, the host uses APIPA to assign itself an IP address.</li> <li>• The host only configures the IP address and mask. It does not assign itself the default gateway and DNS server addresses. For this reason, APIPA can only be used on a single subnet.</li> </ul> <p>Use APIPA as a fail safe for when a DHCP server is unavailable to provide limited communication capabilities.</p>
Static (manual) assignment	<p>Using static addressing, IP configuration information must be manually configured on each host. Use static addressing:</p> <ul style="list-style-type: none"> <li>• On networks with a very small number of hosts.</li> <li>• On networks that do not change often or that will not grow.</li> <li>• To permanently assign IP addresses to hosts that must always have the same address (such as printers, servers, or routers).</li> <li>• For hosts that cannot accept an IP address from DHCP.</li> <li>• To reduce DHCP-related traffic.</li> </ul> <p><b>Note:</b> Static addressing is very susceptible to configuration errors and duplicate IP address configuration errors (two hosts that have been assigned the same IP address). Static addressing also disables both APIPA and DHCP capabilities on the host.</p>

### Switch IP Configuration Facts

Keep in mind the following facts about IP addresses configured on switches:

- Basic switches operate at Layer 2, and therefore do not need an IP address to function. In fact, a switch performs switching functions just fine without an IP address set.
- You only need to configure a switch IP address if you want to manage the switch from a Telnet or Web session.
- The switch itself has only a single (active) IP address. Each switch port does *not* have an IP address (unless the switch is performing Layer 3 switching, a function which is not supported on all switches). The IP address identifies the switch as a host on the network but is not required for switching functions.

To configure the switch IP address, you set the address on the VLAN interface. This is a logical interface defined on the switch to allow management functions. By default, this VLAN is VLAN 1. Use the following commands to configure the switch IP address:

```
switch#config terminal
switch(config)#interface vlan 1
switch(config-if)#ip address 1.1.1.1 255.255.255.0
switch(config-if)#no shutdown
```

To enable management from a remote network, you will also need to configure the default gateway. Use the following command in global configuration mode:

```
switch(config)#ip default-gateway 1.1.1.254
```

**Note:** You can use the **ip address dhcp** command to configure a switch (or a router) to get its IP address from a DHCP server. The DHCP server can be configured to deliver the default gateway and DNS server addresses to the Cisco device as well. The manually-configured default gateway address overrides any address received from DHCP.

## DHCP

As you study this section, answer the following questions:

- What is the difference between the ARP and RARP protocols?
- What is the difference between the BootP and DHCP protocols?
- What type of information is delivered by DHCP options?
- How can you make sure a specific host gets the same IP address from the DHCP server each time it boots?
- How does the router determine which interfaces will respond to DHCP requests?
- How can you enable DHCP messages to work across subnets?

After finishing this section, you should be able to complete the following tasks:

- Use the SDM interface to configure the DHCP service on a router.

This section covers the following exam objectives:

- 302. Explain the operation and benefits of using DHCP and DNS
- 303. Configure, verify and troubleshoot DHCP and DNS operation on a router
- **Address Resolution Protocols**
- You should know the following protocols that perform address resolution.

Protocol	Description
Address Resolution Protocol (ARP)	Used by hosts to discover the MAC address of a computer from its IP address.
Reverse Address Resolution Protocol (RARP)	Used by a host to discover the IP address of a computer from its MAC address.
Bootstrap Protocol (BootP)	Used by a host (such as a diskless workstation) to query a bootstrap computer and receive an IP address assignment. A BootP server has a static list of MAC addresses and their corresponding IP addresses.
Dynamic Host Configuration Protocol (DHCP)	An improvement on BootP, DHCP is used to dynamically assign IP address and other TCP/IP configuration parameters. A DHCP server can use a static list to assign a specific IP address to a specific host. More commonly, however, the DHCP server automatically assigns an IP address from a preset range of possible addresses.

### DHCP Configuration Facts

Dynamic Host Configuration Protocol (DHCP) is a protocol used by hosts to obtain various parameters necessary for the clients to operate in a network. You can configure DHCP on a Cisco device through the command line interface (CLI) or the Security Device Manager (SDM). DHCP configuration parameters include the following:

Component	Description
Address pool	The <i>address pool</i> is the range of addresses which can be assigned to requesting hosts. The DHCP server only assigns addresses within the address pool. The DHCP server can also be configured to not assign specific addresses in the range, known as <i>exclusions</i> .
Lease	The <i>lease</i> is the length of time for which the assignment is valid. It contains the assigned IP address and other information for the client. Periodically and when the client reboots, it contacts the DHCP server to renew the lease on the IP address.



DHCP options	<p>In addition to the IP address and subnet mask, the DHCP server can also deliver the following:</p> <ul style="list-style-type: none"> <li>• Domain Name Server (DNS) server address(es)</li> <li>• Default router (or default gateway) address</li> <li>• WINS server addresses</li> <li>• Additional TCP/IP configuration parameters</li> </ul>
Binding	<p>A <i>binding</i> is an association of a MAC address with a specific IP address. When you create a binding, the client with the specified MAC address is assigned the same IP address each time it requests an address. For example, if you have servers which should be accessible from outside the local network, the servers' IP addresses should remain the same. A binding is also known as <i>DHCP reservation</i>.</p>
Interface	<p>The interface that responds to DHCP requests is identified automatically according to the IP address assigned to the interface. When you configure the DHCP service on a Cisco device, it compares the subnet address specified in the address pool with the IP addresses assigned to the router interfaces. If the interface has been assigned an IP address in the address pool, that interface will listen for and respond to DHCP requests.</p> <ul style="list-style-type: none"> <li>• To allow an interface to listen and respond to DHCP requests, assign it an IP address within the address pool. If the interface does not have an IP address, or if the IP address is not within the address pool, client DHCP requests will be ignored.</li> <li>• You should exclude the interface IP address from the DHCP address pool.</li> </ul>

A DHCP client uses the following process to obtain an IP address:

1. Lease Request. The client initializes a limited version of TCP/IP and broadcasts a DHCPDISCOVER packet requesting the location of a DHCP server.
2. Lease Offer. All DHCP servers with available IP addresses send DHCPOFFER packets to the client. These include the client's hardware address, the IP address the server is offering, the subnet mask, the duration of the IP lease, and the IP address of the DHCP server making the offer.
3. Lease Selection. The client selects the IP address from the first offer it receives and broadcasts a DHCPREQUEST packet requesting to lease the IP address in that offer.
4. IP Lease Acknowledgment. The DHCP server that made the offer responds and all other DHCP servers withdraw their offers. The IP addressing information is assigned to the client and the offering DHCP server sends a DHCPACK (acknowledgement) packet directly to the client. The client finishes initializing and binding the TCP/IP protocol.

The DHCP lease process uses frame-level broadcasts. For this reason, DHCP requests typically do not pass through routers to other subnets. To enable DHCP across subnets:

- Enable BootP (DHCP broadcast) requests through the router.
- Configure a computer for BootP forwarding to request IP information on behalf of other clients.

## DNS

After finishing this section, you should be able to complete the following tasks:

- Disable name resolution on a Cisco device.
- Create static DNS entries on a router.

This section covers the following exam objectives:

- 302. Explain the operation and benefits of using DHCP and DNS
- 303. Configure, verify and troubleshoot DHCP and DNS operation on a router

### **DNS Services Command List**

The Domain Name System (DNS) is a database that maps logical host names to IP addresses. The following table describes the difference between a router and a workstation when resolving a logical host name to an IP address:

Device	Details
Router	A router's DNS name resolution looks for information in the following places (in this order): <ol style="list-style-type: none"><li>1. Static DNS entries</li><li>2. DNS server query (if enabled)</li></ol>
Workstation	A workstation's DNS name resolution looks for information in the following places (in this order): <ol style="list-style-type: none"><li>1. Local DNS cache</li><li>2. HOSTS file</li><li>3. DNS server query (Primary)</li><li>4. DNS server query (Secondary)</li></ol> <p><b>Note:</b> Additional DNS servers are only consulted if the primary DNS server did not respond (i.e. it is offline).</p>

Use the following commands to configure DNS services on a router:

Use...	To...
<code>router(config)#ip host &lt;name&gt; a.b.c.d</code>	Create static DNS entries
<code>router(config)#ip domain-name &lt;name&gt;</code>	Configure the router default domain (for DNS)
<code>router(config)#ip name-server a.b.c.d</code>	Set the default DNS name server
<code>router(config)#ip domain-lookup</code>	Enable the router to use DNS to identify IP addresses from host names
<code>router(config)#no ip domain-lookup</code>	Disable the broadcast name resolution of host names.
<code>router#show hosts</code>	Display a list of known IP hosts

## Routing

As you study this section, answer the following questions:

- What is the difference between a static and a default route?
- In what cases would you use a static route rather than a routing protocol?
- What does a route to network 0.0.0.0 identify?
- What happens to a packet that does not match any of the routes in a routing table?
- What does an asterisk ( \* ) on a route indicate?
- How does a router choose between two routes to the same destination network?

After finishing this section, you should be able to complete the following tasks:

- Configure static routes.
- Configure RIPv2 routing.

This section covers the following exam objectives:

- 401. Describe basic routing concepts (including: packet forwarding, router lookup process)
- 404. Configure, verify, and troubleshoot RIPv2
- 408. Perform and verify routing configuration tasks for a static or default route given specific routing requirements

### **Static and Default Route Command List**

Most networks will use one (or more) routing protocols to automatically share and learn routes. Listed below are several situations when you might want to configure static routes.

- To configure a default route or a route out of a *stub* network (a stub network is one that has a single route into and out of the network).
- For small networks that do not change very often and that have only a few networks.
- To turn off all routing protocols and reduce traffic or improve security.
- To configure routes that are lost due to [route summarization](#).

A *default route* is a route that is considered to match all destination IP addresses. With a default route, when a packet's destination IP address does not match any other routes, the router uses the default route for forwarding the packet. Be aware of the following default route details:

- Default routes work best when only one path exists to a part of the network.
- One default route in the routing table could replace hundreds of static route entries in the routing table.
- When the default route is not set, the router discards packets that do not match a route in the routing table.

The following table lists the commands for configuring static routes:

<b>Use ...</b>	<b>To ...</b>
Router(config)#ip route <destination> <next_hop>	Identify a next hop router to receive packets sent to the specified destination network.
Router(config)#ip route <destination> <interface>	Identify the interface used to forward packets to the specified destination network.
Router(config)#ip route 0.0.0.0 0.0.0.0 <next hop or interface>	Identify a default route to the specified destination network or through an interface. This is a method to set the gateway of last resort on a router.

Router(config)#ip classless	Enables the router to match routes based on the number of bits in the mask and not the default subnet mask.
Router#show ip route	View the routing table.
Router#show ip route <hostname or address>	View details about the specific route.

**Note:** Configuring a static route to network 0.0.0.0 with mask of 0.0.0.0 is the most common method of configuring a default gateway. However, the following methods can also be used under certain circumstances:

- Use the **ip default-network** command to designate a route already in the routing table as the default route. For example, if the router had learned of network 10.0.0.0/8 through a routing protocol, you could use the following command to designate that network as the default network:  
**ip default-network 10.0.0.0**  
Be aware that the **ip default-network** command only makes a route a *candidate* for the default route, it does not necessarily guarantee that the route will be used to route packets to unknown destinations.
- Use the **ip default-gateway** command if IP routing has been disabled on the router. With IP routing disabled, routes will not be learned through a routing protocol, nor will static routes be used if configured. With IP routing enabled, the **ip default-gateway** setting will not be used.

### Examples

The following command creates a static route to network 192.168.1.0 through the router with the IP address 192.168.1.35 and gives it an administrative distance value of 25.

```
Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.35 25
```

The following command identifies a default route through an interface with address 10.1.1.2.

```
Router(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

### RIP Command List

The Routing Information Protocol (RIP) is a simple, effective routing protocol for small- to medium-sized networks. By using a routing protocol, routers automatically share route information, reducing the amount of administration required for maintaining routes between networks.

To configure any routing protocol, use the following three steps:

1. Enable IP routing if it is not already enabled (use the **ip routing** command). By default, IP routing is already enabled, so this step is rarely required.
2. Switch to router configuration mode (use the **router** command, followed by the routing protocol you want to configure).
3. Identify the networks that will participate in dynamic routing (use the **network** command, followed by the address of a network to which the router is directly connected). This identifies the interfaces that will share and process received routing updates.
4. Configure any additional parameters based on the routing protocol.

The following table lists commands for configuring RIP.

Use ...	To ...
Router (config) #ip routing	Enable IP routing for the entire router. IP routing is enabled by default. Use this command only if it has been disabled.

	Use the <b>no ip routing</b> command to disable routing.
Router (config)#router rip	Enter router RIP configuration mode. Use the <b>no router rip</b> command to disable rip, removing all defined networks.
Router (config- router)#version 2	Enable RIP version 2 on the router.
Router (config- router)#network <address>	Identify networks that will participate in the router protocol. Notice that you identify <i>networks</i> , and not <i>interfaces</i> .  When you use the network command to identify the networks that will participate in RIP routing, follow these rules. <ul style="list-style-type: none"> <li>• Identify only networks to which the router is directly connected.</li> <li>• Use the <i>classful</i> network address, not a subnetted network address. (The router will automatically convert a subnetted network address into a classful network address by removing subnetted network information.)</li> </ul> Use the <b>no network</b> command to remove any network entries.
Router#show ip route	View the routing table.
Router#show ip route <hostname or address>	View details about the specific route.

### Example

The following commands enable IP routing and identify two networks that will participate in the RIPv2 routing protocol.

```
Router (config)#ip routing
Router (config)#router rip
Router (config-router)#version 2
Router (config-router)#network 10.0.0.0
Router (config-router)#network 192.168.10.0
```

### Routing Table Facts

The router uses the routing table to determine where to send packets. When a packet is received, it compares the destination IP address contained in the packet with all known routes in the routing table.

- The destination address is compared to the networks in the routing table looking for a match.
- A match is made when the destination IP address is on the same subnet as indicated by the route in the routing table.
- The IP address might match more than one route in the routing table. If that is the case, the most specific routing table entry is used (i.e. the network with the subnet mask that has the greatest number of significant bits).
- When a match is found, the packet is sent out the specified router interface to the next hop router address.
- If no match is found, the packet is dropped (not forwarded).

Use the **show ip route** command to view the routing table. A sample output of this command is shown below.

```
Router1841#sh 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 192.168.2.1 to network 0.0.0.0

```
R   172.16.0.0/16 [120/1] via 192.168.1.1, 00:00:08, FastEthernet0/0
R   172.17.0.0/16 [120/2] via 192.168.1.1, 00:00:08, FastEthernet0/0
C   192.168.1.0/24 is directly connected, FastEthernet0/0
C   192.168.2.0/24 is directly connected, FastEthernet0/1
S*  0.0.0.0 [1/0] via 192.168.2.1
```

The following table describes important information shown in the command output:

Component	Description
Gateway of last resort	<p>The gateway of last resort identifies a route to use if the packet does not match any other route. In this example, the route of 0.0.0.0 with a mask of 0.0.0.0 matches every packet. If the destination IP address does not match any other route, the next hop address of 192.168.2.1 is used for this packet.</p> <p><b>Note:</b> If the output shows the line <b>Gateway of last resort is not set</b>, then the router can only send packets to the specific routes listed in the routing table. Packets that do not match a specific route will be dropped.</p>
Route type	<p>The first characters of a routing table entry identifies the source or type of the route.</p> <ul style="list-style-type: none"> <li>• <b>C</b> is for directly connected networks</li> <li>• <b>S</b> is for static routes</li> <li>• <b>R</b> is for routes learned through RIP</li> <li>• Additional codes indicate routes learned through other routing protocols</li> </ul> <p>A route marked with * indicates a route that is a candidate for the default route. The router uses this route to determine whether the route can be used to set the gateway of last resort information. If it meets several conditions, the information in the route marked with * is used for the gateway of last resort information.</p>
Network	<p>Following the route type is the network address and subnet mask. This identifies the specific subnet address for the route.</p>
Administrative distance and cost	<p>The numbers in brackets following non-connected routes identify the following two items:</p> <ul style="list-style-type: none"> <li>• The first number is the administrative distance. The administrative distance is a description of the trustworthiness or preferability of a route learned from a specific source. Each source type (such as each routing protocol) is given a different administrative distance value. A lower number indicates a more preferred route. For example, a static route (AD = 1) is preferred over a route learned through RIP (AD = 120).</li> <li>• The second number is the cost to reach the route. The meaning of the route cost number is different depending on the source of the route, but generally it identifies how far away the destination is, either in distance or time. The cost is also referred to as the <i>metric</i>. The cost is only comparable when talking about routes learned from the same routing protocol. For example:</li> </ul>

	<ul style="list-style-type: none"> <li>○ For two RIP routes, a cost of 1 indicates a lower-cost (shorter) route than a route with a cost of 2.</li> <li>○ For a route learned through EIGRP, a cost of 312560 might identify a route that is faster than a route learned through RIP with a cost of 2.</li> </ul> <p><b>Note:</b> Be aware that the administrative distance is used to select a route learned between different protocols, while the cost is used to select the best route learned by the same protocol.</p>
Next hop router	The address indicated by <b>via</b> identifies the router address where packets will be sent when sending to the destination network. The next hop router address is a router on the same subnet as a directly connected interface. However, this does not mean that the next hop router is connected directly to the destination network, but rather that it is the next stop in the path to the destination.
Last update	For routes learned through a routing protocol, the time value (such as 00:00:08) indicates the elapsed time since the last update about the route was received. Most protocols periodically send information about known routes. The update time helps you to know the age of the route information.
Out interface	The interface designation at the end of the route identifies the local router interface used to reach the next hop router and therefore to reach the destination network.

Be aware of the following:

- Connected routes will only show if the interface has been assigned an IP address and is also up.
- Static routes will only show if the interface used to reach the next hop router is up.
- Having a route marked as a candidate default route does not necessarily mean that the router has a gateway of last resort set. To determine whether the router will route packets to unknown networks, examine the **Gateway of last resort** line for a next hop address.



## Verifying TCP/IP Configuration

As you study this section, answer the following questions:

- What are the differences and similarities between **ping** and **tracert**?
- You can ping a device but can't open a Telnet session with that device. What is the problem?
- Which utility can you use to test upper-layer protocols as well as lower-layer connectivity?
- Which utility would you use on a workstation to view the IP address received from the DHCP server?

After finishing this section, you should be able to complete the following tasks:

- Use **ping** and **tracert** to verify connectivity between devices.

This section covers the following exam objectives:

- 110. Identify and correct common network problems at layers 1, 2, 3 and 7 using a layered model approach
- 206. Verify network status and switch operation using basic utilities (including: ping, tracert, telnet, SSH, arp, ipconfig), SHOW & DEBUG commands
- 309. Identify and correct common problems associated with IP addressing and host configurations
- 407. Verify device configuration and network connectivity using ping, tracert, telnet, SSH or other utilities
- 414. Verify network connectivity (including: using ping, tracert, and telnet or SSH)
- **ICMP Messages**
- The Internet Control Message Protocol (ICMP) is a special-purpose message mechanism added to the TCP/IP suite that lets computers and routers in an internetwork report errors or provide information about unexpected circumstances. Remember that IP is a connectionless protocol and as such, contains no procedures that help to monitor successful packet delivery or test connectivity. Hosts use ICMP to send error messages to other hosts.
- ICMP messages include the following types:

Message	Characteristics
Echo	The ICMP echo message is used to discover hosts and networks, and to verify that they are reachable. The ping utility is a popular utility that uses ICMP echo messages.
Destination unreachable	The destination unreachable message is sent if a packet cannot reach its destination for a variety of reasons. It might indicate the host is unavailable, or that there were problems detected in the packet header.
Time exceeded	The time exceeded message is sent when the packet's time-to-live (TTL) counter has expired.
Redirect	The redirect message is sent from a router to the sending device to indicate that a different route should be chosen for the packet. The redirect message can be sent if a better route is in the router's table, or if the selected route is unavailable or congested.
Source quench	The source quench message is sent by a receiving device to indicate that the flow of packets is too fast. When a sending device receives a source quench message, it slows its rate of transmission.
Router discovery	The router discovery message is a special broadcast message sent by hosts to discover the routers on a network. Routers respond to the message indicating their presence. They do not exchange routing information, but simply announce their availability.



## TCP/IP Utilities

The following table describes three utilities you can use to test network connectivity between devices. You can use these utilities on Windows workstations as well as Cisco devices.

Utility	Description
Ping	<p>Ping sends an ICMP echo request/reply packet to a remote host. A response from the target device verifies that the host can communicate with the destination.</p> <ul style="list-style-type: none"><li>• Ping operates at the Network layer.</li><li>• A successful ping test verifies Network-layer connectivity between devices as well as the TCP/IP configuration of all devices in the path.</li><li>• Ping reports success or failure, together with round-trip statistics.</li></ul>
Traceroute	<p>Traceroute uses ICMP echo request/reply packets together with the Time-to-Live (TTL) value in those packets to identify the path between two devices. Traceroute sends successive ICMP messages to a destination with increasing TTL values. For example, the first test pings the destination using a TTL of 1, the second pings with a TTL of 2, and so on. By default, traceroute sends three ping tests for each TTL value.</p> <ul style="list-style-type: none"><li>• Traceroute operates at the Network layer.</li><li>• Like ping, a successful test verifies Network-layer connectivity and TCP/IP configuration of devices in the path.</li><li>• Traceroute reports success or failure for each hop in the path, along with the IP address and hostname (if available) of each hop. Statistics for each hop are also reported.</li></ul> <p>On a Windows workstation, use the <b>tracert</b> command to perform a traceroute test.</p>
Telnet	<p>Telnet is an application that establishes a remote session with a destination device. For example, you use Telnet from a workstation or a Cisco device to create a remote console session with another device.</p> <ul style="list-style-type: none"><li>• Telnet operates at the Application layer.</li><li>• A successful test verifies Application-layer connectivity. Because Telnet relies on lower-layer protocols, a successful Telnet session also verifies Network-layer and TCP/IP configuration.</li><li>• A successful Telnet test opens a remote connection to the target device.</li></ul> <p><b>Note:</b> A successful Telnet test means that ping and traceroute will also be successful. A failed Telnet test only indicates a failure at the Application layer or below. By itself, it does not tell you at which layer the problem exists.</p>

Be aware of the following when working with these utilities on Cisco devices:

- When using ping, an exclamation mark indicates a successful ping, while a period indicates a failure.
- Both ping and traceroute include a standard or an extended mode.
  - Extended mode is available only in privileged EXEC mode.
  - Use extended mode to modify the number of tests performed or the timeout period.
  - Use extended mode to test non-IP protocols (such as AppleTalk or Novell IPX).
- Responses to each test within the traceroute command are as follows:
  - A **time exceeded** message indicates that a router has received the packet but the TTL has expired. For example, if the TTL is set to 3, the third router in the path responds with the time exceeded message.

- A **destination unreachable** message indicates that the router in the path does not have a route to the destination network or device, or the destination device is down.
- An asterisk ( \* ) indicates that the timer has expired without a response.

**Note:** The **time exceeded** and **destination unreachable** messages depend on the configuration of the intermediary and destination devices. Many devices are configured to not respond to ICMP messages, so you might see an asterisk even if the router in the path has received the packet.

- When using Telnet:
  - To suspend a Telnet session, press Ctrl + Shift + 6, then X.
  - To resume a Telnet session, use the **resume** command.
  - By default, debug information shows only on the console, not in the Telnet session window. Use the **terminal monitor** command to show debug information in a Telnet session.

### Workstation TCP/IP Utilities

In addition to using ping, tracer, and Telnet on a Windows workstation to test Network- and Application-layer connectivity, you can use the following utilities to verify the configuration of the workstation.

Utility	Description
Ipconfig	<p><b>Ipconfig</b> displays IP configuration information for network adapters including:</p> <ul style="list-style-type: none"> <li>• IP address and mask</li> <li>• Default gateway</li> <li>• DNS and WINS server addresses</li> <li>• IP address of the DHCP server used for configuration</li> <li>• MAC address</li> </ul> <p>Use the <b>ipconfig</b> command as follows:</p> <ul style="list-style-type: none"> <li>• Use <b>ipconfig</b> to view IP address, subnet mask, and default gateway configuration</li> <li>• Use <b>ipconfig /all</b> to view detailed configuration information.</li> <li>• Use <b>ipconfig /release</b> to release the IP configuration information obtained from the DHCP server.</li> <li>• Use <b>ipconfig /renew</b> to request new IP configuration information from the DHCP server.</li> </ul>
Arp	<p>The ARP cache keeps a mapping of IP address to MAC addresses. If the IP address or MAC address changes, the value in the cache might be out of date.</p> <ul style="list-style-type: none"> <li>• Use the <b>arp -a</b> to list a host's ARP cache.</li> <li>• Use <b>arp -d</b> to clear the ARP cache. Use <b>arp -d *</b> to remove all dynamic ARP entries from the ARP list.</li> </ul> <p><b>Note:</b> Switches used with <b>arp</b> are case-sensitive. <b>Arp -a</b> is not the same thing as <b>arp -A</b>.</p>
Nslookup	<p><b>Nslookup</b> resolves (looks up) the IP address of a host name. Displays other name resolution-related information such as the DNS server used for the lookup request.</p>

### IP Troubleshooting Tips

One important step in troubleshooting network communications is to verify the IP address, subnet mask, and default gateway settings of each host. Keep in mind the following as you troubleshoot IP:

- All computers must be assigned a unique IP address.
- Hosts on the same physical network should have IP addresses in the same address range.
- The subnet mask value for all computers on the same physical network must be the same.
- Configure the default gateway value to enable internetwork communication.
- The default gateway address must be on the same subnet as the host's IP address.
- You do not need to configure an IP address on a switch for frames to be switched through the switch. To ping to and from a switch or to remotely manage the switch, configure an IP address on the switch.

Listed below are several common symptoms and things to try to correct communication problems.

Problem	Symptoms	Solution
A single host cannot communicate with any other host.	Ping to any other host fails.	Because the problem exists with only one host, troubleshoot the configuration of the host with the problem.
A single host can communicate with all hosts on the same network, but can't communicate with any host on any other network.	Ping to hosts on the same network succeed, ping to hosts on other networks fails.	Verify the default gateway setting of the host with the problem. Because only a single host has the problem, you should be able to assume that the default gateway device is functioning correctly.
	Traceroute on the host times out with only a single entry.	
All hosts can communicate within the same network, but cannot communicate with any host outside of the local network.	Ping to hosts on the same network succeed, ping to hosts on other networks fails.	Check for the following: <ul style="list-style-type: none"> <li>• If hosts have an IP address on the 169.254.0.0/16, then APIPA was used to assign the IP address and the default gateway value will be missing. Verify that the DHCP server is up.</li> <li>• If DHCP is used to assign IP information to hosts, verify the default gateway setting delivered by the DHCP server.</li> <li>• Verify that the default gateway device is up, has a valid connection to all networks, and has routing table information to reach destination networks.</li> </ul>
	Traceroute on the host times out with only a single entry.	
All hosts cannot communicate with hosts on a specific outside network. Communication with other networks is fine.	Ping to the remote network fails, traceroute on the host times out with only a single entry.	Add a route to the routing table, or configure the gateway of last resort (default route) on the router. The gateway of last resort is also known as the default gateway for the router.
	The routing table on the router does not show the destination network, or the gateway of last resort is	

	not set.	
	The routing table has a route to the destination network. Traceroute on the router times out.	Troubleshoot other routers in the path to the destination network. Use traceroute to identify the last responding router and begin troubleshooting there.
All hosts cannot communicate with a specific remote host. Communication with other remote hosts in the same remote network is fine.	Ping to the remote host fails. Traceroute to the remote host indicates no response from the host.	Troubleshoot the configuration of the remote host.
	The routing table shows a route to the destination network (or the gateway of last resort is used).	

## LAN Segmentation

As you study this section, answer the following questions:

- What is the difference between a collision domain and a broadcast domain?
- Your network uses only hubs as connection devices. What happens to the number of collisions on the network as you add devices?
- Your network uses only switches as connection devices. All devices have a dedicated switch port. What happens to the number of collisions on the network as you add devices?
- What happens to the collision and broadcast domains as you segment the network with routers?
- Which device provides guaranteed bandwidth between devices?
- Which device can you use to filter broadcast traffic?
- What is the relationship between *delay* and *jitter* with VoIP?
- What special features might you need on a switch to support VoIP?

This section covers the following exam objectives:

- 106. Describe the impact of applications (Voice Over IP and Video Over IP) on a network
- 203. Explain network segmentation and basic traffic management concepts

### Segmentation Facts

LAN segmentation is the process of dividing the network to overcome problems such as excessive collisions, broadcast traffic, or heavy network traffic. By segmenting a LAN, you can increase network performance, maximize bandwidth, and reduce congestion.

As you segment the network, you will need to consider the collision and broadcast domains on the network.

- A *collision domain* is any network or subnetwork where devices share the same transmission medium and where packets can collide. Collisions naturally increase as the number of devices in a collision domain increase.
- A *broadcast domain* is any network or subnetwork where computers can receive frame-level broadcasts from their neighbors. As you add devices to a network segment, the amount of broadcast traffic on a segment also increases. **Note:** A special condition called a *broadcast storm* happens when broadcast traffic is sent, regenerated, and responded to. In this condition, the amount of broadcast traffic consumes network bandwidth and prevents normal communications. Faulty devices or improper configuration conditions can lead to a broadcast storm.

Segmentation may increase the number of both the collision and broadcast domains. Membership within collision or broadcast domains differs depending on the connection device used.

Device	Collision Domain	Broadcast Domain
Hub	All devices connected to the hub are in the same collision domain.	All devices are in the same broadcast domain.
Bridge or Switch	All devices connected to a single port are in the same collision domain (each port is its own collision domain).	All devices connected to the bridge or the switch are in the same broadcast domain.
Router	All devices connected to a single interface are in the same collision domain.	All devices accessible through an interface (network) are in the same broadcast domain. Each interface represents its own broadcast domain if the router is configured to not forward broadcast packets.

In considering a network expansion solution, it is important to identify the connectivity problems you need to resolve, and then identify the device that is best suited for that situation. The main differences between routers, switches, and bridges are the range of services each performs and the OSI layer at which they operate.

Device	Characteristics
Router	<p>Routers perform the following functions that are not performed by bridges or switches.</p> <ul style="list-style-type: none"> <li>• Route packets between separate networks</li> <li>• Modify packet size through fragmentation and combination</li> <li>• Route packets based on service address</li> </ul> <p>Choose a router if you need to:</p> <ul style="list-style-type: none"> <li>• Connect your network to a WAN, such as the Internet</li> <li>• Filter broadcast traffic to prevent broadcast storms</li> <li>• Connect two separate networks that use the same protocol</li> <li>• Improve performance in the event of a topology change (routers recover faster than bridges or switches)</li> <li>• Reduce the number of devices within a domain (effectively increasing the number of broadcast domains)</li> <li>• Enforce network security</li> <li>• Dynamically select the best route through an internetwork</li> <li>• Connect two networks of different architectures, for example Ethernet to Token Ring</li> </ul>
Switch	<p>Choose a switch if you need to:</p> <ul style="list-style-type: none"> <li>• Provide guaranteed bandwidth between devices</li> <li>• Reduce collisions by decreasing the number of devices in a collision domain (effectively creating multiple collision domains)</li> <li>• Implement full-duplex communication</li> <li>• Connect two network segments or devices using the same protocol</li> <li>• Provide improved performance over a current bridged network</li> <li>• Switch traffic without the cost or administration involved with routers</li> </ul>
Bridge	<p>Choose a bridge if you need to:</p> <ul style="list-style-type: none"> <li>• Isolate data traffic to one network segment</li> <li>• Route traffic from one segment to another (with the same network ID)</li> <li>• Link unlike physical media (e.g. twisted pair and coaxial Ethernet) of the same architecture type</li> <li>• Link segments that use the same protocol</li> <li>• Create segments without the expense and administration of routers</li> </ul> <p><b>Note:</b> In most cases where you might use a bridge, choose a switch instead.</p>

In general, follow these guidelines to make decisions about the appropriate connectivity device.

- Use a bridge to segment the network (divide network traffic) and to provide fault tolerance.
- Use a switch to reduce collisions and offer guaranteed bandwidth between devices.
- Use a router to filter broadcast messages, implement security, or connect different networks.

LAN segmentation and design may be affected by the types of applications and protocols running over the network. For instance, Voice over Internet Protocol (VoIP) requires a well-engineered,

end-to-end network that provides little latency for data stream transmission. Fine-tuning the network to adequately support VoIP involves overcoming the following challenges:

- VoIP requires a very *low delay* as data is transferred between the sending and receiving phones, e.g. less than 200 milliseconds (.2 seconds).
- During transfer, the *jitter* (variations in delay) must be low as well, e.g. less than 30 milliseconds (.03 seconds).
- When packets do not arrive at the destination it is known as *packet loss*. If a VoIP packet was lost in transit, there is no need to recover the packet. This is because by the time the packet is recovered, it would sound like a break in the sound of the VoIP call.
- *Echo* is hearing your own voice in the telephone receiver while you are talking. When timed properly, echo is reassuring to the speaker; if the echo exceeds approximately 25 milliseconds, it can be distracting and cause breaks in the conversation. VoIP implementations use echo cancellers to regulate the echo.
- To secure VoIP data, the network should have a VoIP *Virtual Private Network* (VPN) solution. A VPN is a network that uses encryption to allow IP traffic to travel securely over the TCP/IP network. Without a VoIP VPN solution, it is relatively easy to eavesdrop on VoIP calls and even change their content.
- In some cases, IP telephones require *Power over Ethernet* (PoE). PoE is useful for powering IP telephones and other appliances where it would be inconvenient, expensive, or infeasible to supply power separately.

### VoIP Considerations

Voice over IP (VoIP) is a protocol optimized for the transmission of voice through the Internet or other packet switched networks. Voice over IP protocols carry telephony signals as digital audio encapsulated in a data packet stream over IP.

VoIP requires a well-engineered, end-to-end network that provides little latency for data stream transmission. Fine-tuning the network to adequately support VoIP involves overcoming the following issues:

Issue	Description
Delay	<p><i>Delay</i> (or <i>latency</i>) is the amount of time required for the spoken voice to be carried to the receiver's ear.</p> <ul style="list-style-type: none"> <li>• Delays cause long pauses between speaking and receiving, and might result in callers continually interrupting each other.</li> <li>• Callers notice roundtrip delays of 250 milliseconds (ms) or more.</li> <li>• International standards call for a delay of 150 ms or less.</li> </ul>
Jitter	<p><i>Jitter</i> is the variation of delay in transmissions.</p> <ul style="list-style-type: none"> <li>• Jitter causes strange sound effects as the delay of packets fluctuates.</li> <li>• Acceptable levels of jitter vary by vendor, but should be very low (between .5 and 30 ms).</li> <li>• Jitter can be controlled to some extent by packet buffers in VoIP equipment.</li> </ul>
Packet loss	<p>Packet <i>loss</i> occurs when packets do not arrive.</p> <ul style="list-style-type: none"> <li>• Packet loss causes drop-outs in the conversation.</li> <li>• Because voice traffic is time sensitive, lost packets do not need to be retransmitted.</li> <li>• Voice traffic is very sensitive to packet loss. Even a 1% loss of packets can be detected.</li> </ul>

	<ul style="list-style-type: none"> <li>• Ideally, Cisco recommends 0% packet loss, although very low (.1-.5% maximum) might still be acceptable.</li> </ul>
Echo	<p><i>Echo</i> is hearing your own voice in the telephone receiver while you are talking.</p> <ul style="list-style-type: none"> <li>• When timed properly, echo is reassuring to the speaker.</li> <li>• If echo exceeds approximately 25 milliseconds, it can be distracting and cause breaks in the conversation.</li> <li>• Excessive delay can cause unacceptable echo.</li> <li>• VoIP implementations use echo cancellers to regulate the echo.</li> </ul>

VoIP is typically implemented using switches with additional configuration required on both switches and routers to ensure delivery of VoIP packets for acceptable quality.

- To minimize the number of switch ports required, VoIP phones connect to the switch port, and a corresponding workstation connects to the VoIP phone. Both voice and data traffic is sent through the same switch port.
- Switches with Power over Ethernet (PoE) capability provide electrical power through the Cat 5 cable. This eliminates the need to have a separate power cable for the phone.
- Switches and routers are configured with Quality of Service (QoS) settings to elevate the priority of voice traffic. This helps control delay and jitter.
- To secure VoIP data, the network should have a VoIP Virtual Private Network (VPN) solution. A VPN is a network that uses encryption to allow IP traffic to travel securely over the TCP/IP network. Without a VoIP VPN solution, it is relatively easy to eavesdrop on VoIP calls and even change their content.



## Wireless Standards

As you study this section, answer the following questions:

- How are the FCC and ITU-R similar?
- How are FHSS and DSSS different?
- What are the differences between 802.11a and 802.11g specifications?
- What is the difference between channel *bonding* and *dual band*?
- When should you implement a dual band access point?
- What improvements are included with 802.11n standards that improve speed and distance?

This section covers the following exam objectives:

- 501. Describe standards associated with wireless media (including: IEEE WI-FI Alliance, ITU/FCC)

### Wireless Facts

Four organizations influence the standards used for wireless communication:

Organization	Details
Federal Communication Commission (FCC)	The FCC is the regulating US government agency over communication frequencies, including the frequencies used by wireless networking devices.
International Telecommunication Union Radiocommunications Sector (ITU-R)	The ITU-R is the regulating international agency over communication frequencies.
Wi-Fi Alliance	The Wi-Fi Alliance is an industry consortium that encourages interoperability of products that implement wireless standards.
Institute of Electrical and Electronics Engineers (IEEE)	The IEEE is a technical professional group that, among other contributions, developed the 802.11 series that became the national and international standard.

Wireless networks use radio waves for data transmission instead of electrical signals on Ethernet cables. In order to use radio waves as the medium for transmission, specific characteristics of radio waves are defined:

Characteristic	Description
Frequency range or band	Many radio devices operate within a specified frequency range which limits the frequencies on which it is allowed to transmit. In the United States, radio frequency wireless LANs use one of two frequency ranges defined by the FCC: <ul style="list-style-type: none"><li>• Industrial, Scientific, and Medical (ISM) operating between 2.4 - 2.4835 GHz.</li><li>• Unlicensed National Information Infrastructure (U-NII) operating between 5.75 - 5.85 GHz.</li></ul>
Channel	The frequency range is divided into equal segments called <i>channels</i> . Wireless networking channels are much like television channels, where each channel allows for separate data transmission. However, channels within the range overlap with adjacent channels. By using specific channels and not others, you can ensure that the channels do not overlap, eliminating interference caused by wireless devices

	<p>operating on different channels.</p> <ul style="list-style-type: none"> <li>In the 5 GHz range, there are 23 total channels. 12 channels are non-overlapping channels.</li> <li>In the 2.4 GHz range, there are 11 total channels, with 3 non-overlapping channels.</li> </ul>
Modulation technique	<p>When a device sends data over a wireless network, it can change (or modulate) the radio signal's specifications. The three common modulation techniques used in wireless networking include:</p> <ul style="list-style-type: none"> <li><i>Frequency Hopping Spread Spectrum (FHSS)</i> uses a narrow frequency band and 'hops' data signals in a predictable sequence from frequency to frequency over a wide band of frequencies. This type of modulation is no longer used with current wireless standards.</li> <li><i>Direct Sequence Spread Spectrum (DSSS)</i> uses an 11-bit Barker sequence to break data into pieces and sends the pieces across multiple frequencies in a defined range.</li> <li><i>Orthogonal Frequency Division Multiplexing (OFDM)</i> is not a spread spectrum frequency. It uses 48 discrete radio frequency channels that can carry data.</li> </ul> <p>Most newer devices use additional modulation techniques and enhancements including:</p> <ul style="list-style-type: none"> <li>Complementary Code Keying (CCK)</li> <li>Quadrature Phase-shift Keying/Differential Quadrature Phase-Shift Keying (QPSK/DQPSK)</li> <li>Binary Phase-Shift Keying/Differential Binary Phase-Shift Keying (BPSK/DBPSK)</li> </ul>

### Wireless Standard Facts

The original 802.11 specification operated in the 2.4 GHz range and provided up to 2 Mbps. Additional IEEE subcommittees have further refined wireless networking. Three of the most common standards as well as a new standard in draft stage are listed in the following table:

Specification	Standard			
	802.11a	802.11b	802.11g	<a href="#">802.11n</a>
Frequency	5 GHz (U-NII)	2.4 GHz (ISM)	2.4 GHz (ISM)	2.4 GHz (ISM) or 5 GHz (U-NII)
Maximum speed	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Maximum range	150 Ft.	300 Ft.	300 Ft.	1200 Ft.
Channels (non-overlapped)	23 (12)	11 (3)	11 (3)	2.4 GHz--23 (12 or 6) 5 GHz--11 (3 or 1)
Modulation technique	OFDM	DSSS, CCK, DQPSK, DBPSK	DSSS (and others) at lower data rates At higher data rates, OFDM, QPSK, BPSK	OFDM and others, depending on implementation
Backwards-compatibility	N/A	No	With 802.11b	With 802.11a/b/g, depending on

Be aware of the following regarding the wireless network implementation:

- The actual speed depends on several factors including distance, obstructions (such as walls), and interference.
- The actual maximum distance depends on several factors including obstructions, antenna strength, and interference. For example, for communications in a typical environment (with one or two walls), the actual distance would be roughly half of the maximums.
- The speed of data transmission decreases as the distance between the transmitter and receiver increases. In other words, in practice, you can get the maximum distance or the maximum speed, but not both.
- Some newer 802.11a or 802.11g devices provide up to 108 Mbps using 802.11n pre-draft technologies (MIMO and channel bonding).
- The ability of newer devices to communicate with older devices depends on the capabilities of the transmit radios in the access point. For example:
  - Some 802.11n devices can transmit at either 2.4 GHz or 5 GHz. This means that the radio is capable of transmitting at either frequency. However, a single radio cannot transmit at both frequencies at the same time.
  - Most 802.11g devices can transmit using DSSS, CCK, DQPSK, and DBPSK for backwards compatibility with 802.11b devices. However, the radio cannot transmit using both DSSS and OFDM at the same time.

This means that when you connect a legacy device to the wireless network, all devices on the network operate at the legacy speed. For example, connecting an 802.11b device to an 802.11n or 802.11g access point slows down the network to 802.11b speeds.

- A *dual band* access point can use one radio to transmit at one frequency, and a different radio to transmit at a different frequency. For example, you can configure many 802.11n devices to use one radio to communicate at 5 GHz with 802.11a devices, and the remaining radios to use 2.4 GHz to communicate with 802.11n devices. Dual band 802.11a and 802.11g devices are also available.

## Wireless Infrastructure

As you study this section, answer the following questions:

- Under which circumstances might you choose an ad hoc wireless network?
- What is an SSID? How does the BSSID differ from the SSID?
- How many access points are in a BSS and an ESS?
- What media access method do wireless networks use? How does this differ from the media access used on Ethernet?

This section covers the following exam objectives:

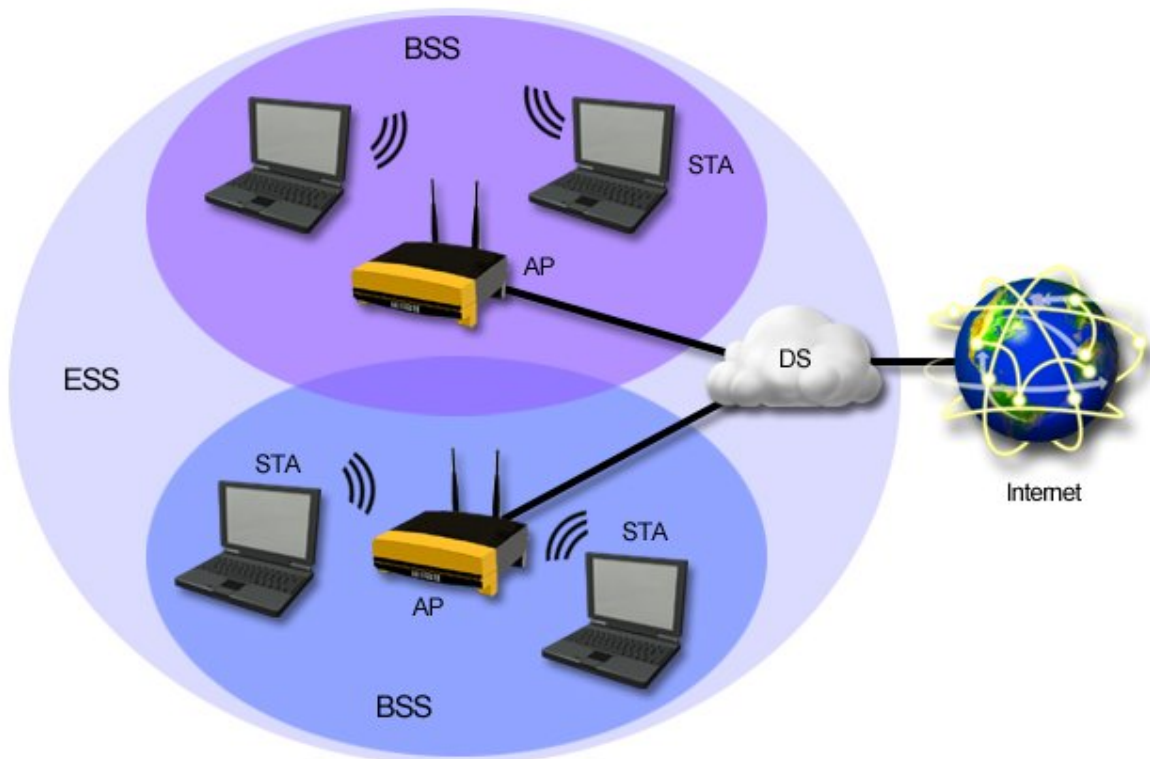
- 502. Identify and describe the purpose of the components in a small wireless network. (Including: SSID, BSS, ESS)
- 503. Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point

### Wireless Infrastructure Facts

There are two methods of wireless networking:

Method	Description
Ad Hoc	<p>An <i>ad hoc</i> network works in peer-to-peer mode. The wireless NICs in each host communicate directly with one another. An ad hoc network:</p> <ul style="list-style-type: none"><li>• Uses a physical mesh topology.</li><li>• Is cheap and easy to set up.</li><li>• Cannot handle more than four hosts.</li><li>• Requires special modifications to reach wired networks.</li></ul> <p>You will typically only use an ad hoc network to create a direct, temporary connection between two hosts.</p>
Infrastructure	<p>An <i>infrastructure</i> wireless network employs an access point (AP) that functions like a hub on an Ethernet network. With an infrastructure network:</p> <ul style="list-style-type: none"><li>• The network uses a physical star topology.</li><li>• You can easily add hosts without increasing administrative efforts (scalable).</li><li>• The access point can be easily connected to a wired network, allowing clients to access both wired and wireless hosts.</li><li>• The placement and configuration of access points require planning to implement effectively.</li></ul> <p>You should implement an infrastructure network for all but the smallest of wireless networks.</p>

The following diagram shows a sample enterprise wireless network operating in infrastructure mode:



The various components of a wireless network are described in the following table.

Component	Description
Station (STA)	An STA is a wireless network card (NIC) in an end device such as a laptop or wireless PDA. STA often refers to the device itself, not just the network card.
Access Point (AP)	An <i>access point</i> (AP), sometimes called a <i>wireless access point</i> , is the device that coordinates all communications between wireless devices as well as the connection to the wired network. It acts as a hub on the wireless side and a bridge on the wired side. It also synchronizes the stations within a network to minimize collisions.
Basic Service Set (BSS)	A BSS, also called a <i>cell</i> , is the smallest unit of a wireless network. All devices in the BSS can communicate with each other. The devices in the BSS depend on the operating mode: <ul style="list-style-type: none"> <li>• In an ad hoc implementation, each BSS contains two devices that communicate directly with each other.</li> <li>• In an infrastructure implementation, the BSS consists of one AP and all STAs associated with the AP.</li> </ul>
Independent Basic Service Set (IBSS)	An IBSS is a set of STAs configured in ad hoc mode.
Extended Service Set (ESS)	An ESS consists of multiple BSSs with a distribution system (DS). The graphic above is an example of an ESS.
Distribution System (DS)	The distribution system (DS) is the backbone or LAN that connects multiple APs (and BSSs) together. The DS allows wireless clients to communicate with the wired network and with wireless clients in other cells.

Wireless networks use the following for identification:

Identifier	Description
Service Set Identifier (SSID)	<p>The Service Set Identifier (SSID), also called the network name, groups wireless devices together into the same logical network.</p> <ul style="list-style-type: none"> <li>• All devices on the same network (within the BSS and ESS) must have the same SSID.</li> <li>• The SSID is a 32-bit value that is inserted into each frame. The SSID is case-sensitive.</li> <li>• The SSID is sometimes called the BSS ID (Basic Service Set ID) or the ESS ID (Extended Service Set ID). In practice, each term means the same thing.</li> </ul> <p><b>Note:</b> Using BSS ID to describe the SSID of a BSS is technically incorrect.</p>
Basic Service Set Identifier (BSSID)	<p>The BSSID is a 48-bit value that identifies an AP in an infrastructure network or a STP in an ad hoc network. The BSSID allows devices to find a specific AP within an ESS that has multiple access points, and is used by STAs to keep track of APs when roaming between BSSs.</p> <p><b>Note:</b> Do not confuse the BSSID with the SSID. They are not the same thing.</p>

### Wireless Media Access Facts

Wireless networks use Carrier Sense, Multiple Access/Collision Avoidance (CSMA/CA) to control media access and avoid (rather than detect) collisions. CSMA/CA uses the following process:

1. The sending device listens to make sure that no other device is transmitting. If another device is transmitting, the device waits a random period of time (called a *backoff* period) before attempting to send again.
2. If no other device is transmitting, the sending device broadcasts a Request-to-send (RTS) message to the receiver or access point. The RTS includes the source and destination, as well as information on the duration of the requested communication.
3. The receiving device responds with a Clear-to-send (CTS) packet. The CTS also includes the communication duration period. Other devices use the information in the RTS and CTS packets to delay attempting to send until the communication duration period (and subsequent acknowledgement) has passed.
4. The sending device transmits the data. The receiving device responds with an acknowledgement (ACK). If an acknowledgement is not received, the sending device assumes a collision and retransmits the affected packet.
5. After the time interval specified in the RTS and CTS has passed, other devices can start the process again to attempt to transmit.

**Note:** Using RTS and CTS (steps 2 and 3 above) is optional and depends on the capabilities of the wireless devices. Without RTS/CTS, collisions are more likely to occur.

Wireless communication operates in *half-duplex* (shared, two-way communication). Devices can both send and receive, but not at the same time. Devices must take turns using the transmission channel. Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting before replying.

## Wireless Security

As you study this section, answer the following questions:

- What is the difference between a rogue access point and a spoofed access point?
- What does open authentication use to authenticate a device?
- How does 802.1x authentication differ from shared key authentication?
- What improvements did WPA make to overcome the weaknesses of WEP?
- You have an older wireless access point that supports WEP. You would like to use WPA instead. What action would you typically take to do this? What would you need to do to use WPA2?
- Which wireless security standards use Temporal Key Integrity Protocol (TKIP) encryption?
- What are three actions you should take to increase the security of a wireless access point?
- How does MAC address filtering improve security of a wireless access point? Why is this action by itself insufficient to prevent unauthorized access?

This section covers the following exam objectives:

- 504. Compare and contrast wireless security features and capabilities of WPA security (including: open, WEP, WPA-1/2)

### Security Issues Facts

Most wireless access points come preconfigured or have an automatic setup routine that lets you simply connect the access point to create a simple wireless network. However, the default configuration typically has little or no security. Wireless networks are vulnerable to the following specific security attacks:

Vulnerability	Description
War driving	With <i>war driving</i> , an attacker scans an area looking for available wireless networks. This is typically accomplished using a high-gain antenna, or by driving around looking for wireless networks in various locations.
Hacker	A <i>hacker</i> is anyone that commits computer and cyber crimes by gaining unauthorized access to computer systems. A hacker can exploit system vulnerabilities, elevate privilege, and introduce new vulnerabilities that allow the attacker greater access to systems and data on the network.
Rogue access point	<p>A <i>rogue access point</i> is an unauthorized access point added to the network.</p> <ul style="list-style-type: none"><li>• A hacker who gains access to your network can install a rogue wireless access point, giving him access to the wired network. Using the rogue access point, the hacker might capture network traffic, or attempt to access other network resources.</li><li>• Employees can easily purchase an access point and add it to the wired network. Often this is done to give the employee wireless access to the network, but is often done with little or no security implemented on the access point. The access point becomes a possible point of entry for hackers or war drivers.</li></ul>
Spoofed access point	A <i>spoofed</i> access point is an access point that is configured to look like a legitimate access point. Spoofed access points generally occur in a public area, such as an Internet cafe or public <i>hotspot</i> . The attacker sets up an open access point using an SSID that resembles the business name. The attacker can then monitor traffic of those connected to the spoofed access point.



Countermeasures to these vulnerabilities include:

Countermeasure	Description
Authentication	<p><i>Authentication</i> is the process of validating identity.</p> <ul style="list-style-type: none"> <li>• <i>Open</i> authentication uses the MAC address of the wireless network adapter to connect to the wireless network, thereby allowing anyone to connect.</li> <li>• <i>Shared key</i> authentication requires that clients supply a predefined key to connect.</li> <li>• 802.1x uses usernames and passwords to authenticate users to the wireless network.</li> </ul>
Encryption	<p><i>Encryption</i> is the process of using an algorithm or other method to transform data from plaintext to unreadable text. Because wireless transmissions are easily captured, you should implement some form of encryption on your wireless network to lower the chances of attackers successfully discovering the packet's contents.</p>
Intrusion Detection System (IDS)	<p>An IDS is a hardware or software device that examines the network to identify possible in-progress attacks. An IDS monitors, logs, and detects security breaches, and generates alerts if the attack is deemed to be severe.</p>
Cisco Structured Wireless-Aware Network (SWAN)	<p>Cisco's SWAN is a proprietary approach to securing and managing wireless networks. With SWAN:</p> <ul style="list-style-type: none"> <li>• Access points must be registered on the network. This eliminates the possibility of rogue access points allowing access to the wired network.</li> <li>• Only authorized clients are allowed to connect to the network.</li> </ul>

### Security Implementation Facts

Security for wireless networking is provided from the following standards:

Method	Description
Wired Equivalent Privacy (WEP)	<p>WEP is an optional component of the 802.11 specifications and was deployed in 1997. WEP was designed to provide wireless connections with the same security as wired connections. WEP has the following weaknesses:</p> <ul style="list-style-type: none"> <li>• Static Pre-shared Keys (PSK) were given to the access point and client and could not be dynamically changed or exchanged without administration. As a result, every host on large networks usually use the same key.</li> <li>• Because it doesn't change, the key can be captured and easily broken. The key values were short, making it easy to predict.</li> </ul>
Cisco interim solution	<p>Cisco's interim solution was deployed in 2001 to address the problems of WEP. The solution included the following:</p> <ul style="list-style-type: none"> <li>• A Cisco proprietary version of Temporal Key Integrity Protocol (TKIP) encryption.</li> <li>• User authentication using 802.1x. 802.1x requires a centralized server (called a RADIUS server) to authenticate users through user account</li> </ul>



	<p>names and passwords.</p> <ul style="list-style-type: none"> <li>• The use of dynamic keys.</li> </ul>
Wi-Fi Protected Access (WPA)	<p>WPA is the implementation name for wireless security based on initial 802.11i drafts and was deployed in 2003. It was intended as an intermediate measure to take the place of WEP while a fully secured system (802.11i) was prepared.</p> <p>WPA:</p> <ul style="list-style-type: none"> <li>• Uses TKIP for encryption.</li> <li>• Supports both Pre-shared Key (referred to as WPA-PSK or WPA Personal) and 802.1x (referred to as WPA Enterprise) authentication.</li> <li>• Can use dynamic keys or pre-shared keys.</li> <li>• Can typically be implemented in WEP-capable devices through a software/firmware update.</li> </ul> <p><b>Note:</b> The Cisco interim solution is not compatible with WPA.</p>
Wi-Fi Protected Access 2 (WPA2) or 802.11i	<p>WPA2 is the implementation name for wireless security that adheres to the 802.11i specifications and was deployed in 2005. It is built upon the idea of <i>Robust Secure Networks</i> (RSN). Like WPA, it resolves the weaknesses inherent in WEP, and is intended to eventually replace both WEP and WPA. WPA2:</p> <ul style="list-style-type: none"> <li>• Uses Advanced Encryption Standard (AES) as the encryption method. It is similar to and more secure than TKIP, but requires special hardware for performing encryption.</li> <li>• Supports both Pre-shared Key (referred to as WPA2-PSK or WPA2 Personal) and 802.1x (referred to as WPA2 Enterprise) authentication.</li> <li>• Can use dynamic keys or pre-shared keys.</li> </ul> <p><b>Note:</b> WPA2 has the same advantages over WEP as WPA. While more secure than WPA, its main disadvantage is that it requires new hardware for implementation.</p>

In addition to using the security measures outlined above, you can provide a level of security using the following practices. These methods by themselves do not provide much security, but rather keep curious people from trying to access the wireless network.

Method	Description
Change the administrator account name and password	The access point typically comes configured with a default username and password that is used to configure the access point settings. If possible, it is important to change the administrator account name and password from the defaults. This helps prevent outsiders from breaking into your system by guessing the default username and password.
Update the firmware	Update the firmware on the access point from the manufacturer's Web site frequently to prevent your system from being exposed to known bugs and security holes.
Enable the firewall on the access point	Most wireless access points come with a built-in firewall that connects the wireless network to a wired network.
Change SSID from defaults	<p>Many manufacturers use a default SSID, so it is important to change your SSID from the defaults. You can also disable the SSID broadcast for further protection, this is known as <i>SSID suppression</i> or <i>cloaking</i>.</p> <p><b>Note:</b> Even with SSID broadcast turned off, a determined hacker can still identify the SSID by analyzing wireless broadcasts.</p>

Disable DHCP	DHCP servers dynamically assign IP addresses, gateway addresses, subnet masks, and DNS addresses whenever a computer on the wireless network starts up. Disabling DHCP on the wireless access points allows only users with a valid, static IP address in the range to connect.
Enable MAC address filtering	<p>Every network board has a unique code assigned to it called a MAC address. By specifying which MAC addresses are allowed to connect to your network, you can prevent unauthorized MAC addresses from connecting to the access point. Configuring a MAC address filtering system is very time consuming and demands upkeep.</p> <p><b>Note:</b> Attackers can still use tools to capture packets and then retrieve valid MAC addresses. An attacker could then spoof their wireless adapter's MAC address and circumvent the filter.</p>

## Wireless Configuration

As you study this section, answer the following questions:

- You have a network with two wireless access points. Should the SSID be the same or different? Should the channel on each be the same or different?
- Where is the best place to locate your wireless access point?
- What type of objects might obstruct radio frequency wireless transmissions?
- How does range and antenna placement affect wireless networks?
- When should you use open authentication on your wireless network?
- What authentication type should you *not* use when using WEP for encryption?
- What is required in order to implement 802.1x authentication?

After finishing this section, you should be able to complete the following tasks:

- Configure basic options and security on a wireless access point.
- Configure a wireless client connection.

This section covers the following exam objectives:

- 503. Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point
- 505. Identify common issues with implementing wireless networks. (Including: Interface, misconfiguration)

### **Wireless Configuration Facts**

A wireless implementation checklist should include the following configuration processes:

Method	Description
Plan access point placement and configuration	<p>The first step in implementing a wireless solution is to plan the wireless network. Consider the following:</p> <ul style="list-style-type: none"><li>• Draw a sketch of the building or location where wireless access is required. Identify possible access point locations, taking into consideration signal strength and maximum signal distances.</li><li>• Place access points in central locations. Radio waves are broadcast in each direction, so the access point should be located in the middle of the area that needs network access.</li><li>• Devices often get better reception from access points that are above or below. In general, place access points higher up to avoid interference problems caused by going through building foundations.</li><li>• For security reasons, do not place access points near outside walls where the signal can be intercepted by non-authorized devices. Placing the access point in the center of the building decreases the range of the signals available outside of the building.</li><li>• Select the SSID for the wireless network. If the network has multiple access points, identify which channel each access point will use. Make sure that neighboring access points use non-overlapping channels.</li></ul> <p>Click <a href="#">here</a> for a diagram of a sample wireless network with multiple access points.</p>
Connect the wireless access point to the wired	Most access points require that you make a connection to the access point through the wired network in order to complete access point configuration tasks.

network	<ul style="list-style-type: none"> <li>• Before connecting the access point, you can verify that the wired connection is valid by connecting a laptop to the network port.</li> <li>• Connect the access point to the existing network with a straight-through Ethernet cable. Optionally, you could use a cross-over cable and connect a laptop or desktop computer directly to the Ethernet port on the access point.</li> <li>• Most access points come configured with a static IP address and a subnet mask. On a host on the wired network, change the host's subnet to the same subnet of the access point.</li> <li>• Most access points use a Web-based program for configuration. Use your browser to connect to the default IP address of the access point, then enter the default administrator name and password to connect to the configuration utility.</li> </ul>
Configure basic access point settings	<p>Once connected to the access point configuration utility, configure the necessary settings:</p> <ul style="list-style-type: none"> <li>• Configure a static IP address (with subnet mask, default gateway, and DNS settings), or configure the access point to use DHCP. Because the access point acts much like a switch, an IP address is not required. However, configuring the IP settings allows you to connect to the access point to make configuration changes. After changing the IP address, you will need to change the IP address of the client that is connected to the access point.</li> <li>• Configure the wireless standards to use (802.11 a/b/g/n) and the operating mode (mixed, legacy, greenfield, etc.).</li> <li>• Configure the SSID. If the access point is part of an ESS, all of the access points should share the same SSID.</li> <li>• Configure the channel. To avoid interference between multiple access points, each access point should have a different, non-overlapping channel. On a small network with a single access point, you can set the channel to Automatic. The access point then senses other access points nearby, and (if possible) selects a channel that is not in use.</li> </ul>
Configure a client	<p>Install and configure a wireless client, such as a laptop with an enabled radio. When you install the wireless adapter, you use a wireless connection manager to view and connect with wireless networks.</p> <ul style="list-style-type: none"> <li>• Windows XP and later comes with a built-in wireless connection manager. This connection manager uses the Wireless Zero Configuration (WZC) service. When roaming between access points, WZC automatically connects to the access point with the strongest signal.</li> <li>• Many wireless adapters come with their own connection manager that might provide additional functionality.</li> </ul> <p>With most connection managers, you can view wireless networks in range that are broadcasting the SSID. Simply select the wireless network and establish the connection. A successful connection verifies that the client can communicate with the access point.</p>
Configure security on the access point	<p>If the access point is left connected to the network without security implementations, attackers may connect to the network, potentially circumventing all security on the wired portion of the network.</p>

	<p>When configuring the authentication method:</p> <ul style="list-style-type: none"> <li>• Use Open authentication to allow anyone to connect to the wireless network. This option is typically used by businesses that provide free Internet access to customers.</li> <li>• Use Shared Key authentication on small, private networks. With Shared Key authentication, all access points and all clients use the same authentication key. Shared Key authentication can be configured using one of three settings: <ul style="list-style-type: none"> <li>◦ A simple Shared Key setting uses the WEP key for authentication. When using this option, you should disable encryption.</li> <li>◦ WPA-PSK (WPA Personal) uses WPA with a shared key.</li> <li>◦ WPA2-PSK (WPA2 Personal) uses WPA2 with a shared key.</li> </ul> </li> <li>• Use 802.1x authentication on large, private networks. 802.1x requires a RADIUS server on the network. Users authenticate with unique usernames and passwords.</li> </ul> <p>When configuring encryption, select the strongest method supported by all devices:</p> <ul style="list-style-type: none"> <li>• AES is used with WPA2. When using AES, all devices must be WPA2 capable.</li> <li>• TKIP is used with WPA. Most existing devices can use WPA. If not, check to see if a firmware update is available to add WPA capabilities to the device.</li> <li>• Use WEP only if no other encryption is supported. <b>Note:</b> Do not use WEP together with Shared Key authentication.</li> <li>• Public networks typically require no encryption.</li> </ul>
Configure client security settings	<p>After configuring security on the access point, you will need to add security to the wireless client. Manually configure the security settings that correspond to the wireless network.</p> <ul style="list-style-type: none"> <li>• When using WEP or Shared Key authentication, enter the same shared key configured on the access point.</li> <li>• If using 802.1x authentication, enable 802.1x and configure any necessary settings. Depending on the implementation, you might be prompted for a username and password when you try to connect.</li> <li>• Select the encryption method used on the wireless access point.</li> </ul> <p>After the security configurations are set, verify that the wireless client can still connect to the wireless network.</p>
Conduct a site survey	<p>A <i>site survey</i> is an evaluation of your wireless network configuration. The site survey looks for advantages and problems with the wireless network and its surroundings. When conducting the site survey:</p> <ul style="list-style-type: none"> <li>• Verify that the SSID broadcast and security settings are correctly configured on each access point.</li> <li>• Assess the signal strength and direction of wireless access points. For example, make sure that access points are not placed near outside walls where the signals will be strong outside of the building where you do not have physical control.</li> <li>• Check for obstructions that could affect the availability of the wireless signal in various locations.</li> </ul>

	<ul style="list-style-type: none"> <li>• Check for other wireless networks in the area, and choose a channel that does not conflict with other networks.</li> <li>• Perform cell-shaping. <i>Cell-shaping</i> uses directional antennae and shielding methods to locate the wireless access points in secured areas in order to adjust their transmittal power.</li> </ul> <p>If you find something of concern during the site survey such as a strong signal strength outside of the building, troubleshoot the issue and then conduct another site survey to confirm that the issue is resolved.</p>
--	--

## Wireless Troubleshooting Facts

If you are having trouble establishing or keeping a wireless connection, consider the following:

Consideration	Description
Incorrect configuration	Probably the most common source of problems with wireless networking is incorrect configuration. Before considering other problems, verify that the correct SSID and WEP/WPA keys have been configured. Remember that WEP/WPA keys are not case-sensitive, but passphrases are case-sensitive.
Range and obstructions	Wireless standards have a limited range. Moving a client outside of the effective range will weaken the signal and likely cause intermittent reception while moving outside of the stated range can cause it to be completely dropped. In addition, many wireless devices have trouble transmitting through obstructions in the path. Infrared requires a line-of-sight path, while radio frequency wireless has trouble transmitting through certain materials such as concrete.
Channel interference	<p>The 2.4 GHz frequency range is divided into 11 channels, with each channel having some overlap with the channels next to it. You might experience problems with your wireless network when other devices are trying to use the same or adjacent channels. Devices that use radio frequency wireless include:</p> <ul style="list-style-type: none"> <li>• Cordless telephones</li> <li>• Other access points in the area (for example, each of your neighbors might have a wireless network, with each configured to use a similar channel)</li> </ul> <p>To avoid interference, try changing the channel used on the access point. If the area has different wireless networks, configure each with a different channel with at least two channels separating the channels in use (for example you can use channels 1, 4, 8, and 11).</p>
Atmospheric and EMI conditions	Interference from atmospheric conditions such as weather or other sources of stray radio waves (electro-magnetic interference) can degrade the signal and cause service interruptions.
Antennae orientation	<p>For some 802.11 devices, the antenna orientation might have a small effect on signal strength. There are two types of antennas you should be aware of:</p> <ul style="list-style-type: none"> <li>• Directional antenna: <ul style="list-style-type: none"> <li>○ Creates a narrow, focused signal in a particular direction.</li> <li>○ Focused signal provides greater signal strength increasing the transmission distance.</li> <li>○ Provide a stronger point-to-point connection, better equipping them to handle obstacles.</li> </ul> </li> <li>• Omni-directional antenna: <ul style="list-style-type: none"> <li>○ Disperses the RF wave in an equal 360-degree pattern.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>○ Used to provide access to many clients in a radius.</li> </ul> <p>For other devices such as infrared or satellite, the orientation of the receiving device is critical. For these types of devices, make sure the receivers have a line-of-sight path to communicate.</p>
<p>Client and access point incompatibility</p>	<p>In some cases, especially when using 802.11n, the wireless client might not be compatible with the wireless access point. Try updating the software that came with the wireless client, update the firmware on the access point, and research the manufacturer's Web site for additional information.</p> <p>Because of the large number of vendors of wireless devices for clients, Cisco wants to ensure that the vendors' devices will work with Cisco access points. The <i>Cisco Compatible Extensions (CCX)</i> program allows manufactures of wireless network devices to send their products to a third-party testing lab to ensure that they will work with Cisco access points.</p>

## Subnet Operations

As you study this section, answer the following questions:

- When should you use the  $2^n - 2$  formula to determine the amount of available subnets?
- What is the magic number and how can it help while subnetting a network?
- What is the difference between a classful and classless subnet mask?

After finishing this section, you should be able to complete the following tasks:

- Given a subnet mask and an IP address, find the network address.
- Given a network address and the number of desired subnets and hosts, select the subnet mask.
- From a network address and subnet mask, identify valid subnet addresses.
- From a subnet address and mask, identify the range of valid host addresses.

This section covers the following exam objectives:

- 305. Calculate and apply an addressing scheme including VLSM IP addressing design to a network

### **Classless Interdomain Routing (CIDR)**

You can think of the Internet as one big network. As such, each device on the network needs its own unique IP address. In the early days of the Internet, every device would receive a registered IP address. As the Internet grew, however, it became apparent that the number of hosts would quickly exceed the number of possible IP addresses.

One solution to the problem is Classless Interdomain Routing (CIDR). *Classfull* addresses are IP addresses that use the default subnet mask. They are classfull because the default subnet mask is used to identify the network and host portions of the address. *Classless* addresses are those that use a custom mask value to separate network and host portions of the IP address. CIDR allows for variable length subnet masking (VLSM) and enables the following features:

- Subnetting, dividing a network address into multiple smaller subnets. For example, this allows a single Class B or Class C addresses to be divided and used by multiple organizations.
- Supernetting, combining multiple network addresses into a single larger subnet. For example, this allows multiple Class C addresses to be combined into a single network.
- Route aggregation (also called [route summarization](#)), where multiple routes are combined in a routing table as a single route.

CIDR routers use the following information to identify networks.

- The beginning network address in the range
- The number of bits used in the subnet mask

For example, the routing table represents the address as 199.70.0.0/21, where 21 is the number of bits in the custom subnet mask.

In addition to CIDR, the following other solutions were put into place to make efficient use of available IP addresses:

- IP version 6. IPv6 uses 128-bit addresses instead of the 32-bit addresses used with IPv4.
- Private addressing with address translation. With private addressing, hosts are assigned an unregistered address in a predefined range. All hosts on the private network use a single



registered IP address to connect to the Internet. A special router (called a Network Address Translation or NAT router) translates the multiple private addresses into the single registered IP address.

- **Binary Calculations**
- To perform subnetting operations, you will need to be proficient at converting decimal and binary numbers. When working with IP addresses, work with each octet separately. The following table shows the decimal value for various binary values with a single 1 bit.

<b>Binary Value</b>	1000000	0100000	0010000	0001000	0000100	0000010	0000001	0000000
	0	0	0	0	0	0	0	1
<b>Decimal Value</b>	128	64	32	16	8	4	2	1

- To find the decimal value of a number with multiple 1 bits, simply add the decimal value of the bits together. For example, the decimal value of the binary number 10010101 is:
- 10000000 = 128  
00010000 = 16  
00000100 = 4  
00000001 = 1  
Total = 128 + 16 + 4 + 1 = 149
- To calculate the number of valid subnets or the number of hosts per subnet, you will need to know how to find the exponential values of 2. Use the following chart to identify the exponent values and the final possible number (after subtracting 2 from each exponent).

<b># of bits</b>	1	2	3	4	5	6	7	8	9	10	11	12
<b>Exponent</b>	2 <sup>1</sup>	2 <sup>2</sup>	2 <sup>3</sup>	2 <sup>4</sup>	2 <sup>5</sup>	2 <sup>6</sup>	2 <sup>7</sup>	2 <sup>8</sup>	2 <sup>9</sup>	2 <sup>10</sup>	2 <sup>11</sup>	2 <sup>12</sup>
<b>Exponent value</b>	2	4	8	16	32	64	128	256	512	1024	2048	4096
<b>Total number (-2)</b>	0	2	6	14	30	62	128	254	510	1022	2046	4094

- **Tip:** Memorize the shaded values. To find smaller or larger values, divide or multiply the exponent value by 2.

## Subnetting Operations

Use the following chart to identify the solutions to common subnetting tasks.

Scenario	Solution
Given a network address and subnet mask, how many subnets can you have?	<p>Begin by converting the subnet mask to a binary number. Then decide which formula to use (<math>n</math> is the number of additional bits borrowed from the default mask):</p> <p>Use <math>2^n</math> if:</p> <ul style="list-style-type: none"> <li>• The network uses a classless routing protocol, such as RIP version 2, EIGRP, or OSPF</li> <li>• The <b>ip subnet zero</b> command is configured</li> <li>• Variable-length Subnet Mask (VLSM) is used</li> </ul> <p>Use <math>2^n - 2</math> if:</p> <ul style="list-style-type: none"> <li>• The network uses a classful routing protocol, such as RIP version 1 or IGRP</li> </ul>

	<ul style="list-style-type: none"> <li>The <b>no ip subnet zero</b> command is configured</li> </ul> <p><b>Note:</b> If no network details are provided, use <math>2^n</math>.</p>
Given a network address and subnet mask, how many hosts per subnet can you have?	$2^n - 2$ Begin by converting the subnet mask to a binary number. Then use the formula to find the number of hosts. To find the number of valid hosts, $n$ = the number of unmasked bits by the custom mask.
Given a network address and customer requirements, what subnet mask should you use?	$2^n, 2^n - 2$ Write out the default subnet mask in binary. Then borrow bits and use the formula to find the number that gives you enough subnets and hosts.
Given a network address and a subnet mask, identify the valid subnet addresses.	<p><i>Magic number</i></p> The magic number is the decimal value of the last 1 bit in the subnet mask. The magic number identifies: <ul style="list-style-type: none"> <li>The first valid subnet address</li> <li>The increment value to find additional subnet addresses</li> </ul>
Given an IP address and subnet mask, find the: <ul style="list-style-type: none"> <li>Subnet address</li> <li>Broadcast address</li> <li>Valid host address range</li> </ul>	<p><i>Trust the line</i></p> Use the following process to find the information you need: <ol style="list-style-type: none"> <li>Identify the subnet and host portions of the mask, draw a line</li> <li>To find the subnet address, set all host bits to 0</li> <li>To find the broadcast address, set all host bits to 1</li> <li>The valid host range is: <ul style="list-style-type: none"> <li>First address = Subnet address + 1</li> <li>Last address = Broadcast address - 1</li> </ul> </li> </ol>

## Subnet Design

After finishing this section, you should be able to complete the following tasks:

- Given a scenario, select and configure subnet addresses, masks, and host addresses.

This section covers the following exam objectives:

- 305. Calculate and apply an addressing scheme including VLSM IP addressing design to a network

### Subnet Design Facts

When setting up a network for IP, you will have to make various decisions about the addresses used on the network. Use the following process to identify and assign IP addresses throughout your network.

1. Identify the number of network addresses. Each network segment will require its own network (subnet) address. In addition, each WAN connection must have its own network address (typically assigned by the WAN service provider).
2. Identify the number of hosts for each subnet. You will need one IP address for each device. Be sure to include an IP address for each router interface.
3. Calculate the subnet mask that provides the necessary number of subnet addresses and the number of host addresses per subnet.
4. Identify the valid subnet addresses, and assign them to network segments.
5. Identify valid IP addresses on each subnet (i.e. the host address range).
6. Assign IP addresses to hosts, or plan on using DHCP to dynamically assign IP addresses.

Instead of using formulas and calculations to perform these steps, you can create a table as follows and use it to quickly identify subnet masks, subnet addresses, and host addresses.

<b>Bits in the mask</b>	/25	/26	/27	/28	/29	/30	/31	/32
<b>Magic number</b>	128	64	32	16	8	4	2	1
<b>Decimal mask value</b>	128	192	224	240	248	252	254	255
<b>Hosts per subnet</b>	126	62	30	14	6	2	n/a	n/a
<b>Number of subnets possible (subnet zero)</b>	2	4	6	8	16	32	n/a	n/a

To construct the table, begin by writing the bit-count in the top row. Then compute the remaining rows as follows:

- To get the magic number, start at 128 and split the value in half for each column.
- To get the decimal mask value, add the magic numbers to the left (for example, a /27 mask can be calculated as  $128 + 64 + 32 = 224$ ).
- To get the number of hosts per subnet, subtract 2 from the magic number.
- To get the number of subnets, start at 2, then double the number for each column.

As an example of using the table, suppose you are given a subnet address of 199.166.12.32/29. Use the /29 column to perform various subnetting operations. For example:

- The decimal form of the mask is 255.255.255.248.
- There are 6 host addresses on the subnet (33, 34, 35, 36, 37, and 38).

- The next subnet address using this mask is 199.166.12.40 (add the magic number to the first subnet address).
- The broadcast address for the subnet is 199.166.12.39 (subtract 1 from the next subnet address).
- Using this mask, there are a total of 16 possible subnets.

Be aware of the following special cases identified in the table:

- Both /31 and /32 masks cannot be used because there are no host addresses available.
- The table works best for subnetting the last octet. You can still use the table for finding the decimal equivalent of bit-count masks that are less than 24-bits. Just subtract 8 from each number in the first row. For example, a 21-bit mask would use the same column as a 29-bit mask, and would have the same decimal value.
- A /24 subnet has 254 available host addresses (256-2) on a single subnet. The magic number is 256. If you need more hosts than this:
  - Decrease the mask bit count (i.e. /23, /22, /21, and so on).
  - Each time you decrease the bit count, double the magic number, then subtract 2.

## Route Summarization

As you study this section, answer the following questions:

- What are the advantages of route summarization?
- If automatic route summarization is used, how does the router determine which routes to summarize? What route becomes the summarized network?
- Which routing protocol does *not* support automatic route summarization?
- Why do discontiguous networks pose a problem for route summarization?

After finishing this section, you should be able to complete the following tasks:

- Given a scenario, select the appropriate subnet addresses and masks to prepare for summarization.
- Given a scenario, identify the summarized route.

This section covers the following exam objectives:

- 306. Determine the appropriate classless addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN/WAN environment

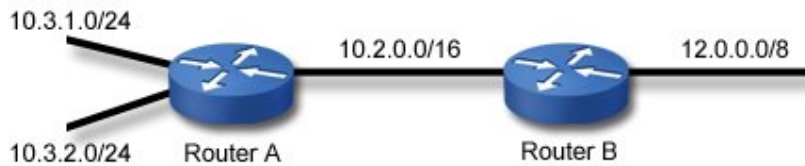
### **Route Summarization Facts**

Route summarization groups contiguous networks that use the same routing path, advertising a single route as the destination for the grouped subnets.

- Summarization reduces the size of the routing table. A single route to the summarized network takes the place of multiple routes to individual subnets.
- Summarization speeds convergence. The reachability of each subnet address is indicated by the reachability of the summarized address.
- Summarization retains all necessary routing information, so all networks are still reachable after summarization.
- Summarization can happen in one of two ways:

Method	Description
Automatic	<p>With automatic summarization, the router identifies adjacent networks and calculates the summarized route.</p> <ul style="list-style-type: none"><li>○ Autosummarization is supported on classless and classful routing protocols.</li><li>○ Autosummarization uses the default class boundary to summarize routes.</li><li>○ RIP (version 1 and version 2) and EIGRP support autosummarization; OSPF does not.</li><li>○ For RIPv2 and EIGRP, you can disable automatic summarization.</li></ul>
Manual	<p>With manual summarization, an administrator identifies the summarized route to advertise. The route you specify includes the summarized subnet address with the subnet mask that includes all summarized subnets.</p>

- Automatic summarization summarizes routes along class boundaries only when advertising those routes on a network of a different classful network. Consider the following graphic:



In this example, if both routers were using automatic summarization:

- Router A would *not* automatically summarize routes from the 10.3.1.0/24 or the 10.3.2.0/24 networks when advertising those networks to Router B. This is because subnet 10.2.0.0/16 that connects the two routers is in the same classful network (10.0.0.0/8) as the subnets connected to Router A.
- Router B would automatically summarize all routes as 10.0.0.0/8 when advertising routes on the 12.0.0.0/8 network. This is because this network is a different classful network than the 10.0.0.0/8 network.
- To prevent Router B from summarizing routes when advertising them to the 12.0.0.0/8 network, disable automatic route summarization on Router B.
- Route summarization works not only for grouping subnetted addresses together into a single route, but can also be used to advertise multiple classful network addresses into a single summarized route. For example, the subnets of 192.168.1.0/24 through 192.168.255.0/24 could be summarized as a single route of 192.168.0.0/16.

To identify a summarized route for a group of subnets, identify a subnet address and mask that includes all of the routes that need to be summarized. While in many cases you could simply advertise the default class boundary, this will often result in a route being advertised that includes subnets and addresses that aren't being used. To eliminate this problem, choose the subnet and mask so that only existing subnets are included. To do this:

1. Convert the last significant octet of the first and the last subnet in the contiguous range to binary. For example, if you had networks 172.16.16.0/24 through 172.16.31.0/24, you would have the following two binary values:  
 16 = 0 0 0 1 0 0 0 0  
 31 = 0 0 0 1 1 1 1 1
2. Identify the last consecutive binary bit that is shared. In this case, the last shared bit is the fourth bit position.
3. Convert all bits to the right of the shared bit to 0. In this example, this gives you the binary value of 00010000. This will be the subnet address of the summarized route. In this example, use 172.16.16.0.
4. Convert all bits to the left of the shared bit to 1. In this example, this gives you the binary value of 11110000. This will be the mask value of the summarized route. In this example, use 255.255.240.0.
5. Finally, identify any subnet addresses included in the range indicated by the advertised subnet and mask. Be aware that you will be unable to use these subnets without additional configuration for discontinuous networks. For example, if the first subnet you used in this example was 172.16.17.0 and the last subnet was 172.16.30.0, you would be unable to use the 172.16.16.0 and 172.16.31.0 subnets using a summarized route of 172.16.16.0/20.

## Wide Area Networks

As you study this section, answer the following questions:

- How does a *packet switched* WAN service differ from a *circuit switched* WAN service?
- Who is responsible for the local loop, the customer or the service provider?
- What is the significance of the *demarc*?
- What is the difference between the Data Terminal Equipment (DTE) and Data Communication Equipment (DCE)?
- Which WAN services use already-installed telephone lines?
- What media type is used by ATM?

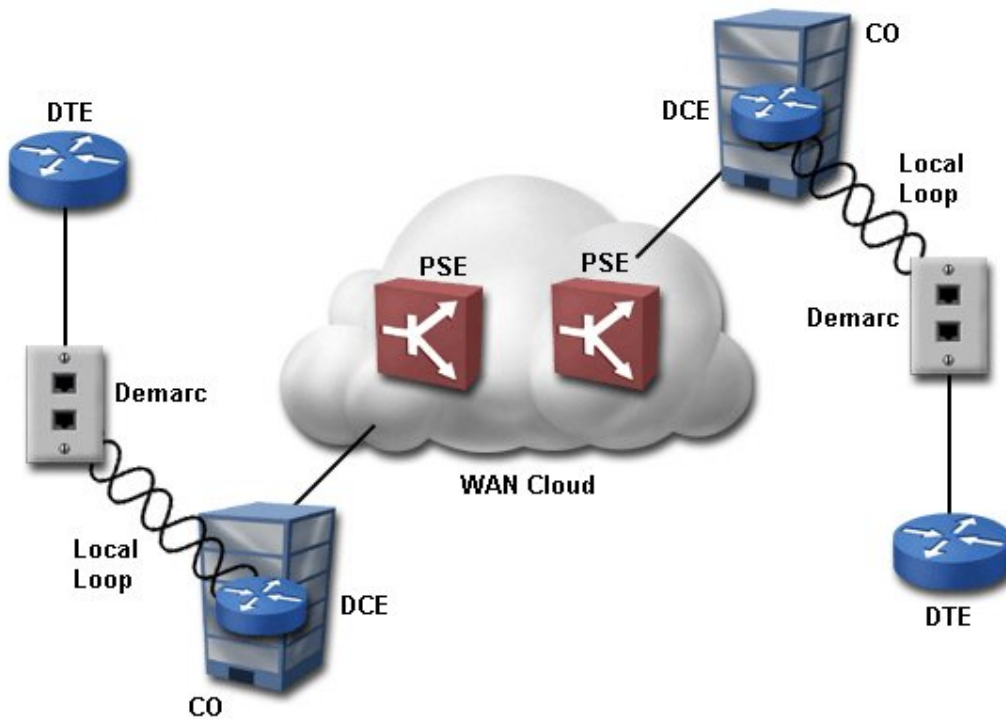
This section covers the following exam objectives:

- 111. Differentiate between LAN/WAN operation and features
- 801. Describe different methods for connecting to a WAN
- **WAN Type Facts**
- WAN types include the following:

Method	Description
Point-to-Point	A <i>point-to-point</i> connection is a single, pre-established path from the customer's network through a carrier network, such as a telco, to a customer's remote network. A point-to-point line is usually leased from a carrier and thus is often called a <i>leased line</i> .
Circuit Switching	A <i>circuit switching</i> network allows data connections that can be initiated when needed and terminated when communication is complete, working much like a telephone line for voice communication. A circuit switched network uses a dedicated connection between sites. It is ideal for transmitting data that must arrive quickly in the order it is sent, as is the case with real-time audio and video.
Packet Switching	A <i>packet switched</i> network allows data to be broken up into packets and sent across the shared resources. Packets are transmitted along the most efficient route to the destination. Packet switching is ideal for transmitting data that can handle transmission delays, as is often the case with Web pages and e-mail.

### **WAN Structure Facts**

A typical WAN structure includes the following components.



Component	Description
Consumer Premises Equipment (CPE)	Devices physically located on the subscriber's premises. CPE includes the telephone wire, telephone, modem, and other equipment, both the devices the subscriber owns and the ones leased from the WAN provider. The wiring typically includes UTP cable with RJ-11 or RJ-45 connectors. CPE is sometimes used synonymously with DTE.
Data Terminal Equipment (DTE)	A device on the network side of a WAN link that sends and receives data. The DTE resides on the subscriber's premises, and marks the point of entry between the LAN and the WAN. DTEs are usually routers, but computers and multiplexers can also act as DTEs. Broadly, DTEs are any equipment at the customer's site, and can include all computers. In a narrow sense, the DTE is the device that communicates with the DCE at the other end.
Channel Service Unit/Data Service Unit (CSU/DSU)	The CSU/DSU is a device that connects a physical circuit installed by the telco to some CPE device, adapting between the voltages, current, framing, and connectors used in the circuit to the physical interface supported by the DTE.
Demarcation point (demarc)	The point where the telephone company's telephone wiring connects to the subscriber's wiring. The demarc can also be called the network interface or point of presence. Typically, the customer is responsible for all equipment on one side of the demarc. The phone company is responsible for all equipment on the other side of the demarc.
Local loop	Cable that extends from the demarc to the central telephone office. The demarc media is owned and maintained by the telephone company. Typically, it is UTP, but it can also be one or a combination of UTP, fiber optic, or other media. Fiber optic cable to the demarc is rare.
Central Office (CO)	The switching facility closest to the subscriber, and the nearest point of presence for the WAN provider. It provides WAN-cloud entry and exit points for incoming and outgoing calls, and acts as a switching point to forward data to other central offices. A CO provides services such as switching incoming telephone signals to outgoing trunk lines. It also provides reliable DC power to the local loop to establish an electric circuit.



	COs use long-distance, or toll, carriers to provide connections to almost anywhere in the world. Long-distance carriers are usually owned and operated by companies such as AT&T or MCI.
Data Communication Equipment (DCE)	A device that communicates with both DTEs and the WAN cloud. DCEs are typically routers at the service provider that relay messages between the customer and the WAN cloud. In a strict sense, a DCE is any device that supplies clocking signals to DTEs. Thus, a modem or CSU/DSU at the customer site is often classified as a DCE. DCEs may be devices similar to DTEs (such as routers), except that each device plays a different role.
WAN cloud	The hierarchy of trunks, switches, and central offices that make up the network of telephone lines. It is represented as a cloud because the physical structure varies, and different networks with common connection points may overlap. Few people thoroughly understand where data goes as it is switched through the "cloud." What is important is that data goes in, travels through the line, and arrives at its destination.
Packet-Switching Exchange (PSE)	A switch on a carrier's packet-switched network. PSEs are the intermediary points in the WAN cloud.

### WAN Services Facts

Listed below are the most common WAN transmission media.

Carrier	Speed	Description
Plain Old Telephone Service (POTS)	56 Kbps	<ul style="list-style-type: none"> <li>Existing wires use only one twisted pair</li> <li>Analog signals are used through the local loop</li> <li>A modem is required to convert digital signals to analog</li> </ul>
T1 (a.k.a. DS1)	1.544 Mbps	<ul style="list-style-type: none"> <li>T-Carrier is a digital standard widely deployed in North America.</li> <li>T1 lines usually run over two-pairs of unshielded twisted pair (UTP) cabling, although they can also run over other media such as coaxial, fiber-optic, and satellite.</li> <li>A T1 line has 24 channels (also known as DS0's) that each run at 64 Kbps.</li> <li>T3 lines usually run over fiber-optic cable.</li> <li>A T3 line has 672 channels that each run at 64 Kbps.</li> <li>A T1/T3 connection requires a CSU/DSU.</li> </ul>
T3 (a.k.a. DS3)	44.736 Mbps	
E1	2.048 Mbps	<ul style="list-style-type: none"> <li>E-Carrier is a digital standard very similar to T-Carrier, but it is widely deployed in Europe.</li> <li>An E1 line has 32 channels (also known as DS0's) that run at 64 Kbps.</li> <li>An E3 line transmits 16 E1 signals at the same time.</li> <li>E1/E3 connections also require a CSU/DSU.</li> </ul>
E3	34.368 Mbps	
J1	1.544 Mbps	<ul style="list-style-type: none"> <li>J-Carrier is a digital standard very similar to T-Carrier, but it is widely deployed in Japan.</li> <li>A J1 line is virtually identical to a T1 line.</li> <li>A J3 line has 480 channels that run at 32 Mbps.</li> <li>J1/J3 connections also require a CSU/DSU.</li> </ul>
J3	32.064 Mbps	

**Note:** WAN services also use fiber optic, wireless, satellite, and other transmission media. However, the use of these media to the local loop is not common at this time.

If your organization needs WAN connectivity, you can choose from the following service options:

Service	Bandwidth (Max.)	Line Type	Signaling Method	Characteristics
Public Switched Telephone Network (PSTN)	56 Kbps	POTS	Analog	Dialup over regular telephone lines
Leased lines	56 Kbps	POTS	Analog	Dedicated line with consistent line quality
X.25	64 Kbps	POTS	Analog	Dedicated line Variable packet sizes (frames) Ideal for low-quality lines
Frame Relay	1.54 Mbps	POTS T-1 T-3	Digital	Variable packet sizes (frames)
Asynchronous Transfer Mode (ATM)	1.2 Gbps	Coaxial, twisted pair, fiber-optic	Digital	Fixed-size cells (53-byte) High-quality, high-speed lines
Integrated Services Digital Network (ISDN)	144 Kbps (BRI) 4 Mbps (PRI)	POTS T-1	Digital	Basic rate operates over regular telephone lines and is a dialup service Primary rate operates over T-carriers
DSL	6.1 Mbps (1.544 or lower is more common)	POTS	Digital	Operates using digital signals over regular telephone lines DSL comes in many different flavors (such as ADSL and HDSL)

There is no clear distinction between WAN services such as Frame Relay and ISDN. For example, you can use Frame Relay protocol over ISDN lines. Once a device connects to the WAN cloud, internal protocols can convert data traffic into the necessary formats, then convert the data again at the other end.

## WAN Connections

As you study this section, answer the following questions:

- Which interface provides clocking in the WAN connection?
- How is a DB-60 connector different from a Smart Serial connector?
- When would you use an RJ-48 connector?
- What is the default encapsulation protocol on Cisco routers?
- When should you use PPP as the encapsulation protocol?

After finishing this section, you should be able to complete the following tasks:

- Configure a serial interface for a basic WAN connection.
- Configure a serial connection between back-to-back routers.

This section covers the following exam objectives:

- 403. Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts
- 406. Connect, configure, and verify operation status of a device interface
- 801. Describe different methods for connecting to a WAN
- 802. Configure and verify a basic WAN serial connection

### **WAN Connection Facts**

Whether ordering a WAN connection from a service provider or configuring a back-to-back router lab, you should know how to connect the devices. There are several different types of cables used in WAN connections and choosing the correct cable largely depends upon identifying the following:

Component	Details
Interface operating mode	<p>When a device communicates over a serial interface, the interface operates in one of the following modes:</p> <ul style="list-style-type: none"><li>• The interface/device providing clocking is known as the DCE (Data Communications Equipment).</li><li>• The interface/device not providing clocking is known as the DTE (Data Terminal Equipment).</li></ul> <p>When you configure a router to connect to a network through a serial interface, the router must be connected to a device (such as a CSU/DSU or another router) that provides clocking signals. When you configure two routers in a back-to-back configuration through their serial ports, one router interface must be configured to provide the clocking signals for the connection.</p>
Service	<p>The following WAN service options will also affect which type of cable is needed for a WAN connection:</p> <ul style="list-style-type: none"><li>• X.25</li><li>• Frame Relay</li><li>• Asynchronous Transfer Mode (ATM)</li><li>• Integrated Services Digital Network (ISDN)</li><li>• DSL</li></ul>

Be aware of the following WAN connection details:

- When ordering a WAN service:
  - The network engineer specifies how fast the circuit should run, such as 1.544 Mbps (T1) or 56 Kbps (POTS or DS0).
  - The Telco installs the circuit running at the specified speed.
  - The network engineer purchases a CSU/DSU to connect to the end of the circuit, and then connects the router to the CSU/DSU.
  - The CSU/DSU clock rate must then be configured to match the circuit speed. Because the router is the DTE, the clock rate is received by the CSU/DSU and does not require configuration.
- When connecting a back-to-back router lab configuration, one router should be chosen as the DCE and the other router as the DTE. The cable connecting the two back-to-back routers has both a DCE and a DTE end. Connect the DCE end of the cable to the interface you want to be the DCE device.
- **WAN Connectors and Ports**
- WAN connections are provided through several different connector types. The following table illustrates the connector types and their ports:

Type	Description
<p><b>DB-60</b></p>  <p>Connector</p>  <p>Serial WIC port</p>	<p>WAN interface cards (WIC) with a single serial port use a DB-60 connector. The connector has 4 rows of 15 pins each.</p>
<p><b>Smart Serial</b></p>  <p>Connector</p>  <p>Smart Serial WIC ports</p>	<p>WICs with two serial ports use the high-density Smart Serial connector.</p>
<p><b>RJ-48</b></p>  <p>Connector</p>  <p>Integrated T1 DSU/DSU WIC port</p>	<p>Integrated T1 DSU/CSU WIC ports use an RJ-48 connector.</p> <p><b>Note:</b> The RJ-48 connector has the same size and shape as the RJ-45 used in Ethernet connections, but has a different pinout.</p>
<p><b>RJ-11</b></p>  <p>Connector</p>	<p>DSL (Digital Subscriber Line) WIC ports use an RJ-11 connector. The RJ-11 port connects to the phone line.</p>



DSL WIC port

## WAN Encapsulation Facts

WAN Physical layer protocols specify the hardware and bit signaling methods. Data Link layer protocols control some or all of the following functions:

- Error checking and correction
- Link establishment
- Frame-field composition
- Point-to-point flow control

Data Link layer protocols also describe the encapsulation method or the frame format. WAN encapsulation methods are typically called HDLC (high-level data link control). This term is both a generic name for Data Link protocols and the name of a specific protocol within a WAN protocol suite or service. Depending on the WAN service and connection method, you will select one of the following encapsulation methods.

- Cisco HDLC for synchronous, point-to-point connections with other Cisco routers. This is the default encapsulation method for synchronous serial links on Cisco routers. **Note:** Cisco HDLC does not communicate with other vendors' implementations of HDLC.
- LAPB for X.25 networks.
- LAPD in combination with another protocol for the B channels in ISDN networks. LAPD is a Layer 2 ISDN protocol that manages flow and signaling.
- PPP for dial-up LAN access, circuit-switched WAN networks, and ISDN networks. PPP is non-proprietary, so it works in implementations that use products from multiple vendors.
- Cisco/IETF for Frame Relay networks.

**Note:** Routers on each side of a WAN link must use the same encapsulation method to be able to communicate.

## Serial Interface Configuration Command List

Use the following commands to configure the router.

Use ...	To ...
<pre>Router(config-if)#clock rate &lt;rate&gt;</pre>	Set the clock rate on the DCE serial interface.  <b>Note:</b> In the back-to-back router lab configuration, if the <b>clock rate</b> command is not issued on the DCE, clocking is not provided, and the interface status between the two routers will not change to up.
<pre>Router(config-if)#ip address &lt;address&gt; &lt;mask&gt;</pre>	Assign an IP address and subnet mask to the interface.
<pre>Router(config- if)#encapsulation hdlc Router(config- if)#encapsulation ppp Router(config- if)#encapsulation frame- relay</pre>	Modify the router encapsulation method.  <b>Note:</b> HDLC is the default encapsulation method. The encapsulation method should match for both routers.

Router#sh interfaces	View all interface configurations, including serial connection encapsulation and bandwidth.
Router#sh ip int brief	View a consolidated message concerning each IP interface, including its IP address, line and protocol status, and how the address was configured (DHCP or Manual)
Router#sh run	View the clock rate and bandwidth of a serial configuration.
Router#sh controllers <serial interface>	View the serial interface configuration, such as the type of serial cable and which end of the cable is connected to the device (DCE or DTE).

### Examples

The following set of commands configures the IP address 192.168.1.229 with a mask of 255.255.255.0 for the first Serial interface on the router and activates the interface.

```
Router(config)#int ser 0/1/0
Router(config-if)#ip address 192.168.1.229 255.255.255.0
Router(config-if)#no shutdown
```

The following set of commands configures the second Serial interface on the router with PPP encapsulation and activates the interface.

```
Router(config)#int ser 0/1/1
Router(config-if)#encapsulation ppp
Router(config-if)#no shutdown
```

## PPP

As you study this section, answer the following questions:

- What is the purpose of LCPs in PPP communications?
- Which authentication method is more secure, PAP or CHAP?
- How do you configure the password used with PPP authentication?

After finishing this section, you should be able to complete the following tasks:

- Configure PPP encapsulation on serial links.
- Configure PPP authentication including username and password combinations.

This section covers the following exam objectives:

- 801. Describe different methods for connecting to a WAN
- 802. Configure and verify a basic WAN serial connection
- 806. Configure and verify a PPP connection between Cisco routers

### **PPP Facts**

The following list represents some of the key features of the Point-to-Point Protocol (PPP):

- It can be used on a wide variety of physical interfaces including asynchronous serial, synchronous serial (dial up), and ISDN.
- It supports multiple Network layer protocols, including IP, IPX, AppleTalk, and numerous others.
- Optional authentication is provided through PAP (2-way authentication) or CHAP (3-way authentication).
- It supports multilink connections, load-balancing traffic over multiple physical links.
- It includes Link Quality Monitoring (LQM) which can detect link errors and automatically terminate links with excessive errors.
- It includes looped link detection that can identify when messages sent from a router are looped back to that router. This is done through routers sending magic numbers in communications. If a router receives a packet with its own magic number, the link is looped.

PPP uses two main protocols to establish and maintain the link.

Protocol	Description
Link Control Protocol (LCP)	<p>The Link Control Protocol (LCP) is responsible for establishing, maintaining, and tearing down the PPP link. LCP packets are exchanged periodically to do the following:</p> <ul style="list-style-type: none"><li>• During link establishment, LCPs are used to agree upon encapsulation, packet size, and compression settings. LCPs also indicate whether authentication should be used.</li><li>• Throughout the session, LCPs are exchanged to detect and correct errors or to control the use of multiple links (multilink).</li><li>• When the session is terminated, LCPs are responsible for tearing down the link.</li></ul> <p>A single Link Control Protocol runs for each physical connection.</p>
Network Control	<p>The Network Control Protocol (NCP) is used to agree upon and configure Network layer protocols to use (such as IP, IPX, or AppleTalk). Each Network layer</p>



Protocol (NCP)	<p>protocol has a corresponding control protocol packet. Examples of control protocols include:</p> <ul style="list-style-type: none"> <li>• IP Control Protocol (IPCP)</li> <li>• CDP Control Protocol (CDPCP)</li> <li>• IPX Control Protocol (IPXCP)</li> <li>• AppleTalk Control Protocol (ATCP)</li> </ul> <p>A single PPP link can run multiple control protocols, one for each Network-layer protocol supported on the link.</p>
----------------	---

PPP establishes communication in three phases.

1. LCP phase. LCPs are exchanged to open the link and agree upon link settings such as encapsulation, packet size, and whether authentication will be used.
2. Authenticate phase (optional). During this phase, authentication-specific packets are exchanged to configure authentication parameters and authenticate the devices. LCPs might also be exchanged during this phase to maintain the link.
3. NCP phase. NCPs are exchanged to agree on upper-layer protocols to use. For example, routers might exchange IPCP and CDPCP packets to agree upon using IP and CDP for Network-layer communications. During this phase, LCPs might continue to be exchanged.

### PPP Command List

PPP configuration is often done in connection with configuring other services. To configure PPP on the router, complete the following tasks:

1. Set PPP encapsulation on the interface. You must set the encapsulation method to PPP before you can configure authentication or compression.
2. Select CHAP and/or PAP as the authentication method (optional).
3. If authentication is used, [configure username/password combinations](#).

PPP options are configured in interface mode for a specific interface.

Use ...	To ...
Router(config-if)#encapsulation ppp	Set the encapsulation type to PPP
Router(config-if)#ppp authentication <chap pap> Router(config-if)#ppp authentication chap pap	Set the authentication method(s) When multiple methods are specified, the first method will be tried first
Router(config-if)#ppp compression	Set compression options
Router(config-if)#ppp chap pap password <password>	Set the password used with CHAP or PAP for an unknown host
Router(config)#username <hostname> password <password>	Set the username and password for the local router
Router(config)#bandwidth <value>	Set a bandwidth value for an interface
Router# <a href="#">show interface</a>	View encapsulation and PPP information on an interface

To hide the CHAP password from view in the configuration file, use the **service password-encryption** command from the global configuration mode.



**Example**

The following commands configure the SFO router to use PPP and enable it to connect to the LAX router using PAP authentication.

```
SFO(config)#hostname LAX password cisco5
SFO(config)#int s0/1/0
SFO(config-if)#encap ppp
SFO(config-if)#ppp auth pap
```

## Network Address Translation (NAT)

As you study this section, answer the following questions:

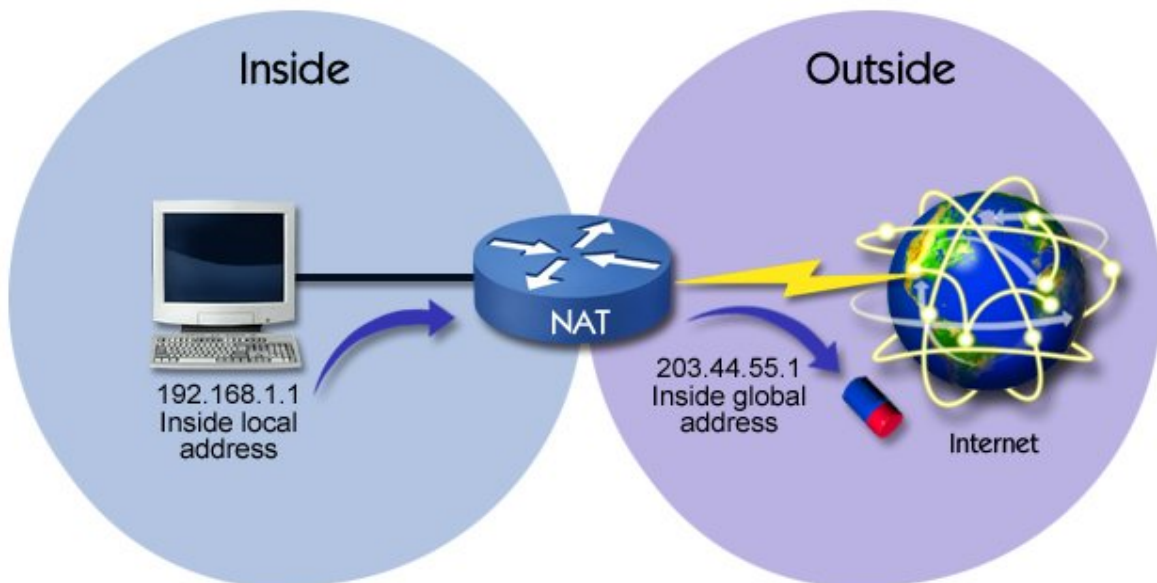
- What are the IP address ranges for private networks?
- Which network devices are most likely to be assigned a *public* IP address?
- What benefits come from using NAT?
- What is the difference between an inside global address and an outside global address?
- What is overloading, and why is it important in a NAT configuration?
- How is PAT different than NAT?

This section covers the following exam objectives:

- 706. Explain the basic operation of NAT
- 707. Configure NAT for given network requirements

### **NAT Facts**

Network Address Translation (NAT) allows you to connect a private network to the Internet without obtaining registered addresses for every host. Private addresses are translated to the public address of the NAT router. NAT can be used to provide a measure of security for your private network, or to provide Internet connectivity with a limited number of registered IP addresses.



As you work with NAT, it's important to understand the following terminology.

<b>Term</b>	<b>Definition</b>
Inside	The inside network is the private network. A router interface that connects to the private network is also called the inside interface.
Outside	The outside network is the public network (the Internet). A router interface that connects to the public network is also called the outside interface.
Inside local address	The inside local address is the IP address of the host on the inside network.

Inside global address	The inside global address is the IP address of the host after it has been translated for use on the Internet. The term <i>global</i> refers to the registered IP address that identifies the inside host on the Internet.
Outside global address	The outside global address is an IP address of an Internet host. For example, when you visit a Web site, your computer will use the global outside address to contact the Web server.
Outside local address	An outside local address is an outside global address that has been translated for inside (or private) use. In other words, the NAT router translates an Internet host IP address into a private IP address. Instead of using the Web server address, the internal computer will use the translated address instead.

When configuring NAT, you have the following options:

Method	Description
Static	Use static translation to translate a single outside address to a single inside address.
Overloaded with PAT	Use overloaded NAT with Port Address Translation (PAT) to translate multiple inside addresses to a single public address. Port numbers are used to identify specific inside local hosts. The port number associated with the private host is appended to the inside global IP address. Use this option to allow multiple inside hosts to access the Internet using a single public IP address.
Dynamic	Use dynamic translation to translate a range of outside addresses to a range of inside addresses. Use this option when you have multiple public addresses for multiple private addresses. If the number of inside addresses is greater than the number of outside addresses, use the overloaded option with dynamic NAT.

Configuring NAT on a Cisco router may be done through the command line interface (CLI) or the Security Device Manager (SDM). When using the SDM to configure NAT, you start a wizard that helps you choose the NAT configuration parameters.

- Choose **Basic NAT** to identify the inside and outside interfaces. Selecting this option configures overloaded NAT with PAT. The public address assigned to the public interface is used for all private hosts.
- Choose **Advanced NAT** to:
  - Identify the outside interface.
  - Configure additional public addresses that can be used for dynamic translation.
  - Identify inside interfaces and additional network addresses that are not directly connected to the NAT router that will be translated. This option lets you configure a single NAT router for your entire private network, even when your network consists of multiple subnets accessible through other routers on the private network.
  - Perform static mappings that translate a public IP address to a private host address. With this option, hosts on the private network are assigned a private IP address, and the private IP address is mapped to a public IP address. Incoming communications sent to the public IP address are translated and forwarded to the private host. The wizard calls these mappings *NAT rules*.

**Note:** To start the NAT wizard, the router must have at least two enabled interfaces.

When configuring a router for NAT, be sure to use an IP address in the private IP address ranges for the inside local IP addresses. Otherwise, hosts on your network might not be able to access outside hosts with the same IP address. A Cisco router can be configured to overcome this problem, but the configuration is difficult. Private IP addresses do not need to be registered, and fall within the following ranges:

- 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

## WAN Troubleshooting

As you study this section, answer the following questions:

- What are possible causes of Layer 1 problems on a serial connection?
- Which interface status indicates a Layer 2 connection problem?
- What steps can you take to correct a Layer 2 problem?
- How does having an incorrect interface IP address affect a WAN connection?
- A ping test to a remote router succeeds, but the Telnet connection fails. What can you assume about the router configuration? Can the router route packets?
- You have Layer 2 connectivity to a remote device but full connectivity does not exist. What steps can you take to identify the problem?

This section covers the following exam objectives:

- 407. Verify device configuration and network connectivity using ping, traceroute, telnet, SSH or other utilities
- 414. Verify network connectivity (including: using ping, traceroute, and telnet or SSH)
- 804. Troubleshoot WAN implementation issues

### WAN Troubleshooting Facts

The following list of commands may help when troubleshooting router connections.

Use...	To...
router#show interfaces	List a large set of information about each interface.
router#show interface status	View summary information about the interface status.
router#show ip interfaces	View a small set of information about each IP interface.
router#show ip interfaces brief	View a single line of information about each IP interface.
router#show ip route <ip address>	View details about the route the router would match for a packet sent to the listed IP address.
router#show running-config	View the currently running configuration file.
router#show controllers <serial interface>	View the serial interface configuration, such as the type of serial cable and which end of the cable is connected to the device (DCE or DTE).
router#ping <ip address>	Test communication with a specific interface using its IP address.

You can use the interface status to understand connectivity problems and quickly see whether the link between the router and the network is operational. The following table summarizes some possible conditions indicated by the interface status:

Line status	Protocol status	Indicates...
administratively down	down	The interface is configured with the <b>shutdown</b> command.
down	down	There is a hardware or network connection problem (Physical layer), such as:

		<ul style="list-style-type: none"> <li>• No cable or bad cable</li> <li>• The device on the other end of the cable is powered off or the other interface is administratively shutdown (with the <b>shutdown</b> command)</li> </ul>
up	down	<p>There is a connection or communication problem (Data Link layer), such as:</p> <ul style="list-style-type: none"> <li>• No clock rate provided by the DCE device</li> <li>• Mismatched encapsulation</li> <li>• Incorrect authentication parameters for PPP, including: <ul style="list-style-type: none"> <li>○ Mismatched authentication method</li> <li>○ Missing <b>username</b> statements</li> <li>○ Mismatched passwords</li> </ul> </li> </ul>
up	up	The interface is working correctly

After verifying that the interfaces have Layer 1 and Layer 2 connectivity, proceed to troubleshoot TCP/IP connectivity including:

- Verifying that devices have unique IP addresses.
- Verifying that the same subnet mask is used on all devices on the same subnet.
- Verifying that the IP address assigned to each device is on the same subnet.
- Verifying routing table entries.

Be aware of the following when troubleshooting connectivity:

- If a problem exists at Layer 1, you must correct that problem before troubleshooting Layer 2 connectivity. If a problem exists at Layer 2, you must correct that problem before you can proceed to troubleshoot upper-layer connectivity.
- Use **ping** and **tracert** to verify Network-layer connectivity, and use Telnet to verify Application-layer connectivity and configuration.
- A failed **ping** or **tracert** test might indicate Layer 1, Layer 2, or Layer 3 problems. Examine the interface status to rule out Layer 1 and Layer 2 problems.
- A successful Telnet test means that **ping** and **tracert** will also be successful. A failed Telnet test only indicates a failure at the Application layer or below. By itself, it does not tell you at which layer the problem exists.
- Because some devices do not respond to ICMP messages, you might have Network-layer connectivity between devices even if **ping** or **tracert** fail.
- A successful **ping** test followed by an unsuccessful Telnet test means that Network-layer connectivity exists. Troubleshoot the upper-layer configuration.
- Even if Telnet to a router fails, the router might still be routing packets. This is because routing happens at the Network layer, while Telnet happens at the Application layer.

## Virtual LANs (VLANs)

As you study this section, answer the following questions:

- What are two advantages to creating VLANs on your network?
- You have two VLANs configured on a single switch. How many broadcast domains are there? How many collision domains are there?
- What happens if two devices on the same switch are assigned to different VLANs?

After finishing this section, you should be able to complete the following tasks:

- Create VLANs and assign switch ports to a VLAN.

This section covers the following exam objectives:

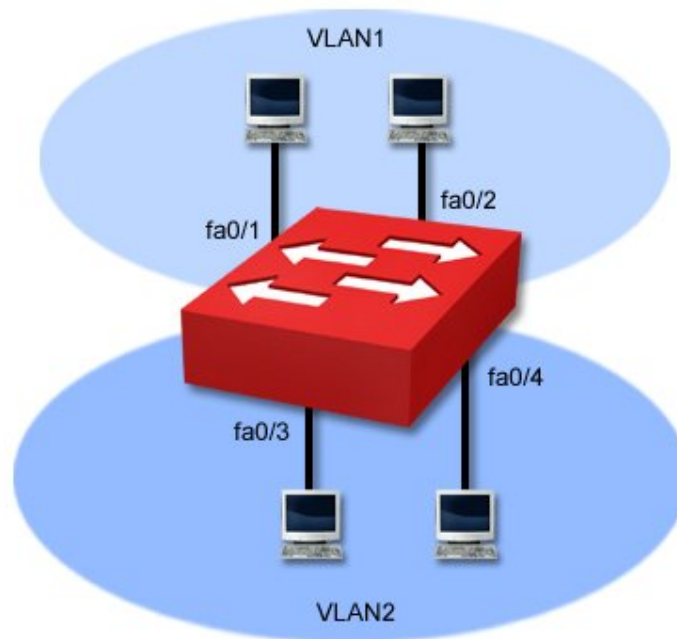
- 208. Describe enhanced switching technologies
- 209. Describe how VLANs create logically separate networks and the need for routing between them
- 210. Configure, verify, and troubleshoot VLANs

### **VLAN Facts**

A virtual LAN (VLAN) can be defined as:

- Broadcast domains defined by switch port rather than network address
- A grouping of devices based on service need, protocol, or other criteria rather than physical proximity

Using VLANs lets you assign devices on different switch ports to different logical (or virtual) LANs. Although each switch can be connected to multiple VLANs, each switch port can be assigned to only one VLAN at a time. The following graphic shows a single-switch VLAN configuration.



Be aware of the following facts about VLANs:

- In the graphic above, FastEthernet ports 0/1 and 0/2 are members of VLAN 1. FastEthernet ports 0/3 and 0/4 are members of VLAN 2.
- In the graphic above, workstations in VLAN 1 will *not* be able to communicate with workstations in VLAN 2, even though they are connected to the same physical switch.
- Defining VLANs creates additional broadcast domains. The above example has two broadcast domains, each of which corresponds to one of the VLANs.
- By default, switches come configured with several default VLANs:
  - VLAN 1
  - VLAN 1002
  - VLAN 1003
  - VLAN 1004
  - VLAN 1005
- By default, all ports are members of VLAN 1.

Creating VLANs with switches offers the following administrative benefits.

- You can create virtual LANs based on criteria other than physical location (such as workgroup, protocol, or service)
- You can simplify device moves (devices are moved to new VLANs by modifying the port assignment)
- You can control broadcast traffic and create collision domains based on logical criteria
- You can control security (isolate traffic within a VLAN)
- You can load-balance network traffic (divide traffic logically rather than physically)

**Note:** VLANs are commonly used with Voice over IP (VoIP) to distinguish voice traffic from data traffic. Traffic on the voice VLAN can be given a higher priority to ensure timely delivery.

Creating VLANs with switches offers the following benefits over using routers to create distinct networks.

- Switches are easier to administer than routers
- Switches are less expensive than routers
- Switches offer higher performance (introduce less latency)

A disadvantage of using switches to create VLANs is that you might be tied to a specific vendor. Details of how VLANs are created and identified can vary from vendor to vendor. Creating a VLAN might mean you must use only that vendor's switches throughout the network. When using multiple vendors in a switched network, be sure each switch supports the 802.1q standards if you want to implement VLANs.

Despite advances in switch technology, routers are still needed to:

- Filter WAN traffic
- Route traffic between separate networks
- Route packets between VLANs
- **VLAN Command List**
- To configure a simple VLAN, first create the VLAN, and then assign ports to that VLAN. The following table shows common VLAN configuration commands.

Task	Command(s)
Define a VLAN Giving the VLAN a name is optional. VLAN names must be unique.	switch(config)#vlan <1-4094> switch(config-vlan)#name WORD
Delete a VLAN When you delete a VLAN, all ports assigned to the VLAN	switch(config)#no vlan <1-4094>



remain associated with the deleted VLAN, and are therefore inactive. You must reassign the ports to the appropriate VLAN.	
Assign ports to the VLAN <b>Note:</b> If you assign a port to a VLAN that does not exist, the VLAN will be created automatically.	switch(config-if)#switchport access vlan <1-4094>
Show a list of VLANs on the system	switch#show vlan switch#show vlan brief
Show information for a specific VLAN	switch#show vlan id <1-4064>

- **Example**

The following commands create VLAN 12 named IS\_VLAN, identifies port 0/12 as having only workstations attached to it, and assigns the port to VLAN 12.

- switch#config t
- switch(config)#vlan 12
- switch(config-vlan)#name IS\_VLAN
- switch(config-vlan)#interface fast 0/12
- switch(config-if)#switchport access vlan 12

## Trunking

As you study this section, answer the following questions:

- Why is trunking important to VLAN configuration?
- Which trunking protocols are supported on a Cisco 2960 switch? Which protocol is an industry standard?
- What protocol does a Cisco switch use to automatically detect trunk ports?
- By default, traffic from which VLANs are allowed on trunk ports?
- A trunk port is set to **dynamic desirable**. What configurations on other switches are allowed so the port enters a trunking state?

After finishing this section, you should be able to complete the following tasks:

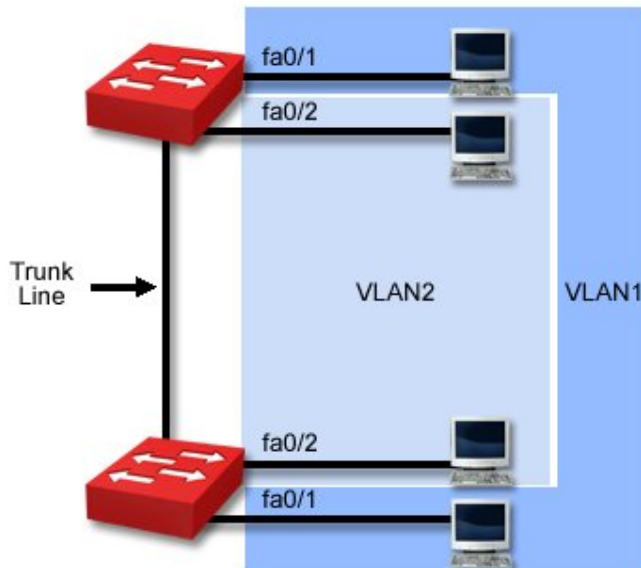
- Configure a switch port as an access port or a trunk port.
- Configure dynamic trunking modes.

This section covers the following exam objectives:

- 208. Describe enhanced switching technologies
- 211. Configure, verify, and troubleshoot trunking on Cisco switches

### Trunking Facts

*Trunking* is a term used to describe connecting two switches together. Trunking is important when you configure VLANs that span multiple switches as shown in the diagram.



Be aware of the following facts regarding trunking and VLANs:

- In the above graphic, each switch has two VLANs. One port on each switch has been assigned to each VLAN.
- Workstations in VLAN 1 can only communicate with workstations in VLAN 1. This means that the two workstations connected to the same switch cannot communicate with each other. Communications within the VLAN must pass through the trunk link to the other switch.
- Trunk ports identify which ports are connected to other switches.

- Trunk ports can automatically carry traffic for all VLANs defined on the switch. You can prevent traffic from a specific VLAN from being carried on the trunk through a specific configuration.
- Typically, Gigabit Ethernet ports are used for trunk ports, although any port can be a trunking port.

When trunking is used, frames that are sent over a trunk port are tagged with the VLAN ID number so that the receiving switch knows to which VLAN the frame belongs.

- Tags are appended by the first switch in the path, and removed by the last.
- Only VLAN-capable devices understand the frame tag.
- Tags must be removed before a frame is forwarded to a non-VLAN-capable device.

The trunking protocol describes the format that switches use for tagging frames with the VLAN ID. Cisco devices support two trunking protocols:

Trunking Protocol	Characteristics
Inter-Switch Link (ISL)	<ul style="list-style-type: none"> <li>• A Cisco-proprietary trunking protocol.</li> <li>• ISL can only be used between Cisco devices.</li> <li>• ISL tags each frame with the VLAN ID.</li> <li>• Catalyst 2960 switches do <i>not</i> support ISL.</li> </ul>
802.1Q	<ul style="list-style-type: none"> <li>• An IEEE standard for trunking and therefore supported by a wide range of devices.</li> <li>• With 802.1Q trunking, frames from the default VLAN 1 are not tagged. Frames from all other VLANs are tagged.</li> </ul>

Cisco switches have the ability to automatically detect ports that are trunk ports, and to negotiate the trunking protocol used between devices. Switches use the Dynamic Trunking Protocol (DTP) to detect and configure trunk ports. For example, when you connect two switches together, they will automatically recognize each other and select the trunking protocol to use.

### Trunking Command List

The following table lists important commands for configuring and monitoring trunking on a switch.

Command	Function
Switch(config-if)#switchport mode trunk	<ul style="list-style-type: none"> <li>• Enables trunking on the interface.</li> <li>• The port will <i>not</i> use DTP on the interface.</li> </ul>
Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)#switchport trunk encapsulation isl	<ul style="list-style-type: none"> <li>• Sets the trunking protocol</li> <li>• Because 2960 switches only support 802.1Q, you will not use this command on 2960 switches</li> </ul>
Switch(config-if)#switchport mode dynamic auto	<ul style="list-style-type: none"> <li>• Enables automatic trunking discovery and configuration.</li> <li>• The switch uses DTP to configure trunking.</li> </ul>
Switch(config-if)#switchport mode dynamic desirable	<ul style="list-style-type: none"> <li>• Enables dynamic trunking configuration.</li> <li>• If a switch is connected, it will attempt to use the desired trunking protocol (802.1Q for 2960</li> </ul>

	<p>switches).</p> <ul style="list-style-type: none"> <li>• If a switch is not connected, it will communicate as a normal port.</li> </ul>
Switch(config-if)#switchport mode access	Disables trunking configuration on the port.
<pre>Switch#show interface trunk Switch#show interface fa0/1 trunk</pre>	<p>Shows interface trunking information with the following:</p> <ul style="list-style-type: none"> <li>• Mode</li> <li>• Encapsulation</li> <li>• Trunking status</li> <li>• VLAN assignments</li> </ul>

**Note:** Two switches both configured to use **desirable** dynamic trunking will not trunk. At least one of the switches must be set to manually trunk or to use **auto** dynamic trunking.

## VLAN Trunking Protocol (VTP)

As you study this section, answer the following questions:

- What is the function of the VTP protocol?
- A switch in transparent mode. Will the switch learn VLAN information from other switches? Will the switch propagate information to other switches?
- Where does a switch in client mode save VLAN information?
- When would a switch in client mode update VLAN information on a switch in server mode?
- Why is the default VTP mode of a switch important?
- What conditions must be met before two switches will share VLAN information using VTP?

After finishing this section, you should be able to complete the following tasks:

- Configure the VTP mode on a switch.
- Set VTP domain and password parameters.

This section covers the following exam objectives:

- 208. Describe enhanced switching technologies
- 213. Configure, verify, and troubleshoot VTP

### VTP Facts

The VLAN Trunking Protocol (VTP) simplifies VLAN configuration on a multi-switch network by propagating configuration changes to other switches. With the VTP, switches are placed in one of the following three configuration modes.

Mode	Characteristics
Server	<p>A switch in server mode is used to modify the VLAN configuration. On a server:</p> <ul style="list-style-type: none"><li>• Changes can be made to the VLAN configuration on the switch.</li><li>• The switch advertises VTP information to other switches in the domain.</li><li>• The switch updates its VLAN configuration from other switches in the domain.</li><li>• The switch saves the VLAN configuration in NVRAM.</li></ul>
Client	<p>A switch in client mode receives changes from a VTP server and passes VTP information to other switches. On a client:</p> <ul style="list-style-type: none"><li>• Changes cannot be made to the VLAN configuration.</li><li>• The switch advertises VTP information to other switches in the domain.</li><li>• The switch updates its VLAN configuration from other switches in the domain.</li><li>• The switch does <i>not</i> save the VLAN configuration in NVRAM.</li></ul>
Transparent	<p>A switch in transparent mode allows for local configuration of VLANs, but does not update its configuration based on the configuration of other switches. On a transparent switch:</p> <ul style="list-style-type: none"><li>• Changes can be made to the VLAN configuration on the switch.</li><li>• Local VLAN information is not advertised to other switches.</li><li>• VTP information received from other switches is passed through the switch.</li></ul> <p><b>Note:</b> The transparent switch only relays VTP information if it is in the same</p>

VTP domain or if it has a null (blank) VTP domain.

- The switch does not update its VLAN configuration from other switches in the domain.
- The switch saves its VLAN configuration in NVRAM.

Keep in mind the following facts about VTP:

- By default, switches are preconfigured in server mode. If you do not intend to use VTP, configure each switch to use transparent mode.
- You can have multiple VTP servers in the same domain on the network. Changes made to any server are propagated to other client and server switches.
- To make VLAN changes on a switch, the switch must be in either server or transparent mode. You cannot modify the VLAN configuration if:
  - The switch is in client mode
  - The switch is in server mode and without a configured domain name.
- VTP uses the following process for communicating updates:
  1. VTP summary advertisement packets contain the domain name, MD5 version of the password, and the revision number.
  2. When a switch receives a summary packet, it compares the domain name and password in the packet with its own values. If the domain name and password do not match, the packet is dropped.
  3. If the domain name and password match, the switch compares the revision number in the packet.
  4. If the revision number in the packet is lower or equal, the packet is ignored. If it is higher, the switch sends an advertisement request for the latest updates.
  5. When the updates are received, the VLAN configuration and the revision number is updated.

If you lose your only VTP server, the easiest way to recover is to change one of the VTP clients to server mode. VLAN information and revision numbers remain the same.

Switches must meet the following conditions before VTP information can be exchanged:

- The switches must be connected by a trunk link. VTP is not used on access ports.
- Switches must be in the same domain. Switches in different domains do not share or forward VTP information. Transparent switches must be in the same domain or have a null domain name to pass VTP information to other switches.
- Passwords on each device must match. The password is included in each VTP advertisement. The receiving switch compares the password in the advertisement with its configured password. It will only accept information in the packet if the passwords match. The password provides a method of authenticating the packet contents that they came from a trusted source.

Connecting two switches with different VTP domains works only if you manually turn trunking on. VTP information is carried in DTP packets, so only switches in the same domain can use DTP for automatic trunking configuration. However, when two switches with different domains are connected, VTP information will not be passed between the switches.

When you change the VLAN configuration on a server, the revision number is incremented. The revision number on a transparent switch remains at 0, even when changes are made to the VLAN configuration.

All devices in the domain must use the same VTP version. By default, VTP version 2 is disabled. Only enable VTP version 2 if all devices support version 2.

### VTP Configuration Facts

The following table lists common VTP commands.

Use...	To...
--------	-------

Switch(config)#vtp mode server client transparent	Configure the VTP mode of the switch. The default mode is <b>server</b> .
Switch(config)#vtp domain WORD	Configure VTP domain of the switch. The default domain name is <null> (blank). All switches must be configured with the same domain name. A new VTP client switch (with a blank domain name) will automatically set its domain name based on the first VTP advertisement it receives. A switch in transparent mode will <i>not</i> automatically set its domain name.
Switch(config)#vtp password WORD	Configure VTP password of the switch. When a password is used, all switches in the same domain must use the same password. You must manually configure the VTP password on each switch.
Switch(config)#vtp pruning	Reduce broadcast traffic by forwarding the messages only through switch trunks which belong to a particular VLAN ID. Enabling or disabling VTP pruning on a server enables or disables it on all devices in the domain.
Switch#show vtp status	View the current VTP configuration of the switch.
Switch#show vtp password	View the current VTP password of the switch.

Be aware of the following when troubleshooting the VTP configuration:

- If you add a switch to the network with a higher revision number, the VLAN configuration on that switch will update (modify) the existing VLAN configuration on all other switches in the domain. This is true *even if the switch you add is a client*. Client switches pass their configuration information on to other switches. This information can be used to update server or client switches with lower revision numbers.
- If you add a switch to the network with a lower revision number, the switch's configuration will be modified to match the configuration currently used on the network. This is true *even if the switch you add is a server*.
- To prevent disruptions to the existing configuration when adding new switches, reset the revision number on all new switches before adding them to the network. The revision number resets to 0 each time you:
  - Change the domain name.
  - Change the VTP mode to transparent.

Before adding a switch back into the network, change the domain name or the mode to transparent, then change it back to its original setting.

- Be sure to place switches in the same domain adjacent to each other through trunk links. If you insert a switch with a different domain name between two switches, VTP information will not be passed through the new switch. To correct this problem, use one of the following solutions:
  - Modify the domain name on the new switch to match the existing switches.
  - Move the new switch so that switches in the same domain are connected directly together.

**Note:** Once set, you cannot completely remove a domain name. In other words, once you have configured a VTP domain name, you can only change the name, you cannot remove it completely.

## **Spanning Tree**

As you study this section, answer the following questions:



- What is the purpose of the spanning tree protocol?
- What is the role of designated bridges?
- What are BPDUs and when are they exchanged?
- A switch port is in the blocking state. Will it learn MAC addresses? Will it send and receive frames?
- A switch port is in the learning state. Will it learn MAC addresses? Will it send and receive frames?
- A switch port is identified as a backup port. What state is it in?
- What advantages are added to spanning tree with the edge port type definition? How does this improve performance?
- How does PVST+ differ from Rapid PVST+?

This section covers the following exam objectives:

- 208. Describe enhanced switching technologies
- 214. Configure, verify, and troubleshoot RSTP operation

### Spanning Tree Facts

To provide for fault tolerance, many networks implement redundant paths between devices using multiple switches. However, providing redundant paths between segments causes packets to be passed between the redundant paths endlessly. This condition is known as a *bridging loop*.

To prevent bridging loops, the IEEE 802.1d committee defined a standard called the spanning tree algorithm (STA), or spanning tree protocol (STP). With this protocol, one bridge (or switch) for each route is assigned as the designated bridge. Only the designated bridge can forward packets. Redundant bridges (and switches) are assigned as backups.

The spanning tree algorithm provides the following benefits:

- Eliminates bridging loops
- Provides redundant paths between devices
- Enables dynamic role configuration
- Recovers automatically from a topology change or device failure
- Identifies the optimal path between any two network devices

The spanning tree algorithm calculates the best loop-free path through a network by assigning a role to each bridge or switch and by assigning roles to the ports of each bridge or switch. The bridge role determines how the device functions in relation to other devices, and whether the device forwards traffic to other segments.

Role	Characteristics
Root bridge	<p>The root bridge is the master or controlling bridge.</p> <ul style="list-style-type: none"> <li>• There is only one root bridge in the network. The root bridge is the logical center of the spanning-tree topology in a switched network.</li> <li>• The root bridge is determined by the switch with the lowest bridge ID (BID). <ul style="list-style-type: none"> <li>○ The bridge ID is composed of two parts: a bridge priority number and the MAC address assigned to the switch.</li> <li>○ The default priority number for all switches is 32,768. This means that for unconfigured switches, the switch with the lowest MAC address becomes the root bridge.</li> <li>○ You can manually configure the priority number to force a specific switch to become the root switch.</li> </ul> </li> <li>• The root bridge periodically broadcasts configuration messages. These</li> </ul>

	<p>messages are used to select routes and reconfigure the roles of other bridges if necessary.</p> <ul style="list-style-type: none"> <li>• All ports on a root bridge forward messages to the network.</li> </ul> <p><b>Note:</b> Newer switches add the VLAN number to the priority value. For example, if you configure a priority value of 4096, the switch will use the priority of 4097 for VLAN 1, 4098 for VLAN 2, and so on.</p>
Designated bridge	<p>A designated bridge is any other device that participates in forwarding packets through the network.</p> <ul style="list-style-type: none"> <li>• They are selected automatically by exchanging bridge configuration packets.</li> <li>• To prevent bridging loops, there is only one designated bridge per segment.</li> </ul>
Backup bridge	<p>All redundant devices are classified as backup bridges.</p> <ul style="list-style-type: none"> <li>• Backup bridges listen to network traffic and build the bridge database. However, they will not forward packets.</li> <li>• A backup bridge can take over if the root bridge or a designated bridge fails.</li> </ul>

Devices send special packets called Bridge Protocol Data Units (BPDUs) out each port. BPDUs sent and received from other bridges are used to determine the bridge roles and port states, verify that neighbor devices are still functioning, and recover from network topology changes. During the negotiation process and normal operations, each switch port is in one of the following states:

Port State	Description
Disabled	A port in the disabled state is powered on but does not participate in listening to network messages or forwarding them. A bridge must be manually placed in the disabled state.
Blocking	When a device is first powered on, its ports are in the blocking state. In addition, backup bridge ports are always in the blocking state. Ports in the blocking state receive packets and BPDUs sent to all bridges, but will not process any other packets.
Listening	The listening state is a transitional state between blocking and learning. The port remains in the listening state for a specific period of time. This time period allows network traffic to settle down after a change has occurred. For example, if a bridge goes down, all other bridges go to the listening state for a period of time. During this time the bridges redefine their roles.
Learning	A port in the learning state is receiving packets and building the bridge database (associating MAC addresses with ports). A timer is also associated with this state. The port goes to the forwarding state after the timer expires.
Forwarding	The root bridge and designated bridges are in the forwarding state when they can receive and forward packets. A port in the forwarding state can both learn and forward. All ports of the root switch are in forwarding mode.

During the configuration process, ports on each switch are configured as one of the following types:

Port type	Description
Root port	<p>The port on the designated switch with the lowest port cost back to the root bridge is identified as the <i>root port</i>.</p> <ul style="list-style-type: none"> <li>• Each designated switch has a single root port (a single path back to the route</li> </ul>

	<p>bridge).</p> <ul style="list-style-type: none"> <li>• Root ports are in the forwarding state.</li> <li>• The root bridge does not have a root port.</li> </ul>
Designated port	<p>One port on each <i>segment</i> is identified as the designated port. The designated port identifies which port on the segment is allowed to send and receive frames onto that segment. Designated ports are selected based on the lowest path cost to get back to the root switch.</p> <ul style="list-style-type: none"> <li>• All ports on the root bridge are designated ports (unless a switch port loops back to a port on the same switch).</li> <li>• Designated ports are selected based on the lowest path cost to get back to the root switch.</li> <li>• Designated ports are used to send frames back to the root bridge.</li> <li>• Designated ports are in the forwarding state.</li> </ul>
Blocking port	<p>A blocking port is any port that is not a root or a designated port. A blocking port is in the blocking state.</p>

When determining both the root port and designated ports on non-root bridge switches, the switches use the following criteria to select the port that is closest to the root bridge.

1. The port with the lowest cost to get back to the root bridge becomes the root or designated port. Default IEEE port costs include the following:
  - 10 Mbps = 1000
  - 100 Mbps = 19
  - 1 Gbps = 4
  - 10 Gbps = 2
2. If two paths have the same cost, the bridge ID of the next switches in each path is compared. The path with the switch with the lowest bridge ID becomes the path back to the root. Remember that the bridge ID is composed of two parts:
  - The priority number assigned to the switch.
  - The MAC address used by the switch.

If the priority numbers are the same on both switches, the switch with the lowest MAC address is the path back to the root.

3. If the switch has two ports that have the same cost back to the root (for example, if two connections exist to the same switch), the port on the switch with the lowest port ID becomes the designated port.
  - The port ID is derived from two numbers: the port priority and the port number.
  - The port priority ranges from 0-255, with a default of 128.
  - The port number is the number of the port. For example, the port number for Fa0/3 is 3.
  - With the default port priority setting, the lowest port number becomes the designated port.

The biggest disadvantage of STP is that it is slow to respond to topology changes. With a link failure, convergence could take up to 30 seconds. By optimizing switch settings, this delay could be reduced to about 14 seconds, but even this was too long. To improve convergence, Cisco introduced several new proprietary features which can reduce this time to about 1 second. These features include the following:

- Port Fast allows ports that do not have any switches attached to transition immediately to the forwarding state. This transition is possible because if a port does not have a switch attached, bridging loops on that port are eliminated.
- Uplink Fast enables a switch to maintain an alternate path back to the root bridge. If the root port or link goes down, the alternate port can be used to quickly re-establish communication with the root bridge.

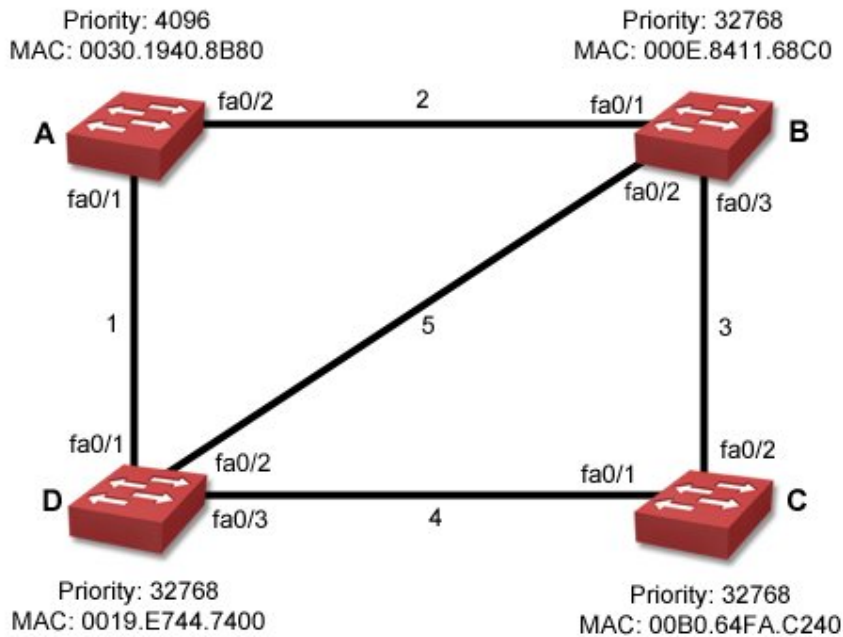
## Spanning Tree Example

By default, spanning tree is enabled on all Cisco switches. When you add switches to the network, spanning tree operates automatically to identify the root bridge and configure each port to prevent loops. In a small environment, you can probably rely on the switches to configure themselves. In a large environment, however, you will need to plan the network so that you can control which switch becomes the root bridge, and so you can identify ports that should be blocking or forwarding.

To identify how spanning tree will configure switches in a network, you will need to know the bridge ID for each bridge (which includes the priority value and the MAC address). If no priority value is included, assume the default priority of 32768. With the bridge ID and MAC addresses, use the following process to identify the state of each port:

1. Identify the root bridge. The root bridge is the switch with the lowest bridge ID.
  - The switch with the lowest priority value is the root bridge.
  - If two or more switches have the same priority value, the switch with the lowest MAC address is the root bridge.
2. On the root bridge, label each port as a designated port.
3. For every other bridge, identify its root port. The root port is the port with the lowest cost back to the root bridge.
  - To identify the cost, add the cost for each segment back to the root bridge.
  - If two paths have the same cost, then look at the bridge ID of the next switch in the path.
4. After labeling each root port, identify a designated port for each segment that does not already have a designated port.
  - The designated port will be the port that connects to the path with the lowest cost back to the root bridge.
  - If two paths have the same cost, compare the bridge ID of the next switch in the path.
5. At this point, each segment should have a designated port identified. For any ports not labeled as a root port or a designated port, indicate that the port is a blocking port.

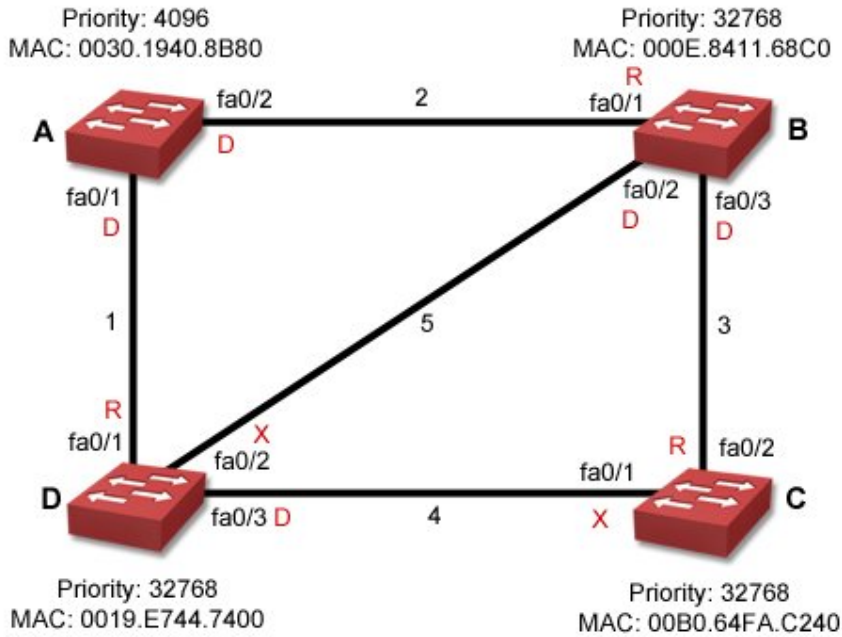
The following graphic illustrates a switched network with redundant paths. The priority values and MAC addresses for each switch are identified. Numbers on each link are used to identify the link. Each link has the same cost value.



Using the steps outlined above:

1. Switch A is the root bridge because it has the lowest priority (4096).
2. Fa0/1 and Fa0/2 on switch A are designated ports and will be forwarding.
3. Root ports on the other switches are as follows:
  - The root port on switch B is Fa0/1.
  - The root port on switch C is Fa0/2.
    - There are two paths back to the root bridge: B to A or D to A.
    - Both paths have the same cost because they involve crossing two segments with equal costs.
    - B to A is preferred because the bridge ID for switch A is lower than that of switch D. The priority values are the same, so the lowest MAC address is used (000E.8411.68C0).
  - The root port on switch D is Fa0/1.
4. At this point, designated ports already exist for segments 1 and 2. For the remaining segments:
  - For segment 3, Fa0/3 on switch B is the designated port because the cost from B to A is less than the cost from C to D to A.
  - For segment 4, Fa0/3 on switch D is the designated port for the same reason.
  - For segment 5, Fa0/2 on switch B is the designated port.
    - There are two paths from segment 5 to the root bridge: B to A or D to A.
    - Both paths have the same cost.
    - B to A is preferred because the bridge ID for switch A is lower than that of switch D. The priority values are the same, so the lowest MAC address is used (000E.8411.68C0).
5. The following remaining ports are blocking ports:
  - Fa0/1 on switch C.
  - Fa0/2 on switch D.

The following graphic shows each port labeled after spanning tree converges.



Be aware of the effect that configuration changes make in this example:

- If all switches had the same priority value, then switch B would have been the root bridge because its MAC address is the lowest. Changing the root bridge would also change several other port states.
- Changing the priority on switch D to 8192 would have the following effects:
  - The root port on switch C would change to Fa0/1. The path through switch D would be preferred over the path through switch B because of the lower priority number.
  - The designated port for segment 5 would change to Fa0/2 on switch D, while Fa0/2 on switch B would be blocking.
  - Fa0/2 on switch C would change to blocking.
- Assuming the default cost value of 19 for FastEthernet links, changing the cost of segment 1 to 100 would have the following effects:
  - The root port on switch D would be Fa0/2. The total cost of that path would be 38.
  - The designated port for segment 4 would be Fa0/1 on switch C. Port Fa0/3 on switch D would now be blocking.
  - Port Fa0/1 on switch D would be blocking because Fa0/2 would be used to reach the root bridge.

### RSTP Facts

Rapid Spanning Tree Protocol (RSTP) is based on the 802.1w standard and provides faster spanning tree convergence after a topology change. Enhancements added to RSTP to improve convergence are similar to the Port Fast and Uplink Fast features introduced by Cisco. RSTP operates much like STP with Cisco's enhancements. RSTP uses the following port states:

RSTP Port State	STP Port State*	Description
Discarding	Disabled	A port in discarding state: <ul style="list-style-type: none"> <li>• Discards frames received on the interface</li> <li>• Discards frames switched from another interface for forwarding</li> <li>• Does not learn MAC addresses</li> </ul>
	Blocking	
	Listening	

		<ul style="list-style-type: none"> <li>• Listens for BPDUs</li> </ul>
Learning	Learning	<p>A port in the learning state:</p> <ul style="list-style-type: none"> <li>• Discards frames received on the interface</li> <li>• Discards frames switched from another interface for forwarding</li> <li>• Learns MAC addresses</li> <li>• Listens for BPDUs</li> </ul>
Forwarding	Forwarding	<p>A port in the forwarding state:</p> <ul style="list-style-type: none"> <li>• Receives and forwards frames received on the interface</li> <li>• Forwards frames switched from another interface</li> <li>• Learns MAC addresses</li> <li>• Listens for BPDUs</li> </ul>

RSTP uses bridge and port roles similarly to STP:

- There is a single root bridge.
- Each segment has a single designated bridge. The port on the designated bridge is identified as the designated port. All ports on the root bridge are designated ports.
- Each designated bridge has a single port identified as the root port. The root port is the best path back to the root bridge. The root bridge is the only bridge that does not have a root port.
- Instead of having blocking ports, RSTP splits this role into two roles:
  - An *alternate port* is the switch's best alternative to its current root port. An alternate port can be used to replace the root port if the root port fails.
  - A *backup port* is the switch's alternative port connected to the same network segment as the designated port. A backup port provides an alternate path to the same segment, but not an alternate path back to the root bridge.

Both port roles are in the blocking state.

In addition to the port roles, RSTP uses the port *type* to determine whether to use advanced features that provide rapid convergence. These port types are:

Port Type	Description
Point-to-point	<p>A point-to-point link is a port that connects only to another switch.</p> <ul style="list-style-type: none"> <li>• The presence of full-duplex communication indicates a point-to-point link.</li> <li>• Because the link has only a single connected switch, it can take advantage of RSTP improvements that help it recover quickly.</li> <li>• A point-to-point link is similar to Cisco's Uplink Fast feature for STP.</li> </ul>
Shared	<p>A shared link is a link with more than a single attached device.</p> <ul style="list-style-type: none"> <li>• The presence of half-duplex communication indicates a shared link.</li> <li>• Ports connected to shared links cannot use RSTP improvements.</li> </ul>
Edge	<p>An edge port is a port that is not connected to another switch.</p>



- Because the edge port does not have a switch, the possibility of a loop is eliminated.
- Edge ports can be put into the forwarding state immediately.
- An edge port is like Cisco's Port Fast feature for STP.
- If the port receives a BPDU, it treats the port as a point-to-point or shared link.

**Note:** When any RSTP port receives legacy 802.1d BPDU, it falls back to legacy STP and the inherent fast convergence benefits of 802.1w are lost when it interacts with legacy bridges. However, this allows you to mix RSTP and STP in the same topology during a staged migration without any problems.

### Spanning Tree Mode

The Cisco 2960 switch supports these spanning-tree modes:

Mode	Description
Per-VLAN Spanning Tree Protocol (PVST+ or PVST)	<p>Per-VLAN Spanning Tree Protocol (PVST+ or PVST) is a spanning-tree mode based on the 802.1d standard and Cisco proprietary extensions. It is the default spanning-tree mode used on all Ethernet port-based VLANs. PVST+ characteristics include the following:</p> <ul style="list-style-type: none"> <li>• Layer 2 load balancing for the VLAN on which it runs</li> <li>• Each instance of PVST+ on a VLAN has a single root switch</li> <li>• A short aging time for learned MAC address entries</li> </ul> <p>PVST+ includes features such as PortFast and UplinkFast to speed convergence.</p>
Rapid PVST+	<p>Rapid PVST+ is the same as PVST+ except that it uses a rapid convergence based on the 802.1w standard. To provide rapid convergence, the rapid PVST+ deletes learned MAC address entries on a per-port basis upon receiving a topology change. Rapid PVST+ characteristics include the following:</p> <ul style="list-style-type: none"> <li>• A similar configuration as PVST+</li> <li>• Needs a minimal amount of extra configuration from PVST+</li> <li>• Each VLAN runs its own spanning-tree instance up to the maximum number supported</li> </ul>
Multiple STP (MSTP)	<p>Multiple STP (MSTP) is the spanning tree mode based on the 802.1s standard. With MSTP you can map multiple VLANs to the same spanning-tree instance. MSTP characteristics include the following:</p> <ul style="list-style-type: none"> <li>• Supports a large number of VLANs with spanning-tree instances</li> <li>• Runs on top of the Rapid Spanning Tree Protocol (RSTP)</li> <li>• MSTP cannot run without RSTP</li> </ul> <p><b>Note:</b> You cannot run both MSTP and PVST+ or both MSTP and rapid PVST+ at the same time.</p>

Be aware of the following regarding spanning tree on a Cisco switch:



- To optimize how spanning tree works when multiple VLANs exist, a switch runs multiple instances of the spanning tree protocol.
  - Each instance includes a single VLAN (each VLAN can be part of only one spanning tree instance).
  - Ports associated with a VLAN participate in the spanning tree instance assigned to the VLAN. Because a port can only be a member of one VLAN, each port is associated with only one instance of spanning tree.
  - Each instance of spanning tree elects its own root bridge. A single switch might be the root bridge for all spanning tree instances, or it might be the root bridge for only one of the instances running on the switch.
- By default, spanning tree is enabled with a single instance of the spanning tree protocol for VLAN1. By default, all switch ports are members of VLAN1, therefore all ports participate in spanning tree by default.
- When you create a new VLAN, a new instance of spanning tree runs automatically.
- You cannot disable spanning tree for a switch port. You can, however, disable it for an entire VLAN or the entire switch. In practice, there are few reasons to do this as disabling spanning tree makes bridging loops possible.

## Spanning Tree Configuration

After finishing this section, you should be able to complete the following tasks:

- Configure the spanning tree mode.
- Configure UplinkFast on access ports.

This section covers the following exam objectives:

- 208. Describe enhanced switching technologies
- 214. Configure, verify, and troubleshoot RSTP operation

### Spanning Tree Command List

By default, spanning tree is enabled on all Cisco switches. Creating an additional VLAN automatically runs another instance of the spanning tree protocol. Spanning tree configuration consists of the following tasks:

- Modifying the spanning tree mode if a mode other than PVST+ is desired.
- Changing the bridge priority to control which switch becomes the root bridge.
- Designating edge ports (ports with no attached switches).
- For PVST+, configuring UplinkFast if desired.

The following table lists commands you would use to configure spanning tree:

Command	Function
<pre>Switch(config)#spanning-tree mode pvst rapid-pvst mst</pre>	Sets the spanning tree mode.
<pre>Switch(config)#spanning-tree vlan &lt;1-4094&gt; root primary</pre>	Forces the switch to be the root of the spanning tree.
<pre>Switch(config)#spanning-tree vlan &lt;1-4094&gt; priority &lt;0-61440&gt;</pre>	Manually sets the bridge priority number. <ul style="list-style-type: none"><li>• The priority value ranges between 0 and 61,440.</li><li>• Each switch has the default priority of 32,768.</li><li>• Priority values are set in increments of 4096. If you enter another number, your value will be rounded to the closest increment of 4096, or you will be prompted to enter a valid value.</li><li>• The switch with the lowest priority number becomes the root bridge.</li></ul>
<pre>Switch(config-if)#spanning-tree portfast</pre>	Enables PortFast on the interface. When the PortFast feature is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes.  <b>Note:</b> This command is for an edge-type interface. Configuring PortFast on interfaces connected to hubs, concentrators, switches, and bridges can cause

	temporary bridging loops.
Switch(config)#spanning-tree uplinkfast	Enables UplinkFast to accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself.  <b>Note:</b> When you configure rapid spanning tree, disable UplinkFast. Similar functionality is built into rapid spanning tree.
Switch(config)#no spanning-tree vlan <1-4094>	Disables spanning tree on the selected VLAN.
Switch#show spanning-tree	Show spanning tree configuration information including the following: <ul style="list-style-type: none"> <li>• Root bridge priority and MAC address</li> <li>• The cost to the root bridge</li> <li>• Local switch bridge ID and MAC address</li> <li>• The role and status of all local interfaces</li> <li>• The priority and number for each interface</li> </ul> <p>To verify that spanning tree is working, look for an entry similar to the following for each VLAN: Spanning tree enabled protocol ieee</p>
Switch#show spanning-tree vlan <1-4094> root	Show information about the root bridge for a specific VLAN. Information shown includes: <ul style="list-style-type: none"> <li>• The root bridge ID, including the priority number and the MAC address</li> <li>• The cost to the root bridge from the local switch</li> <li>• The local port that is the root port</li> </ul>
Switch#show spanning-tree vlan <1-4094> bridge	Show spanning tree configuration information about the local switch for the specified VLAN. Information includes the local bridge ID, including the priority and MAC address.

### Examples

The following commands set the bridge priority for a VLAN and enables PortFast on two ports:

```
Switch(config)#spanning-tree vlan 20 priority 4096
Switch(config)#int fa0/12
Switch(config-if)#spanning-tree portfast
Switch(config-if)#int fa0/13
Switch(config-if)#spanning-tree portfast
```

The following commands enable Rapid PVST+ for the switch, sets the bridge priority to a higher value than the default, and disables UplinkFast:

```
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#spanning-tree vlan 1 priority 36864
Switch(config)#no spanning-tree uplinkfast
```

**Note:** When switching from PVST+ to Rapid PVST+, PortFast designations can still be used.

## EtherChannel

As you study this section, answer the following questions:

- What advantages does the EtherChannel feature provide?
- Why must EtherChannel be used to create multiple links between switches that can be used at the same time? How does EtherChannel interact with spanning tree?

This section covers the following exam objectives:

- 208. Describe enhanced switching technologies

### **EtherChannel Facts**

EtherChannel combines multiple switch ports into a single, logical link between two switches. With EtherChannel:

- You can combine 2-8 ports into a single link.
- All links in the channel group are used for communication between the switches.
- Use EtherChannel to increase the bandwidth between switches.
- Use EtherChannel to establish automatic-redundant paths between switches. If one link fails, communication will still occur over the other links in the group.
- Use EtherChannel to reduce spanning tree convergence times.

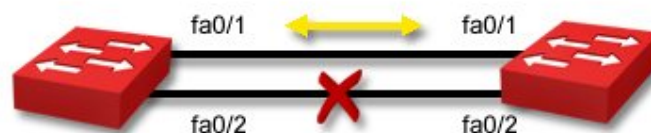
Use the **channel-group** command for a port to enable EtherChannel as follows:

```
Switch(config)#interface fast 0/12
Switch(config-if)#channel-group 1 mode on
```

Each channel group has its own number. All ports assigned to the same channel group will be viewed as a single logical link.

**Note:** If you do not use the **channel-group** command, the spanning tree algorithm will identify each link as a redundant path to the other bridge and will put one of the ports in blocking state.

Without EtherChannel, only one link is used.



With EtherChannel, both links are used.



## Inter-VLAN Routing

As you study this section, answer the following questions:

- What is required before members of two VLANs can communicate with each other?
- Why doesn't trunking enable inter-VLAN communication?
- What method is used to allow a single router to perform inter-VLAN routing using a single physical interface?
- What protocol do you configure on a router to enable inter-VLAN routing?

After finishing this section, you should be able to complete the following tasks:

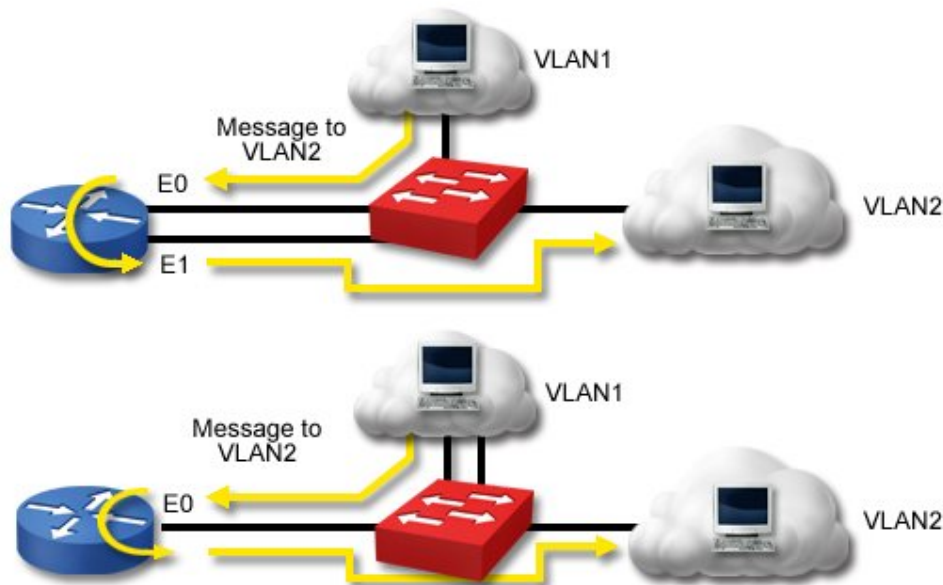
- Configure subinterfaces and ISL encapsulation to enable inter-VLAN routing on a router.

This section covers the following exam objectives:

- 208. Describe enhanced switching technologies
- 209. Describe how VLANs create logically separate networks and the need for routing between them
- 212. Configure, verify, and troubleshoot interVLAN routing

### Inter-VLAN Routing Facts

In a typical configuration with multiple VLANs and a single or multiple switches, workstations in one VLAN will not be able to communicate with workstations in other VLANs. To enable inter-VLAN communication, you will need to use a router (or a Layer 3 switch) as shown in the following graphic.



Be aware of the following conditions with inter-VLAN routing:

- The top example uses two physical interfaces on the router.
- The bottom example uses a single physical interface on the router. In this configuration, the physical interface is divided into two logical interfaces called *subinterfaces*. This configuration is also called a *router on a stick*.
- In each case, the router interfaces are connected to switch trunk ports. The router interfaces or subinterfaces must be running a trunking protocol (either ISL or 802.1Q).

- Each interface or subinterface requires an IP address.
- In this simple configuration, no routing protocol is needed because each interface on the router is directly connected.
- To support additional VLANs, add more physical interfaces or logical subinterfaces to the router.

The following commands configure a router with a single interface to perform inter-VLAN routing for VLAN 1 and VLAN 20:

```
Router(config)#interface fa0/1
Router(config-if)#no ip address
Router(config-if)#interface fa0/1.1
Router(config-if)#description subinterface for VLAN 1
Router(config-if)#encapsulation dot1Q 1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#interface fa0/1.20
Router(config-if)#description subinterface for VLAN 20
Router(config-if)#encapsulation dot1Q 20
Router(config-if)#ip address 192.168.2.1 255.255.255.0
```

## Access List Concepts

As you study this section, answer the following questions:

- You want to create an access list that restricts traffic from host 12.0.15.166. What type of access list can you use?
- You want to create an access list that restricts ICMP traffic. What type of access list would you choose?
- How many access lists can be applied to a single interface?
- What is the last statement in every access list?
- How is a wildcard mask related to the subnet mask?
- What does a 0 in a wildcard mask indicate?

After finishing this section, you should be able to complete the following tasks:

- Given a subnet address and mask, calculate the wildcard mask value to use in an access list statement.

This section covers the following exam objectives:

- 701. Describe the purpose and types of ACLs

### Access List Facts

Routers use access lists to control incoming or outgoing traffic. You should know the following characteristics of an access list.

- Access lists describe the traffic type that will be controlled.
- Access list entries describe the traffic characteristics.
- Access list entries identify either permitted or denied traffic.
- Access list entries can describe a specific traffic type, or allow or restrict all traffic.
- When created, an access list contains an implicit **deny any** entry at the end of the access list.
- Each access list applies only to a specific protocol.
- Each router interface can have up to two access lists for each protocol, one for incoming traffic and one for outgoing traffic.
- When an access list is applied to an interface, it identifies whether the list restricts incoming or outgoing traffic.
- Access lists exist globally on the router, but filter traffic only for the interfaces to which they have been applied.
- Each access list can be applied to more than one interface. However, each interface can only have one incoming and one outgoing list.
- Access lists can be used to log traffic that matches the list statements.
- Access lists applied to inbound traffic filter packets *before* the routing decision is made. Access lists applied to outbound traffic filter packets *after* the routing decision is made.

When you create an access list, it automatically contains a **deny any** statement, although this statement does not appear in the list itself. For a list to allow any traffic, it must have at least one permit statement, either permitting a specific traffic type or permitting all traffic not specifically restricted.

There are two general types of access lists: basic and extended.

Use a standard list to filter on...	Use an extended list to filter on...
Source hostname or host IP address	Source IP protocol (i.e. IP, TCP, UDP, etc.)

	Source hostname or host IP address Source or destination socket number Destination hostname or host IP address Precedence or TOS values
--	--

### Wildcard Mask Facts

The wildcard mask is used with access list statements to identify a range of IP addresses (such as all addresses on a specific network). When used to identify network addresses in access list statements, wildcard masks are the exact opposite of a subnet mask. To calculate the wildcard mask:

1. Identify the decimal value of the subnet mask.
2. Subtract each octet in the subnet mask from 255.

For example, suppose you wanted to allow all traffic on network 10.12.16.0/21. To find the wildcard mask:

1. A mask that covers 21 bits converts to 255.255.248.0
2. The wildcard mask would be:
  - o First octet:  $255 - 255 = 0$
  - o Second octet:  $255 - 255 = 0$
  - o Third octet:  $255 - 248 = 7$
  - o Fourth octet:  $255 - 0 = 255$

This gives you the mask of: 0.0.7.255

Like subnet masks, wildcard masks operate at the bit level. Any bit in the wildcard mask with a 0 value means that the bit must match to match the access list statement. A bit with a 1 value means that the bit does not have to match. For example, let's examine the subnet address, subnet mask, and wildcard mask in binary form for the preceding example.

Address Type	Decimal Values	Binary Values
Subnet address	10.12.16.0	00001010.00001100.00010000.00000000
Subnet mask	255.255.248.0	11111111.11111111.11111000.00000000
Wildcard mask	0.0.7.255	00000000.00000000.00000111.11111111

Notice how the bits in the wildcard mask are exactly opposite of the bits in the subnet mask. Suppose an access list were created with a statement as follows:

```
access-list 12 deny 10.12.16.0 0.0.7.255
```

Suppose that a packet addressed to 10.12.16.15 was received. The router uses the wildcard mask to compare the bits in the address to the bits in the subnet address.

Address Type	Decimal Values	Binary Values
Subnet address	10.12.16.0	00001010.00001100.00010000.00000000
Wildcard mask	0.0.7.255	00000000.00000000.00000111.11111111
Target address #1	10.12.16.15	00001010.00001100.00010000.00001111
How the router applies the mask to the		mmmmmmmmmm.mmmmmmmmm.mmmmmiii.iiiiiiii



address m=match i=ignored x=doesn't match	
--	--

In this example, all bits identified with a 0 in the wildcard mask must match between the address and the network address. Any bit identified with a 1 is ignored. In this example, 10.12.16.15 matches the access list statement and the traffic is denied.

Now suppose that a packet addressed to 10.13.17.15 was received. The router uses the wildcard mask to compare the bits in the address to the bits in the subnet address.

Address Type	Decimal Values	Binary Values
Subnet address	10.12.16.0	00001010.00001100.00010000.00000000
Wildcard mask	0.0.7.255	00000000.00000000.00000111.11111111
Target address #1	10.13.17.15	00001010.00001101.00010001.00001111
How the router applies the mask to the address		<ul style="list-style-type: none"> <li>• m=match</li> <li>• i=ignored</li> <li>• x=doesn't match</li> </ul> <pre> mmmmmmmmmm . mmmmmmmmmx . mmmmmmmiii . iiiiiiiiii </pre>

Notice that this address does not match the access list statement as identified with the wildcard mask. In this case, traffic would be permitted.

**Tip:** If you use a table to help you identify subnet masks, be aware that the wildcard mask value is one less than the magic number, as shown in the following table:

Bits in the mask	/25	/26	/27	/28	/29	/30	/31	/32
Magic number	128	64	32	16	8	4	2	1
Decimal mask value	128	192	224	240	248	252	254	255
Wildcard mask value	127	63	31	15	7	3	1	0

## Configuring Access Lists

After finishing this section, you should be able to complete the following tasks:

- Based on filtering requirements, construct access list statements.
- Create an access list and apply it to an interface.

This section covers the following exam objectives:

- 702. Configure and apply ACLs based on network filtering requirements
- 703. Configure and apply an ACLs to limit telnet and SSH access to the router
- 704. Verify and monitor ACLs in a network environment
- 705. Troubleshoot ACL issues

### Access List Configuration Facts

Configuring access lists involves two general steps:

1. Create the list and list entries with the **access-list** command.
2. Apply the list to a specific interface or line.
  - Use the **ip access-group** command to apply the list to an interface.
  - Use the **access-class** command to apply the list to a line.

When constructing access list statements, keep in mind the following:

- The access list statement includes the access list number. The type of list (standard or extended) is indicated by the access list number. Use the following number ranges to define the access list:
  - 1-99 = Standard IP access lists
  - 100-199 = Extended IP access lists
- A single access list can include multiple access list statements. The access list number groups all statements into the same access list.
- List statements include an action, either **permit** or **deny**.
- To identify a host address in the access list statement, use the following formats:  
**n.n.n.n**  
**n.n.n.n 0.0.0.0**  
OR **host n.n.n.n**  
Where n.n.n.n is the IP address of the host.
- To identify a network address, use the format:  
**n.n.n.n w.w.w.w**  
Where n.n.n.n is the subnet address and w.w.w.w is the wildcard mask.
- Enter access list statements in order, with the most restrictive statements at the top. Traffic is matched to access list statements in the order they appear in the list. If the traffic matches a statement high in the list, subsequent statements will not be applied to the traffic.
- Each access list has an implicit **deny any** statement at the end of the access list. Your access list must contain at least one **allow** statement, or no traffic will be allowed.
- When you remove an access list statement, the entire access list is deleted. Use Notepad or another text editor to construct and modify access lists, then paste the list into the router console.
- A single access list can be applied to multiple interfaces.
- Extended access lists include a protocol designation (such as IP, TCP, or UDP). Use IP to match any Internet Protocol (including TCP and UDP). Use other keywords to match specific protocols.
- Newer routers include an access list command prompt mode.
  - Before you can enter access list statements, you must first enter the configuration mode for access lists. For example, typing **ip access-list standard 3** creates the

standard IP address list number 3, and changes the router prompt to: **Router(config-std-nacl)#**

- In access list mode, you can use a sequence number to identify the order of access list statements.
- Removing an access list statement removes only that statement, not the entire access list.

### Examples

The following commands create a standard IP access list that permits all outgoing traffic except the traffic from network 10.0.0.0, and applies the list to the Ethernet0 interface.

```
Router(config)#access-list 1 deny 10.0.0.0 0.255.255.255
Router(config)#access-list 1 permit any
Router(config)#int e0
Router(config-if)#ip access-group 1 out
```

The following commands create a standard IP access list that rejects all traffic except traffic from host 10.12.12.16, and applies the list to the Serial0 interface.

```
Router(config)#access-list 2 permit 10.12.12.16
Router(config)#int s0
Router(config-if)#ip access-group 2 in
```

The following commands create an extended IP access list that rejects packets from host 10.1.1.1 sent to host 15.1.1.1, and applies the list to the second serial interface.

```
Router(config)#access-list 101 deny ip 10.1.1.1 0.0.0.0 15.1.1.1 0.0.0.0
Router(config)#access-list 101 permit ip any any
Router(config)#int s1
Router(config-if)#ip access-group 101 in
```

The following commands create an extended IP access list that does not forward TCP packets from any host on network 10.0.0.0 to network 11.12.0.0, and applies the list to the first serial interface.

```
Router(config)#access-list 111 deny tcp 10.0.0.0 0.255.255.255 11.12.0.0
0.0.255.255
Router(config)#access-list 111 permit ip any any
Router(config)#int s0
Router(config-if)#ip access-group 111 in
```

The following commands create a standard access list that allows VTY lines 0-4 access only from the internal network of 192.168.1.0/24:

```
Router(config)#access-list 12 permit 192.168.1.0 0.0.0.255
Router(config)#line vty 0 4
Router(config-line)#access-class 12 in
```

### Monitoring Access Lists

The following list summarizes the commands to use for viewing specific access list information on the router.

If you want to view...	Use...
All access lists that exist on the router	<a href="#">show run</a> <a href="#">show access-lists</a>
All access lists applied to an interface	<a href="#">show ip int</a> show run
Rejected traffic information	<a href="#">show log</a>

IP access lists configured on the router	show run show ip access-lists
A specific access list	show access-lists <number>

## Access List Implementation

As you study this section, answer the following questions:

- How do you identify where to place an access list (on a specific router, a specific interface, and a specific direction)?
- Why should each access list contain at least one allow statement?

After finishing this section, you should be able to complete the following tasks:

- Create an access list given customer requirements.
- Apply an existing access list to the appropriate router and interface.

This section covers the following exam objectives:

- 702. Configure and apply ACLs based on network filtering requirements
- 703. Configure and apply an ACLs to limit telnet and SSH access to the router
- 704. Verify and monitor ACLs in a network environment
- 705. Troubleshoot ACL issues

### Access List Implementation Facts

A carefully-designed access list provides a measure of security to both the router and any connected networks. You can use an access list to prevent some forms of Internet attacks, or to restrict the devices that are allowed to send packets through a router. A router that uses access lists is a form of *firewall* because it allows or denies the flow of packets between networks. You can use a Cisco router with access list statements to protect your private network from the Internet, or to protect Internet servers from specific attacks.

After you have created an access list, you must apply it to an interface. In many cases, this means you will need to decide which router, with port, and which direction to apply the access list to. Keep in mind the following:

- The access list is applied to traffic with a specific direction (either **in** or **out**).
- Each interface can only have one inbound and one outbound access list for each protocol. This means that an interface can have either a standard inbound or an extended inbound IP access list, but not both.
- You can have two access lists for the same direction applied to an interface if the lists restrict different networking protocols. For example, you can have one outbound IP access list and one outbound IPX access list.
- When constructing access lists, place the most restrictive statements at the top. Traffic is matched to access list statements in the order they appear in the list. If traffic matches a statement high in the list, subsequent statements will not be applied to the traffic.
- Each access list has an implicit **deny any** statement at the end of the access list. Your access list must contain at least one **allow** statement, or no traffic will be allowed.
- As a general rule, apply *extended* access lists as close to the *source* router as possible. This keeps the packets from being sent throughout the rest of the network.
- As a general rule, apply *standard* access lists as close to the *destination* router as possible. This is because standard access lists can only filter on source address. Placing the list too close to the source will prevent any traffic from the source from getting to any other parts of the network.
- When making placement decisions, carefully read all access lists statements and requirements. Identify blocked and allowed traffic, as well as the direction that traffic will be traveling. Place the access list on the interface where a single list will block (or allow) all necessary traffic.

## TCP/IP Ports

Network ports are logical connections, provided by the TCP or UDP protocols at the Transport layer, for use by protocols in the upper layers of the OSI model. The TCP/IP protocol stack uses port numbers to determine what protocol incoming traffic should be directed to. Some characteristics of ports are listed below:

- Ports allow a single host with a single IP address to run network services. Each port number identifies a distinct service.
- Each host can have over 65,000 ports per IP address.
- Port use is regulated by the Internet Corporation for Assigning Names and Numbers (ICANN).

ICANN specifies three categories for ports.

Categories	Characteristics
Well Known	<ul style="list-style-type: none"><li>• Assigned for specific protocols and services</li><li>• Port numbers range from 0 to 1023</li></ul>
Registered	<ul style="list-style-type: none"><li>• ICANN can assign a specific port for a newly created network service</li><li>• Port numbers range from 1024 to 49151</li></ul>
Dynamic (Private or High)	<ul style="list-style-type: none"><li>• Assigned when a network service establishes contact and released when the session ends</li><li>• Allows applications to 'listen' to the assigned port for other incoming requests (traffic for a protocol can be received through a port other than the port which the protocol is assigned, as long as the destination application or service is 'listening' for that type of traffic on that port)</li><li>• Port numbers range from 49,152 to 65,535</li></ul>

The following table lists the well known ports that correspond to common Internet services.

Protocol(s)	Port(s)	Service
TCP	20, 21	File Transfer Protocol (FTP)
TCP UDP	22	Secure Shell (SSH)
TCP UDP	23	Telnet
TCP UDP	25	Simple Mail Transfer Protocol (SMTP)
TCP UDP	53	Domain Name Server (DNS)
UDP	67, 68	Dynamic Host Configuration Protocol (DHCP)
UDP	69	Trivial File Transfer Protocol (TFTP)
TCP	80	HyperText Transfer Protocol (HTTP)
TCP	110	Post Office Protocol (POP3)
TCP	119	Network News Transport Protocol (NNTP)
UDP	123	NTP
TCP	143	Internet Message Access Protocol (IMAP4)

UDP		
TCP UDP	161, 162	Simple Network Management Protocol (SNMP)
TCP UDP	389	Lightweight Directory Access Protocol
TCP	443	HTTP with Secure Sockets Layer (SSL)

**Note:** When creating access lists, allow only the port numbers that correspond to the services running on the servers.

## Routing Protocols

As you study this section, answer the following questions:

- What is the difference between a routing protocol and a routed protocol?
- What is the difference between distance vector routing and link state routing?
- What is a flash update?
- What is poison reverse?
- Why don't link state protocols use hold down timers, split horizon, or poison reverse?
- What is in an LSP?
- What is a designated router?

This section covers the following exam objectives:

- 401. Describe basic routing concepts
- 411. Compare and contrast methods of routing and routing protocols

### **Routing Protocol Facts**

Each organization that has been assigned a network address from an ISP is considered an Autonomous System (AS). That organization is free to create one large network, or divide the network into subnets. Each autonomous system is identified by an AS number. This number can be locally administered, or registered if the AS is connected to the Internet.

Routers are used within an AS to segment (subnet) the network. In addition, they are used to connect multiple ASs together. Routers use a routing protocol to dynamically discover routes, build routing tables, and make decisions about how to send packets through the internetwork.

Routing protocols can be classified based on whether they are routing traffic within or between autonomous systems.

- Interior Gateway Protocol (IGP)--protocol that routes traffic within the AS
- Exterior Gateway Protocol (EGP)--protocol that routes traffic outside of or between ASs
- Border Gateway Protocol (BGP)--enhancement of EGP that routes traffic between ASs

In this course, you will learn about the following interior gateway protocols:

- Routing Information Protocol version 2 (RIPv2)
- Open Shortest Path First (OSPF)
- Enhanced Interior Gateway Routing Protocol (EIGRP)

### **Distance Vector Facts**

Keep in mind the following principles about the distance vector method.

- Routers send updates only to their neighbor routers
- Routers send their entire routing table
- Tables are sent at regular intervals (each router is configured to specify its own update interval)
- Routers modify their tables based on information received from their neighbors

Because routers using the distance vector method send their entire routing table at specified intervals, they are susceptible to a condition known as a routing loop (also called a count-to-infinity condition). Like a bridging loop, a routing loop occurs when two routers share different information. The following methods can be used to minimize the effects of a routing loop.



Method	Characteristics
Split horizon	Using the split horizon method (also called <i>best information</i> ), routers keep track of where the information about a route came from. Routers do not report route information to the routers on that path. In other words, routers do not report information back to the router from which their information originated.
Split horizon with poison reverse	Using the split horizon with poison reverse method (also called <i>poison reverse</i> or <i>route poisoning</i> ), routers continue to send information about routes back to the next hop router, but advertise the path as unreachable. If the next hop router notices that the route is still reachable, it ignores the information. If, however, the path timeout has been reached, the route is immediately set to unreachable (16 hops for RIP). Convergence happens faster with poison reverse than with simple split horizon. However, it results in greater network traffic because the entire table is broadcast each time an update is sent.
Triggered updates	With the triggered update method (also known as a <i>flash updates</i> ), routers that receive updated (changed) information broadcast those changes immediately rather than waiting for the next reporting interval. With this method, routers broadcast their routing tables periodically, punctuated by special broadcasts if conditions have changed. This method reduces the convergence time.
Hold-downs	With the hold-down method, routers will, for a period of time, "hold" an update that reinstates an expired link. The time period typically reflects the time required to attain convergence on the network. The hold-down timer is reset when the timer runs out or when a network change occurs.

The distance vector method has the following advantages:

- Stable and proven method (distance vector was the original routing algorithm)
- Easy to implement and administer
- Bandwidth requirements negligible for a typical LAN environment
- Requires less hardware and processing power than other routing methods

Distance vector has the following disadvantages:

- Relatively long time to reach convergence (updates sent at specified intervals)
- Routers must recalculate their routing tables before forwarding changes
- Susceptible to routing loops (count-to-infinity)
- Bandwidth requirements can be too great for WAN or complex LAN environments

### Link State Routing Facts

Keep in mind the following information about the link-state method.

- Routers broadcast Link-State Packets (LSPs) to all routers (this process is known as *flooding*).
- Routers send information about only their own links.
- Link-state protocols send hello packets to discover new neighbors.
- LSPs are sent at regular intervals and when any of the following conditions occur.
  - There is a new neighbor.
  - A neighbor has gone down.
  - The cost to a neighbor has changed.
- Neighboring routers exchange Link-state Advertisements (LSAs) to construct a topological database.
- The Shortest Path First (SPF) algorithm is applied to the topological database to create an SPF tree from which a table of routing paths and associated ports is built.

- Routers use LSPs to build their tables and calculate the best route.
- Routers use the SPF algorithm to select the shortest route.
- Network administrators have greater flexibility in setting the metrics used to calculate routes.

The link-state method has the following advantages over the distance vector method.

- Less convergence time (because updates are forwarded immediately)
- Not susceptible to routing loops
- Less susceptible to erroneous information (because only firsthand information is broadcast)
- Bandwidth requirements negligible for a typical LAN environment

Although more stable than the distance vector method, the link-state method has the following problems:

- The link-state algorithm requires greater CPU and memory capability to calculate the network topology and select the route because the algorithm re-creates the exact topology of the network for route computation.
- It generates a high amount of traffic when LSPs are initially flooded through the network or when the topology changes. However, after the initial configuration occurs, the traffic from the link-state method is smaller than that from the distance vector method.
- It is possible for LSPs to get delayed or lost, resulting in an inconsistent view of the network. This is particularly a problem for larger networks, if parts of the network come on line at different times, or if the bandwidth between links varies (i.e. LSPs travel faster through parts of the network than through others).

In particular, the last problem is of greatest concern. The following solutions are often implemented to overcome some of the effects of inconsistent LSP information.

- Slowing the LSP update rate keeps information more consistent.
- Routers can be grouped into *areas*. Routers share information within the area, and routers on area borders share information between areas. (Areas logically subdivide an Autonomous System (AS), a collection of areas under common administration.)
- One router in each area is designated as the authoritative source of routing information (called a *designated router*). Each area router receives updates from the designated router.
- LSPs can be identified with a time stamp, sequence or ID number, or aging timer to ensure proper synchronization.

## RIP

As you study this section, answer the following questions:

- What are the differences between RIP version 1 and RIP version 2?
- What is the metric used with RIP? What is the maximum metric value?
- Can RIP v2 do load balancing across multiple paths? If so, what are the limitations?
- How does RIP v2 perform auto-summarization?

After finishing this section, you should be able to complete the following tasks:

- Enable IP routing.
- Configure RIP networks.

This section covers the following exam objectives:

- 404. Configure, verify, and troubleshoot RIPv2

### **RIP Facts**

The Routing Information Protocol (RIP) is a simple, effective routing protocol for small- to medium-sized networks. Be aware of the following facts about RIP:

- RIP is a distance vector routing protocol.
- RIP uses split horizon with poison reverse to prevent routing loops.
- RIP shares its entire routing table at each update interval (except for routes that are not being advertised to prevent routing loops).
- By default, routing updates are sent every 30 seconds. The invalid timer default is 180, the holddown timer default is 180, and the flush timer default is 240.
- RIP uses the hop count as the routing metric. The *hop count* is the number of routers between the source network and the destination network.
- RIP has a maximum of 15 hops from the source to the destination network. An unreachable network (or a network that is no longer available) is indicated by a hop count of 16.
- There are two versions of RIP: RIP (version 1), and RIP version 2.
  - RIP (version 1) uses broadcasts to send routing updates. RIPv2 uses multicasts sent to the multicast address 224.0.0.9.
  - RIP (version 1) uses only classful routing, so it uses full address classes, not subnets. Autosummarization with RIP happens on default class boundaries. RIPv2 supports VLSM, sends subnet masks in the routing update, and supports manual route summarization.
- RIP can maintain up to six multiple paths to each network, but only if the cost is the same. It supports load balancing over same-cost paths. The default is support for up to four equal-cost routes.

**Note:** Because RIP uses the hop count in determining the best route to a remote network, it might end up selecting a less than optimal route. For example, suppose that two routes exist between two networks. One route uses a 56 Kbps link with a single hop, while the other route uses a Gigabit link that has two hops. Because the first route has fewer hops, RIP will select this route as the optimal route.

### **RIP Command List**

The Routing Information Protocol (RIP) is a simple, effective routing protocol for small- to medium-sized networks. By using a routing protocol, routers automatically share route information, reducing the amount of administration required for maintaining routes between networks.

To configure any routing protocol, use the following three steps:

1. Enable IP routing if it is not already enabled (use the **ip routing** command). By default, IP routing is already enabled, so this step is rarely required.
2. Switch to router configuration mode (use the **router** command, followed by the routing protocol you want to configure).
3. Identify the networks that will participate in dynamic routing (use the **network** command, followed by the address of a network to which the router is directly connected). This identifies the interfaces that will share and process received routing updates.
4. Configure any additional parameters based on the routing protocol.

The following table lists commands for configuring RIP.

Use ...	To ...
Router(config)#ip routing	Enable IP routing for the entire router. IP routing is enabled by default. Use this command only if it has been disabled. Use the <b>no ip routing</b> command to disable routing.
Router(config)#router rip	Enter router RIP configuration mode. Use the <b>no router rip</b> command to disable rip, removing all defined networks.
Router(config-router)#version 2	Enable RIP version 2 on the router.
Router(config-router)#network <address>	<p>Identify networks that will participate in the router protocol. Notice that you identify <i>networks</i>, and not <i>interfaces</i>.</p> <p>When you use the network command to identify the networks that will participate in RIP routing, follow these rules.</p> <ul style="list-style-type: none"> <li>• Identify only networks to which the router is directly connected.</li> <li>• Use the <i>classful</i> network address, not a subnetted network address. (The router will automatically convert a subnetted network address into a classful network address by removing subnetted network information.)</li> </ul> <p>Use the <b>no network</b> command to remove any network entries.</p>
Router(config)#passive-interface <interface>	Prevent routing update messages from behind sent through a router interface.
Router(config-router)#no auto-summary	Turn off automatic route summarization. With automatic route summarization, subnets are summarized based on classful boundaries when advertising routes on networks with a different class boundary. You must disable automatic summarization if you have a network address (such as 10.0.0.0) subnetted into smaller subnets and separated by a network with a different classful network address (such as 12.0.0.0).
Router#show ip route	View the routing table.
Router#show ip route <hostname or address>	View details about the specific route.

**Example**

The following commands enable IP routing and identify two networks that will participate in the RIPv2 routing protocol.

```
Router(config)#ip routing
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.0.0.0
Router(config-router)#network 192.168.10.0
```

## OSPF

As you study this section, answer the following questions:

- Must the process ID number used on different OSPF routers match?
- What is Area 0 in an OSPF implementation?
- How many areas can a single subnet be in?
- How does the DR and BDR reduce network traffic?
- When is the DR *not* used?
- How is the DR elected? How can you ensure that a specific device becomes the DR?
- What conditions must be met before two routers running OSPF will share information?

After finishing this section, you should be able to complete the following tasks:

- Configure OSPF routing.

This section covers the following exam objectives:

- 412. Configure, verify, and troubleshoot OSPF

### **OSPF Facts**

The Open Shortest Path First (OSPF) routing protocol is a robust link state routing protocol well-suited for large networks. OSPF:

- Is a public (non-proprietary) routing protocol.
- Is considered a classless routing protocol because it does not assume the default subnet masks are used. It sends the subnet mask in the routing update and supports manual route summarization and VLSM. OSPF does *not* perform automatic route summarization.
- Is *not* susceptible to routing loops. Instead, OSPF uses built-in loop avoidance techniques. Mechanisms such as holddown timers, split horizon, or poison reverse are not needed.
- Is scalable and does not have the 16 hop limitation of RIP.
- Uses multicasts to share routing information (using 224.0.0.5 and 224.0.0.6).
- Uses link costs (bandwidth) as a metric for determining best routes. The Shortest Path First (SPF) algorithm (also called the Dijkstra SPF algorithm) is used to identify and select the optimal route.
- Supports load balancing over equal-cost paths. Up to 16 equal-cost paths can be used (the default is 4).
- Uses hello packets to discover neighbor routers.
- Shares routing information through Link State Advertisements (LSAs). LSAs contain small bits of information about routes. (Unadvertised links save on IP space, but they cannot be pinged because they won't appear in an OSPF routing table.)
- Under normal conditions, OSPF only sends out updated information rather than exchanging the entire routing table.
- Converges faster than a distance vector protocol. Following convergence sends updates when routes change or every 30 minutes.
- Can require additional processing power (and therefore increased system requirements). Good design can minimize this impact.
- Maintains a logical topographical map of the network in addition to maintaining routes to various networks.
- Uses *areas* to subdivide large networks. Routers within an area share information about the area. Routers on the edge of areas (called Area Border Routers (ABR)) share summarized information between areas.
  - The *backbone* is a specialized area connected to all other areas. It contains networks not held within another area, and distributes routing information between areas. You

can think of the backbone as the "master" or "root" area. Its address is always 0.0.0.0. All OSPF networks must have a backbone area.

- A *stub* area is an area with a single path in to and out of the area.

To help minimize traffic caused by routing updates, OSPF defines the following router roles:

Role	Description
Designated Router (DR)	<p>On each subnet, a single OSPF router is elected as the designated router (DR). The DR is responsible for coordinating routing table updates for all routers on the subnet.</p> <ul style="list-style-type: none"> <li>• Routing information is sent from other routers to the DR.</li> <li>• The DR manages the changes and forwards any necessary information to other routers on the subnet.</li> </ul>
Backup Designated Router (BDR)	<p>On each subnet, a single OSPF router is identified as the backup designated router (BDR). The BDR becomes the DR if the DR becomes unavailable.</p>
DROTHER	<p>Any other router that is not a DR or a BDR is called a DROTHER. This is simply a term used to describe a non-DR or non-BDR router. It is not technically an OSPF router role.</p>

Be aware of the following facts about the DR and BDR:

- Based on the network link type, a DR/BDR might not be used. A DR/BDR is used on broadcast networks (like Ethernet) where multiple routers exist on the same subnet. For point-to-point networks, a DR/BDR is not used. By default, the network type is identified based on the media type used. You can manually configure the network type if desired.
- If the network type uses a DR/BDR, a single DR and a single BDR is identified for each subnet.
- When routers first come on line, they exchange hello packets. Part of this process is used to elect (identify) the DR and the BDR.
- The following values are used to elect the DR and BDR:
  - The router with the highest OSPF priority becomes the DR. The priority value is a number between 0-255. By default, all routers have a priority of 1.
  - If two or more routers have the same highest priority value, the router with the highest router ID becomes the DR. The router ID is a 32-bit number expressed in A.B.C.D format. The router ID for a specific router is chosen in the following order:
    1. For a specific OSPF process, you can manually configure a router ID. If a router ID has been configured, that value is used.
    2. If no router ID has been manually configured, the system uses the highest IP address assigned to a loopback address.
    3. If the router does not have a loopback address, the router ID is the highest IP address assigned to *any* interface in the up state.

**Note:** Using a loopback address is preferred over using the interface IP address because it allows you to control which router becomes the DR, and because loopback interfaces never go down. If an interface address is used for the router ID, the router ID might change if that interface goes down.

- In most cases, the BDR is the router with the next highest priority or router ID.
- Configuring a priority of 0 for a router means that the router will never become the DR or BDR.
- Once a DR has been elected, it remains the DR, even if another router with a higher priority or router ID comes on line. You must clear or reset the OSPF process to force a new election.

- If the DR goes down, the BDR automatically becomes the DR. When the original DR comes back on line, it will not automatically resume the DR role unless a reset is performed.

OSPF routers share route information only with *adjacent* neighbor routers. The following conditions must be met for two routers to become fully adjacent:

- Both routers must be on the same subnet and use the same subnet mask.
- Both routers must have the same hello and dead intervals configured.
  - The hello interval identifies how frequently neighbor routers exchange hello packets.
  - The dead interval identifies the amount of time to allow without an expected hello packet. If a periodic hello packet has not been received within the dead interval, the router assumes that its neighbor has gone offline.
- Both routers must use the same OSPF area.
- If authentication is required, both routers must pass the authentication requirements.
- The stub area flag (value) for each router must match.

### OSPF Command List

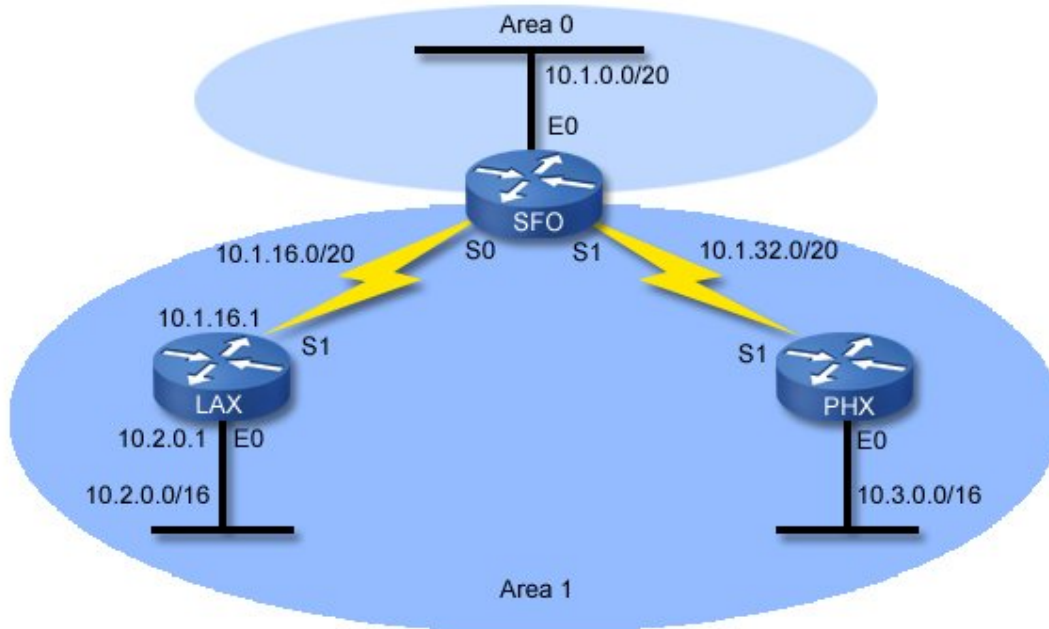
OSPF is fairly simple, with only a few variations from the RIP and IGRP configuration steps you have previously use. Configuration is as simple as defining the OSPF process using the **router ospf** command, and then identifying the networks that will participate in OSPF routing. The following table lists the commands and details for configuring OSPF.

Command	Purpose
Router(config)#router ospf <i>process-id</i>	Use to enter configuration mode for OSPF. The process ID identifies a separate routing process on the router. <b>Note:</b> Process IDs do <i>not</i> need to match between routers (in other words, two routers configured with different process IDs might still share OSPF information).
Router(config-router)#network <i>a.b.c.d w.w.w.w area number</i>	Identifies networks that participate in OSPF routing. <i>a.b.c.d</i> is the network address. This can be a subnetted, classless network. <i>w.w.w.w</i> is the wildcard mask. The wildcard mask identifies the subnet address. <i>number</i> is the area number in the OSPF topology. The area number must match between routers.
Router(config-router)#router-id <i>a.b.c.d</i>	Configures the router ID for the OSPF process. The router ID is used to identify the DR/BDR if two routers have matching priority values.
Router(config)#interface ethernet0/1 Router(config-if)#ip ospf priority <0-255>	Sets the OSPF priority number for an interface. The priority number is used in the DR/BDR election process. The router with the highest priority becomes the DR. Configure a value of 0 to ensure that a router never becomes the DR or BDR. <b>Note:</b> The priority is set on an interface, and applies to the DR/BDR election process on that interface.
Router(config)#interface loopback0 Router(config-if)#ip address <i>a.b.c.d m.m.m.m</i>	Sets an IP address for a loopback interface. The IP address is used as the router ID and is used to determine the DR and BDR if two routers have the same priority value.



### Example

The following graphic shows a sample network with two OSPF areas.



Use the following commands to configure OSPF on each router:

Router	Configuration
<b>SFO</b>	<pre>router ospf 1 network 10.1.0.0 0.0.15.255 area 0 network 10.1.16.0 0.0.15.255 area 1 network 10.1.32.0 0.0.15.255 area 1</pre>
<b>LAX</b>	<pre>router ospf 2 network 10.1.16.1 0.0.0.0 area 1 network 10.2.0.1 0.0.0.0 area 1</pre>
<b>PHX</b>	<pre>router ospf 1 network 10.1.32.0 0.0.15.255 area 1 network 10.3.0.0 0.0.255.255 area 1</pre>

Notice the following in the configuration:

- The process ID on each router does not have to match. OSPF uses areas to identify sharing of routes, not the process ID.
- You can use the subnet address with the appropriate wildcard mask (as in 10.1.16.0 0.0.15.255), or you can use the IP address of the router interface with a mask of 0.0.0.0.
- The **network** command identifies the subnet, wildcard mask, and the OSPF area of the subnet. A subnet can only be in one area.

## EIGRP

As you study this section, answer the following questions:

- What type of routing protocol is EIGRP?
- What is the metric used with EIGRP?
- How does the router calculate the feasible distance?
- What condition must be met for a route to become a feasible successor route?
- What is the difference between a feasible successor and a successor?
- How does EIGRP determine how many paths to keep in its topology database?
- What conditions must be met before two routers running OSPF will share information?

After finishing this section, you should be able to complete the following tasks:

- Configure EIGRP routing.
- Use show commands to monitor EIGRP routing.

This section covers the following exam objectives:

- 413. Configure, verify, and troubleshoot EIGRP

### **EIGRP Facts**

Enhanced IGRP is a Cisco-proprietary *balanced hybrid* routing protocol that combines the best features of distance vector and link state routing. EIGRP:

- Sends the subnet mask in the routing update. It supports route summarization and VLSM.
- Supports automatic classful route summarization at major network boundaries (this is the default in EIGRP). Unlike IGRP and RIP, manual route summarization can also be configured on arbitrary network boundaries to reduce the routing table size.
- Is not susceptible to routing loops. Instead, EIGRP uses built-in loop avoidance techniques. Under certain conditions, EIGRP will use split horizon, but not hold downs or flush timers.
- Is scalable and does not have the 16 hop limitation of RIP.
- Uses hello packets to discover neighbor routers. Hello intervals on EIGRP routers do *not* need to match.
- Exchanges the full routing table at startup, and then partial routing updates thereafter.
- Uses unicasts or multicasts to 224.0.0.10 for routing updates. Hello packets always use the multicast address.
- Uses bandwidth, delay, reliability, and load for the route metric. The metric is expressed as the number of microseconds.
  - The degree to which each value is used to calculate the metric can be customized by modifying one of five K values.
  - By default, K1 and K3 are set to 1, while K2, K4, and K5 are set to 0. These settings mean that with the default configuration, only delay and bandwidth have an effect on the metric.
  - On serial links, a default bandwidth of 1544 is used. EIGRP does not detect the actual bandwidth on the link. You must manually configure bandwidth values for accurate metric calculations.
- Uses an autonomous system (AS) number to identify routers that are to share EIGRP information. The AS number on both routers must match.
- Maintains partial network topology information in addition to routes.
- Supports load balancing on equal-cost and unequal cost links. This means that EIGRP can keep multiple paths to a single network, even if they have a different cost. With IOS 12.4 and above, EIGRP supports up to 16 paths (earlier versions supported up to 6), with the default being 4 equal-cost paths.

- Minimizes network bandwidth usage for routing updates. During normal operation EIGRP transmits only hello packets across the network. EIGRP does not send periodic routing updates like RIP and IGRP. When change occurs, only routing table changes are propagated in EIGRP not the entire table.
- Requires less processing and memory than link state protocols.
- Converges more quickly than distance vector protocols. In some cases, convergence can be almost instantaneous because an EIGRP router stores backup routes for destinations. If no appropriate route or backup exists in the routing table, EIGRP will query neighbor routers to discover an alternate route. In this manner, EIGRP can quickly adapt to alternate routes when changes occur.
- Uses the DUAL link-state algorithm for calculating routes.
- Supports multiple protocols. EIGRP can exchange routes for IP, AppleTalk and IPX/SPX networks.
- Uses a neighbors table to keep track of neighbor routers. The neighbors table includes the following for each neighbor:
  - A hold time. Each hello packet includes a hold time that identifies how long the hello information is valid. If the hold time expires without receipt of a hello packet, the neighbor is assumed to be unreachable.
  - Round-trip timers that help the router identify cost values to reach the neighbor router.
- Uses a topology database to keep track of all known networks.
  - The topology table has a list of each destination network and all neighbor routers that reported routes to that network.
  - The best routes that will be used for routing packets are copied from the topology table into the routing table.
  - The topology table holds up to 16 known routes (previously up to 6 before IOS version 12.4).

To understand how EIGRP can provide load balancing and fast recovery for failed links, you need to understand the following concepts:

Term	Definition
Advertised Distance (AD)	The <i>advertised distance</i> (AD) is the cost to the destination network as reported by the neighbor router. The AD is also called the <i>reported distance</i> (RD).
Feasible Distance (FD)	<p>The <i>feasible distance</i> (FD) is the lowest total cost to a destination network. The feasible distance is identified for each destination network, and is determined as follows:</p> <ol style="list-style-type: none"> <li>1. For each neighbor, a total cost to the network through the neighbor is calculated by adding the AD to the cost required to reach the neighbor router (the cost of the link used to reach the neighbor router).</li> <li>2. The router compares the total cost of all routes. The lowest total cost to the destination network is the feasible distance to the network.</li> </ol> <p><b>Note:</b> Sometimes the total cost for each neighbor route is referred to as a feasible distance. However, the term more correctly identifies the lowest known cost to the network, not the total cost for each reported (possible) route.</p>
Successor	<p>A <i>successor</i> is the route to a destination network with the lowest total cost.</p> <ul style="list-style-type: none"> <li>• When a new route is first learned, the total cost to the successor route is used as the feasible distance to that network.</li> <li>• The successor route is copied from the topology table into the routing table.</li> <li>• You can have multiple successor routes if multiple routes to the same network exist with the same lowest metric.</li> </ul>

Feasible Successor	<p>A <i>feasible successor</i> is an alternate route to a destination network. The total cost to the route through the feasible successor is higher than the total cost of successor routes. A route must meet the following condition to qualify as a feasible successor route:</p> <p>The advertised distance of the route through that neighbor must be less than the feasible distance used for that network (<math>AD &lt; FD</math>).</p> <p>Be aware of the following regarding feasible successors:</p> <ul style="list-style-type: none"> <li>• Satisfying the <math>AD &lt; FD</math> condition ensures that the route is loop free. In other words, the router knows for sure that the route does not include itself in the path if the AD is lower than the FD. <b>Note:</b> Successor routes must also meet this condition.</li> <li>• Feasible successor routes are kept in the topology table but are not copied to the routing table.</li> <li>• Successor routes can also be classified as feasible successor routes.</li> <li>• When all successor routes to a network are lost, the router can immediately begin to use the next best feasible successor route. This provides for rapid recovery in the event of a topology change.</li> </ul>
-----------------------	---

Be aware of the following regarding the EIGRP and routes:

- All known routes to a destination are kept in the topology table. Only successor routes are copied to the routing table.
- If the successor route goes down and there are no feasible successors, routes whose advertised distance is greater than the feasible distance for the route are *not* used because they might be routes that include loops.
- When the last feasible successor route to a network is lost, the router recalculates all routes for the lost neighbor. Instead of using other routes that are not feasible successor routes, it first communicates with neighbor routers. If necessary, the router recalculates the feasible distance for the route.
- A route whose AD is greater than the FD does not prove that a loop exists, only that a loop *might* exist. After the last feasible successor route is lost, a previously unacceptable route could be identified as a feasible successor route as long as its AD is less than the newly-calculated FD.
- By default, EIGRP uses equal-cost load balancing. To use unequal-cost load balancing, configure the *variance* value. The variance is a multiplier that identifies the degree to which alternate paths can be used.
  - The variance value ranges from 1 to 255.
  - The default variance is 1, meaning that only routes that match the best route can be used.
  - Setting the variance to 2 allows alternate routes to be used whose total costs are within a factor of 2 (double or less) of the best cost route.
  - Only feasible successor routes can be used. This means that a route whose AD is greater than the FD cannot be used as an alternate route, even if its total cost is within the variance amount.

For an EIGRP router to share information with a neighbor, the following conditions must be met:

- Both routers are on the same subnet with the same subnet mask.
- If used, authentication checks must pass.
- Both routers must be configured with the same AS number.
- Metric weight values (K values) must match on both routers.
- **EIGRP Command List**
- You configure EIGRP just the same as you would configure IGRP. The following table lists the applicable commands.

Command	Function
Router (config) #router eigrp <i>number</i>	Defines an EIGRP process. The number must match between routers for information to be shared.
Router (config- router) #network n.n.n.n Router (config- router) #network n.n.n.n w.w.w.w	Identifies a network that participates in the routing process. Networks can be specified with or without the wildcard mask. If you do not use a wildcard mask, the network address you add will be automatically truncated based on classful network boundaries. You must use a wildcard mask to identify VLSM subnets.
Router (config-router) #no auto-summary	Turn off automatic route summarization. With automatic route summarization, subnets are summarized based on classful boundaries when advertising routes on networks with a different class boundary. You must disable automatic summarization if you have a network address (such as 10.0.0.0) subnetted into smaller subnets and separated by a network with a different classful network address (such as 12.0.0.0).

- **Example**  
The following commands enable EIGRP on a router and define three networks that participate in the routing process.
- Router (config) #router eigrp 2  
Router (config-network) #network 172.16.1.0 0.0.0.255  
Router (config-network) #network 172.16.2.0 0.0.0.255  
Router (config-network) #network 172.16.3.0 0.0.0.255
- Use the following commands to manage and monitor EIGRP.

Command	Features
show ip route	View EIGRP-learned routes.
show eigrp neighbors	View neighboring routers from which EIGRP routes can be learned. Lists the IP address of the connected router.
show eigrp interfaces	View the interfaces that are running EIGRP and the number of connected routers.

## Routing Protocol Comparison

As you study this section, answer the following questions:

- Which routing protocols support route summarization and variable length subnet masks (VLSM)?
- Which routing protocols are public-standard protocols?
- Which routing protocol uses areas for configuration?
- Which routing protocol uses wildcard masks for configuration?
- If a router learns of a route to network B through both EIGRP and OSPF, which route will it prefer?

This section covers the following exam objectives:

- 411. Compare and contrast methods of routing and routing protocols
- **Routing Protocol Comparison**
- The following table compares various features of the routing protocols you will need to know for this course.

<b>Characteristic</b>	<b>RIP</b>	<b>OSPF</b>	<b>EIGRP</b>
Routing method	Distance vector	Link state	Balanced hybrid
Public standard	Yes	Yes	No
Metric	Hop count	Link cost	Bandwidth and delay
VLSM support Classless routing Sends mask in updates	Version 2 only	Yes	Yes
Route summarization	Automatic and manual, version 2 only	Manual only, and only between areas*	Automatic and manual
Convergence time	Slow	Fast	Faster than OSPF
Discovers neighbors before sending routing information	No	Yes	Yes
Sends full routing table at each update	Yes	No	No
Loop avoidance	Hold down timers, split horizon, poison reverse	Full network topology	Partial network topology
Memory and CPU requirements	Low	Can be high	Lower than OSPF
Uses areas in network design	No	Yes	No
Uses wildcards to define participating networks	No	Yes	Optional
Maintains multiple paths to the same network (load balancing support)	Yes, equal-cost only (version 2)	Yes, equal-cost only	Yes, both equal- and unequal-cost
Update address used	Version 1 uses broadcasts Version 2 uses multicasts to 224.0.0.9	Multicast to 224.0.0.5 for hello packets and updates to non-DR routers Multicast to 224.0.0.6 for sending updates to the DR	Multicast to 224.0.0.10 for hello packets Unicast for updates

- **\*Note:** Summarization with OSPF is only possible on area border routers (ABR) and autonomous system border routers (ASBR). This means that you need multiple areas before you can do route summarization with OSPF.

## Routing Administrative Distances

The administrative distance is a number assigned to a source of routing information (such as a static route or a specific routing protocol). The router uses these values to select the source of information to use when multiple routes to a destination exist. A smaller number indicates a more trusted route. The following table shows the default administrative values for a Cisco router.

Route Source	Administrative Distance
Connected interface	0
Static route	1
EIGRP summary route	5
EIGRP internal route	90
IGRP	100
OSPF	110
RIP	120
EIGRP external route	170

**Note:** You can modify how routes are selected by modifying the administrative distance associated with a source.

Routers can learn about routes to other networks using multiple routing protocols. In addition, there might be multiple paths between any two points. When making routing decisions, the router uses the following criteria for choosing between multiple routes:

1. If a router has learned of two routes to a single network through different routing protocols (such as RIP and OSPF), it will choose the route with the lowest administrative distance (OSPF in this example).
2. If a router has learned of two routes through the same protocol (for example two routes through EIGRP), the router will choose the route that has the best cost as defined by the routing metric (for EIGRP the link with the highest bandwidth and least delay will be used).

## Troubleshooting Routing

As you study this section, answer the following questions:

- The **show ip route** command on a router does not show two directly-connected networks. What conditions might be causing this problem?
- When might static routes configured on a router not show in the routing table?
- What does an asterisks ( \* ) next to a route in the routing table indicate?
- How can you tell how many paths a routing protocol can use for load balancing?
- For the **show ip protocols** command, what does the **Routing for Networks** section indicate?
- Why might subnetted routes be missing from the routing table? Which settings control this behavior?

This section covers the following exam objectives:

- 415. Troubleshoot routing issues

### Show IP Route Facts

When troubleshooting routing problems, one of the first steps might be to use **ping** or **tracert** to check communication with a host on the destination network. If **ping** or **tracert** fails, use the **show ip route** command to verify that the router has a route to the destination network. The following table lists things to check when troubleshooting missing routing information.

Problem	Description
Missing connected route	<p>A route to every directly-connected network should appear in the routing table. If a directly-connected network is missing, check the following:</p> <ul style="list-style-type: none"><li>• Verify the operational status of the interface. Make sure that the interface has not been shut down, and that you have Layer 1 and Layer 2 connectivity.</li><li>• Verify the TCP/IP configuration for the interface. The interface must be assigned an IP address before its network will show in the routing table.</li></ul>
Missing static route	<p>Static routes appear in the routing table only if the interface used to reach the next hop router is up and has been assigned an IP address. If a static route is missing:</p> <ul style="list-style-type: none"><li>• Verify that the interface used to reach the next hop router has an entry as a directly-connected network.</li><li>• Verify that the static route was configured properly (with the correct out interface or with a next hop router that is on the same subnet as an interface that is up).</li></ul>
Missing gateway of last resort	<p>A missing gateway of last resort is indicated by the line: Gateway of last resort is not set</p> <p>If the gateway value is not recognized by the route, only traffic that matches a current entry in the routing table can be forwarded. To correct the problem:</p> <ul style="list-style-type: none"><li>• Create a static route to network 0.0.0.0 using mask 0.0.0.0.</li><li>• Make sure that the static route references an interface or next hop router address that is on a reachable subnet.</li></ul>



	<p><b>Note:</b> Simply having a route labeled as a candidate for the default route (with the asterisks * ) does <i>not</i> ensure that the default route is correctly configured. The <b>gateway of last resort</b> entry must indicate the route and next hop router to be valid.</p>
<p>Missing route learned through a routing protocol</p>	<p>If a route that should be learned from a routing protocol is missing, begin by verifying that the interface used to learn the route has a directly-connected entry in the routing table. If not, then troubleshoot the directly-connected routing table entry first. If this entry exists, then the most likely problem is a misconfiguration in the routing protocol at one or more of the routers. The exact parameters to examine depend on the routing protocol.</p> <ul style="list-style-type: none"> <li>• For all routing protocols, verify that the correct <b>network</b> statements have been configured. The router uses the network statements to identify the network information to share with other routers, as well as the interfaces on which to send and receive routing information. Verify that IP addresses have been correctly configured for each interface.</li> <li>• If network information is being shared with neighbor routers, but routes are not being learned from routers accessible on that interface, check for a <b>passive-interface</b> statement. This configuration prevents routing updates from being sent or received on that interface.</li> <li>• For RIP, verify that all routers are using the correct version. A missing <b>version</b> statement indicates that the router is using version 1.</li> <li>• For OSPF, make sure that the <b>network</b> statements on each router use the same area number. The process ID for the <b>router</b> section does <i>not</i> have to match between routers.</li> <li>• For OSPF, make sure that the same hello and dead timer intervals are used. Hello intervals do <i>not</i> need to match on EIGRP routers.</li> <li>• For EIGRP, make sure that the AS number for the <b>router eigrp</b> section matches on both routers.</li> <li>• If specific routes have been replaced by summarized routes on RIP or EIGRP, remove the <b>auto-summary</b> entry to prevent automatic summarization.</li> <li>• For EIGRP and OSPF, verify that authentication settings match on all routers.</li> <li>• If multiple routing protocols are being used, be aware that the route with the lowest administrative distance will be used. This means that an EIGRP route might replace a RIP or OSPF route.</li> </ul>

### Show IP Protocols Facts

One useful command to use in verifying the routing protocol configuration is the **show ip protocols** command. This command lists all configured routing protocols, with various configuration parameters as well as limited communication capabilities of the protocol. Below is a sample output for this command for a router that runs OSPF, EIGRP, and RIP:

```

Routing Protocol is "ospf 200"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    1.1.1.0 0.0.0.255 area 0
    1.1.2.0 0.0.0.255 area 1
  Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway          Distance          Last Update

```

Distance: (default is 110)

```
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 2
  Redistributing: eigrp 1
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Maximum path: 5
  Routing for Networks:
    192.168.1.0
    192.168.2.0
    192.168.3.0
  Passive Interface(s):
    FastEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.12    90           00:55:50
    192.168.2.15    90           00:55:50
  Distance: internal 90 external 170
```

```
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 0 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 1, receive any version
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    2.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 120)
```

Entry	Description
Routing Protocol	<p>The command will show each routing process running on the router as a separate section.</p> <ul style="list-style-type: none"><li>• For OSPF, the entry includes the process ID defined with the <b>router ospf</b> command.</li><li>• For EIGRP, the entry includes the autonomous system number defined with the <b>router eigrp</b> command.</li><li>• You might have multiple OSPF or EIGRP sections if you have defined multiple process or AS numbers. All RIP information is in a single section.</li></ul>
Maximum path	<p>The <b>maximum path</b> entry identifies the maximum number of paths that can be used for load balancing.</p> <ul style="list-style-type: none"><li>• For RIP and OSPF, these are equal-cost routes.</li><li>• For EIGRP, the paths are equal-cost if the <b>EIGRP maximum metric variance</b> value is 1. They are unequal-cost routes if this value is greater than 1.</li></ul>
Routing for Networks	<p>The <b>Routing for Networks</b> section corresponds to the <b>network</b> statements in the router section of the configuration file. This section shows the same</p>

	<p>information that you can view using <b>show running-config</b>.</p> <ul style="list-style-type: none"> <li>• For RIP, these will be the classful network addresses.</li> <li>• For OSPF, the network statements include the wildcard mask and the area number.</li> <li>• For EIGRP, the networks might be classful networks or include a wildcard mask.</li> </ul>
Routing Information Sources	<p>The <b>Routing Information Sources</b> section identifies neighbor routers. Each line indicates a different neighbor router that is connected to the same subnet as one of the router's interfaces. If this section is blank, this means that the router has not been able to communicate with other routers, and will therefore not learn routes from any other router.</p>
Automatic network summarization	<p>For RIP and EIGRP, the <b>Automatic network summarization</b> line indicates the presence of the auto-summary parameter in the configuration file.</p>
Passive Interfaces	<p>The <b>Passive Interface(s)</b> section lists the interfaces that are excluded from sending and receiving routing updates. Interfaces in this section correspond to the <b>passive-interface</b> entries in the configuration file.</p>
Additional information	<p>Additional information depends on the routing protocol:</p> <ul style="list-style-type: none"> <li>• For OSPF, you can view the current router ID and the number of areas.</li> <li>• For RIP, you can view update intervals and the RIP version in use (see the <b>Default version control</b> line).</li> <li>• For EIGRP, you can view the variance setting and the K values.</li> </ul>

## Route Summarization Issues

When troubleshooting routing protocols, you might have cases where the routing table does not look as expected due to route summarization issues. Be aware of the following facts regarding automatic route summarization:

- Automatic route summarization is supported on RIP version 2 and EIGRP; it is not supported on OSPF.
- To enable automatic summarization, add the **auto-summary** parameter to the **router** section. For example, the following enabled automatic summarization for EIGRP autonomous system 300:

```
router eigrp 300
 auto-summary
```
- Use the **no auto-summary** command to disable automatic summarization. When disabled, all routes that match a **network** entry will be advertised with the configured subnet mask.
- Auto-summarization summarizes routes along classful network boundaries. For example:
  - 192.168.2.64/27 and 192.168.2.96/27 will be summarized as 192.168.2.0/24.
  - 172.16.1.0/24 and 172.16.2.0/24 will be summarized as 172.16.0.0/16.
  - 10.1.1.0/24 and 10.5.0.0/16 will be summarized as 10.0.0.0/8.
- The router will only use automatic summarization when advertising routes on interfaces that are in different classful networks from the summarized route. For example consider a router with the following interfaces:
  - Fa0/0 = 10.0.1.0/24
  - Fa0/1 = 10.0.2.0/24
  - Ser0/1/0 = 10.0.3.0/24
  - Ser0/1/1 = 192.168.12.0/24

When routes are advertised with a neighbor router connected to the Ser0/1/0 interface, the 10.0.1.0/24 and 10.0.2.0/24 routes are *not* summarized. This is because the Ser0/1/0 interface is in the same classful network as the Fa0/0 and Fa0/1 interfaces. When advertising routes to a neighbor on Ser0/1/1, all other routes *will* be summarized as 10.0.0.0/8.

- To summarize routes within classful network boundaries, or to use summarization with OSPF, you must use manual summarization.
- The **network** entries for a router section do not effect summarization; they only effect the following:
  - Which interfaces will participate in the routing protocol.
  - Which routes will be shared by the routing protocol.

Having a **network** statement that matches multiple interfaces does *not* mean that those routes will be summarized. Instead, it simply means that the single **network** statement has been used to enable the routing protocol on multiple interfaces.

- When using multiple routing protocols to share routes about the same networks, you might lose specific routes if those routes are included in summarized routes and if the source of the routing information is preferred.

## Troubleshooting RIP

After finishing this section, you should be able to complete the following tasks:

- Interpret the output of the **debug ip rip** command to troubleshoot RIP routing.
- Verify the RIP configuration of a network and correct any problems to restore full connectivity.

This section covers the following exam objectives:

- 404. Configure, verify, and troubleshoot RIPv2
- 415. Troubleshoot routing issues

### RIP Debugging

You should be familiar with the RIP routing update sequences and messages. From the output of a **debug ip rip** command, you should be able to identify the consequences of the various messages. Listed below is sample output from the **debug ip rip** command.

```
1  RIP: received v2 update from 192.168.1.1 on Ethernet0
2      10.0.0.0/8 via 0.0.0.0 in 1 hops
3      192.168.5.0/24 via 0.0.0.0 in 15 hops
4  RIP: sending v2 update to 224.0.0.9 via Serial0 (192.168.2.201)
5      network 10.0.0.0/8 via 0.0.0.0, metric 2, tag 0
6      network 192.168.1.0/24 via 0.0.0.0, metric 1, tag 0
7      network 192.168.5.0/24 via 0.0.0.0 in 16 hops (inaccessible)
8  RIP: received v2 update from 192.168.2.202 on Serial0
9      192.168.3.0/24 via 0.0.0.0 in 1 hops
10     192.168.4.0/24 via 0.0.0.0 in 2 hops
11  RIP: sending v2 update to 224.0.0.9 via Ethernet0 (192.168.1.201)
12     network 192.168.2.0/24 via 0.0.0.0, metric 1, tag 0
13     network 192.168.3.0/24 via 0.0.0.0, metric 2, tag 0
14     network 192.168.4.0/24 via 0.0.0.0, metric 3, tag 0
```

The following table interprets each line in the sample output.

Line Number(s)	Meaning
1, 8	<p>This line identifies the router and the interface where RIP updates are received. In this example, the router is connected to two other routers:</p> <ul style="list-style-type: none"><li>• Router 192.168.1.1 on Ethernet0</li><li>• Router 192.168.2.202 on Serial0</li></ul>
2-3, 9-10	<p>Indented below each RIP line are the specific routing entries that are received. This example shows the following routes received:</p> <ul style="list-style-type: none"><li>• 10.0.0.0 and 192.168.5.0 from router 192.168.1.1 on Ethernet0</li><li>• 192.168.3.0 and 192.168.4.0 from router 192.168.2.202 on Serial0</li></ul> <p>The hop count shown in the received route will be the metric used when the route is placed in the routing table of the local router.</p>
4, 11	<p>This line identifies the interface on which RIP updates are sent. In this example, the following interfaces have been enabled to share RIP information:</p> <ul style="list-style-type: none"><li>• Serial0 with an IP address of 192.168.2.201</li></ul>

	<ul style="list-style-type: none"> <li>Ethernet0 with an IP address of 192.168.1.201</li> </ul> <p>This means that the following commands have been entered on the router:</p> <pre>router rip  network 192.168.1.0  network 192.168.2.0</pre> <p>Notice that updates for version 2 are sent to the multicast address of 224.0.0.9.</p>
5-7, 12-14	<p>Indented below the RIP line are the entries that are shared with other routers. Be aware of the following items:</p> <ul style="list-style-type: none"> <li>Before sending the information, the router increments the hop count. To identify the hop count in the local routing table, subtract 1 from the sent hop count.</li> <li>Line 7 (network 192.168.5.0) is advertised as inaccessible (16 hops). This is because the local router has a hop count of 15 for that network. 16 hops is the maximum hop count for RIP.</li> </ul>

For comparison, here's how the routing table of the local router would appear:

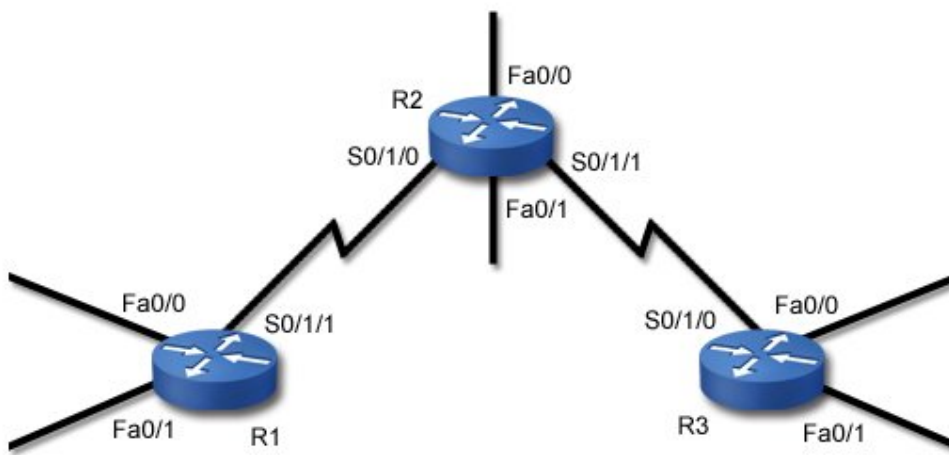
```
R 10.0.0.0/8 [120/1] via 192.168.1.1, 00:00:05, Ethernet0
C 192.168.1.0/24 is directly connected, Ethernet0
C 192.168.2.0/24 is directly connected, Serial0
R 192.168.3.0/24 [120/1] via 192.168.2.202, 00:00:04, Serial0
R 192.168.4.0/24 [120/2] via 192.168.2.202, 00:00:04, Serial0
R 192.168.5.0/24 [120/15] via 192.168.1.1, 00:00:05, Ethernet0
```

Common problems indicated by RIP debugging include:

- Inaccessible routes
- Mismatched RIP versions (one router using version 1, with another router using version 2)
- Routes not being advertised as expected (caused by missing **network** statements)

### RIP Troubleshooting Introduction

The next set of labs give you a chance to troubleshoot RIP routing. All labs use the same network layout as shown.



- Subnets are assigned addresses as follows:

Router	Interface	Subnet
R1	Fa0/0	192.168.1.0/25
	Fa0/1	192.168.1.128/25
	S0/1/1	172.17.0.0/30
R2	S0/1/0	172.17.0.0/30
	Fa0/0	192.168.2.0/26
	Fa0/1	192.168.2.128/26
	S0/1/1	172.18.0.64/30
R3	S0/1/0	172.18.0.64/30
	Fa0/0	192.168.3.0/27
	Fa0/1	192.168.3.128/27

- For DCE devices, the clock rate is set to 56000.
- All routers use RIP v2 to share information about all connected networks. No static routes are allowed.

For each scenario, one or more routers have been misconfigured. Your job is to diagnose and fix the problem.

In each case, begin by verifying the problem. From router R1, ping the R3 Fa0/0 interface. The following commands may be useful in identifying the problem.

- ping or traceroute
- show ip route
- show ip protocols
- sh int/sh ip int
- show controllers
- sh run (**Note:** While you could probably catch most problems by just examining the running-config, you should be able to troubleshoot the problem without using this command at all.)

For example, one way to use the **sh ip route** command in troubleshooting is to view the routing table for each router, identifying which networks are missing from the routing table. Based on the missing networks, you can then examine the configuration of specific routers to identify the problem.

## Troubleshooting OSPF

After finishing this section, you should be able to complete the following tasks:

- Use **show** commands to verify the OSPF operation.
- Verify the OSPF configuration of a network and correct any problems to restore full connectivity.

This section covers the following exam objectives:

- 412. Configure, verify, and troubleshoot OSPF
- 415. Troubleshoot routing issues

### OSPF Troubleshooting Facts

When troubleshooting OSPF configuration, remember that OSPF routers share route information only with *adjacent* neighbor routers. The following conditions must be met for two routers to become fully adjacent:

- Both routers must be on the same subnet and use the same subnet mask.
- Both routers must have the same hello and dead intervals configured.
- Both routers must use the same OSPF area.
- If authentication is required, both routers must pass the authentication requirements.
- Both routes must be using the same area type (stub area flag).

**Note:** The process ID used when configuring OSPF does not need to match between routers.

The following table lists some commands that are useful in monitoring and troubleshooting OSPF.

Command	Function
<code>show ip protocols</code>	Use <b>show ip protocols</b> to view OSPF configuration information such as: <ul style="list-style-type: none"><li>• The OSPF process ID</li><li>• The OSPF router ID for the current router</li><li>• Configured networks and areas for the process</li><li>• IP addresses of neighbor routers</li></ul>
<code>show ip ospf</code>	Use <b>show ip ospf</b> to view OSPF information including: <ul style="list-style-type: none"><li>• The process ID</li><li>• The local router ID and its role (such as DR or BDR)</li><li>• Configured areas</li></ul>
<code>show ip ospf neighbor</code>	Use <b>show ip ospf neighbor</b> to view information about neighbor OSPF routers including: <ul style="list-style-type: none"><li>• Router ID of the neighbor router</li><li>• Neighbor state or status (the Full state indicates that the DR/BDR election has occurred and they are exchanging routing information)</li><li>• The role of the neighbor (DR, BDR, DROTHER)</li><li>• Time remaining before the neighbor is declared missing if a hello packet is not received</li><li>• The IP address of the neighbor</li></ul>



	<ul style="list-style-type: none"> <li>• The local interface used to reach the neighbor</li> </ul>
<pre>show ip ospf interface</pre>	<p>Use <b>show ip ospf interface</b> to view interfaces that are running OSPF including the following information:</p> <ul style="list-style-type: none"> <li>• Interface status and IP address assigned to the interface</li> <li>• Area number</li> <li>• Process ID</li> <li>• Router ID</li> <li>• The router ID and IP address of the DR and BDR on the network</li> <li>• Hello and dead timer settings</li> <li>• Adjacent routers</li> </ul>
<pre>debug ip ospf events</pre>	<p>Use <b>debug ip ospf events</b> to view debugging information about hello exchanges, DR selection information, SPF calculation, and errors related to negotiating adjacency.</p> <ul style="list-style-type: none"> <li>• Use <b>debug ip ospf hello</b> to view only hello packet information.</li> <li>• Use <b>debug ip ospf adj</b> to view adjacency information.</li> </ul>

Most error messages shown in the debug output adequately describe the nature of the problem. Shown below are some errors that display with the **debug ip ospf events** command:

Error	Meaning
<pre>OSPF: mismatched hello parameters from 10.0.0.1 OSPF: Dead R 20 C 40, Hello R 5 C 5 Mask R 255.255.255.0 C 255.255.255.0</pre>	<p>Hello timer, dead timer, or subnet mask mismatch detected. In this example, the dead timer intervals do not match: R (received) = 20, C (configured) = 40</p>
<pre>OSPF: hello packet with mismatched E bit</pre>	<p>Area types (not area numbers) configured on each router do not match. The E bit is also called the stub area flag.</p>
<pre>Neighbor Down: Dead timer expired</pre>	<p>An expected hello timer has not been received. When the dead timer reaches 0, it is assumed that the neighbor router has gone down. The dead timer resets itself each time a hello packet is received.</p>

## Troubleshooting EIGRP

After finishing this section, you should be able to complete the following tasks:

- Use **show** commands to verify the EIGRP operation.
- Interpret the output of the **show ip eigrp topology all-links** command.
- Verify the EIGRP configuration of a network and correct any problems to restore full connectivity.

This section covers the following exam objectives:

- 413. Configure, verify, and troubleshoot EIGRP
- 415. Troubleshoot routing issues

### **EIGRP Troubleshooting Facts**

When troubleshooting EIGRP, keep in mind that the following conditions must be met for an EIGRP router to share information with a neighbor:

- Both routers must be on the same subnet with the same subnet mask.
- If used, authentication checks must pass.
- Both routers must be configured with the same AS number.
- Metric weight values (K values) must match on both routers.

**Note:** Hello intervals do *not* need to match for EIGRP.

The following table lists some commands you can use to verify EIGRP.

Command	Function
<code>show ip protocols</code>	Use <b>show ip protocols</b> to view: <ul style="list-style-type: none"><li>• EIGRP autonomous system number</li><li>• Configured networks</li><li>• K values and variance</li><li>• Neighbor router IP addresses</li></ul> <b>Note:</b> In the labs, this is the only listed troubleshooting command that has been enabled.
<code>show ip eigrp interfaces</code>	Use <b>show ip eigrp interfaces</b> to view interfaces that are sending and receiving EIGRP updates. Passive interfaces will <i>not</i> be shown.
<code>show ip eigrp neighbors</code>	Use <b>show ip eigrp neighbors</b> to view the following information for neighbor routers: <ul style="list-style-type: none"><li>• IP address</li><li>• Local interface to reach the neighbor router</li></ul>
<code>show ip eigrp topology</code>	Use <b>show ip eigrp topology</b> to view the contents of the topology table for EIGRP. Information for each known network includes: <ul style="list-style-type: none"><li>• The number of successor routes to that network.</li><li>• The feasible distance (FD) for the network.</li><li>• Feasible successors to that network.</li></ul> <b>Show ip eigrp topology</b> only shows feasible success routes (routes whose

AD is less than the network FD). To view all routes, including those that did not qualify as feasible successor routes, use **show ip eigrp topology all-links**.

The following example shows some sample output from the **show ip eigrp topology all-links** command.

```
Router# show ip eigrp topology all-links
IP-EIGRP Topology Table for process 77
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status
P 172.16.90.0 255.255.255.0, 2 successors, FD is 46251776
   via 172.16.80.28 (46251776/46226176), Ethernet0
   via 172.16.81.28 (46251776/46226176), Ethernet1
   via 172.16.80.31 (46277376/46251000), Serial0
P 172.16.81.0 255.255.255.0, 1 successors, FD is 307200
   via 172.16.82.28 (307200/281600), Ethernet1
   via 172.16.80.28 (308500/281600), Ethernet0
   via 172.16.80.31 (332800/307900), Serial0
```

Important items in the command output are explained in the following table:

Information	Description
Destination network	<p>Each destination network is indicated by a subsection in the command output. For example, the route 172.16.90.0 has the following information:</p> <ul style="list-style-type: none"> <li>• <b>P</b> = The computational status of the route. A status of P means that the route has been calculated and the router is not waiting for information or calculating information for the route. A passive state indicates a converged route.</li> <li>• Network address and mask</li> <li>• <b>2 successors</b> = the number of successor routes to that network. Successor routes are the best feasible successor routes. Successor routes meet the following conditions: <ul style="list-style-type: none"> <li>○ Their advertised distance (AD) is less than the feasible distance for the network.</li> <li>○ Their total cost is the lowest of the total cost for all feasible successor routes.</li> </ul> </li> <li>• <b>FD is 46251776</b> = The feasible distance (FD) to the network. The FD for the network is the lowest total cost of all routes to the destination network at the time that routes were calculated.</li> </ul>
Known routes	<p>Known routes to the destination are identified by the <b>via</b> entries. For example, the first route for network 172.16.90.0 shows the following information:</p> <ul style="list-style-type: none"> <li>• <b>172.16.80.28</b> = The next hop router address.</li> <li>• <b>46251776</b> = The total cost to the destination network. The total cost is calculated by the router by taking the advertised cost and adding the actual bandwidth and delay to reach the next hop router. Be aware that the total cost value is sometimes called the feasible distance of the route; however, this is not the same thing as the feasible distance of the network. <b>Note:</b> The total cost of the first route typically matches the FD for the destination network. However, the values will not necessarily match.</li> <li>• <b>46226176</b> = The advertised distance (AD) to the destination (also called the reported distance (RD)). This is the distance as reported by the next hop router.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Ethernet0</b> = The local router interface used to reach the next hop router.</li> </ul>
Successor routes	Successor routes are identified by taking the number of successors and counting down the list of known routes. In this example for network 172.16.90.0, there are 2 successors, meaning that 172.16.80.28 and 172.16.81.28 are both successor routes.
Feasible successor routes	<p>Feasible successor routes are additional routes that match the following requirement:  The AD for the route must be lower than the FD for the network.  <b>Note:</b> Any route that matches this condition is called a feasible route. This includes those routes that are the successor routes (a successor route is a feasible route, but not every feasible route is a successor route).</p> <p>This requirement ensures that the route is loop free. For network 172.16.90.0, all three routes listed are feasible routes because their AD cost is less than <b>46251776</b>. For network 172.16.81.0, the last route is not a feasible successor route because its AD (<b>307900</b>) is greater than the FD for the route (<b>307200</b>). <b>Note:</b> This last route would not have shown if the <b>show ip eigrp topology</b> command was used without the <b>all-links</b> parameter.</p>

## Frame Relay Concepts

As you study this section, answer the following questions:

- What is the CIR?
- What does *locally significant* mean in relation to the DLCI number?
- What functions are performed by LMI?
- What is the difference between a point-to-point and a multipoint link?
- When are the FECN and BECN bits set? What do each mean?
- How does inverse ARP simplify Frame Relay configuration?
- What is a *subinterface*?

This section covers the following exam objectives:

- 801. Describe different methods for connecting to a WAN
- 803. Configure and verify Frame Relay on Cisco routers

### **Frame Relay Facts**

Frame relay is a standard for packet switching WAN communications over high-quality, digital lines. Frame-relay networks:

- Provide error detection but not error recovery. It is up to end devices to request a retransmission of lost packets.
- Can provide data transfer up to 1.54 Mbps.
- Have a variable packet size (called a *frame*).
- Can be used as a backbone connection to LANs.
- Can be implemented over a variety of connection lines (56K, T-1, T-3).
- Operate at the Physical and Data Link layers of the OSI model.

When you sign up for Frame Relay service, you are assigned a level of service called a Committed Information Rate (CIR). The CIR is the maximum *guaranteed* data transmission rate you will receive on the Frame Relay network. When network traffic is low, you will likely be able to send data faster than the CIR. As network traffic increases, priority is given to data coming from customers with a higher CIR, and the effective rate may drop. In any case, you are guaranteed to have at least the amount of bandwidth specified by the CIR.

You should be familiar with the following concepts about how Frame Relay networks send data.

- Routers connect to a Frame Relay switch either directly or through a CSU/DSU.
- Frame relay networks simulate an "always on" connection with PVCs.
- Sending routers send data immediately without establishing a session.
- Frame Relay switches perform error checking but not correction.
- Corrupted packets are simply dropped without notification.
- Packets travel through the Frame Relay cloud without acknowledgments.
- Error correction is performed by sending and receiving devices.
- Frame Relay switches begin dropping packets when congestion occurs.
- Congestion is the most common cause of packet loss on a Frame Relay network.
- Packets are discarded based on information in the Discard Eligibility (DE) bit.
- Frame Relay switches set a bit in each packet to indicate that the path is experiencing congestion:
  - The Backward Explicit Congestion Notification (BECN) bit is set in packets sent back to the sending device. This lets the sending device know that the path it is using to send on has experienced congestion.

- The Forward Explicit Congestion Notification (FECN) bit is set as packets are forwarded to the destination. This lets the receiving device know that the packet has experienced congestion along the path.

The action devices take in response to these messages depends on the upper-layer protocol configuration. However, a common response to a BECN message is to slow the rate of data transmissions. A common response to a FECN message might be to slow the rate of data requests.

### Frame Relay Addressing Facts

Most Frame Relay installations involve connecting to a Frame Relay network through a T-1 line. The router connects to a CSU/DSU, which is connected to the Frame Relay network. The Frame Relay network is made up of multiple switches for moving packets. You should be aware of the following Frame Relay concepts:

Concept	Description
Data-Link Connection Identifier (DLCI)	<p>Like an Ethernet MAC address, a DLCI identifies each virtual circuit.</p> <ul style="list-style-type: none"> <li>• The DLCI ranges between 16 and 1007.</li> <li>• The DLCI represents the connection between two frame relay devices.</li> <li>• The Frame Relay service provider assigns the DLCI when the virtual circuit is set up.</li> <li>• Each DLCI is unique for the local network, but not for the entire WAN. In other words, the same DLCI number can be used multiple times in the entire network to identify different devices.</li> </ul>
Local Management Interface (LMI)	<p>Local Management Interface (LMI) is a set of management protocol extensions that automates many Frame Relay management tasks. LMI is responsible for managing the connection and reporting connection status. LMI can:</p> <ul style="list-style-type: none"> <li>• Maintain the link between the router and the switch.</li> <li>• Gather status information about other routers and connections on the network.</li> <li>• Enable dynamic DLCI assignment through multicasting support.</li> <li>• Make DLCIs globally significant for the entire network. Although DLCI numbers are only locally significant, through LMI these numbers can be globally significant (i.e. the same number is used throughout the entire network to identify a specific link).</li> </ul> <p>Cisco routers support three LMI types: Cisco, ANSI, and Q933a.</p>

### Frame Relay Configuration Facts

When configuring a router for Frame Relay, the DLCI number acts like a Data Link or physical device address. Because Frame Relay supports multiple upper-layer protocols (such as IP, IPX, and DECnet), you will need to associate logical, Network layer destination addresses with the DLCI number used to reach that address. For multipoint connections, you have the following configuration options.

Configuration Method	Description
Inverse ARP	The router uses the inverse ARP protocol to dynamically discover destination

	addresses associated with a specific DLCI. To use inverse ARP, simply enable Frame Relay encapsulation on the interface. Using inverse ARP is the default.
Manual mappings	The administrator identifies the address of each destination device, and associates each address with a DLCI. Although more work, results are less prone to errors than when using inverse ARP.
Subinterfaces	<p>A <i>subinterface</i> is a virtual interface that you configure on a Cisco router's physical interface. Instead of adding physical interfaces, using subinterfaces lets you subdivide a single physical interface into several separate virtual channels. Subinterfaces make it possible to support multiple connections and/or networks through a single physical port.</p> <p>When you connect a router to the Frame Relay network, the router interface has a direct line to the Frame Relay switch at the service provider. Although there is only one physical path between the router and the switch, Frame Relay supports multiple virtual circuits. When configuring a Frame Relay connection or circuit, you have the following options:</p> <ul style="list-style-type: none"> <li>• Point-to-Point. A point-to-point link simulates a direct connection with a destination device. With a point-to-point connection, the circuit is configured to talk to only one other device.</li> <li>• Multipoint. A multipoint link configures each circuit to communicate with more than one destination device. The same circuit is used for multiple conversations.</li> </ul> <p>To configure a subinterface for Frame Relay, you set the encapsulation type, then assign a DLCI number to the subinterface or use manual mappings to identify IP address and DLCI pairs.</p>

To configure Frame Relay on an interface, complete the following tasks:

- Enable Frame Relay on the interface by setting the encapsulation type.
- Assign a Network layer address to the interface (such as an IP address).
- Configure dynamic (inverse ARP) or static (mapped) addresses.
- For a point-to-point subinterface, or a multipoint subinterface with dynamic addressing, assign a DLCI to the subinterface.
- Configure the LMI settings (optional). By default, Cisco routers autosense the LMI type and configure themselves accordingly. You only need to set the LMI type if autosensing does not work or if you want to manually assign it.

**Note:** You must set the encapsulation method on the interface before you can issue any other Frame Relay commands.

## Enabling Frame Relay

After finishing this section, you should be able to complete the following tasks:

- Set frame relay encapsulation on a serial interface.
- Configure frame relay to use inverse arp for address discovery.

This section covers the following exam objectives:

- 803. Configure and verify Frame Relay on Cisco routers

### Frame Relay Command List

The simplest method of configuring Frame Relay is to set the encapsulation type and let the router discover the LMI type and the DLCI values automatically. The following table lists various commands you can use for a simple Frame Relay configuration.

Use ...	To ...
<pre>Router(config- if)#encapsulation frame-relay</pre>	<p>Set the encapsulation method Continue this command by adding various keywords to set a specific frame relay encapsulation protocol.</p> <ul style="list-style-type: none"><li>• Use the <b>cisco</b> encapsulation type to use the proprietary encapsulation method. Setting encapsulation without an encapsulation keyword uses this method.</li><li>• Use the <b>ietf</b> type when connecting to a Frame Relay network. This is the industry-standard encapsulation method.</li></ul>
<pre>Router(config- if)#frame-relay inverse-arp</pre>	<p>Turn on inverse ARP (it is on by default).</p>
<pre>Router(config- if)#frame lmi-type &lt;LMI type&gt;</pre>	<p>Configure the LMI type used. By default, the LMI type is automatically detected.</p> <p><b>Note:</b> When you manually set the LMI type, you disable automatic LMI discovery. You might also need to manually configure the <b>keepalive</b> parameter for the interface so the router uses a keepalive value equal to or less than what is used by the Frame Relay provider's equipment.</p>
<pre>Router#show frame map</pre>	<p>Display the contents of the frame-relay map cache (showing IP address to DLCI number mappings).</p>
<pre>Router#clear frame- relay-inarp</pre>	<p>Clear the dynamic entries from the frame-relay map cache.</p>
<pre>Router#show frame pvc</pre>	<p>Show DLCI statistics and information.</p>

**Note:** The **show** commands listed here are not enabled in the labs.

### Example

The following commands enable Frame Relay on serial interface 1 using IETF as the encapsulation method and dynamic addressing.

```
Router(config)#int s1  
Router(config-if)#encap frame-relay ietf
```



## Address Mapping

After finishing this section, you should be able to complete the following tasks:

- Disable inverse arp.
- Configure static Frame Relay mappings.

This section covers the following exam objectives:

- 803. Configure and verify Frame Relay on Cisco routers

### **Frame Relay Map Command List**

Use the **frame-relay map** command to create the static mapping, associating IP addresses with DLCI numbers.

- Add the **broadcast** parameter to the command to configure the router to forward broadcast traffic over the link.
- You can also specify the Frame Relay encapsulation to use for the virtual circuit by adding the **cisco** or the **ietf** keywords. If not used, the circuit uses the encapsulation method specified for the interface. If used, you can use one type of encapsulation for one DLCI, and another type for another DLCI.

The following commands enable Frame Relay on serial interface 0 using Cisco as the encapsulation method, disable inverse ARP, and map IP address 10.1.1.55 to DLCI 25.

```
Router(config)#int s0
Router(config-if)#encap frame-relay
Router(config-if)#no frame inverse
Router(config-if)#frame-relay map ip 10.1.1.55 25
```

## Subinterfaces

After finishing this section, you should be able to complete the following tasks:

- Configure a multipoint subinterface.
- Configure a point-to-point subinterface.

This section covers the following exam objectives:

- 803. Configure and verify Frame Relay on Cisco routers

### **Frame Relay Subinterface Command List**

Using subinterfaces also lets you send routing updates out the same physical interface on which they were received. Using subinterfaces in this manner overcomes the split horizon problem that can occur when sending updates out the same interface. To configure Frame Relay on a subinterface, complete the following tasks:

- Enable Frame Relay on the interface and set the encapsulation method.
- Create the subinterface, specifying either point-to-point or multipoint.
- For a point-to-point connection or a multipoint connection using inverse ARP, assign the DLCI number to the subinterface.
- For a multipoint connection using static assignments, map DLCIs to protocol addresses.

In addition, you will need to assign a Network layer address to the subinterface. Do *not* assign an IP address to the main interface.

Use ...	To ...
Router(config-if)#int sX.X <type>	Create the subinterface
Router(config-subif)#frame-relay interface-dlci	Assign the DLCI to the interface
Router(config-subif)#frame-relay map	Map protocol addresses to DLCIs

### **Examples**

The following commands create a point-to-point subinterface on the first serial interface and assign it to DLCI 44. The subinterface is configured to use inverse ARP.

```
Router(config)#int s0
Router(config-if)#encap frame
Router(config-if)#int s0.55 point
Router(config-subif)#frame interface-dlci 44
```

The following commands create a multipoint subinterface on the second serial interface, and configure it with a static IP mapping of device 199.12.16.155 to DLCI 111.

```
Router(config)#int s1
Router(config-if)#encap frame
Router(config-if)#int s1.103 mult
Router(config-subif)#frame map ip 199.12.16.155 111
```

## Troubleshooting Frame Relay

As you study this section, answer the following questions:

- Which command would you use to view the DLCI numbers for each interface?
- Why wouldn't you use the DLCI number included in the show interfaces command to identify assigned DLCIs?
- Which commands can you use to view the LMI type used on your router?
- Which Frame Relay encapsulation type should you use when connecting to routers from different vendors?

After finishing this section, you should be able to complete the following tasks:

- Use show commands to monitor Frame Relay on a router.
- Troubleshoot a Frame Relay configuration.

This section covers the following exam objectives:

- 803. Configure and verify Frame Relay on Cisco routers

### Frame Relay Monitoring and Troubleshooting

The following list summarizes the commands to use for viewing specific Frame Relay information on the router.

If you want to view . . .	Use . . .
DLCI numbers	show run <a href="#">show frame pvc</a>
Frame Relay encapsulation method	<a href="#">show int</a> show run
LMI information and traffic statistics	<a href="#">show frame lmi</a> show int
Interface configuration (DCE or DTE)	show frame pvc show int
Global traffic statistics	<a href="#">show frame traffic</a>
Addresses and associated DLCIs	<a href="#">show frame map</a>

**Note:** Output for the show interfaces command shows an entry for DLCI followed by a number. This information is *not* the DLCI number associated with the interface.

As you troubleshoot Frame Relay, keep in mind the following tips:

- All routers at all locations must be configured to use the same frame relay encapsulation method.
- When using all Cisco routers, you can use the default Frame Relay encapsulation type (**cisco**). When using routers of multiple vendors, use the **ietf** encapsulation type.
- Frame Relay routers must know the DLCI number that is used to reach remote routers.
  - Use inverse arp to dynamically discover DLCI numbers.
  - Use static mappings to associate DLCI numbers with IP addresses manually.
- When configuring subinterfaces, do not set an IP address on the main interface. Instead, set IP addresses on each subinterface.
- For a point-to-point subinterface, or a multipoint subinterface with dynamic addressing, you must manually assign a DLCI to the subinterface.

- By default, Cisco routers autosense the LMI type and configure themselves accordingly. You only need to set the LMI type if autosensing does not work or if you want to manually assign it.

Shown here is sample output from the **show frame-relay pvc** command.

```
PVC Statistics for interface Serial5/1 (Frame Relay DTE)

DLCI = 55, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial5/1.1
  input pkts 64589   output pkts 3865   in bytes 15400
  out bytes 33896   dropped pkts 66   in FECN pkts 12
  in BECN pkts 15   out FECN pkts 0   out BECN pkts 0
  in DE pkts 5     out DE pkts 1
  out bcast pkts 15 out bcast bytes 128
pvc create time 00:35:11, last time pvc status changed 00:00:22
```

The following table describes major components of the output.

Entry	Description
DLCI = 55	Lists the DLCI number assigned to the PVC.
DLCI USAGE	Identifies the role of the router on the virtual circuit. For DTE frame relay devices, the usage will be <b>LOCAL</b> . For DCE devices, the usage will be <b>SWITCHED</b> .
PVC STATUS	<p>Reports the PVC status as reported from the DCE through the LMI protocol. When you connect the DTE to the circuit, the LMI protocol communicates the PVC status as sent from the DCE device. The status will be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>ACTIVE</b> indicates the PVC is configured, is operational, and can transmit packets. LMI is active.</li> <li>• <b>INACTIVE</b> indicates that the PVC has been configured, but has not received an active state from the DCE. This status identifies the PVC as down. The interface line status is also down.</li> <li>• <b>STATIC</b> indicates that LMI has been disabled. A configuration exists, but status information cannot be received from the DCE because LMI has been disabled.</li> <li>• <b>DELETED</b> indicates that the PVC has been configured, but that the LMI protocol has not reported status information.</li> </ul>
FECN/BECN pkts	<p>Identifies the number of packets received (<b>in</b>) or sent (<b>out</b>) that had the FECN or BECN bit set. Both flags identify that network congestion exists. Receiving devices use these flags to decide what to do about the congestion, such as slowing down or implementing a flow control mechanism. On a DTE device:</p> <ul style="list-style-type: none"> <li>• <b>in FECN pkts</b> are packets sent from the DCE to the destination DTE device to indicate that congestion has occurred. A DTE that receives a FECN packet might slow its rate of data request, or it might implement flow control to detect and recover from lost packets.</li> <li>• <b>in BECN pkts</b> are packets sent from the DCE to the sending DTE device to indicate that congestion has occurred. A DTE that receives a BECN packet might slow down its transmission rate.</li> <li>• <b>out FECN pkts</b> and <b>out BECN pkts</b> are packets sent from the DTE. On a DTE device, these values have little meaning as the DTE is typically the terminating point in the circuit.</li> </ul>
DE pkts	Identifies the number of packets sent or received that had the Discard Eligibility (DE) bit set. The DE bit is used to identify packets with a lower priority that could be dropped if necessary.

## IPv6 Concepts

As you study this section, answer the following questions:

- How does IPv6 help route summarization on the Internet?
- How many hexadecimal numbers are in an IPv6 address?
- Which of the following can be left out of an IPv6 address: leading zeros or trailing zeros?
- How many bits do most organizations have for creating subnets with IPv6 addresses?
- How do you transform a MAC address into an IPv6 interface ID?
- What does IPv6 use instead of a broadcast address?
- How can you easily identify IPv6 multicast addresses?
- What does the special address FF02::2 mean? When is address ::1 used?

This section covers the following exam objectives:

- 308. Describe IPv6 addresses

### **IPv6 Feature Facts**

The current IP addressing standard, version 4, will eventually run out of unique addresses, so a new system is being developed. It is named IP version 6 or IPv6. You should know about the following IPv6 features:

Feature	Description
Geographic assignment of addresses	<p>The Internet Corporation for Assigned Names and Numbers (ICANN) assigns IPv6 addresses based on the following strategy:</p> <ul style="list-style-type: none"><li>• Public IPv6 addresses are grouped by major geographic region, such as a continent.</li><li>• Inside each region, the address is further subdivided by each ISP.</li><li>• Inside each ISP, the address is further subdivided for each customer or other smaller Internet registries.</li></ul>
Efficient route summarization	<p>Route summarization combines blocks of addresses in a routing table as a single route. As IPv6 addresses are assigned by geographic region, then ISP, and then the customer, the route summarization of IPv6 addresses is efficient when compared to IPv4 route summarization.</p>
No need for Network Address Translation (NAT) or Port Address Translation (PAT)	<p>From the large amount of IP addresses afforded by IPv6, each device has a publicly registered address. Having a unique address for each device removes the need for NAT and PAT.</p>
Native Internet Protocol Security (IPSec)	<p>IPSec can be used to encrypt any traffic supported by the IP protocol. This includes Web, e-mail, Telnet, file transfer, and SNMP traffic as well as countless others.</p> <p>IPv6 has built-in support for the IPSec security protocol. Within an IPv4 environment, IPSec security features are available as add-ons but are required in IPv6.</p>
Header improvements	<p>IPv6 packet headers do not need to have their logical link address changed as the packet hops from router to router. This leads to a reduction in per-packet overhead.</p>
Built-in Quality of Service	<p>Built-in support for bandwidth reservations make guaranteed data</p>

(QoS)	transfer rates possible. Within an IPv4 environment, Quality of Service features are available as add-ons but are not part of the native protocol.
Flow label	The <i>flow label</i> is a field in the IPv6 packet header. Packets belonging to the same stream, session, or flow share a common flow label value, making the session easily recognizable without having to open the inner packet to identify the flow.

## IPv6 Address Facts

The IPv6 address is a 128-bit binary number. A sample IPv6 IP address looks like: 35BC:FA77:4898:DAFC:200C:FBBC:A007:8973. The following list describes the features of an IPv6 address:

- The address is made up of 32 hexadecimal numbers, organized into 8 quartets.
- The quartets are separated by colons.
- Each quartet is represented as a hexadecimal number between 0 and FFFF. Each quartet represents 16-bits of data (FFFF = 1111 1111 1111 1111).
- Leading zeros can be omitted in each section. For example, the quartet 0284 could also be represented by 284.
- Addresses with consecutive zeros can be expressed more concisely by substituting a double-colon for the group of zeros. For example:
  - FEC0:0:0:0:78CD:1283:F398:23AB
  - FEC0::78CD:1283:F398:23AB (concise form)
- If an address has more than one consecutive location where one or more quartets are all zeros, only one location can be abbreviated. For example, FEC2:0:0:0:78CA:0:0:23AB could be abbreviated as:
  - FEC2::78CA:0:0:23AB or
  - FEC2:0:0:0:78CA::23AB

But *not* FEC2::78CA::23AB

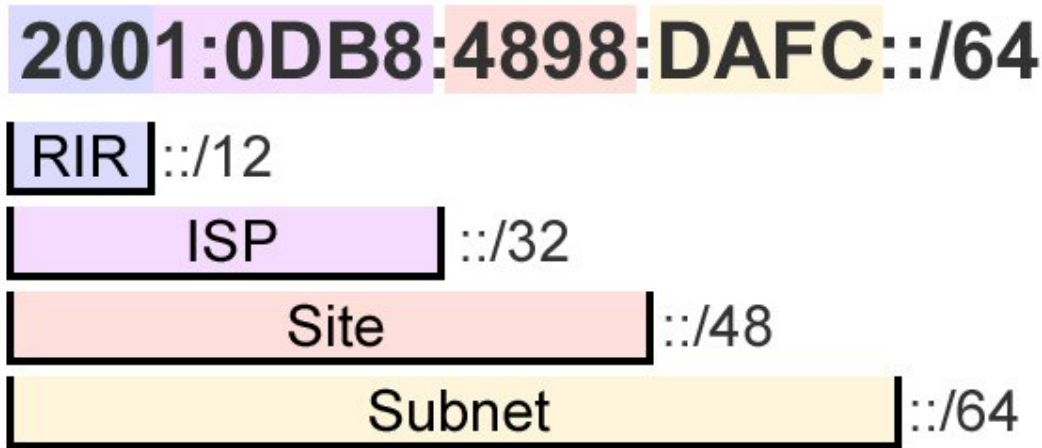
- The 128-bit address contains two parts:
  - The first 64-bits is known as the *prefix*. The prefix includes the network and subnet address. Because addresses are allocated based on physical location, the prefix also includes global routing information. The 64-bit prefix is often referred to as the *global routing* prefix.
  - The last 64-bits is the *interface ID*. This is the unique address assigned to an interface. **Note:** Addresses are assigned to interfaces (network connections), not to the host. Technically, the interface ID is *not* a host address.

The 64-bit prefix can be divided into various parts, with each part having a specific meaning.

- The *prefix length* identifies the number of bits in the relevant portion of the prefix. To indicate the prefix length, add a slash (/) followed by the prefix length number.
- Bits past the end of the prefix length are all binary 0s. For example, the full 64-bit prefix for address 2001:0DB8:4898:DAFC:200C:FBBC:A007:8973 is 2001:0DB8:4898:DAFC:0000:0000:0000:0000/64.
- Full quartets with trailing 0's in the prefix address can be omitted (for example 2001:0DB8:4898:DAFC::/64).
- If the prefix is not on a quartet boundary (this applies to any prefix that is not a multiple of 16), any hex values listed after the boundary should be written as 0's. For example, the prefix 2001:0DB8:4898:DAFC::/56 should be written as 35BC:FA77:4898:DA00::/56. Remember, only *leading* 0's within a quartet can be omitted.

- Be aware that the prefix length number is a binary value, while the prefix itself is a hexadecimal value.

Global routing information is identified within the 64-bit prefix by subdividing the prefix using varying prefix lengths. The following graphic is an example of how the IPv6 prefix could be divided:



This sample assignment of IPv6 addresses is explained in the following table:

Prefix	Description
Regional Internet Registry (RIR)	<p>The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the assignment of IPv6 addresses. ICANN assigns a range of IP addresses to Regional Internet Registry (RIR) organizations. Each current regional organization corresponds roughly to a continent.</p> <p>The exact size of the address range assigned to the RIR may vary, but current guidelines assign a minimum prefix of 12-bits. In the above example, the RIR has been assigned a 12-bit prefix, and is responsible for addresses in the following range:</p> <p>2000::/12 to 200F:FFFF:FFFF:FFFF::/64</p>
Internet Service Provider (ISP)	<p>A regional organization subdivides its block of IP addresses into smaller blocks and assigns those blocks to National Internet Registries (NIR), Local Internet Registries (LIR), or Internet Service Providers (ISP). Larger organizations can further subdivide the address space to allocate to smaller ISPs.</p> <p>The exact size of the address range assigned by the RIR may vary, but current guidelines assign a minimum prefix of 32-bits. In the above example, the ISP has been assigned a 32-bit prefix, and is therefore responsible for addresses in the following range:</p> <p>2001:0DB8::/32 to 2001:0DB8:FFFF:FFFF::/64</p>
Site	<p>Individual companies and other organizations request blocks of IP addresses from an ISP for use in their private networks. Each network organized by a single entity is often called a <i>site</i>, although the exact definition of the term is under debate.</p> <p>Although the exact size of the address range assigned to a site may vary, by convention, each site is assigned a 48-bit site ID. In the above example, the site is</p>



	<p>responsible for managing the addresses in the following range:</p> <p>2001:0DB8:4898::/48 to 2001:0DB8:4898:FFFF::/64</p> <p>ISPs typically follow these guidelines for assigning address ranges to sites:</p> <ul style="list-style-type: none"> <li>• By default, all sites that represent a network, including home networks, get an address with a 48-bit prefix.</li> <li>• Sites that require an address space larger than this might be assigned two consecutive blocks, or might be allocated an address with a 47-bit prefix.</li> <li>• If the network is known to have only a single subnet, the ISP might assign a 64-bit prefix. This is typically used for mobile devices.</li> <li>• If the network is known to have only a single device, such as a dialup connection, the ISP might assign a 128-bit prefix.</li> </ul>
Subnet ID	<p>Most networks receive an address range identified with a 48-bit prefix. The remaining 16-bits in the global routing prefix are then used by the local network administrator for creating subnets. In the example above, the site has received the prefix of 2001:0DB8:4898::/48. The following list shows some of the subnets that could be created by the administrator using a 64-bit prefix:</p> <p>2001:0DB8:4898:0001::/64  2001:0DB8:4898:0002::/64  2001:0DB8:4898:0003::/64  ...  2001:0DB8:4898:FFFD::/64  2001:0DB8:4898:FFFE::/64  2001:0DB8:4898:FFFF::/64</p>

In most cases, individual interface IDs are not assigned by ISPs, but are rather generated automatically or managed by site administrators. Interface IDs must be unique within a subnet, but can be the same if the interface is on different subnets. All addresses that identify a single interface, except those that start with 000 binary, but use a 64-bit interface ID that follows the modified EUI-64 format. On Ethernet networks, the modified EUI-64 format interface ID can be automatically derived from the MAC address using the following process:

1. The MAC address is split into 24-bit halves.
2. The hex constant FFFE is inserted between the two halves to complete the 64-bit address. For example, 20-0C-FB-BC-A0-07 becomes:  
200C:FB**FF:FE**BC:A007.
3. The seventh bit of the MAC address (reading from left to right) is set to binary 1. This bit is called the *universal/local (U/L)* bit.
  - Modifying the seventh binary bit modifies the second hex value in the address.
  - For a MAC address of 20-0C-FB-BC-A0-07, the first two hex values translate to the following binary number:  
0010 0000
  - Setting the seventh bit to 1 yields 0010 0010, which translates into 22 hex.

In this example, the MAC address of 20-0C-FB-BC-A0-07 in modified EUI-64 format becomes: 220C:FB**FF:FE**BC:A007 (portions in red indicate modified values).

## IPv6 Address Types

In IPv6, addresses are assigned to interfaces (network connections). All interfaces are required to have some addresses, and interfaces can have more than one address. IPv6 identifies the following types of addresses:



Address Type	Description
Unicast	<p><i>Unicast</i> addresses are assigned to a single interface for the purpose of allowing that one host to send and receive data. Packets sent to a unicast address are delivered to the interface identified by that address.</p> <p>Described below are three types of unicast addresses.</p>
	<p><i>Link-local</i> addresses (also known as <i>local link</i> addresses) are addresses that are valid on only the current subnet.</p> <ul style="list-style-type: none"> <li>• Link-local addresses have a FE80::/10 prefix. This includes any address beginning with FE8, FE9, FEA, or FEB.</li> <li>• All nodes must have at least one link-local address, although each interface can have multiple addresses.</li> <li>• Routers never forward packets destined for local link addresses to other subnets.</li> <li>• Link-local addresses are used for automatic address configuration, neighbor discovery, or for subnets that have no routers.</li> </ul>
	<p><i>Unique local</i> addresses are private addresses used for communication within a site or between a limited number of sites.</p> <ul style="list-style-type: none"> <li>• Unique local addresses have a FC00::/7 prefix. Currently, however, the 8th bit is always set to 1 to indicate that the address is local (and not global). Thus, addresses beginning with FC or FD are unique local addresses.</li> <li>• Following the prefix, the next 50-bits are used for the Global ID. The Global ID is generated randomly such that there is a high probability of uniqueness on the entire Internet.</li> <li>• Following the Global ID, the remaining 16-bits in the prefix are used for subnet information.</li> <li>• Unique local addresses are globally unique, but are not globally routable. Unique local addresses might be routed between sites by a local ISP.</li> <li>• Earlier IPv6 specifications defined a site-local address that was not globally unique and had a FEC0::/10 prefix. The site-local address has been replaced with the unique local address.</li> </ul>
	<p><i>Global unicast</i> addresses are addresses that are assigned to individual interfaces that are globally unique (unique throughout the entire Internet).</p> <p>Global unicast addresses are any addresses that are not link-local, unique local, or multicast addresses. Currently, ISPs assign global unicast addresses with a 2000::/3 prefix (this includes any address beginning with a 2 or a 3). In the future, however, global unicast addresses might not have this restriction.</p>
Multicast	<p><i>Multicast</i> addresses represent a dynamic group of hosts. Packets sent to a multicast address are sent to all interfaces identified by that address. By using a different multicast address for different functions, only the devices that need to participate in the particular function will respond to the multicast; devices that have no need to participate in the function will ignore the multicast.</p> <ul style="list-style-type: none"> <li>• All multicast addresses have a FF00::/8 prefix.</li> <li>• Multicast addresses that are restricted to the local link only have a FF02::/16</li> </ul>

	<p>prefix. Packets starting with FF02 are not forwarded by routers.</p> <ul style="list-style-type: none"> <li>• Multicast addresses with a FF01::<!--16 prefix are restricted to a single node.</li--> </li></ul> <p>You should be familiar with the following well-known multicast addresses:</p> <ul style="list-style-type: none"> <li>• FF02::1 is for all nodes on the local link. This is the equivalent of the IPv4 subnet broadcast address. FF01::1 is for all interfaces on a node.</li> <li>• FF02::2 is for all routers on the local link. FF01::1 is for all routers on the node.</li> <li>• FF02::1:2 is for all DHCP servers or DHCP relay agents on the local link. DHCP relay agents forward these packets to other subnets.</li> </ul>
Anycast	<p>The <i>anycast</i> address is a unicast address that is assigned to more than one interface, typically belonging to different hosts. An anycast packet is routed to the nearest interface having that address (based on routing protocol decisions).</p> <ul style="list-style-type: none"> <li>• An anycast address is the same as a unicast address. Assigning the same unicast address to more than one interface makes it an anycast address.</li> <li>• You can have link-local, unique local, or global unicast anycast addresses.</li> <li>• When you assign an anycast address to an interface, you must explicitly identify the address as an anycast address (to distinguish it from a unicast address).</li> <li>• Anycast addresses can be used to locate the nearest server of a specific type, for example the nearest DNS or network time server.</li> </ul>
Loopback	<p>The local loopback address for the local host is 0:0:0:0:0:0:1 (also identified as ::1 or ::1/128). The local loopback address is not assigned to an interface. It can be used to verify that the TCP/IP protocol stack has been properly installed on the host.</p>
Unspecified	<p>The unspecified address is 0:0:0:0:0:0:0 (also identifies as :: or ::/128). The unspecified address is used when there is no IPv6 address. It is typically used during system startup when the host has not yet configured its address. The unspecified address should not be assigned to an interface.</p>

**Note:** There are no broadcast addresses in IPv6. IPv6 multicast addresses are used instead of broadcast addresses.

## IPv6 Implementation

As you study this section, answer the following questions:

- How does a host get its IPv6 address when using stateless autoconfiguration?
- What information does the DHCP server provide when using stateless DHCPv6?
- What address does a host use to request an address from a DHCP server?
- What limitations does ISATAP have for IPv6 implementation?
- Which IPv6 tunneling methods work through NAT?
- What is the only method possible to enable an IPv6-only host to communicate with an IPv4-only host?

After finishing this section, you should be able to complete the following tasks:

- Configure IPv6 host addresses.
- Enable IPv6 support on a Cisco router.

This section covers the following exam objectives:

- 307. Describe the technological requirements for running IPv6 in conjunction with IPv4

### IPv6 Configuration Facts

An IPv6 address is configured by any one of the following methods:

Method	Description
Static full assignment	<i>Static full assignment</i> is where the entire 128-bit IPv6 address and all other configuration information is statically assigned to the host.
Static partial assignment	<i>Static partial assignment</i> is where the prefix is statically assigned and the interface ID uses the modified EUI-64 format derived from the MAC address.
Stateless autoconfiguration	<p><i>Stateless autoconfiguration</i> is where clients automatically generate the interface ID, and learn the subnet prefix and default gateway through the Neighbor Discovery Protocol (NDP). NDP uses the following messages for autoconfiguration:</p> <ul style="list-style-type: none"><li>• <i>Router solicitation</i> (RS) is a message sent by the client to request that routers respond.</li><li>• <i>Router advertisement</i> (RA) is a message sent by the router periodically and in response to RS messages to inform clients of the IPv6 subnet prefix and the default gateway address.</li></ul> <p>NDP is also used by hosts to discover the address of other interfaces on the network, replacing the need for Address Resolution Protocol (ARP).</p> <p><b>Note:</b> Even though NDP provides enough information for the addressing of the client and for clients to learn the addresses of other clients on the network, it does not provide the client with DNS server information or other IP configuration information besides the IP address and the default gateway.</p>
DHCPv6	<p>IPv6 uses an updated version of DHCP (called DHCPv6) that operates in one of two different modes:</p> <ul style="list-style-type: none"><li>• <i>Stateful</i> DHCPv6 is when the DHCP server provides each client with the IP address, default gateway, and other IP configuration information (such as the DNS server IP address). The DHCP server tracks the status</li></ul>

	<p>(or state) of the client.</p> <ul style="list-style-type: none"> <li>• <i>Stateless</i> DHCPv6 does not provide the client an IP address and does not track the status of each client, but rather is used to supply the client with the DNS server IP address. Stateless DHCPv6 is most useful when used in conjunction with stateless autoconfiguration.</li> </ul>
--	---

When a host starts up, it uses the following process to configure the IPv6 address for each interface:

1. The host generates an IPv6 address using the link-local prefix (FE80::/10) and modifying the MAC address to get the interface ID. For example, if the MAC address is 20-0C-FB-BC-A0-07, the link-local address for the interface would be: FE80::220C:FBFF:FEBC:A007.
2. The host then sends a neighbor solicitation (NS) message addressed to its own link-local address to see if the address it has chosen is already in use.
  - If the address is in use, the other network host responds with a neighbor advertisement (NA) message. The process stops and manual configuration of the host is required.
  - If the address is not in use (no NA message), the process continues.
3. The host waits for a router advertisement (RA) message from a router to learn the prefix.
  - If an RA message is not received, the host sends out a router solicitation (RS) message addressed to all routers on the subnet using the multicast address FF02::2.
  - The router sends out an RA message addressed to all interfaces on the subnet using the multicast address FF02::1.
  - If no routers respond, the host attempts to use stateful DHCPv6 to receive configuration information.
4. The RA message contains information that identifies how the IPv6 address and other information is to be configured. Possible combinations are:

Configuration Method	Description
Use stateful autoconfiguration	Obtain the interface ID, subnet prefix, default gateway, and other configuration information from a DHCPv6 server. The host sends out a REQUEST message addressed to the multicast address FF02::1:2 to request this information from the DHCPv6 server.
Use stateless autoconfiguration	Set the interface ID automatically. Get the subnet prefix and default gateway from the RA message. Get DNS and other configuration information from a DHCPv6 server. The host sends out an INFORMATION-REQUEST message addressed to the multicast address FF02::1:2 to request this information from the DHCPv6 server.

5. If a manual address or stateful autoconfiguration is used, the host sends an NS message to make sure the address is not already in use. If stateless autoconfiguration is used, the NS message at this step is unnecessary because the interface ID has already been verified in step 2.

### IPv6 Implementation Facts

The worldwide implementation from IPv4 to IPv6 will be a long process. Although not yet widely adopted, you can implement IPv6 if your systems support it. As the implementation of IPv6 proceeds, there will be cases when compatibility with IPv4 is required. The following table lists various strategies for deploying IPv6:

Method	Description	
<a href="#">Dual stack</a>	<p>With a <i>dual stack</i> configuration, both the IPv4 and IPv6 protocol stacks run concurrently on a host. IPv4 is used to communicate with IPv4 hosts, and IPv6 is used to communicate with IPv6 hosts. When implemented on hosts, intermediate routers and switches must also run both protocol stacks.</p> <p>Use a dual stack configuration to enable a host to communicate with both IPv4 and IPv6 hosts.</p>	
Tunneling	<p><i>Tunneling</i> wraps an IPv6 packet within an IPv4 packet, allowing IPv6 hosts or sites to communicate over the existing IPv4 infrastructure. With tunneling, a device encapsulates IPv6 packets in IPv4 packets for transmission across an IPv4 network, and then the packets are de-encapsulated to their original IPv6 packets by another device at the other end.</p> <p>Several tunneling solutions are listed below.</p>	
	<a href="#">Manually configured tunnel</a>	<p>With a manually configured tunnel, tunnel endpoints are configured as point-to-point connections between devices. Manual tunneling:</p> <ul style="list-style-type: none"> <li>• Is configured between routers at different sites.</li> <li>• Requires dual-stack routers as the tunnel endpoints. Hosts can be IPv6-only hosts.</li> <li>• Works through NAT.</li> <li>• Uses a static (manual) association of an IPv6 address with the IPv4 address of the destination tunnel endpoint.</li> </ul> <p>Because of the time and effort required for configuration, use manually configured tunnels only when you have a few sites that need to connect through the IPv4 Internet, or when you want to configure secure site-to-site associations.</p>
	<a href="#">6-to-4 tunneling</a>	<p>With 6-to-4 tunneling, tunneling endpoints are configured automatically between devices. 6-to-4 tunneling:</p> <ul style="list-style-type: none"> <li>• Is configured between routers at different sites.</li> <li>• Requires dual-stack routers as the tunnel endpoints. Hosts can be IPv6-only hosts.</li> <li>• Works through NAT.</li> <li>• Uses a dynamic association of an IPv6 site prefix to the IPv4 address of the destination tunnel endpoint.</li> <li>• Automatically generates an IPv6 address for the site using the 2002::/16 prefix followed by the public IPv4 address of the tunnel endpoint router. For example, a router with the IPv4 address of 207.142.131.202 would serve the site with the following prefix: 2002:CF8E:83CA::/48 (CF8E:83CA is the hexadecimal equivalent of 207.142.131.202).</li> </ul> <p>Use 6-to-4 tunneling to dynamically connect multiple sites through the IPv4 Internet. Because of its dynamic configuration, 6-to-4 tunneling is easier to administer than manual tunneling.</p>
<a href="#">Intra-site</a>	<p>The Intra-site Automatic Tunnel Addressing Protocol</p>	

<p><a href="#">Automatic Tunnel Addressing Protocol (ISATAP)</a></p>	<p>(ISATAP) is a tunneling method for use <i>within</i> a site to provide IPv6 communication over a private IPv4 network. ISATAP tunneling:</p> <ul style="list-style-type: none"> <li>• Is configured between individual hosts and an ISATAP router.</li> <li>• Requires a special dual-stack ISATAP router to perform tunneling, and dual-stack or IPv6-only clients. Dual stack routers and hosts perform tunneling when communicating on the IPv4 network.</li> <li>• Does <i>not</i> work through NAT.</li> <li>• Automatically generates link-local addresses that includes the IPv4 address of each host: <ul style="list-style-type: none"> <li>◦ The prefix is the well-known link-local prefix: FE80::/16.</li> <li>◦ The remaining prefix values are set to 0.</li> <li>◦ The first two quartets of the interface ID are set to 0000:5EFE.</li> <li>◦ The remaining two quartets use the IPv4 address, written in either dotted-decimal or hexadecimal notation.</li> </ul> </li> </ul> <p>A host with an IPv4 address of 192.168.12.155 would have the following IPv6 address when using ISATAP: FE80::5EFE:C0A8:0C9B (also designated as FE80::5EFE:192.168.12.155).</p> <p>Use ISATAP to begin a transition to IPv6 <i>within</i> a site. You can start by adding a single ISATAP router and configuring each host as an ISATAP client.</p>
<p><a href="#">Teredo tunneling</a></p>	<p>Teredo tunneling establishes the tunnel between individual hosts so they can communicate through a private or public IPv4 network. Teredo tunneling:</p> <ul style="list-style-type: none"> <li>• Is configured between individual hosts.</li> <li>• Hosts are dual-stack hosts and perform tunneling of IPv6 to send on the IPv4 network.</li> <li>• Works through NAT.</li> </ul> <p>Use Teredo tunneling to enable host-to-host communications between IPv6 devices through a public or private IPv4 network.</p>
<p><a href="#">Network Address Translation-Protocol Translation (NAT-PT)</a></p>	<p>NAT-PT is a protocol that converts the IPv6 packet header into an IPv4 packet header, and vice versa. With NAT-PT, a translation table is referenced by the device, such as a Cisco router, as it converts the headers to ensure that the packet is sent to the correct host. This method is different than tunneling because the packet headers are converted between the IPv4 and IPv6, whereas tunneling wraps the IPv6 packet into an IPv4 packet. NAT-PT:</p> <ul style="list-style-type: none"> <li>• Is configured on a single router running NAT-PT.</li> <li>• The router is a dual-stack router. Hosts run either IPv4 or IPv6.</li> </ul> <p>Use NAT-PT to allow IPv4 hosts to communicate with IPv6 hosts.</p>

## DHCP and NAT

As you study this section, answer the following questions:

- How does the DHCP service determine on which interfaces to listen for DHCP requests?
- How is an access list used in NAT configuration?
- How do you link a NAT address pool to an access list and an interface?
- What parameter must you use in your NAT configuration if you have more private hosts than public IP addresses?
- Which NAT configuration method do you use to associate a specific outside IP address with an inside host?

After finishing this section, you should be able to complete the following tasks:

- Create DHCP address pools.
- Configure NAT inside and outside interfaces.
- Configure static NAT and NAT pools.

This section covers the following exam objectives:

- 303. Configure, verify and troubleshoot DHCP and DNS operation on a router
- 707. Configure NAT for given network requirements
- 708. Troubleshoot NAT issues

### **Advanced DHCP Configuration**

In addition to configuring DHCP using the SDM interface, you can configure DHCP using the command line. Before discussing the configuration steps, be sure you understand the following terms:

- A *pool* is a range of IP addresses that the DHCP server can assign.
- DHCP *options* are the configuration parameters in addition to the IP address and mask that the DHCP server will deliver to hosts. Options include DNS server addresses and the default gateway address.
- An *exclusion* is a single address or a range of addresses in the pool that will not be assigned by the DHCP server.
- A *binding* is an IP address that is associated with a MAC address. Each time the specified host requests an IP address, the DHCP server will assign it the address specified in the binding.

Configuring DHCP through the command line involves the following steps:

1. Create a pool for the subnet. After creating the pool, define the following parameters for the pool:
  - The subnet address and mask.
  - DHCP options to assign (such as the default gateway, DNS server addresses, or domain name).
  - Configure the lease time.
2. Create a pool for each binding. Within the pool, configure:
  - The IP address and mask
  - The MAC address of the host
3. Configure any exclusions (addresses you don't want assigned).

**Note:** When you define the pool for the subnet, the router automatically responds to DHCP requests that come in on the interface whose IP address matches the pool you defined.



The following table lists various commands for completing the DHCP configuration:

Use . . .	To . . .
Router(config)#ip dhcp pool WORD	Create a DHCP pool Pools are used to define a range of addresses to assign, as well as create bindings.
Router(dhcp-config)#network A.B.C.D m.m.m.m	Identify the subnet address and mask for the address pool.
Router(dhcp-config)#default- router A.B.C.D	Identify the default gateway address that will be assigned to hosts. This address should be inside the address pool. You can identify up to 8 addresses. However, most hosts can accept only a single default gateway address.
Router(dhcp-config)#dns-server A.B.C.D <A.B.C.D>	Identify DNS server addresses delivered to hosts. You can configure multiple DNS server addresses. Simply include multiple addresses separated by a space. You can specify up to 8 server addresses.
Router(dhcp-config)#domain- name WORD	Sets the domain name to be delivered to hosts.
Router(dhcp-config)#lease 0- 365	Configures the IP address lease time (in days). Use the <b>infinite</b> keyword for a lease that does not expire.
Router(config)#ip dhcp excluded-address A.B.C.D <A.B.C.D>	Exclude addresses from being assigned. Identify start and ending addresses in the range, or a single address. Typically, you will exclude the DHCP server's own IP address from the range. <b>Note:</b> This command is a global configuration command; it is not issued as part of the pool.
Router(config)#ip dhcp pool WORD Router(dhcp-config)#host A.B.C.D m.m.m.m Router(dhcp-config)#hardware- address aabb.ccdd.eeff	Create a binding. When you create a binding, you create a separate pool that is different than the pool that identifies the subnet. This pool must have a unique name. As part of the pool, you configure the IP address and mask that will be assigned to the host, as well as the MAC address of the host.
Switch(config)#interface vlan 1 Switch(config-if)#ip address dhcp	Configure a Cisco device to get its IP address from the DHCP server. Most routers and servers have static IP addresses and do not use DHCP for obtaining an IP address. However, you could create a binding to make sure the same address is always assigned to network infrastructure devices such as servers, switches, and routers.

### Example

In the following example, the router has an IP address of 172.19.1.129/25 assigned to its Fa0/1 interface. The following commands create a pool for the subnet, configures DNS and default gateway addresses to assign to hosts, sets the lease time to 10 days, excludes the router's IP address from the pool, and creates a binding for a host named Dns-Srv1 that assigns that host an address of 172.19.1.132 each time it requests an address.

```
Router#ip dhcp pool SubnetA
Router(dhcp-config)#network 172.19.1.128 255.255.255.128
Router(dhcp-config)#default-router 172.19.1.129
Router(dhcp-config)#dns-server 172.19.1.132
Router(dhcp-config)#lease 10
Router(dhcp-config)#exit
```



```

Router(config)#ip dhcp excluded-address 172.19.1.129
Router(config)#ip dhcp pool Dns-Srv1
Router(dhcp-config)#host 172.19.1.132 255.255.255.128
Router(dhcp-config)#hardware-address 0fe8.11a7.ab89

```

## Advanced NAT Configuration

Network Address Translation (NAT) allows you to connect a private network to the Internet without obtaining registered addresses for every host. Private addresses are translated to the public address of the NAT router. When configuring NAT, you have the following options:

Method	Description
Static	<p>Use static translation to translate a single outside address to a single inside address. To configure static NAT, use the following general process:</p> <ol style="list-style-type: none"> <li>1. Define a static map that associates the inside address with the outside address.</li> <li>2. Identify which router interface is the inside interface, and which interface is the outside interface.</li> </ol>
Overloaded with PAT	<p>Use overloaded NAT with Port Address Translation (PAT) to translate multiple inside addresses to a single public address. To configure overloaded NAT, use the following general process:</p> <ol style="list-style-type: none"> <li>1. Create an access list that allows the specified inside addresses to be translated.</li> <li>2. Link the access list to the internal interface using the <b>overloaded</b> option. The IP address assigned to the outside interface will automatically be used as the outside address for all inside hosts.</li> <li>3. Identify which router interface is the inside interface, and which interface is the outside interface.</li> </ol>
Dynamic	<p>Use dynamic translation to translate a range of outside addresses to a range of inside addresses. To configure dynamic NAT, use the following general process:</p> <ol style="list-style-type: none"> <li>1. Define the pool of outside addresses that can be used for translation.</li> <li>2. Create an access list that allows the specified inside addresses to be translated.</li> <li>3. Link the pool with the access list.</li> <li>4. Identify which router interface is the inside interface, and which interface is the outside interface.</li> </ol> <p><b>Note:</b> If the number of outside addresses defined in the pool is less than the number of inside addresses allowed by the access list, the number of inside hosts that can gain outside access will be limited to the number of outside addresses in the pool. To allow a greater number of inside hosts to use a smaller number of outside addresses, add the <b>overloaded</b> parameter to step 3. This uses dynamic NAT with PAT.</p>

The following table lists the configuration steps and commands for each method.

Method	Configuration Task	Command Examples
Static NAT	Configure static mappings (mapping inside local addresses to outside local addresses)	<pre> Router(config)#ip nat inside source static 192.168.1.1 203.44.55.1 </pre>

	Identify inside and outside interfaces	Router(config)#interface ethernet0 Router(config-if)#ip nat inside Router(config-if)#interface serial0 Router(config-if)#ip nat outside
Overloaded with PAT	Identify allowed translated inside local addresses	Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
	Associate the allowed list with the outside interface and identify the translation type as overloaded	Router(config)#ip nat inside source list 1 interface serial0 overload
	Identify inside and outside interfaces	Router(config)#interface ethernet0 Router(config-if)#ip nat inside Router(config-if)#interface serial0 Router(config-if)#ip nat outside
Dynamic NAT	Define an inside global address pool	Router(config)#ip nat pool pooled_addr 203.44.55.1 203.44.55.254 netmask 255.255.255.0
	Identify allowed translated inside local addresses	Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
	Associate the allowed list with the pool	Router(config)#ip nat inside source list 1 pool pooled_addr
	Identify inside and outside interfaces	Router(config)#interface ethernet0 Router(config-if)#ip nat inside Router(config-if)#interface serial0 Router(config-if)#ip nat outside

### Example

In this example, you have been given six public addresses from your ISP (177.211.5.89 to 177.211.5.94) using a 29-bit mask. You will use one of those addresses for the router interface, and want to use the remaining 5 addresses for dynamic NAT with PAT for inside hosts. You want to configure Internet access for all inside hosts on the 10.0.1.0/24 network. The following commands create the pool, define the allowed inside addresses, link the access list to the pool, and configure the inside and outside interfaces.

```
Router(config)#ip nat pool public_addr 177.211.5.90 177.211.5.94 netmask
255.255.255.248
Router(config)#access-list 1 permit 10.0.1.0 0.0.0.255
Router(config)#ip nat inside source list 1 pool public_addr overloaded
Router(config)#int eth0/1
Router(config)#ip addr 10.0.1.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#int ser0/1/0
Router(config-if)#ip addr 177.211.5.89 255.255.255.248
Router(config-if)#ip nat outside
```

**Note:** The `ip nat pool` command can use the `prefix-length` keyword instead of the `netmask` keyword as in the following example:

```
ip nat pool public_addr 177.211.5.89 177.211.5.94 netmask 29
```

Use the following commands to monitor NAT:

Use ...	To ...
Router#clear ip nat translation	Clear (delete) the dynamic entries in the NAT table.

Router#show ip nat statistics	View counters for packets and NAT table entries, as well as basic configuration information.
Router#show ip nat translations	View the NAT/PAT translation table entries.

## Network Security

As you study this section, answer the following questions:

- What is *social engineering*? What is the best defense against social engineering?
- How does a worm differ from a boot sector virus? A Trojan horse?
- How are Denial of Service (DoS) attacks a security threat?
- In addition to implementing virus scanning software, what must you do to ensure that you are protected from the latest virus variations?
- Which types of attacks are directed against passwords?
- How does a firewall protect a network?
- What is an IPS and how does it differ from an IDS?
- What are the benefits of using centralized authentication?

This section covers the following exam objectives:

- 601. Describe today's increasing network security threats and explain the need to implement a comprehensive security policy to mitigate the threats
- 602. Explain general methods to mitigate common security threats to network devices, hosts, and applications
- 603. Describe the functions of common security appliances and applications

### Security Threat Facts

Consider the following security threats:

- *Internal* threats are intentional or accidental acts by employees including:
  - Accidental exposure to information or assets that happens when employees explore or experiment.
  - Errors and omissions that negatively impact company assets.
  - Malicious acts such as theft or fraud.
- *External* threats are those events originating outside of the organization that typically focus on compromising the organization's information assets. Examples include hackers, fraud perpetrators, and viruses.
- *Structured* threats include attacks where the attacker is knowledgeable of network vulnerabilities and systematically attempts to exploit the vulnerabilities.
- *Unstructured* threats are where an unknowledgeable attacker may download a tool or program from the Internet and attempt to use it.

Be aware of the following types of security threats:

Threat	Description
Reconnaissance	<p>A <i>reconnaissance</i> attack is exploring or probing a system to discover information about the system. Most malicious attacks are preceded by a reconnaissance attack. There are two types of reconnaissance attacks:</p> <ul style="list-style-type: none"><li>• <i>Passive reconnaissance</i> is characterized by gathering data. Passive reconnaissance does not directly affect the target. Examples of this stage include:<ul style="list-style-type: none"><li>◦ Eavesdropping on employee conversations.</li><li>◦ Looking over the shoulder of an employee.</li><li>◦ Going through the trash looking for information (<i>dumpster diving</i>).</li><li>◦ Browsing the organization's website.</li></ul></li><li>• <i>Active scanning</i> is coming into contact with the system. Active scanning can include:</li></ul>

	<ul style="list-style-type: none"> <li>○ Scanning for wireless access points within the organization (<i>war driving</i>).</li> <li>○ Trying to access phone lines that will answer a calling modem (<i>war dialing</i>).</li> <li>○ Capturing information transmitted by the remote host including the application type, application version and even operating system type and version (<i>banner grabbing</i>).</li> <li>○ Probing the corporate network with scanning tools.</li> </ul>
Social engineering	<p><i>Social engineering</i> is a form of reconnaissance attack that exploits human nature by convincing someone to reveal information or perform an activity. Examples of social engineering include:</p> <ul style="list-style-type: none"> <li>• Impersonating support staff or management, either in person or over the phone.</li> <li>• Asking for someone to hold open a door rather than using a key for entrance.</li> <li>• Spoofed e-mails that ask for information or ask for tasks to be performed (such as delete a file or go to a Web site and enter sensitive information). This is also known as <i>phishing</i>.</li> <li>• Looking on desks for usernames and passwords.</li> </ul>
Denial of service	<p>Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks impact system availability by flooding the target system with traffic or requests or by exploiting a system or software flaw. The main purpose of a DoS attack is to overwhelm the system to make it unavailable for legitimate use. Examples include:</p> <ul style="list-style-type: none"> <li>• A <i>ping flood</i> is a where the victim is overwhelmed with ICMP Echo Request (ping) packets.</li> <li>• The <i>SYN flood</i> exploits the TCP three-way handshake.</li> <li>• <i>Spam</i> is sending unwanted e-mail messages.</li> <li>• A <i>buffer overflow</i> is when software code receives more input than it was designed to handle and when the programmer of that code failed to include input validation checks, thus allowing the attacker to perform any operation on a system.</li> </ul>
Malware	<p><i>Malicious code</i> (sometimes called <i>malware</i>) is a type of software designed to take over or damage a computer user's operating system without the user's knowledge or approval. Common malware examples are listed below:</p> <ul style="list-style-type: none"> <li>• A <i>virus</i> is a program that attempts to damage a computer system and replicate itself to other computer systems.</li> <li>• A <i>worm</i> is a self-replicating program that can be designed to do any number of things, such as delete files or send documents via e-mail.</li> <li>• A <i>Trojan horse</i> is a malicious program that is disguised as legitimate software.</li> <li>• <i>Spyware</i> monitors the actions you take on your machine and sends the information back to its originating source.</li> <li>• <i>Adware</i> is a software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.</li> </ul>
Access attacks	Access attacks refer to attackers trying to gain unauthorized access to networks or

computer systems. Common access attacks are listed below:

- *Spoofing* is used to hide the true source of packets or redirect traffic to another location. The most common form of spoofing on a typical IP packet is modification of the source address.
- *Man-in-the-middle* attacks are used to intercept information passing between two communication partners.
- *Password cracking* is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system. Examples include the following:
  - A *brute force* attack is a method of defeating a password by exhaustively working through all possibilities in order to find the password.
  - A *dictionary* attack refers to the technique of trying to guess a password by running through a list of words from a dictionary.
  - A *hybrid* attack refers to the technique of adding appendages to known dictionary words. For example, 1password, password07, p@ssword1.

### Security Solution Facts

Use the following general measures to improve security:

- Use passwords to protect consoles and ports.
- Restrict physical access to devices.
- Update device firmware and BIOS.
- Use ACLs on routers and firewalls to filter and control traffic.
- Install antivirus software on the network.
- Create a written security policy. The security policy outlines security measures to implement to protect the network.
- Implement training so that users are aware of security policies and understand the need to follow established procedures. Training and education is often the most effective solution for social engineering attacks.
- Periodically review the security policy and security methods to ensure that they are adequate.
- Implement multiple security measures to protect the same asset. *Defense in depth* or *security in depth* is the premise that no single layer is completely effective in securing the organization.

Specific network security methods and devices include the following:

Implementation	Description
Firewall	<p>A <i>firewall</i> is a network device installed on the border of secured networks to protect a private network from a public network or to separate one private network from another.</p> <ul style="list-style-type: none"> <li>• Most firewalls use an access list to control traffic entering and leaving the trusted network environment.</li> <li>• Firewalls that use access lists filter traffic based on source or destination IP address, port number, service protocol, or application or service type.</li> <li>• Firewalls typically examine each packet separately, and make decisions on a single packet.</li> </ul>

	<p>Cisco implemented a brand of firewall products called <i>PIX firewalls</i>. PIX firewalls are being replaced by Cisco's Adaptive Security Appliance (ASA) line of devices.</p>
<p>Demilitarized zone (DMZ)</p>	<p>A <i>demilitarized zone</i> (DMZ), or screened subnet, is a subnet protected by two firewalls: the outer firewall screens traffic coming from the Internet, while the inner firewall controls the traffic that is allowed inside the private network. If the firewall managing traffic into the DMZ fails, only the servers in the DMZ are subject to compromise.</p>
<p>Adaptive Security Appliance (ASA)</p>	<p>Cisco's Adaptive Security Appliance (ASA) is a security appliance that provides a range of security features including:</p> <ul style="list-style-type: none"> <li>• <i>Anti-virus</i> tools prevent the transmission of known viruses (and other types of malware) based on signatures.</li> <li>• <i>Anti-spyware</i> tools scan network traffic to prevent the transmission of spyware programs.</li> <li>• <i>Anti-spam</i> tools examine and delete or segregate unwanted e-mail before it reaches the user.</li> <li>• <i>Anti-phishing</i> tools monitor URLs sent in messages through the network, looking for the fake URLs inherent in phishing attacks.</li> <li>• <i>URL filtering</i> prevents users from connecting to inappropriate sites based on URLs.</li> <li>• <i>E-mail filtering</i> prevents e-mail containing offensive materials from reaching the user, potentially protecting the enterprise from lawsuits.</li> </ul> <p>Because the names of several of the tools start with <i>anti-</i>, Cisco uses the term <i>anti-x</i> to refer to the whole of the class of security tools.</p> <p><b>Note:</b> Cisco's ASA hardware can act as a firewall. So when speaking about security, the term firewall still refers to the firewall functions, but today the Cisco product may be an older, still-installed PIX firewall or a new ASA.</p>
<p>Network Admission Control (NAC)</p>	<p>Network Admission Control (NAC), Cisco's version of Network Access Control, is an access control function that can restrict a device's access to the network to ensure network security. When a network device (such as a switch, router, access point, or DHCP server) is configured for NAC, it can force user or machine authentication prior to granting access to the network. It can also perform checks to ensure that the connecting device meets minimum standards for security such as having an installed antivirus software.</p>
<p>Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS)</p>	<p>An Intrusion Detection System (IDS) is a hardware or software device that examines the network to identify possible in-progress attacks.</p> <ul style="list-style-type: none"> <li>• A passive IDS looks for security breaches but effectively takes no action. A passive IDS can log suspicious activity and generate alerts if the attack is deemed to be severe. It is the network administrator's job to interpret the degree of the threat and to respond accordingly.</li> <li>• An active IDS (also called an Intrusion Prevention System or IPS) can also be configured to take specific actions when security breaches occur. If it detects a security breach or identifies possible in-progress attacks (such as a Denial of Service attack), the IPS will react to the attack and take measures to stop the attack altogether or prevent further damage from happening.</li> </ul>



	<p>Both an IDS or an IPS uses the following mechanisms for identifying attacks:</p> <ul style="list-style-type: none"> <li>• The <i>anomaly recognition engine</i> monitors normal traffic to define a standard activity pattern as normal.</li> <li>• The <i>signature recognition engine</i> looks for patterns in network traffic and compares it to known attack patterns called <i>signatures</i>.</li> </ul> <p>Network traffic is compared to the signature files for a match. If the traffic does not match a known signature, it is allowed. If the traffic matches a signature, the alert or action is triggered. One disadvantage to a signature-based IDS is the potential for errors:</p> <ul style="list-style-type: none"> <li>• A <i>false positive</i> means that the legitimate traffic was identified as malicious, and was not allowed. False positives result in lost data. An e-mail from a business associate identified as spam is an example of a false positive.</li> <li>• A <i>false negative</i> means that malicious traffic was not properly identified as malicious was allowed. Spam that is not caught but is delivered to your inbox is an example of a false negative.</li> </ul> <p>Be aware of the following:</p> <ul style="list-style-type: none"> <li>• Antivirus software is the most common form of a host-based IDS.</li> <li>• For adequate protection, keep the signature files up to date.</li> <li>• A false negative is typically worse than a false positive. A false negative allows malicious traffic that can cause damage, while a false positive only results in lost data that can be resent if required.</li> <li>• Unlike an access list that filters only on individual packets, IDS and IPS devices can look for patterns that cross multiple packets.</li> <li>• The actions that the IPS might take in response to an attack could expose you to legal risk. For example, a wireless IPS could spoof the attacker and send de-authentication frames to the wireless victim in response to a perceived threat. In the case of a litigation suit, you must provide proof that the incident was an attack and not just the result of a misconfiguration.</li> </ul>
Virtual Private Network (VPN)	<p>A Virtual Private Network (VPN) is a network that uses encryption to allow IP traffic to travel securely over the TCP/IP network. A VPN can be used over a local area network, across a WAN connection, over the Internet, and even between a client and a server over a dial-up connection through the Internet. VPNs work by using a <i>tunneling</i> protocol that wraps and encrypts packets in transit. Only the destination device can unwrap the packets to read them.</p>
Network Operation Center (NOC)	<p>A Network Operation Center (NOC) is one or more locations from which control is exercised over a computer or telecommunications network. Large organizations may operate more than one NOC, either to manage different networks or to provide geographic redundancy in the event of one site being unavailable or offline.</p>
Centralized Authentication	<p>Centralized authentication is where a protocol centrally validates or authenticates remote clients through user account names and passwords. Centralized authentication protocols include the following:</p>



- Remote Authentication Dial In User Service (RADIUS)
- Terminal Access Controller Access-Control System (TACACS)

Centralized authentication simplifies administration and reduces errors caused by needing to configure multiple devices.

## Network Hardening

As you study this section, answer the following questions:

- What is the most important method of protecting network devices?
- What measures should you take to increase the security of remote connections to your router?
- What benefits come from disabling the broadcast of CDP information?
- How do banners add to the security of a device?
- Why is SSH more secure than Telnet?

After finishing this section, you should be able to complete the following tasks:

- Configure a Cisco device to accept SSH remote connections.

This section covers the following exam objectives:

- 602. Explain general methods to mitigate common security threats to network devices, hosts, and applications
- 604. Describe security recommended practices including initial steps to secure network devices

### Hardening Facts

*Hardening* is the process of securing devices and software by reducing the security exposure and tightening security controls. Take the following general actions to secure your devices and network:

Security Measure	Description
Physical security	Ensure physical security by keeping network devices in a locked room. If someone can gain access to the physical Cisco device, they can easily bypass any configured passwords. Passwords are useless if physical access is not controlled.
Secure passwords	Use the following methods to secure Cisco device passwords: <ul style="list-style-type: none"><li>• Set the <b>enable secret</b> password instead of the enable password. Make sure the two passwords are different.</li><li>• Use the <b>service password-encryption</b> command to encrypt other passwords in the configuration file. This provides a low level of security, but passwords can be easily broken.</li></ul>
Control remote access	Secure remote access through the following actions: <ul style="list-style-type: none"><li>• Configure VTY passwords. Use the <b>login</b> command with a password to require a password. Use the <b>login</b> command without a password to prevent access.</li><li>• Configure SSH (Secure Shell) as an allowable (default) method for VTY lines.</li><li>• Use an access list on VTY lines to prevent access from specific locations.</li></ul>
Access lists	Use access lists to control incoming or outgoing traffic with the following criteria: <ul style="list-style-type: none"><li>• Source IP protocol (i.e. IP, TCP, UDP, etc.)</li><li>• Source hostname or host IP address</li><li>• Source or destination socket number</li></ul>

	<ul style="list-style-type: none"> <li>• Destination hostname or host IP address</li> <li>• Precedence or TOS values</li> </ul>
Banner	<p>Use the <b>banner</b> command to provide a warning banner to users who try to log into the router. Be aware of the following:</p> <ul style="list-style-type: none"> <li>• In some jurisdictions, civil and criminal prosecution of crackers who break into your systems is made much easier if you provide a banner that informs unauthorized users that their use is unauthorized.</li> <li>• In other jurisdictions, you can be forbidden to monitor the activities of even unauthorized users unless you have taken steps to notify them of your intent.</li> </ul>
CDP	<p>Use <b>no cdp run</b> on the device or <b>no cdp enable</b> on an interface to avoid sharing information about the Cisco device with neighboring devices. This helps to reduce exposure due to reconnaissance attacks.</p>

### SSH Configuration Facts

SSH (Secure Shell) is a secure and acceptable alternative to Telnet. SSH uses RSA public key cryptography for both connection and authentication. Use the following commands to configure SSH on a VTY line.

Use ...	To ...
<pre>router_name(config)#crypto key generate rsa</pre>	<p>Generate a matched public and private key pair, as well as a shared encryption key. To generate the key pair, the device must have both a hostname (other than <i>Router</i>) and an ip domain-name configured.</p>
<pre>router_name(config)#aaa new-model router_name(config)#username &lt;value&gt; password &lt;value&gt;</pre>	<p>Enable advanced security features for authentication and configure a local username and password that will be used for SSH authentication.</p>
<pre>router_name(config- line)#transport input ssh router_name(config- line)#transport input telnet router_name(config- line)#transport input telnet ssh</pre>	<p>Tell the device which type of connections to allow. Use the <b>telnet</b> or <b>ssh</b> keyword to identify the type of allowed access. Use both keywords to accept both access types.</p>

### Example

The following commands configure SSH to accept a username of **admin** with a password of **cisco**, allowing only SSH on lines VTY 0-4:

```
RouterA#config t
RouterA(config)#ip domain-name westsim.com
RouterA(config)#crypto key generate rsa
RouterA(config)#aaa new-model
RouterA(config)#username admin password cisco
RouterA(config)#line vty 0 4
RouterA(config-line)#transport input ssh
```

## Switch Port Security

As you study this section, answer the following questions:

- How does switch port security increase the security of your network?
- What does the **sticky** keyword do when used with the **switchport port-security** command?
- What can you do to save sticky addresses?
- How does switchport security differ from an access list?
- How does using VoIP effect switchport security settings?
- What is the difference between the **protect** and **restrict** violation actions?
- How does a switch identify which MAC addresses to allow if you do not manually configure the allowed addresses?

After finishing this section, you should be able to complete the following tasks:

- Configure switch port security.

This section covers the following exam objectives:

- 216. Implement basic switch security
- 604. Describe security recommended practices including initial steps to secure network devices

### **Port Security Facts**

Under normal circumstances, there are no restrictions on the devices that can be attached to a switch port. With switch port security, the devices that can connect to a switch through the port are restricted.

- Port security uses the MAC address to identify allowed and denied devices.
- By default, port security allows only a single device to connect through a switch port. You can, however, modify the maximum number of allowed devices.
- MAC addresses are stored in RAM in a table, and are identified with the port and by a MAC address type. Port security uses the following three MAC address types:

Type	Description
SecureConfigured	A SecureConfigured address is a MAC address that has been manually identified as an allowed address. The address is configured in interface mode and stored in the running-config file.
SecureDynamic	A SecureDynamic address is a MAC address that has been dynamically learned and allowed by the switch. <ol style="list-style-type: none"><li>1. When a device connects to the switch port, its MAC address is identified.</li><li>2. If the maximum number of allowed devices has not been reached, its MAC address is added to the table, and use of the port is allowed.</li></ol> <p>SecureDynamic addresses are only saved in the MAC address table in RAM, and are not added to the configuration file.</p>
SecureSticky	A SecureSticky address is a MAC address that is manually configured or dynamically learned and saved. With sticky learning enabled: <ol style="list-style-type: none"><li>3. When a device connects to the switch port, its MAC address is</li></ol>

	<p>identified.</p> <ol style="list-style-type: none"> <li>4. If the maximum number of allowed devices has not been reached, its MAC address is added to the table, and use of the port is allowed.</li> <li>5. The MAC address is automatically entered into the running-config file as a sticky address.</li> </ol> <p>Be aware of the following:</p> <ul style="list-style-type: none"> <li>○ You can manually configure an address and identify it as a sticky address.</li> <li>○ If you disable the sticky feature, all sticky addresses are converted to SecureDynamic addresses.</li> <li>○ If you enable the sticky feature, all SecureDynamic addresses are converted to SecureSticky addresses, even if they have been learned before the sticky feature was enabled.</li> </ul>
--	--

A *port violation* occurs when the maximum number of MAC addresses has been seen on the port, and an unknown MAC address is then seen.

You can configure the switch to take one of the following actions when a violation occurs:

- Shut down the port. This is the default setting.
- Drop all frames from unauthorized MAC addresses.
- Drop all frames and generate an SNMP trap.

Be aware of the following when using port security:

- You can only enable port security on an access port.
- Port security does not protect against MAC address spoofing (where an attacker changes the MAC address to match the MAC address of an allowed device).
- If you do not manually configure allowed MAC addresses for a port, the switch will allow the first MAC addresses it detects to connect, up to the maximum number.
- Once the maximum number of MAC addresses for a port has been reached, either through manual, dynamic, or sticky learning, no more MAC addresses will be allowed, and a violation will occur.
- Save the running-config file to the startup-config to make manually-configured and sticky addresses available when the system restarts. Otherwise, the switch will need to relearn sticky addresses.
- When using Voice-over-IP phones and workstations on a single port, increase the maximum allowed number above 1, allowing at least one MAC address for the phone and one for the workstation. The recommended value is 3.

### Port Security Configuration Facts

Each switch port has its own port security settings. To configure port security, take the following general actions:

- Explicitly configure the port as an *access* port.
- Enable switch port security.
- (Optional) Configure MAC addresses and other settings. When you enable port security, the following default settings are used:
  - A maximum of 1 device
  - Violation mode is shutdown
  - Dynamic learning is enabled, but sticky learning is disabled

Use the following commands to manage switch port security:

Command	Function
<code>switch(config-if)#switchport mode access</code>	Identifies the port as an access port. <b>Note:</b> You can only configure port security after explicitly making the port an access port.
<code>switch(config-if)#switchport port-security</code>	Enables port security. <b>Note:</b> You can enter port security commands for an interface without port security being enabled. However, port security will not be enforced (enabled) if this entry is missing.
<code>switch(config-if)#switchport port-security maximum &lt;1-8320&gt;</code>	Configures the maximum number of MAC addresses that can be allowed for a port. The default allows only a single MAC address per port. Use the <b>no</b> form of the command to reset the value to its default.
<code>switch(config-if)#switchport port-security mac-address sticky</code>	Enables sticky learning of MAC addresses. Without this command, addresses are dynamically learned but not recorded. With this command, learned addresses are added to the running-config file. Using the <b>no</b> form of the command disables sticky learning, removes any sticky entries from the configuration file, and converts the sticky addresses to dynamic addresses.
<code>switch(config-if)#switchport port-security mac-address h.h.h</code>	Identifies an allowed MAC address (h.h.h is a hexadecimal number).
<code>switch(config-if)#switchport port-security mac-address sticky h.h.h</code>	Identifies an allowed MAC address, making it a sticky address.
<code>switch(config-if)#switchport port-security violation action</code>	Identifies the action the switch will take when an unauthorized device attempts to use the port. Action keywords are: <ul style="list-style-type: none"> <li>• <b>protect</b> drops the frames from the unauthorized device</li> <li>• <b>restrict</b> does the same as <b>protect</b> and also generates an SNMP trap</li> <li>• <b>shutdown</b> disables the port</li> </ul>
<code>switch#errdisable recovery cause psecure-violation</code>	Recovers from a port security violation (enables disabled ports). You can also enable disabled ports by using the <b>shutdown/no shutdown</b> commands for the interface.

**Note:** You cannot configure more MAC addresses for a port than the maximum allowed number. To add more MAC addresses to an interface after the limit has been reached, increase the maximum number first or delete existing MAC addresses. This limitation applies to MAC addresses with or without the **sticky** parameter.

### Examples

The following commands configure switch port security to allow only host 5ab9.0012.02af to use Fast Ethernet port 0/12:

```
switch(config)#interface fast 0/12
switch(config-if)#switchport mode access
switch(config-if)#switchport port-security
switch(config-if)#switchport port-security mac-address 5ab9.0012.02af
```

The following commands configures Fast Ethernet port 0/15 to accept the first MAC address it receives as the allowed MAC address for the port:

```
switch(config)#interface fast 0/15
switch(config-if)#switchport mode access
switch(config-if)#switchport port-security
switch(config-if)#switchport port-security mac-address sticky
```

### Port Security Monitoring Facts

Use the following commands to verify port security operations:

Command	Description
switch#show port-security	Shows a summary of port security settings for enabled interfaces. Information includes: <ul style="list-style-type: none"> <li>• An interface that has port security enabled</li> <li>• The maximum allowed MAC addresses</li> <li>• The current number of MAC addresses allowed on the port</li> <li>• The number of security violations</li> <li>• The action to take for a violation</li> </ul>
switch#show port-security address	Shows a list of MAC addresses used by port security. Information includes: <ul style="list-style-type: none"> <li>• The MAC address</li> <li>• Its type (SecureConfigured, SecureDynamic, SecureSticky)</li> <li>• The associated interface</li> </ul>
switch#show port-security interface <type and number>	Shows detailed port security information for a specific interface. Shows all details included with the show port-security command and adds: <ul style="list-style-type: none"> <li>• Enabled or disabled state of port security on the interface</li> <li>• The port status</li> <li>• The total numbers of configured and sticky addresses</li> <li>• The MAC address and VLAN of the last device to use the port</li> </ul>

Listed below is a sample output from the **show port-security interface** command:

```
switch#show port-security interface fa0/3
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
```

```

SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0800.46f5.491c:1
Security Violation Count   : 1

```

Individual entries are explained in the following table:

Entry	Description
Port Security	Shows the enabled or the disabled state of port security. <ul style="list-style-type: none"> <li>• <b>Enabled</b> means that the switchport port-security command has been issued for the interface.</li> <li>• <b>Disabled</b> means that the interface is not enforcing port security. It does <i>not</i> mean that the interface is shut down or is not operational.</li> </ul>
Port Status	The port status indicates the operational status of the port as viewed by port security. A status of <b>Secure-down</b> could mean any of the following conditions: <ul style="list-style-type: none"> <li>• The interface has been shut down</li> <li>• There is no device connected to the interface</li> <li>• Port security is disabled, but the interface is operational and in use by a device</li> <li>• The interface has been disabled because of a port security violation</li> </ul> A status of <b>Secure-up</b> indicates that the line is operational and port security is being enforced.
Violation Mode	Identifies the configured violation mode for the interface (shutdown, protect, or restrict).
Maximum MAC Addresses	Identifies the configured maximum number of allowed devices.
Total MAC Addresses	Identifies the total number of known MAC addresses on this port. This includes all addresses in the running-config file (including sticky addresses) and all dynamic addresses that have been learned.
Configured MAC Addresses	Identifies the number of addresses configured with the <b>switchport port-security mac-address</b> command (excluding sticky addresses).
Sticky MAC Addresses	Identifies the number of addresses in the running-config file identified with the <b>switchport port-security mac-address sticky</b> entries.
Security Violation Count	Identifies the number of violations detected. If this value is anything other than 1, then the port has already taken the action specified by the Violation Mode line.



## Virtual Private Networks (VPNs)

As you study this section, answer the following questions:

- What is the difference between *confidentiality* and *integrity*?
- Which VPN technology is commonly used on Web servers?
- What is the main difference between a site-to-site VPN and a remote access VPN?
- Which IPSec protocol provides data confidentiality?
- Which IPSec mode is used for host-to-host communications?
- What are the client requirements for operating in full tunnel mode with the AnyConnect VPN Client? What advantages does full tunnel mode provide over the other modes?
- Which Cisco SSL VPN mode would you choose for a public computer? Why?

This section covers the following exam objectives:

- 805. Describe VPN technology

### VPN Facts

A Virtual Private Network (VPN) is a network that uses encryption to allow IP traffic to travel securely over the TCP/IP network.

- A VPN uses encrypted and authenticated links that provide remote access and routed connections between private networks or computers.
- A VPN can be used over a local area network, across a WAN connection, over the Internet, and even between a client and a server over a dial-up connection through the Internet.
- VPNs work by using a *tunneling* protocol that encrypts packet contents and wraps them in an unencrypted packet.
- Tunnel endpoints are devices that can encrypt and decrypt packets. When you create a VPN, you establish a security association between the two tunnel endpoints. These endpoints create a secure, virtual communication channel. Only the destination tunnel endpoint can unwrap packets and decrypt the packet contents.
- Routers use the unencrypted packet headers to deliver the packet to the destination device. Intermediate routers along the path cannot (and do not) read the encrypted packet contents.

Benefits provided by VPNs include the following:

- *Confidentiality* protects information or data from disclosure to unauthorized users.
- *Authentication* verifies that the sender of the VPN packet is a legitimate device and not a device used by an attacker.
- *Integrity* protects data against alteration during transmission.
- *Anti-replay* is a security service in which the receiver can reject old or duplicate packets in order to protect itself against replay attacks.
- *Non-repudiation* is when a third party can prove that a communication between two other parties took place. Non-repudiation is desirable if you want to be able to trace your communications and prove that they occurred.

The following table shows some common VPN security technologies:

Protocol	Description
Internet Protocol Security (IPSec)	IPSec is a security mechanism that: <ul style="list-style-type: none"><li>• Is the most widely deployed VPN technology</li><li>• Used with IP only and can encrypt any traffic supported by the IP protocol</li></ul>

	<ul style="list-style-type: none"> <li>Requires either digital certificates or pre-shared keys.</li> </ul>
Secure Sockets Layer (SSL)	<p>SSL is a communication protocol that:</p> <ul style="list-style-type: none"> <li>Provides secure Internet-based client/server interactions</li> <li>Authenticates the server to the client using public key cryptography and digital certificates and encrypts the entire communication session</li> <li>Protects Web (HTTP) traffic as well as Telnet, FTP, and e-mail</li> </ul>
Transport Layer Security (TLS)	<p>TLS is a communication protocol based on SSL that:</p> <ul style="list-style-type: none"> <li>Requires a digital certificate from <i>both</i> the client and server.</li> <li>Provides security for traffic above the Transport layer.</li> <li>Does <i>not</i> provide security for Web traffic at the Transport layer.</li> </ul>
Point-to-Point Tunneling Protocol (PPTP)	<p>PPTP is a Microsoft VPN technology that:</p> <ul style="list-style-type: none"> <li>Uses standard authentication protocols, such as Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).</li> <li>Supports TCP/IP only.</li> <li>Encapsulates other LAN protocols and carries the data securely over an IP network.</li> <li>Does not encrypt data. It must be used in conjunction with a Microsoft-supported encryption mechanism.</li> <li>Is supported by most operating systems and servers.</li> </ul>
Layer 2 Forwarding (L2F)	<p>L2F is a VPN technology developed by Cisco that:</p> <ul style="list-style-type: none"> <li>Offers mutual authentication</li> <li>Does not encrypt data</li> <li>Merged with PPTP to create L2TP</li> </ul>
Layer Two Tunneling Protocol (L2TP)	<p>L2TP is an open standard for secure multi-protocol routing that:</p> <ul style="list-style-type: none"> <li>Uses IPSec for encryption</li> <li>Supports multiple protocols (not just IP)</li> <li>Is not supported by older operating systems</li> </ul>

### Cisco VPN Facts

There are two basic types of Cisco VPNs:

Type	Description
<a href="#">Site-to-site</a>	<p><i>Site-to-site</i> VPNs connect entire networks to each other, for example, connecting a branch office network to a company headquarters network.</p> <ul style="list-style-type: none"> <li>All traffic between sites is encrypted using IP Security (IPsec).</li> <li>Hosts do not have VPN client software; they send and receive normal TCP/IP traffic through a VPN gateway, such as a Cisco Adaptive Security Appliance (ASA).</li> </ul>

	<ul style="list-style-type: none"> <li>• The VPN gateway is responsible for encapsulating and encrypting outbound traffic, sending it through a VPN tunnel over the Internet, to a peer VPN gateway at the target site.</li> <li>• The peer VPN gateway strips the headers of received packets, decrypts the content, and relays the packet towards the target host inside its private network.</li> </ul> <p>Implementations of site-to-site VPNs include:</p> <ul style="list-style-type: none"> <li>• <i>Intranet</i> VPNs provide secure connections within the same organization.</li> <li>• <i>Extranet</i> VPNs provide secure connections between two different organizations. Typically, an extranet VPN is used to connect a company's network to a third-party organization, such as customers, suppliers, partners, and other businesses.</li> </ul>
<a href="#">Remote access</a>	<p><i>Remote access</i> VPNs connect individual hosts to private networks, for example, travelers and telecommuters who need to access their company's network securely over the Internet.</p> <ul style="list-style-type: none"> <li>• Traffic between the host and target site is encrypted using IPSec or Secure Sockets Layer (SSL) technology.</li> <li>• The host is responsible for encapsulating and encrypting outbound traffic, sending it through a VPN tunnel over the Internet, to a peer VPN gateway at the target site.</li> <li>• The target VPN gateway behaves the same as site-to-site VPNs.</li> <li>• Hosts using IPSec encryption need VPN client software.</li> <li>• Hosts using SSL need a modern Internet browser (that includes built-in SSL support).</li> </ul>

Devices used in a VPN connection may include the following:

- An Adaptive Security Appliance (ASA) is Cisco's security appliance that is configured for many security functions, such as VPNs.
- Routers can provide VPN functions aside from packet forwarding, such as VPN encryption.
- PIX Firewalls are an older product line of Cisco. The firewall performs the VPN functions, as well as firewall functions. New installations now use an ASA.
- VPN accelerator cards are PCI cards that fit in Cisco devices, such as the PIX Firewall, to provide encryption, tunneling, and firewall functions.
- VPN concentrators are an older product line of Cisco, and provide a specific endpoint of a VPN tunnel.
- VPN client-side software is for access VPNs. It is software installed on the individual's client to perform the VPN functions.
- VPN client-side hardware is used to provide a VPN to multiple clients on the same device.

### IPSec VPN Facts

IPSec provides encryption for site-to-site and remote access VPNs. IPSec encrypts any traffic supported by the IP protocol, such as Internet, e-mail, Telnet, file transfer, as well as countless others. IPSec includes the following three protocols for authentication, data encryption, and connection negotiation:

Protocol	Description
Authentication Header (AH)	<p>Authentication Header (AH) provides integrity and authentication.</p> <ul style="list-style-type: none"> <li>• AH provides a message integrity check with the Hashed Keyed Message Authentication Code (HMAC). With HMAC, a symmetric key is</li> </ul>

	<p>embedded into a message before the message is hashed. When the message is received, the recipient's symmetric key is added back into the message before hashing the message. If the hash values match, message integrity is proven.</p> <ul style="list-style-type: none"> <li>• AH uses SHA-1 (Secure Hashing Algorithm 1) or MD5 (Message Digest v5) for integrity validation.</li> </ul> <p><b>Note:</b> AH does not encrypt data, so it does not provide confidentiality.</p>
Encapsulating Security Payload (ESP)	<p>Encapsulating Security Payload (ESP) provides encryption, integrity, anti-replay, and a weak form of authentication. ESP encrypts with the following standards:</p> <ul style="list-style-type: none"> <li>• Data Encryption Standard (DES) uses a 56-bit key and is easily broken.</li> <li>• Triple DES (3DES) applies DES three times and uses a 168-bit key. 3DES is IPSec's strongest and slowest method of encryption.</li> <li>• Advanced Encryption Standard (AES) uses variable key length (128-, 192-, or 256-bit keys), and is resistant to all known attacks. It is computationally more efficient than 3DES.</li> </ul> <p><b>Note:</b> If the VPN uses ESP, then the HMAC is not needed because the attacker would have had to break the ESP encryption key before altering the message.</p>
Internet Key Exchange (IKE)	<p>The Internet Key Exchange (IKE) negotiates the connection. As two end points are securing an IPSec network, they have to negotiate what is called a <i>Security Association</i> (SA). An inbound and outbound SA is necessary for each connection with a remote endpoint. IKE uses the following functions:</p> <ul style="list-style-type: none"> <li>• Internet Security Association Key Management Protocol (ISAKMP) establishes a framework for the negotiation.</li> <li>• The Diffie-Hellman key exchange generates symmetric keys used for the encryption of the negotiation of the SA. The Diffie-Hellman key exchange: <ul style="list-style-type: none"> <li>○ Provides for key distribution but does not provide any cryptographic services.</li> <li>○ Is based on calculating discreet logarithms in a finite field.</li> <li>○ Is used in many algorithms and standards such as DES.</li> <li>○ Is subject to man-in-the-middle attacks and requires strong authentication to validate the end points.</li> <li>○ Provides three key length configurations: DH-1 (768-bit key), DH-2 (1024-bit key), &amp; DH-5 (1536-bit key).</li> </ul> </li> </ul>

After the parameters of the SA have been established, IPSec functions in a mode of operation based on the relationship of the communicating devices to each other. The two IPSec modes of operation are:

Mode	Characteristics
Tunnel mode	<p><i>Tunnel</i> mode is used for site-to-site communications.</p> <ul style="list-style-type: none"> <li>• Tunnel mode is often referred to as <i>subnet-to-subnet</i>.</li> <li>• The entire data packet, including original headers, is encapsulated in a new packet when using IPSec in tunnel mode.</li> <li>• The new packet has a new unencrypted layer two and layer three header that contains the endpoint addresses and all necessary AH and ESP information.</li> <li>• The VPN server acts as a gateway by providing encryption support for other</li> </ul>

	devices on the LAN.
Transport mode	<p><i>Transport</i> mode is used for end-to-end (or host-to-host) data encryption.</p> <ul style="list-style-type: none"> <li>• The end communicating devices are the tunnel endpoints.</li> <li>• The packet data is encrypted, but the header is left intact, allowing intermediary devices (such as routers) to examine the packet header and use the information in routing packets.</li> <li>• Transport mode operates at layer four, encrypting from level four and up.</li> </ul>

## SSL VPN Facts

A remote access VPN can use Secure Sockets Layer (SSL) to encrypt VPN traffic. SSL encrypts the entire communication session between the server and client. *Cisco SSL VPN* (also known as *WebVPN*) is a technology that provides remote-access VPN capability by using the security features that are already built into a modern Internet browser. An SSL VPN allows users from any Internet-enabled location to launch an Internet browser to establish remote access VPN connections. There are three modes of Cisco SSL VPNs:

Mode	Description
Clientless	<p>A <i>clientless</i> SSL VPN (browser-based) allows a user to use any common Web browser to securely access the internal or corporate network. This mode is useful for accessing most content that you would expect to access in a browser, such as Web content, databases, and online tools that employ a Web interface.</p> <ul style="list-style-type: none"> <li>• Because SSL is already built in to the client Internet browsers, there is no setup required on the client side.</li> <li>• The client must run the Windows 2000, Windows XP, or Linux operating system.</li> <li>• Applications that cannot be accessed through a browser are not available.</li> </ul> <p>Use clientless SSL VPNs when the client is a public or private computer or when the user only needs to access Web-enabled applications.</p>
Thin-Client	<p>Cisco's <i>thin-client</i> SSL VPN (also referred to as <i>port forwarding</i>) downloads a small Java-based applet (plug-in) to the remote client which is used to secure remote access for Transmission Control Protocol (TCP) applications.</p> <ul style="list-style-type: none"> <li>• The remote client must allow the Java applet to download and install through the Internet browser. This typically requires administrative privileges on the system.</li> <li>• SSL tunnels can also be established using a <i>smart tunnel</i>. A smart tunnel does not require installation and therefore does not require administrative privileges.</li> <li>• Proxy services are an option with the thin-client mode. A <i>proxy</i> acts as an intermediary between the client and the Internet, intercepting all requests to the Internet to see if it can fulfill the request using its cache to improve performance. If the proxy service is enabled, the Java applet acts as a TCP proxy server through the Internet browser.</li> <li>• Applications such as FTP, where the ports are negotiated dynamically cannot be used. You can use TCP port forwarding only with applications that use static ports, such as: <ul style="list-style-type: none"> <li>○ Telnet, port 23</li> <li>○ Secure Shell (SSH), port 22</li> <li>○ Post Office Protocol 3 (POP3), port 110</li> <li>○ Internet Message Access Protocol 4 (IMAP4), port 143</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>○ Simple Mail Transfer Protocol (SMTP), port 25</li> <li>○ Microsoft Outlook Express</li> <li>○ Lotus Notes</li> </ul> <p>Microsoft Outlook using the MAPI protocol is not supported.</p> <ul style="list-style-type: none"> <li>● Thin-Client access can be used to access shared folders on network servers.</li> <li>● Local administrator privileges are required to install the Sun Microsystems Java Runtime Environment (JRE) and configure the local system. <b>Note:</b> The port-forwarding proxy works only with JRE version 1.4 or later versions. The Java applet verifies the JRE version and will refuse to run if a compatible JRE version is not detected.</li> </ul> <p>Use the Thin-Client SSL VPN to provide application access for applications that can be forwarded on a specific port and to provide access to shared folders on network servers. It typically cannot be used on a public computer because administrative privileges are required to download the Java plug-ins.</p>
Full Tunnel	<p><i>Full tunnel</i> mode downloads client-side VPN software to the remote workstation and allows secure access to most IP-based applications on an internal or corporate network.</p> <ul style="list-style-type: none"> <li>● The client software is called the AnyConnect VPN Client. Previous versions of the client software were called the Cisco SSL VPN Client (SVC).</li> <li>● The client software can be loaded on the security appliance, where it will download and install on the client automatically as needed. It can also be manually installed on the client prior to making the connection.</li> <li>● The client software can be uninstalled automatically when the session is closed, or it can be configured to remain on the system.</li> <li>● Local administrator privileges are required for the initial installation of the Cisco AnyConnect VPN Client.</li> <li>● AnyConnect uses TLS in addition to SSL to improve performance.</li> <li>● The client software can run as a standalone application (not running in the browser).</li> <li>● The client software supports IPv6, Windows Vista, running scripts, password caching, logon using certificates only, and drive mapping.</li> </ul> <p>Use the client software for VPN access to configure a permanent client, or to provide access to resources not allowed by the clientless or thin-client solutions (such as Microsoft Outlook using MAPI).</p>

Client requirements for SSL VPNs include:

- An SSL VPN account (username and password).
- An SSL VPN supported browser, such as Internet Explorer 6.0 or 7.0, FireFox 2.0, or Safari 2.0.3.
- Local administrative privileges for the thin-client and full tunnel installation requirements.

### VPN Implementation Facts

When implementing a VPN solution first consider the type of VPN you need:

Type	Description
Site-to-site	<p>Use a site-to-site VPN to connect multiple devices in a remote site to the local site.</p> <ul style="list-style-type: none"> <li>● Tunnel endpoints are configured on routers or security appliance devices at each site.</li> </ul>

	<ul style="list-style-type: none"> <li>• All site-to-site VPNs use IPsec.</li> <li>• IPsec tunnel mode is used.</li> <li>• No client configuration is required on individual hosts in each site.</li> </ul>
Remote access	<p>Use a remote access VPN to connect individual users to resources in your local site.</p> <ul style="list-style-type: none"> <li>• The tunnel endpoint is defined on the client on one end, and a router or security appliance at the site.</li> <li>• Remote access VPNs can use either IPsec or SSL VPN.</li> <li>• Client configuration is as follows: <ul style="list-style-type: none"> <li>○ When using IPsec, client software is required.</li> <li>○ SSL VPN in <i>clientless</i> mode requires only an SSL-enabled browser and no client configuration. It provides access to Web-applications only.</li> <li>○ SSL VPN in <i>thin-client</i> mode requires the Java runtime and the ability to download and install Java plug-ins. It provides access to TCP applications through port forwarding and shared folder content.</li> <li>○ SSL VPN in <i>full tunnel</i> mode uses client software that can be permanently or temporarily installed. It provides full remote access with features that require access to the local operating system.</li> </ul> </li> </ul>