RWANDA POLYTECHNIC
IPRC KARONGI
Integrated Polytechnic Regional College
P.O. Box85 KARONGI- RWANDA
Tel:+250 788871075
Email:info@iprcwest.ac.rw
www.iprckarongi.rp.ac.rw

Information Communication Technology Department

Large Networks

Program: Information Technology

Module code: ITLWN601

Module name: Large Networks Administration

Credits: 10

Year/ Level: RTQF lev VI, year2

Semester: one

Academic year: 2023/2024

Prerequisites: Small Networks or Introduction to networks

Module leader: Eng. HARERIMANA SOPHONIE San
Assistant Lecturer, RP/IPRC KARONGI.

December 2024

Purpose statement

This core module describes the skills, knowledge and attitude required to design, Configure and Administer Wide Network. The learner will be able to describe WAN concept, implement routing protocols, implement point to point protocol (PPP), configure VLAN, apply security network policies, apply quality of service to converged network and enable management protocols. He/she will also be able to select and arrange different materials, equipment and tools used when connecting large enterprise networks.

Copyright

Module Assessment criteria

Within this module, assessment criteria are used to evaluate the level of attainment students achieve against the learning outcomes. All assessment in Higher Education is criterion referenced, which means that students are assessed based on their performance against clearly stated criteria.

The assessment is added after detailed description of a topic. The practical exercises are attached to this document.

Table of Contents

LEARNING UNIT 1 - DESCRIBE WAN CONCEPT

Learning Outcomes: 1.1. Describe WAN technology
1.2. Describe private infrastructure
1.3. Describe public infrastructure

Networks allow people to communicate, collaborate, and interact in many ways. Networks are used to access web pages, talk using IP telephones, participate in video conferences, compete in interactive gaming, shop using the Internet, complete online coursework, and more.

Ethernet switches function at the data link layer, Layer 2, and are used to forward Ethernet frames between devices within the same network. However, when the source IP and destination IP addresses are on different networks, the Ethernet frame must be sent to a router.

A router connects one network to another network. The router is responsible for the delivery of packets across different networks. The destination of the IP packet might be a web server in another country or an email server on the local area network.

The router uses its routing table to determine the best path to use to forward a packet. It is the responsibility of the routers to deliver those packets in a timely manner. The effectiveness of internetwork communications depends, to a large degree, on the ability of routers to forward packets in the most efficient way possible.

When a host sends a packet to a device on a different IP network, the packet is forwarded to the default gateway because a host device cannot communicate directly with devices outside of the local network. The default gateway is the destination that routes traffic from the local network to devices on remote networks. It is often used to connect a local network to the Internet.

This chapter will answer the question, “What does a router do with a packet received from one network and destined for another network?” Details of the routing table will be examined, including connected, static, and dynamic routes.

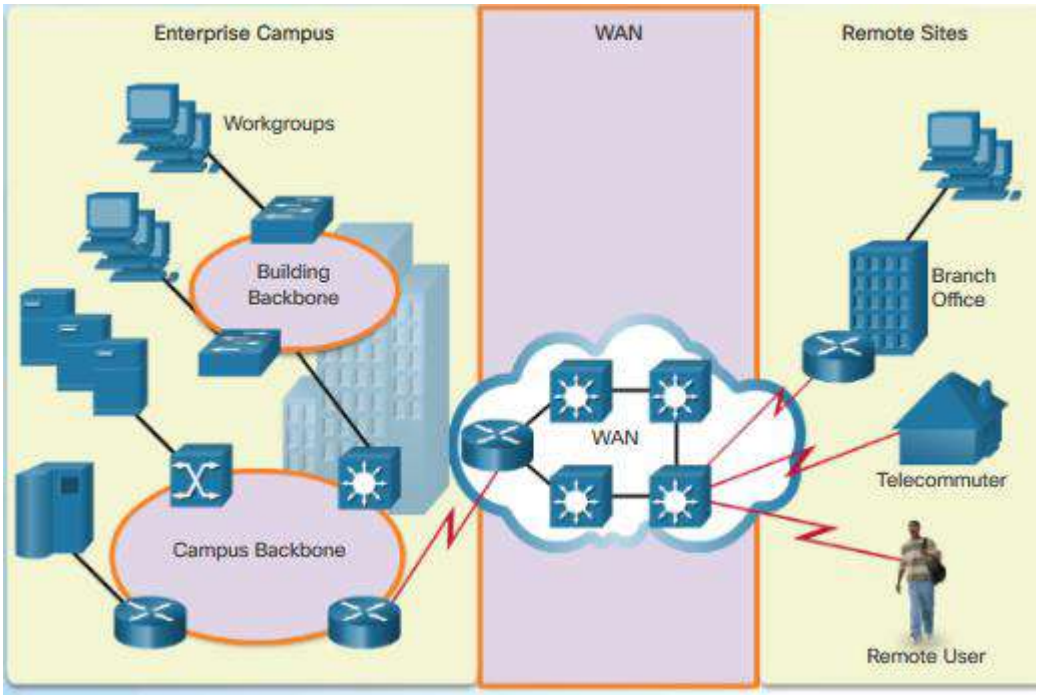
Because the router can route packets between networks, devices on different networks can communicate. This chapter will introduce the router, its role in networks, its main hardware and software components, and the routing process. Exercises which demonstrate how to access the router, configure basic router settings, and verify settings will be provided.

Learning Outcome 1.1: Describe Wan Technology

Businesses must connect LANs to provide communications between them, even when these LANs are far apart. Wide-area networks (WANs) are used to connect remote LANs. A WAN may cover a city, country, or global region. A WAN is owned by a service provider, and a business pays a fee to use the provider's WAN network services.

Different technologies are used for WANs than for LANs. This chapter introduces WAN standards, technologies, and purposes. It covers selecting the appropriate WAN technologies, services, and devices to meet the changing business requirements of an evolving enterprise.

A WAN operates beyond the geographic scope of a LAN. As shown in the figure, WANs are used to interconnect the enterprise LAN to remote LANs in branch sites and telecommuter sites.



A WAN is owned by a service provider. An organization must pay a fee to use the provider's network services to connect remote sites. WAN service providers include carriers, such as a telephone network, cable company, or satellite service. Service providers provide links to interconnect remote sites for the purpose of transporting data, voice, and video.

In contrast, LANs are typically owned by an organization and used to connect local computers, peripherals, and other devices within a single building or other small geographic are **WAN Topologies**

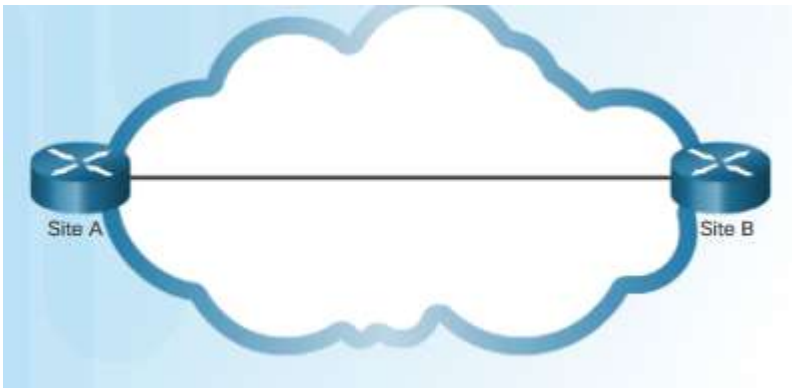
.

Interconnecting multiple sites across WANs can involve a variety of service provider technologies and WAN topologies. Common WAN topologies are:

- Point-to-Point
- Hub-and-Spoke
- Full Mesh

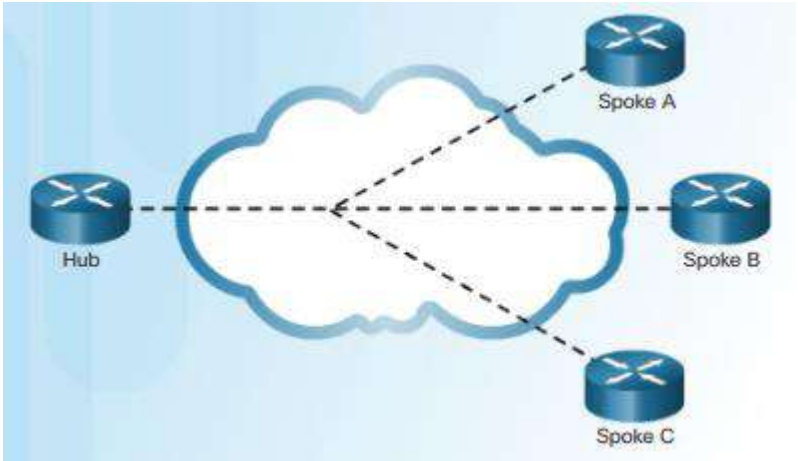
- Dual-Homed
- Point-to-Point

A point-to-point topology, as shown in Figure , employs a point-to-point circuit between two endpoints. Typically involving dedicated leased-line connections like T1/E1 lines, a point-to-point connection involves a Layer 2 transport service through the service provider network. Packets sent from one site are delivered to the other site and vice versa. A point-to-point connection is transparent to the customer network, as if there was a direct physical link between two endpoints.



Hub-and-Spoke

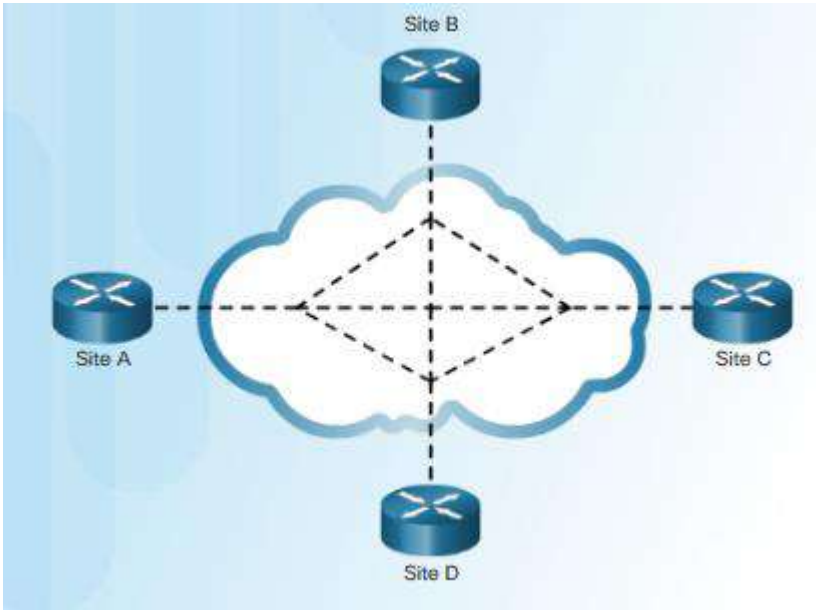
If a private network connection between multiple sites is required, then a point-to-point topology with multiple point-to-point circuits is one option. Each point-to-point circuit requires its own dedicated hardware interface which will require multiple routers with multiple WAN interface cards. This can be expensive. A less expensive option is a point-to-multipoint topology, also known as a hub and spoke topology.



With a hub-and-spoke topology a single interface to the hub can be shared by all spoke circuits. For example, spoke sites can be interconnected through the hub site using virtual circuits and routed subinterfaces at the hub. A hub-and-spoke topology is also an example of a single-homed topology. Figure displays a sample hub-and-spoke topology consisting of four routers with one router as hub connected to the other three spoke routers across a WAN cloud.

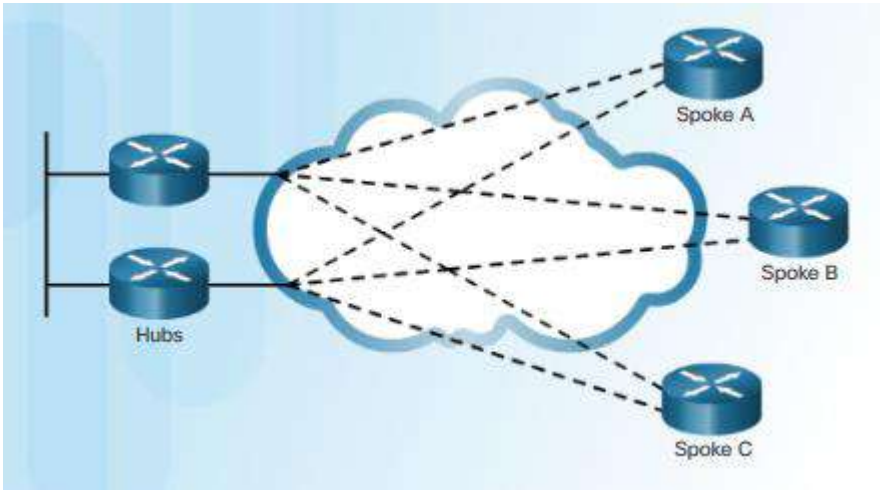
Full Mesh

One of the disadvantages of hub-and-spoke topologies is that all communication has to go through the hub. With a full mesh topology using virtual circuits, any site can communicate directly with any other site. The disadvantage here is the large number of virtual circuits that need to be configured and maintained. Figure displays a sample full mesh topology consisting of four routers connected to each other across a WAN cloud.



Dual-homed Topology

A dual-homed topology provides redundancy. As shown in Figure 4, two hub routers are dual-homed and redundantly attached to three spoke routers across a WAN cloud. The disadvantage to dual-homed topologies is that they are more expensive to implement than single-homed topologies. This is because they require additional networking hardware, like additional routers and switches. Dual-homed topologies are also more difficult to implement because they require additional, and more complex, configurations. However, the advantage of dual-homed topologies is that they offer enhanced network redundancy, load balancing, distributed computing or processing, and the ability to implement backup service provider connections.



WAN technology network type

Small Office

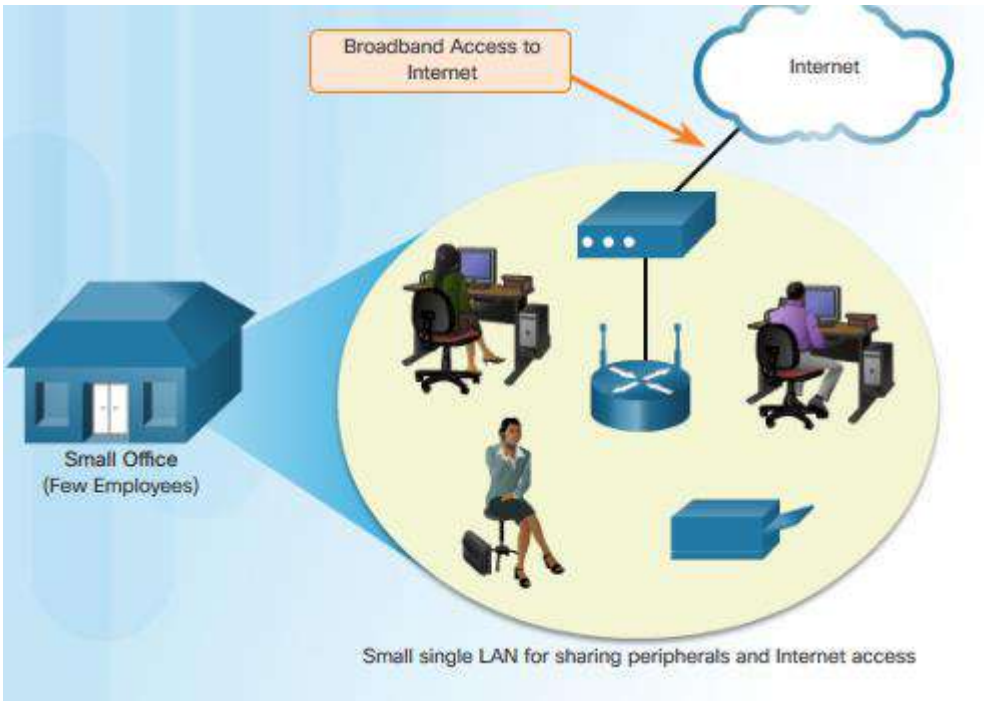
SPAN Engineering, an environmental consulting firm, has developed a special process for converting household waste into electricity and is developing a small pilot project for a municipal government in its local area. The company, which has been in business for four years, has grown to include 15 employees: six engineers, four computer-aided drawing (CAD) designers, a receptionist, two senior partners, and two office assistants.

SPAN Engineering's management is working to win full-scale contracts after the pilot project successfully demonstrates the feasibility of their process. Until then, the company must manage its costs carefully.

For their small office, SPAN Engineering uses a single LAN to share information between computers, and to share peripherals, such as a printer, a large-scale plotter (to print engineering drawings), and fax equipment. They have recently upgraded their LAN to provide inexpensive Voice over IP (VoIP) service to save on the costs of separate phone lines for their employees.

Connection to the Internet is through a common broadband service called Digital Subscriber Line (DSL), which is supplied by their local telephone service provider. With so few employees, bandwidth is not a significant problem.

The company cannot afford in-house IT support staff, and uses support services purchased from the DSL provider. The company also uses a hosting service rather than purchasing and operating its own FTP and email servers.



Campus Network

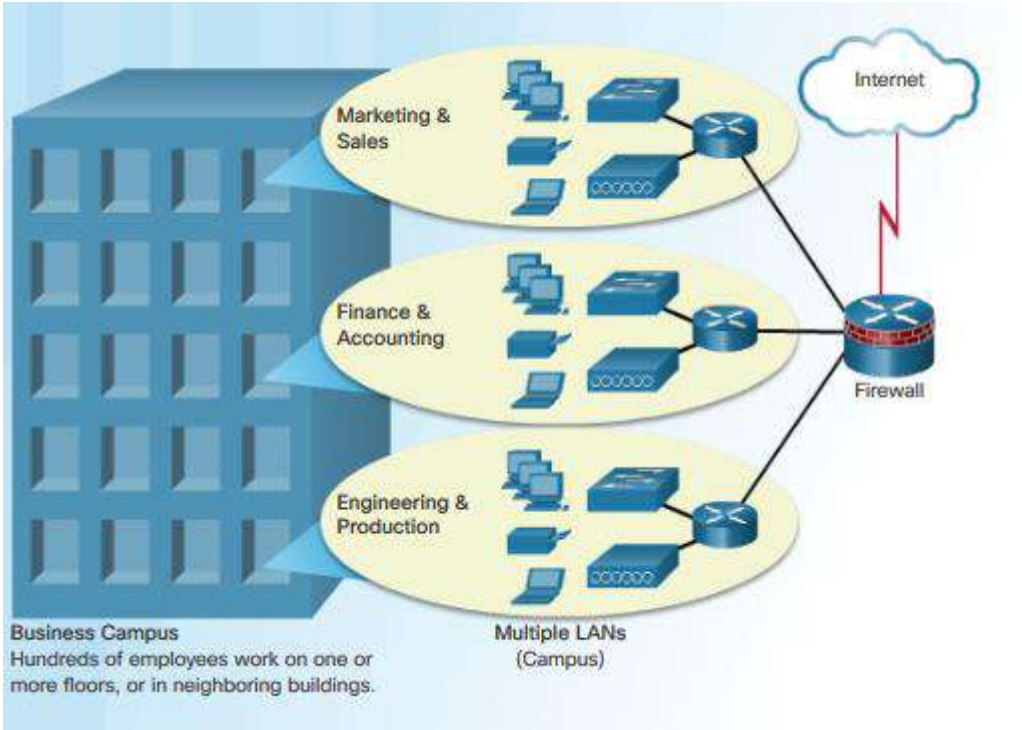
Five years later, SPAN Engineering has grown rapidly. The company was contracted to design and

implement a full-sized waste conversion facility soon after the successful implementation of their first pilot plant. Since then, SPAN has won other projects in neighboring municipalities, and in other parts of the country.

To handle the additional workload, the business has hired more staff and leased more office space. It is now a small- to medium-sized business with several hundred employees. Many projects are being developed at the same time, and each requires a project manager and support staff. The company has organized itself into functional departments, with each department having its own organizational team. To meet its growing needs, the company has moved into several floors of a larger office building.

As the business has expanded, the network has also grown. Instead of a single small LAN, the network now consists of several subnetworks, each devoted to a different department. For example, all the engineering staff is on one LAN, while the marketing staff is on another LAN. These multiple LANs are joined to create a company-wide network, or campus, which spans several floors of the building.

The business now has in-house IT staff to support and maintain the network. The network includes dedicated servers for email, data transfer, and file storage, and web-based productivity tools and applications. There is also a company intranet to provide in-house documents and information to employees. An extranet provides project information to designated customers.



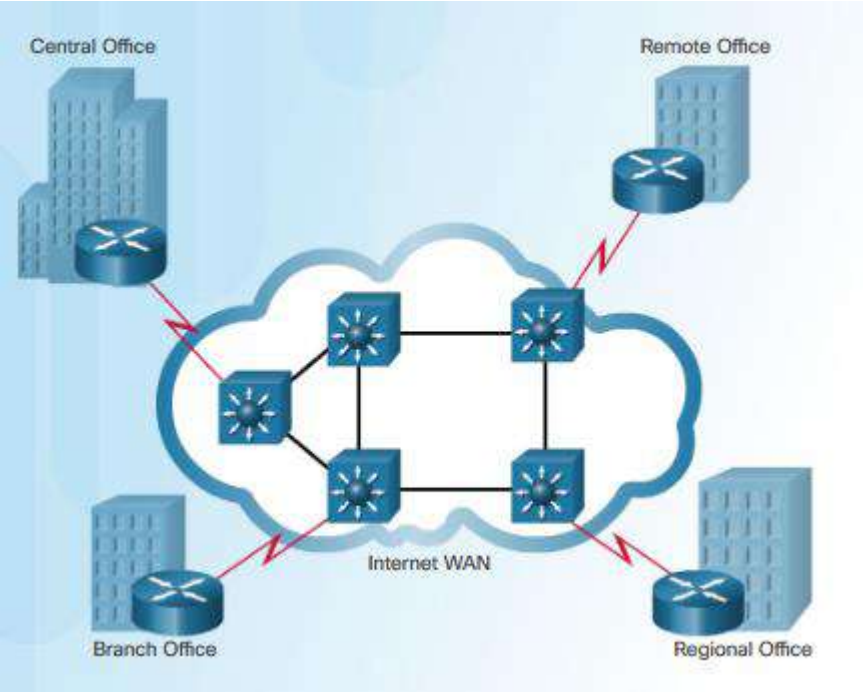
Branch Networks

Another six years later, SPAN Engineering has been so successful with its patented process that demand for its services has skyrocketed. New projects are underway in multiple cities. To manage those projects, the company has opened small branch offices closer to the project sites.

This situation presents new challenges to the IT team. To manage the delivery of information and services throughout the company, SPAN Engineering now has a data center, which houses the various

databases and servers of the company. To ensure that all parts of the business are able to access the same services and applications regardless of where the offices are located, the company must now implement a WAN.

For its branch offices that are in nearby cities, the company decides to use private dedicated lines through their local service provider. However, for those offices that are located in other countries, the Internet is an attractive WAN connection option. Although connecting offices through the Internet is economical, it introduces security and privacy issues that the IT team must address.



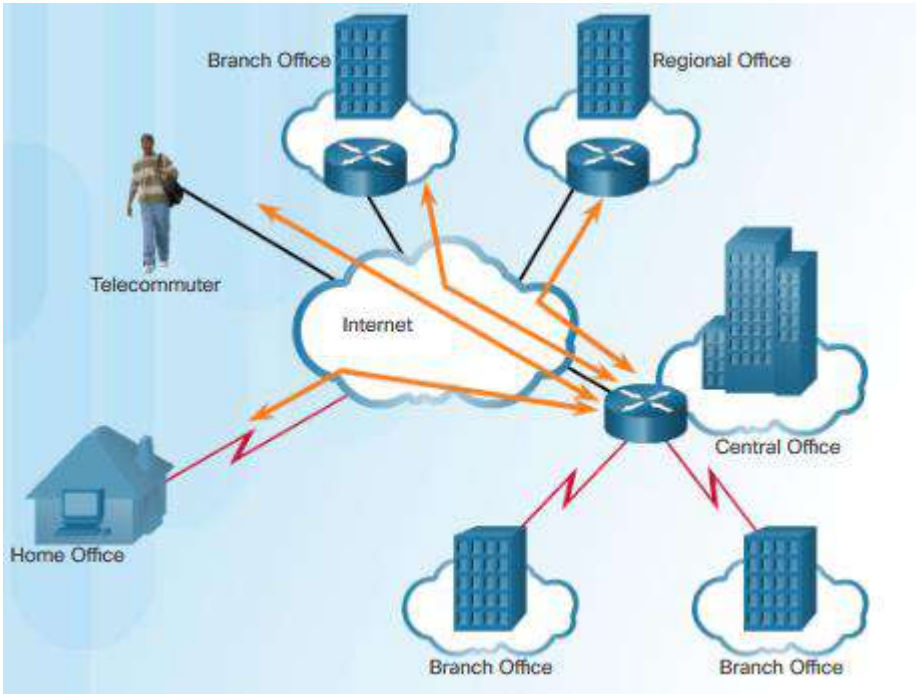
Distributed Network

SPAN Engineering has now been in business for 20 years and has grown to thousands of employees distributed in offices worldwide, as shown in Figure 1. The cost of the network and its related services is a significant expense. The company is looking to provide its employees with the best network services at the lowest cost. Optimized network services would allow each employee to work at a high rate of efficiency.

To increase profitability, SPAN Engineering must reduce its operating expenses. It has relocated some of its office facilities to less expensive areas. The company is also encouraging teleworking and virtual teams. Web-based applications, including web-conferencing, e-learning, and online collaboration tools, are being used to increase productivity and reduce costs. Site-to-site and remote access Virtual Private Networks (VPNs) enable the company to use the Internet to connect easily and securely with employees and facilities around the world. To meet these requirements, the network must provide the necessary converged services and secure Internet WAN connectivity to remote offices and individuals, as shown in Figure 2.

As seen in this example, network requirements of a company can change dramatically as the company

grows over time. Distributing employees saves costs in many ways, but it puts increased demands on the network. Not only must a network meet the day-to-day operational needs of the business, but it must be able to adapt and grow as the company changes. Network designers and administrators meet these challenges by carefully choosing network technologies, protocols, and service providers. They must also optimize their networks by using many of the network design techniques and architectures described in this course.



WANs in the OSI Model

WAN operations focus primarily on the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2). WAN access standards typically describe both physical layer delivery methods and data link layer requirements. The data link layer requirements include physical addressing, flow control, and

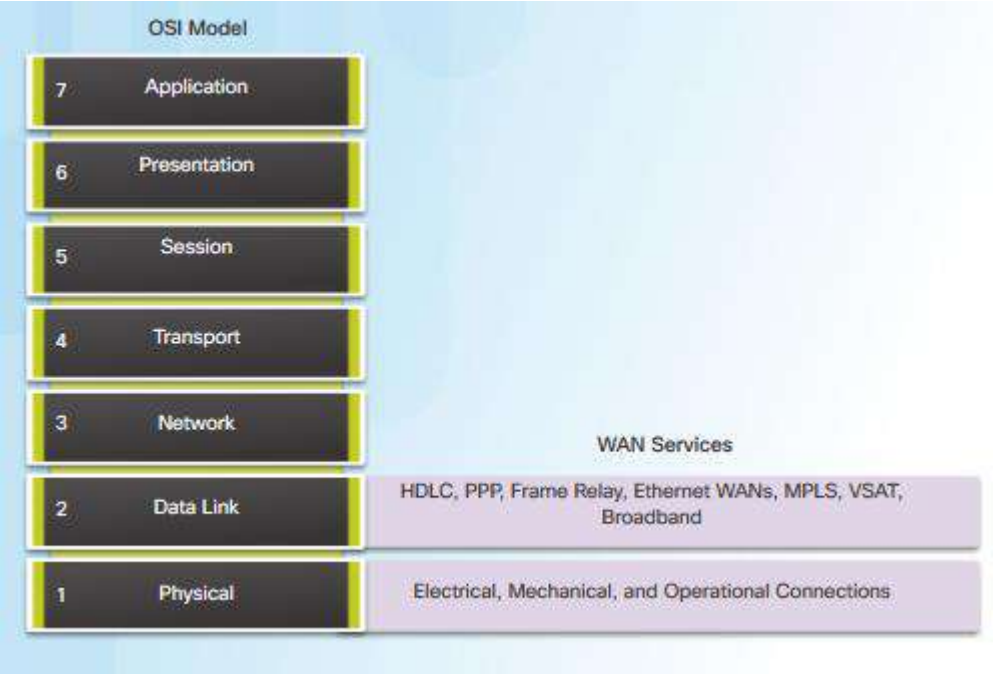
encapsulation.

- WAN access standards are defined and managed by a number of recognized authorities:
- Telecommunications Industry Association and the Electronic Industries Alliance (TIA/EIA)
- International Organization for Standardization (ISO)
- Institute of Electrical and Electronics Engineers (IEEE)

Layer 1 protocols describe how to provide electrical, mechanical, operational, and functional connections to the services of a communications service provider.

Layer 2 protocols define how data is encapsulated for transmission toward a remote location, and the mechanisms for transferring the resulting frames. A variety of different technologies are used, such as the Point-to-Point Protocol (PPP), Frame Relay, and ATM. Some of these protocols use the same basic framing or a subset of the High-Level Data Link Control (HDLC) mechanism.

Most WAN links are point-to-point. For this reason, the address field in the Layer 2 frame is usually not used.



Common WAN Terminology

One primary difference between a WAN and a LAN is that a company or organization must subscribe to an outside WAN service provider to use WAN carrier network services. A WAN uses data links provided by carrier services to access the Internet and connect different locations of an organization to each other. These data links also connect to locations of other organizations, to external services, and to remote users.

The physical layer of a WAN describes the physical connections between the company network and the service provider network. The figure illustrates the terminology commonly used to describe WAN

connections:

Customer Premises Equipment (CPE) - The CPE consists of the devices and inside wiring located on the enterprise edge connecting to a carrier link. The subscriber either owns the CPE or leases the CPE from the service provider. A subscriber, in this context, is a company that arranges for WAN services from a service provider.

Data Communications Equipment (DCE) - Also called data circuit-terminating equipment, the DCE consists of devices that put data on the local loop. The DCE primarily provides an interface to connect subscribers to a communication link on the WAN cloud.

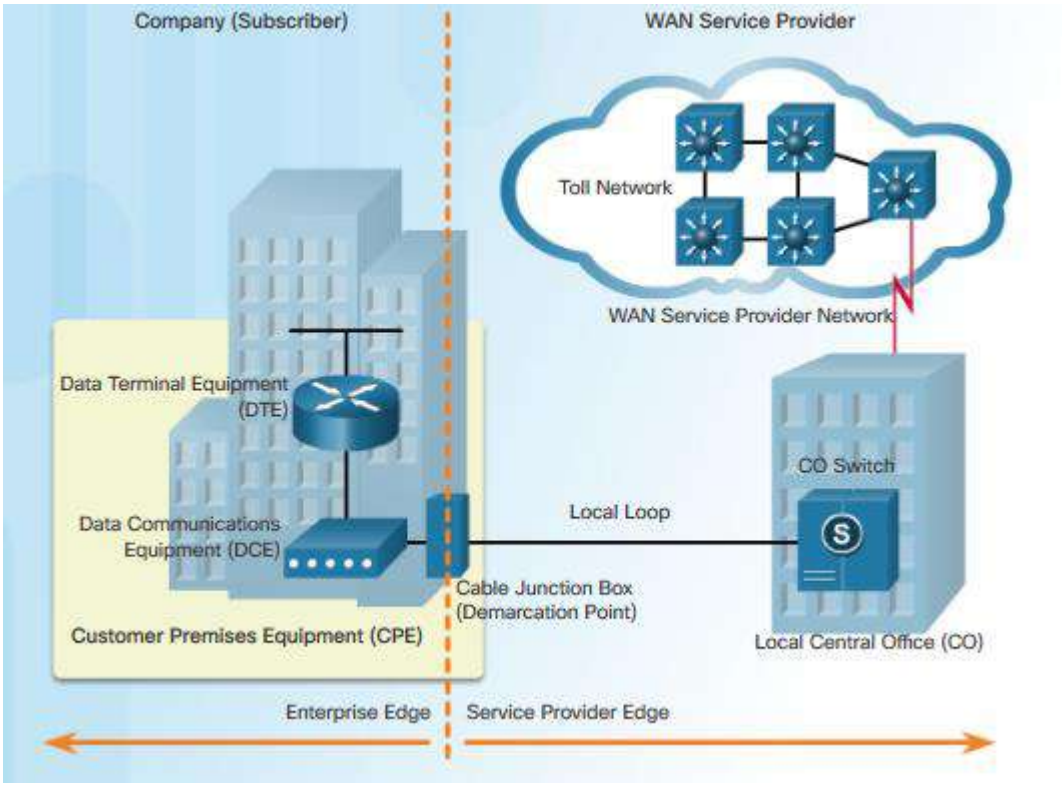
Data Terminal Equipment (DTE) - The customer devices that pass the data from a customer network or host computer for transmission over the WAN. The DTE connects to the local loop through the DCE.

Demarcation Point – This is a point established in a building or complex to separate customer equipment from service provider equipment. Physically, the demarcation point is the cabling junction box, located on the customer premises, that connects the CPE wiring to the local loop. It is usually placed for easy access by a technician. The demarcation point is the place where the responsibility for the connection changes from the user to the service provider. When problems arise, it is necessary to determine whether the user or the service provider is responsible for troubleshooting or repair.

Local Loop - The actual copper or fiber cable that connects the CPE to the CO of the service provider. The local loop is also sometimes called the "last-mile".

Central Office (CO) - The CO is the local service provider facility or building that connects the CPE to the provider network.

Toll network - This consists of the long-haul, all-digital, fiber-optic communications lines, switches, routers, and other equipment inside the WAN provider network.



WAN Devices

There are many types of devices that are specific to WAN environments:

Dialup modem - Voiceband modems are considered to be a legacy WAN technology. A voiceband modem converts (i.e., modulates) the digital signals produced by a computer into voice frequencies. These frequencies are then transmitted over the analog lines of the public telephone network. On the other side of the connection, another modem converts the sounds back into a digital signal (i.e., demodulates) for input to a computer or network connection.

Access server – This server controls and coordinates dialup modem, dial-in and dial-out user communications. Considered to be a legacy technology, an access server may have a mixture of analog and digital interfaces and support hundreds of simultaneous users.

Broadband modem - A type of digital modem used with high-speed DSL or cable Internet service. Both operate in a similar manner to the voiceband modem, but use higher broadband frequencies and transmission speeds.

CSU/DSU - Digital-leased lines require a CSU and a DSU. A CSU/DSU can be a separate device like a modem or it can be an interface on a router. The CSU provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The DSU converts the line frames into frames that the LAN can interpret and vice versa.

WAN switch - A multiport internetworking device used in service provider networks. These devices typically switch traffic, such as Frame Relay or ATM, and operate at Layer 2.

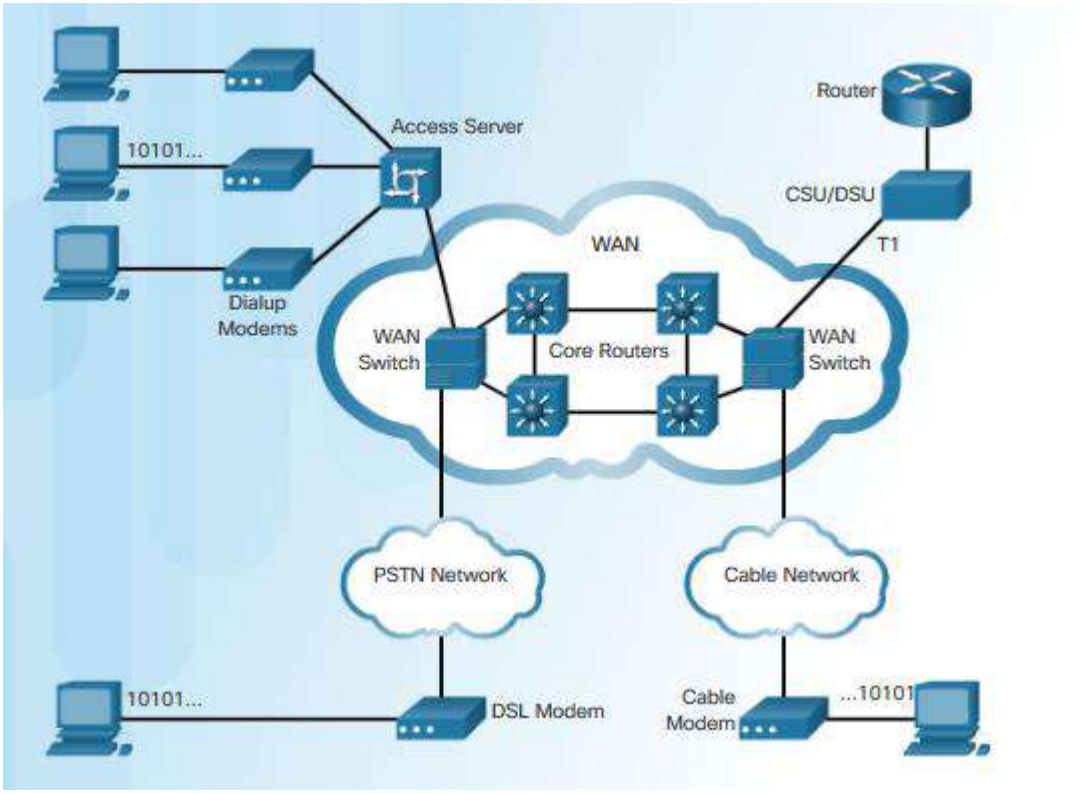
Router - Provides internetworking and WAN access interface ports that are used to connect to the service provider network. These interfaces may be serial connections, Ethernet, or other WAN

interfaces. With some types of WAN interfaces, an external device, such as a DSU/CSU or modem (analog, cable, or DSL), is required to connect the router to the local service provider.

Core router/Multilayer switch - A router or multilayer switch that resides within the middle or backbone of the WAN, rather than at its periphery. To fulfill this role, a router or multilayer switch must be able to support multiple telecommunications interfaces of the highest speed used in the WAN core. It must also be able to forward IP packets at full speed on all of those interfaces. The router or multilayer switch must also support the routing protocols being used in the core.

Note: The preceding list is not exhaustive and other devices may be required, depending on the WAN access technology chosen.

WAN technologies are either circuit-switched or packet-switched. The type of devices used depends on the WAN technology implemented.



Circuit Switching

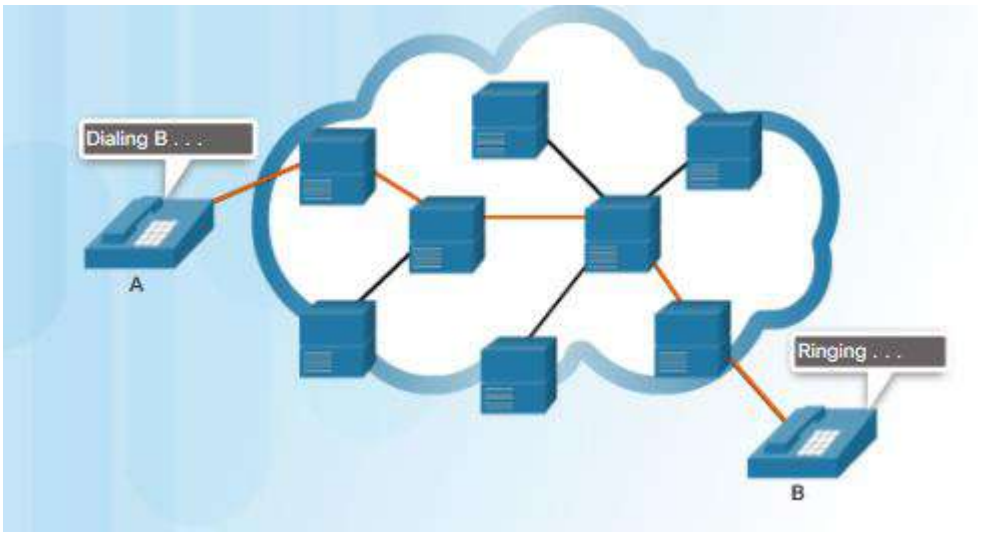
A circuit-switched network is one that establishes a dedicated circuit (or channel) between nodes and terminals before the users may communicate. Specifically, circuit switching dynamically establishes a dedicated virtual connection for voice or data between a sender and a receiver. Before communication can start, it is necessary to establish the connection through the network of the service provider.

As an example, when a subscriber makes a telephone call, the dialed number is used to set switches in the exchanges along the route of the call so that there is a continuous circuit from the caller to the called

party. Because of the switching operation used to establish the circuit, the telephone system is called a circuit-switched network. If the telephones are replaced with modems, then the switched circuit is able to carry computer data.

If the circuit carries computer data, the usage of this fixed capacity may not be efficient. For example, if the circuit is used to access the Internet, there is a burst of activity on the circuit while a web page is transferred. This could be followed by no activity while the user reads the page, and then another burst of activity while the next page is transferred. This variation in usage between none and maximum is typical of computer network traffic. Because the subscriber has sole use of the fixed capacity allocation, switched circuits are generally an expensive way of moving data.

The two most common types of circuit-switched WAN technologies are the public switched telephone network (PSTN) and the Integrated Services Digital Network (ISDN).



Packet Switching

In contrast to circuit switching, packet switching splits traffic data into packets that are routed over a shared network. Packet-switching networks do not require a circuit to be established, and they allow many pairs of nodes to communicate over the same channel.

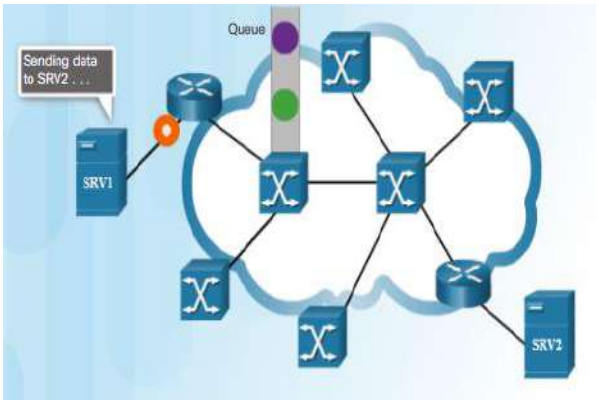
The switches in a packet-switched network (PSN) determine the links that packets must be sent over based on the addressing information in each packet. The following are two approaches to this link determination:

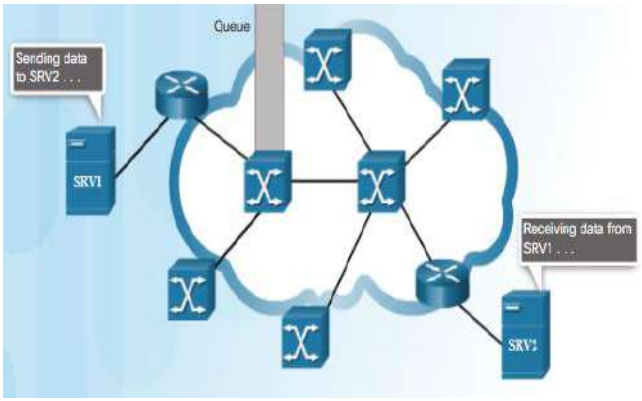
Connectionless systems - Full addressing information must be carried in each packet. Each switch must evaluate the address to determine where to send the packet. An example of a connectionless system is the Internet.

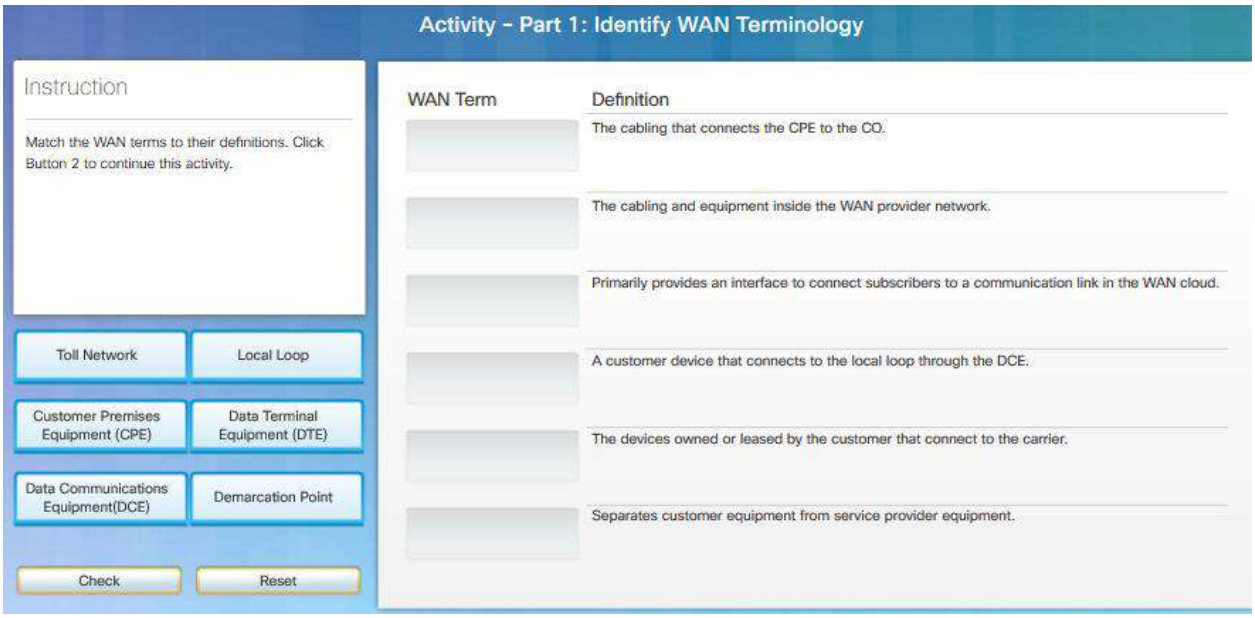
Connection-oriented systems - The network predetermines the route for a packet, and each packet only has to carry an identifier. The switch determines the onward route by looking up the identifier in tables held in memory. The set of entries in the tables identifies a particular route or circuit through the system. When the circuit is established temporarily while a packet is traveling through it, and then breaks down again, it is called a virtual circuit (VC). An example of a connection-oriented system is

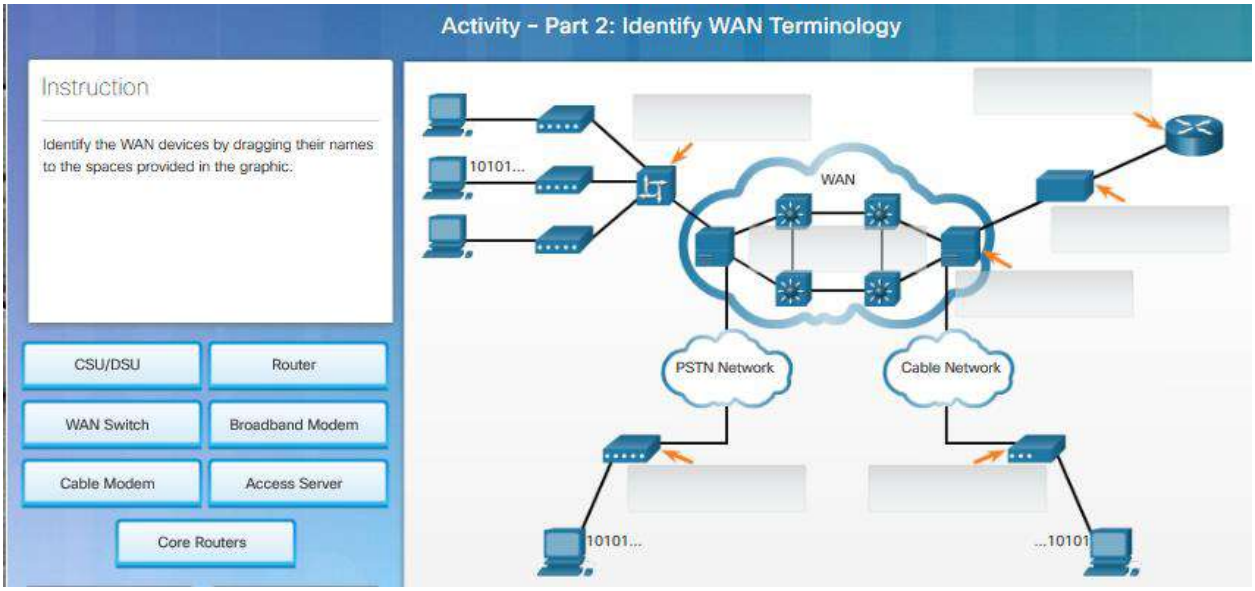
Frame Relay. In the case of Frame Relay, the identifiers used are called data-link connection identifiers (DLCIs).

Because the internal links between the switches are shared between many users, the cost of packet switching is lower than that of circuit switching. However, delays (latency) and variability of delay (jitter) are greater in packet-switched networks than in circuit-switched networks. This is because the links are shared, and packets must be entirely received at one switch before moving to the next. Despite the latency and jitter inherent in shared networks, modern technology allows satisfactory transport of voice and video communications on these networks.



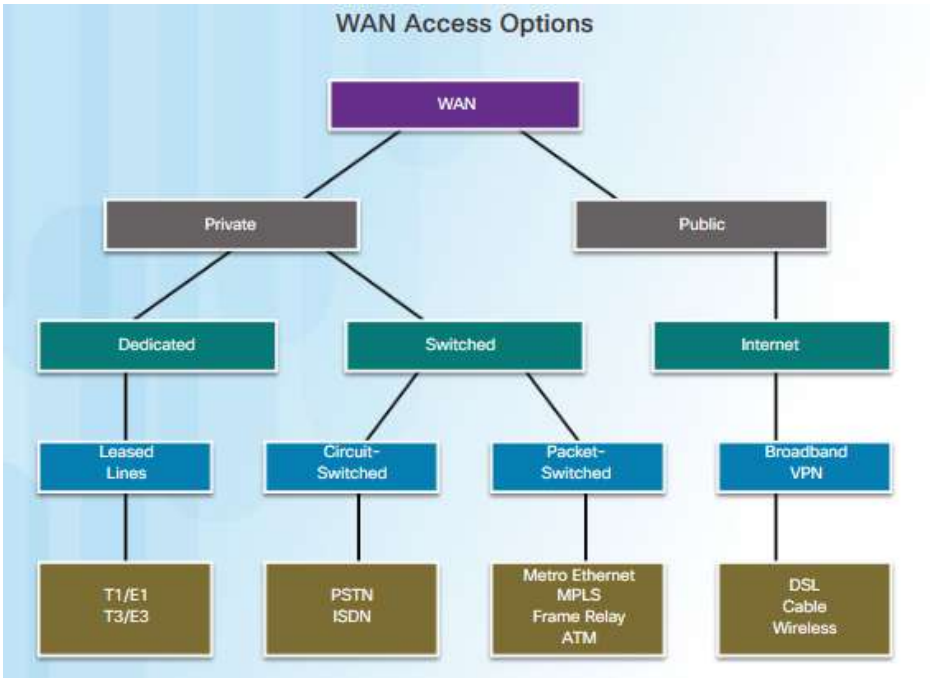






WAN Link Connection Options

There are several WAN access connection options that ISPs can use to connect the local loop to the enterprise edge. These WAN access options differ in technology, speed, and cost. Each has distinct advantages and disadvantages. Familiarity with these technologies is an important part of network design.

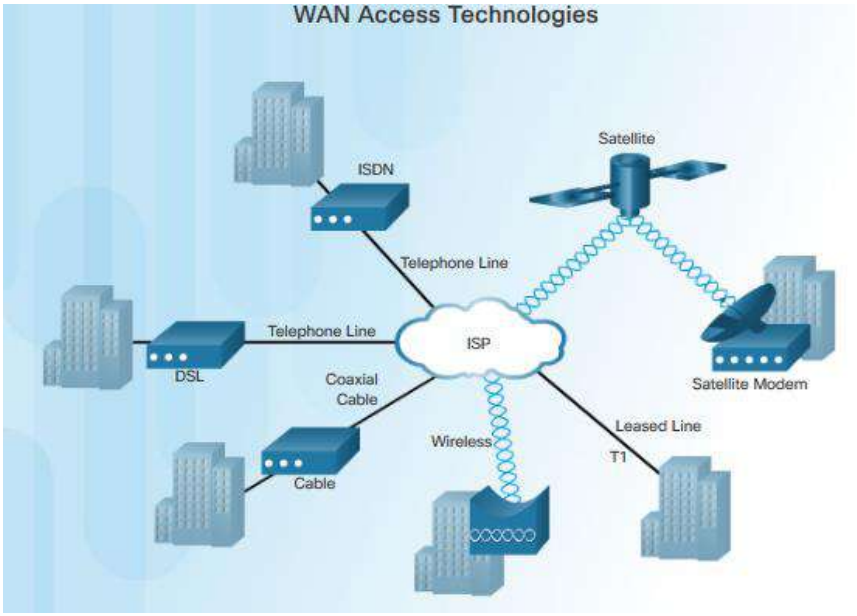


As shown in Figure , there are two way that an enterprise can get WAN access:

Private WAN infrastructure - Service providers may offer dedicated point-to-point leased lines, circuit-switched links, such as PSTN or ISDN, and packet-switched links, such as Ethernet WAN, ATM, or Frame Relay.

Public WAN infrastructure - Service providers may offer broadband Internet access using digital subscriber line (DSL), cable, and satellite access. Broadband connection options are typically used to

connect small offices and telecommuting employees to a corporate site over the Internet. Data travelling between corporate sites over the public WAN infrastructure should be protected using VPNs.



Service Provider Network Infrastructure

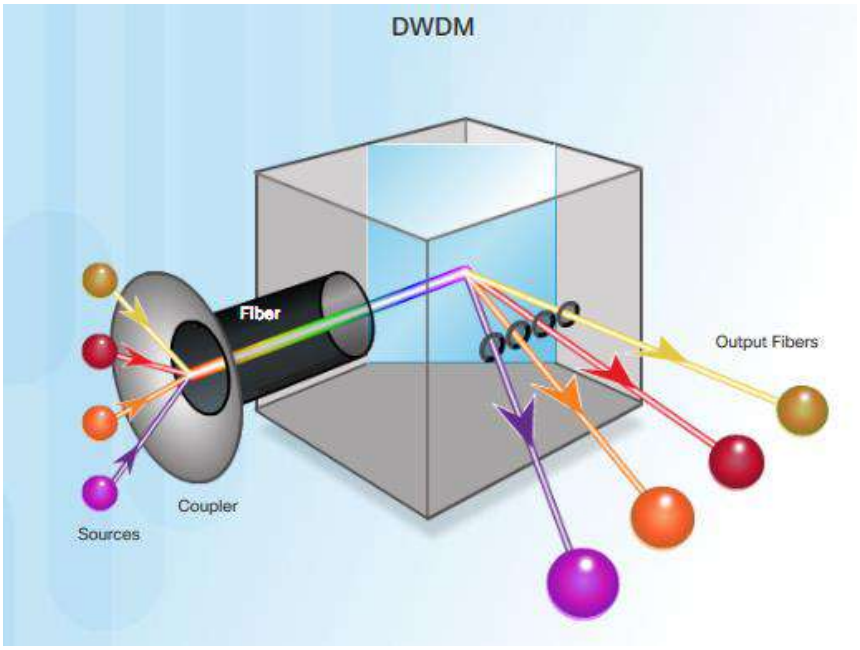
When a WAN service provider receives data from a client at a site, it must forward the data to the remote site for final delivery to the recipient. In some cases, the remote site may be connected to the same service provider as the originating site. In other cases, the remote site may be connected to a different ISP, and the originating ISP must pass the data to the connecting ISP.

Long-range communications are usually those connections between ISPs, or between branch offices in very large companies.

Service provider networks are complex. They consist mostly of high-bandwidth fiber-optic media, using either the Synchronous Optical Networking (SONET) or Synchronous Digital Hierarchy (SDH) standard. These standards define how to transfer multiple data, voice, and video traffic over optical fiber using lasers or light-emitting diodes (LEDs) over great distances.

Note: SONET is an American-based ANSI standard, while SDH is a European-based ETSI and ITU standard. Both are essentially the same and, therefore, often listed as SONET/SDH.

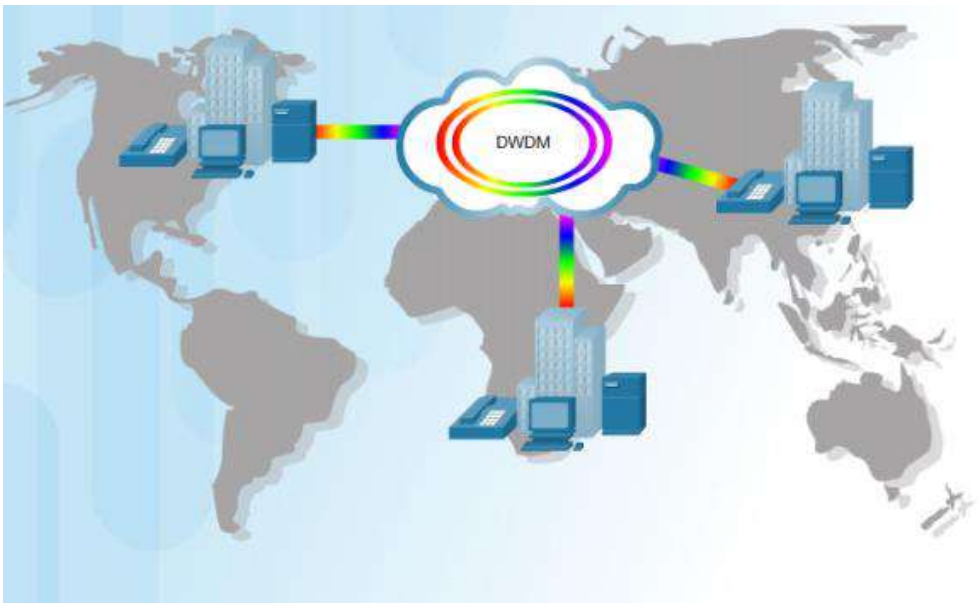
A newer fiber-optic media development for long-range communications is called dense wavelength division multiplexing (DWDM). DWDM multiplies the amount of bandwidth that a single strand of fiber can support, as shown in Figure .

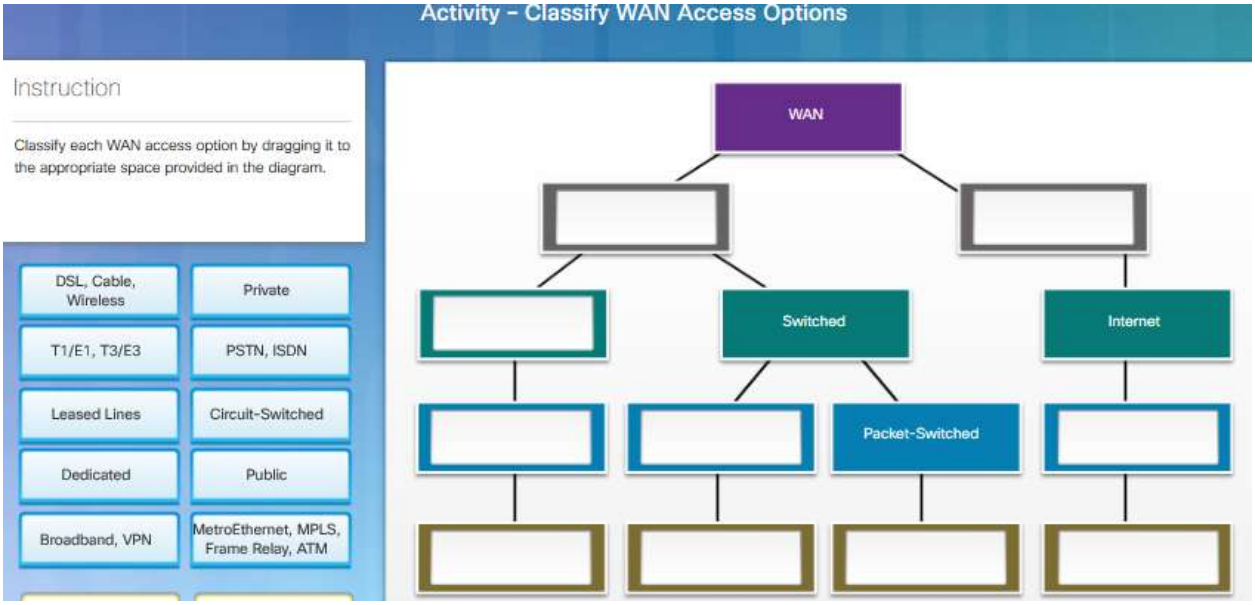


There are several ways that DWDM enables long-range communication:

- Enables bidirectional communications over one strand of fiber.
- Can multiplex more than 80 different channels of data (i.e., wavelengths) onto a single fiber.
- Each channel is capable of carrying a 10 Gb/s multiplexed signal.
- Assigns incoming optical signals to specific wavelengths of light (i.e., frequencies).
- Can amplify these wavelengths to boost the signal strength.
- Supports SONET and SDH standards.

DWDM circuits are used in all modern submarine communications cable systems and other long-haul circuits,





Exercise 01

Draw Your Concept of the Internet Now

In this activity, you will use the knowledge you have acquired throughout Chapter 1, and the modeling activity document that you prepared at the beginning of this chapter. You may also refer to the other activities completed in this chapter, including Packet Tracer activities.

Draw a map of the Internet as you see it now. Use the icons presented in the chapter for media, end devices, and intermediary devices.

In your revised drawing, you may wish to include some of the following:

• WANs

• LANs

• Cloud computing

• Internet Service Providers (tiers)

Save your drawing in hard-copy format. If it is an electronic document, save it to a server location provided by your instructor. Be prepared to share and explain your revised work in class.

Learning outcome 1.2: Describe private infrastructure

Leased Lines

When permanent dedicated connections are required, a point-to-point link is used to provide a pre-established WAN communications path from the customer premises to the provider network. Point-to-point lines are usually leased from a service provider and are called leased lines.

Leased lines have existed since the early 1950s and for this reason, are referred to by different names such as leased circuits, serial link, serial line, point-to-point link, and T1/E1 or T3/E3 lines. The term leased line refers to the fact that the organization pays a monthly lease fee to a service provider to use the line. Leased lines are available in different capacities and are generally priced based on the bandwidth required and the distance between the two connected points.

In North America, service providers use the T-carrier system to define the digital transmission capability of a serial copper media link, while Europe uses the E-carrier system, as shown in the figure. For instance, a T1 link supports 1.544 Mb/s, an E1 supports 2.048 Mb/s, a T3 supports 43.7 Mb/s, and an E3 connection supports 34.368 Mb/s. Optical Carrier (OC) transmission rates are used to define the digital transmitting capacity of a fiber-optic network.

There are advantages to the use of leased lines:

Simplicity - Point-to-point communication links require minimal expertise to install and maintain.

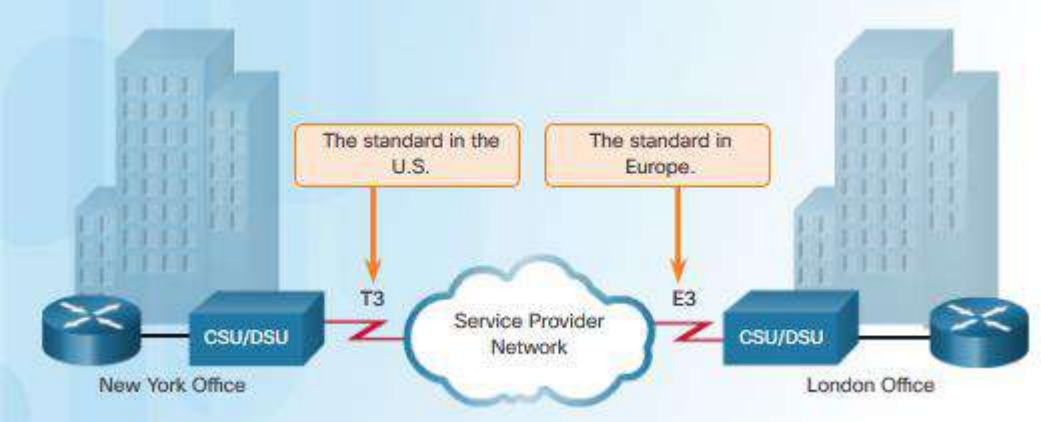
Quality - Point-to-point communication links usually offer high service quality, if they have adequate bandwidth. The dedicated capacity removes latency or jitter between the endpoints.

Availability - Constant availability is essential for some applications, such as e-commerce. Point-to-point communication links provide permanent, dedicated capacity which is required for VoIP or Video over IP.

There are also disadvantages to the use of leased lines:

Cost - Point-to-point links are generally the most expensive type of WAN access. The cost of leased line solutions can become significant when they are used to connect many sites over increasing distances. In addition, each endpoint requires an interface on the router, which increases equipment costs.

Limited flexibility - WAN traffic is often variable, and leased lines have a fixed capacity, so that the bandwidth of the line seldom matches the need exactly. Any change to the leased line generally requires a site visit by ISP personnel to adjust capacity.



Dialup

Dialup WAN access may be required when no other WAN technology is available. For example, a remote location could use modems and analog dialed telephone lines to provide low capacity and dedicated switched connections. Dialup access is suitable when intermittent, low-volume data transfers are needed.

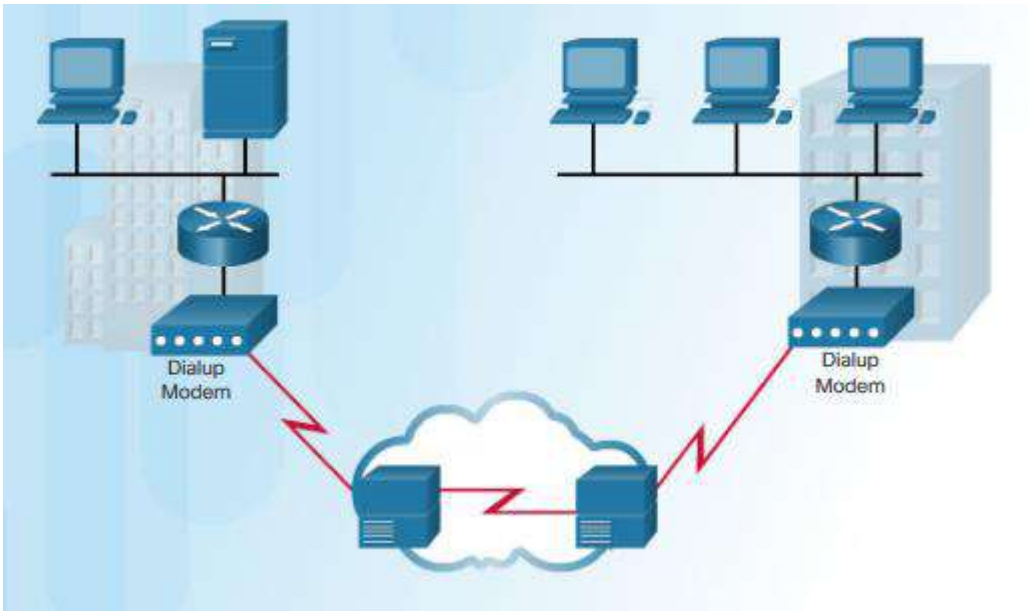
Traditional telephony uses a copper cable, called the local loop, to connect the telephone handset in the subscriber premises to the CO. The signal on the local loop during a call is a continuously varying electronic signal that is a translation of the subscriber voice into an analog signal.

Traditional local loops can transport binary computer data through the voice telephone network using a modem. The modem modulates the binary data into an analog signal at the source and demodulates the analog signal to binary data at the destination. The physical characteristics of the local loop and its connection to the PSTN limit the rate of the signal to less than 56 kb/s.

For small businesses, these relatively low-speed dialup connections are adequate for the exchange of sales figures, prices, routine reports, and email. Using automatic dialup at night or on weekends for large file transfers and data backup can take advantage of lower off-peak tariffs (toll charges). Tariffs are based on the distance between the endpoints, time of day, and the duration of the call.

The advantages of modem and analog lines are simplicity, availability, and low implementation cost. The disadvantages are the low data rates and a relatively long connection time. The dedicated circuit has little delay or jitter for point-to-point traffic, but voice or video traffic does not operate adequately at these low bit rates.

Note: Although very few enterprises support dialup access, it is still a viable solution for remote areas with limited WAN access options.



ISDN

Integrated Services Digital Network (ISDN) is a circuit-switching technology that enables the local loop of a PSTN to carry digital signals, resulting in higher capacity switched connections.

ISDN changes the internal connections of the PSTN from carrying analog signals to time-division multiplexed (TDM) digital signals. TDM allows two or more signals, or bit streams, to be transferred as subchannels in one communication channel. The signals appear to transfer simultaneously; but physically, the signals are taking turns on the channel.

Figure 1 displays a sample ISDN topology. The ISDN connection may require a terminal adapter (TA) which is a device used to connect ISDN Basic Rate Interface (BRI) connections to a router.

There are two types of ISDN interfaces:

Basic Rate Interface (BRI) - ISDN BRI is intended for the home and small enterprise and provides two 64 kb/s bearer channels (B) for carrying voice and data and a 16 kb/s delta channel (D) for signaling, call setup and other purposes. The BRI D channel is often underused, because it has only two B channels to control (Figure 2).

Primary Rate Interface (PRI) – ISDN is also available for larger installations. In North America, PRI delivers 23 B channels with 64 kb/s and one D channel with 64 kb/s for a total bit rate of up to 1.544 Mb/s. This includes some additional overhead for synchronization. In Europe, Australia, and other parts of the world, ISDN PRI provides 30 B channels and one D channel, for a total bit rate of up to 2.048 Mb/s, including synchronization overhead (Figure 3).

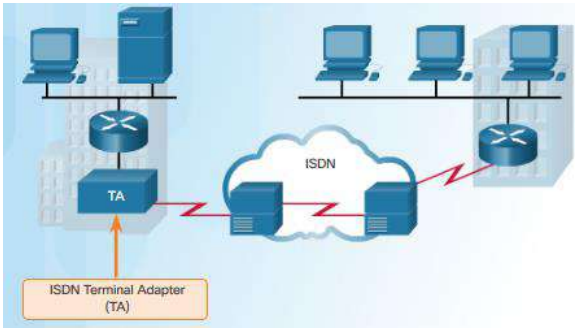
BRI has a call setup time that is less than a second, and the 64 kb/s B channel provides greater capacity than an analog modem link. If greater capacity is required, a second B channel can be activated to provide a total of 128 kb/s. This permits several simultaneous voice conversations, a voice conversation and data transfer, or a video conference using one channel for voice and the other for video.

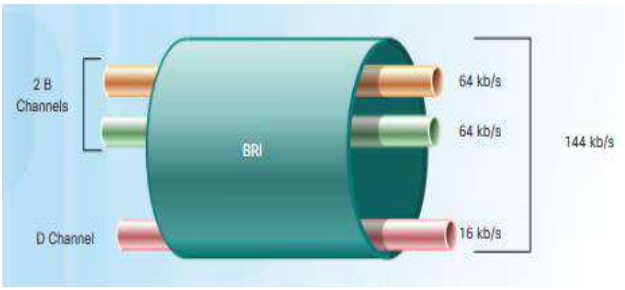
Another common application of ISDN is to provide additional capacity as needed on a leased line

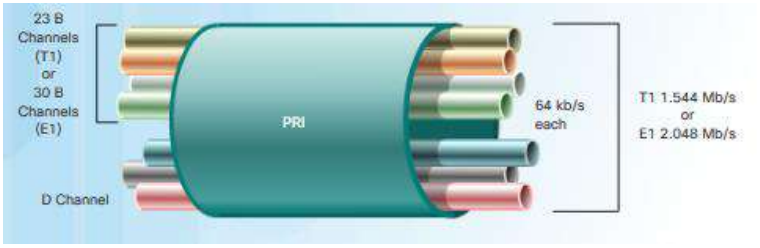
connection. The leased line is sized to carry average traffic loads while ISDN is added during peak demand periods. ISDN is also used as a backup if the leased line fails. ISDN tariffs are based on a per-B channel basis and are similar to those of analog voice connections.

With PRI ISDN, multiple B channels can be connected between two endpoints. This allows for videoconferencing and high-bandwidth data connections with no latency or jitter. However, multiple connections can be very expensive over long distances.

Note: Although ISDN is still an important technology for telephone service provider networks, it has declined in popularity as an Internet connection option with the introduction of high-speed DSL and other broadband services.







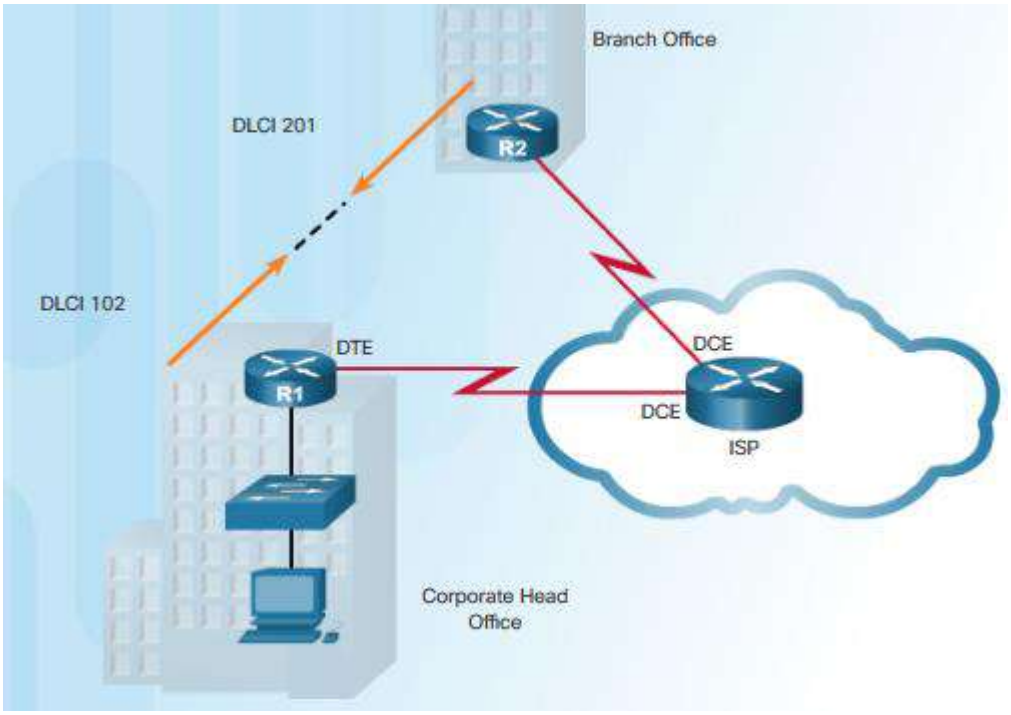
Frame Relay

Frame Relay is a simple Layer 2 non-broadcast multi-access (NBMA) WAN technology used to interconnect enterprise LANs. A single router interface can be used to connect to multiple sites using PVCs. PVCs are used to carry both voice and data traffic between a source and destination, and support data rates up to 4 Mb/s, with some providers offering even higher rates.

An edge router only requires a single interface, even when multiple virtual circuits (VCs) are used. The leased line to the Frame Relay network edge allows cost-effective connections between widely scattered LANs.

Frame Relay creates PVCs which are uniquely identified by a data-link connection identifier (DLCI). The PVCs and DLCIs ensure bidirectional communication from one DTE device to another.

For instance, in the figure, R1 will use DLCI 102 to reach R2 while R2 will use DLCI 201 to reach R1.



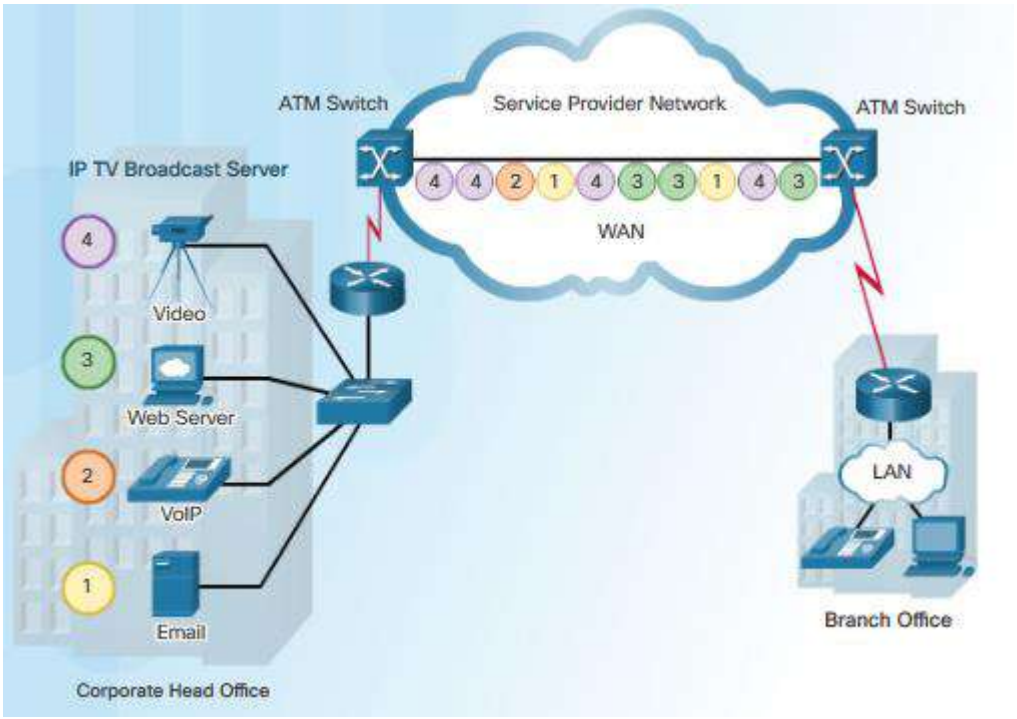
ATM

Asynchronous Transfer Mode (ATM) technology is capable of transferring voice, video, and data through private and public networks. It is built on a cell-based architecture rather than on a frame-based architecture. ATM cells are always a fixed length of 53 bytes. The ATM cell contains a 5-byte ATM header followed by 48 bytes of ATM payload. Small, fixed-length cells are well-suited for carrying voice and video traffic because this traffic is intolerant of delay. Video and voice traffic do not have to wait for larger data packets to be transmitted.

The 53-byte ATM cell is less efficient than the bigger frames and packets of Frame Relay. Furthermore, the ATM cell has at least 5 bytes of overhead for each 48-byte payload. When the cell is carrying segmented network layer packets, the overhead is higher because the ATM switch must be able to reassemble the packets at the destination. A typical ATM line needs almost 20 percent greater bandwidth than Frame Relay to carry the same volume of network layer data.

ATM was designed to be extremely scalable and to support link speeds of T1/E1 to OC-12 (622 Mb/s) and faster.

ATM offers both PVCs and SVCs, although PVCs are more common with WANs. As with other shared technologies, ATM allows multiple VCs on a single leased-line connection to the network edge.



Ethernet WAN

Ethernet was originally developed to be a LAN access technology. Originally Ethernet was not suitable as a WAN access technology because at that time, the maximum cable length was one kilometer. However, newer Ethernet standards using fiber-optic cables have made Ethernet a reasonable WAN access option. For instance, the IEEE 1000BASE-LX standard supports fiber-optic cable lengths of 5 km, while the IEEE 1000BASE-ZX standard supports cable lengths up to 70 km.

Service providers now offer Ethernet WAN service using fiber-optic cabling. The Ethernet WAN service can go by many names, including Metropolitan Ethernet (MetroE), Ethernet over MPLS (EoMPLS), and Virtual Private LAN Service (VPLS).

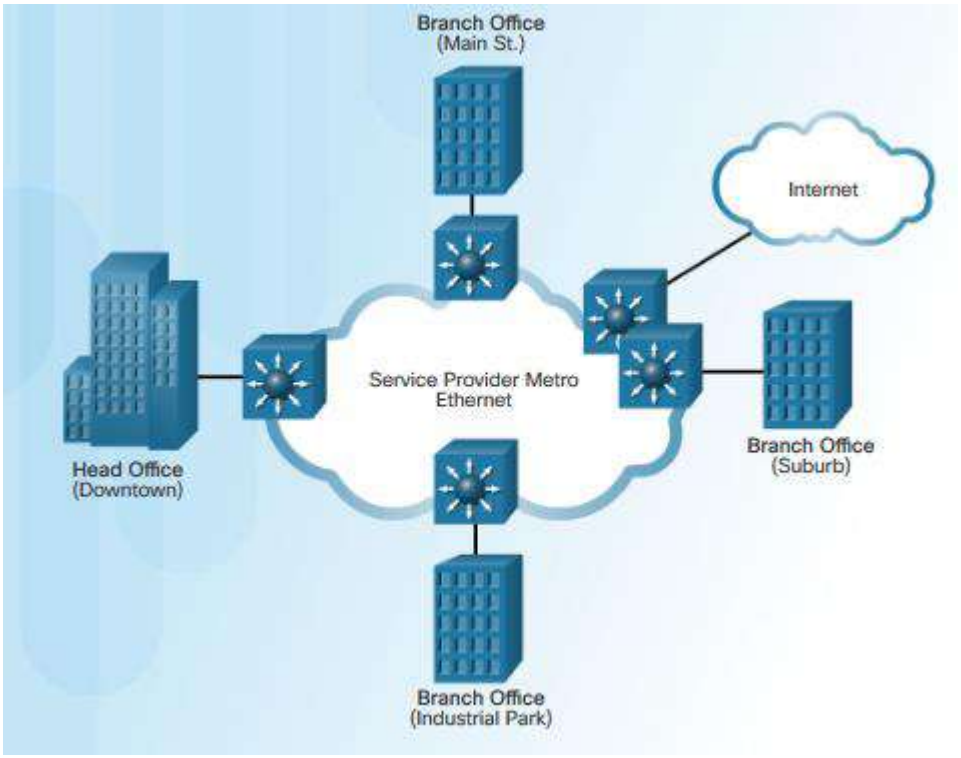
There are several benefits to an Ethernet WAN:

Reduced expenses and administration - Ethernet WAN provides a switched, high-bandwidth Layer 2 network capable of managing data, voice, and video all on the same infrastructure. This characteristic increases bandwidth and eliminates expensive conversions to other WAN technologies. The technology enables businesses to inexpensively connect numerous sites in a metropolitan area, to each other, and to the Internet.

Easy integration with existing networks - Ethernet WAN connects easily to existing Ethernet LANs, reducing installation costs and time.

Enhanced business productivity - Ethernet WAN enables businesses to take advantage of productivity-enhancing IP applications that are difficult to implement on TDM or Frame Relay networks, such as hosted IP communications, VoIP, and streaming and broadcast video.

Note: Ethernet WANs have gained in popularity and are now commonly being used to replace the traditional Frame Relay and ATM WAN links.



MPLS

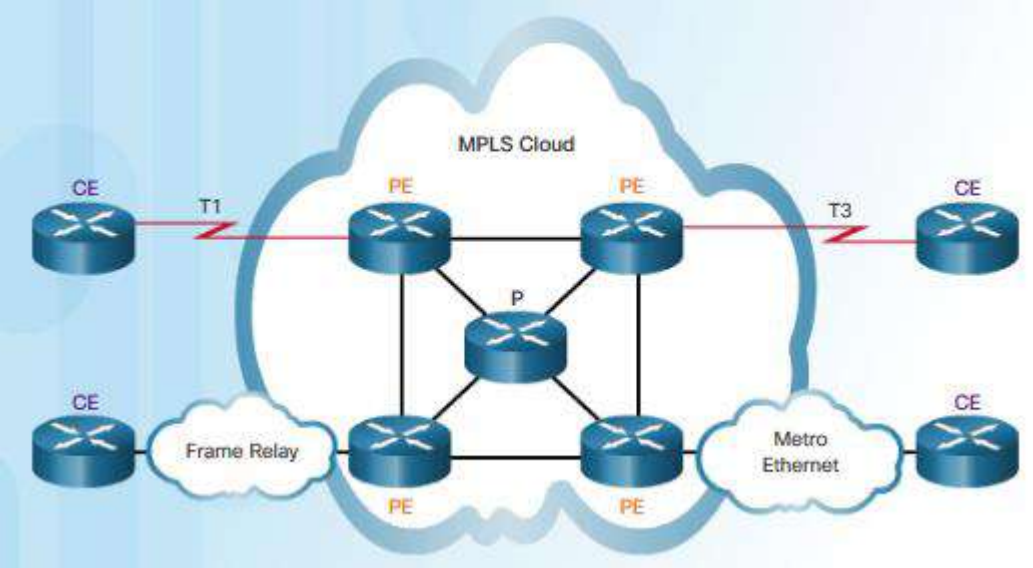
Multiprotocol Label Switching (MPLS) is a multiprotocol high-performance WAN technology that directs data from one router to the next. MPLS is based on short path labels rather than IP network addresses.

MPLS has several defining characteristics. It is multiprotocol, meaning it has the ability to carry any payload including IPv4, IPv6, Ethernet, ATM, DSL, and Frame Relay traffic. It uses labels which tell a router what to do with a packet. The labels identify paths between distant routers rather than endpoints, and while MPLS actually routes IPv4 and IPv6 packets, everything else is switched.

MPLS is a service provider technology. Leased lines deliver bits between sites, and Frame Relay and Ethernet WAN deliver frames between sites. However, MPLS can deliver any type of packet between sites. MPLS can encapsulate packets of various network protocols. It supports a wide range of WAN technologies including T-carrier / E-carrier links, Carrier Ethernet, ATM, Frame Relay, and DSL.

The sample topology in the figure illustrates how MPLS is used. Notice that the different sites can connect to the MPLS cloud using different access technologies. In the figure, CE refers to the customer edge, PE is the provider edge router which adds and removes labels, while P is an internal provider router which switches MPLS labeled packets.

Note: MPLS is primarily a service provider WAN technology.



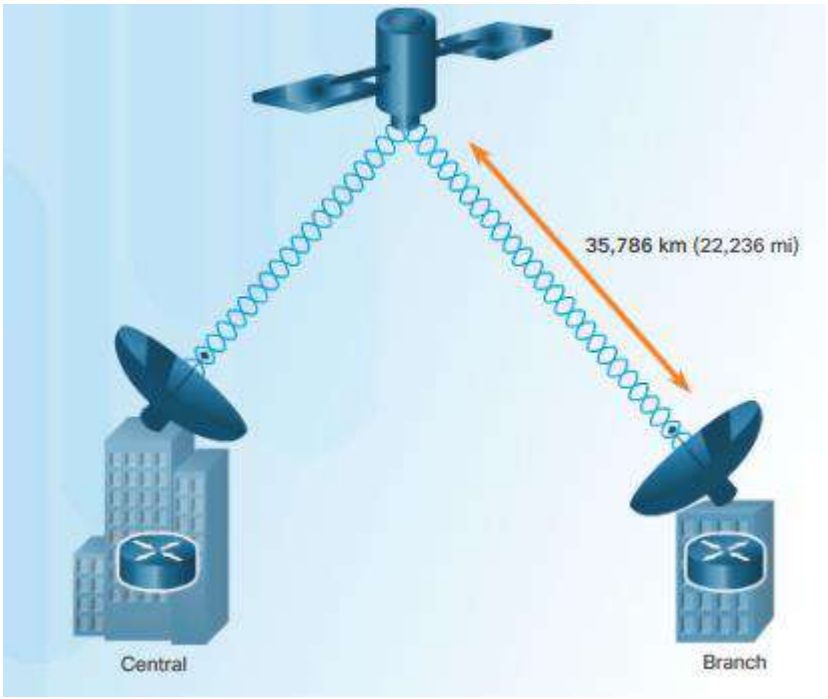
VSAT

All private WAN technologies discussed so far used either copper or fiber-optic media. What if an organization needed connectivity in a remote location where there are no service providers that offer WAN service?

Very small aperture terminal (VSAT) is a solution that creates a private WAN using satellite communications. A VSAT is a small satellite dish similar to those used for home Internet and TV. VSATs create a private WAN while providing connectivity to remote locations.

Specifically, a router connects to a satellite dish which is pointed to a service provider's satellite. This satellite is in geosynchronous orbit in space. The signals must travel approximately 35,786 kilometers (22,236 miles) to the satellite and back.

The example in the figure displays a VSAT dish on the roofs of the buildings communicating with a satellite thousands of kilometers away in space.



Review questions

Describe in brief the private connections in WAN .

Learning Outcome1.3: Describe public infrastructure

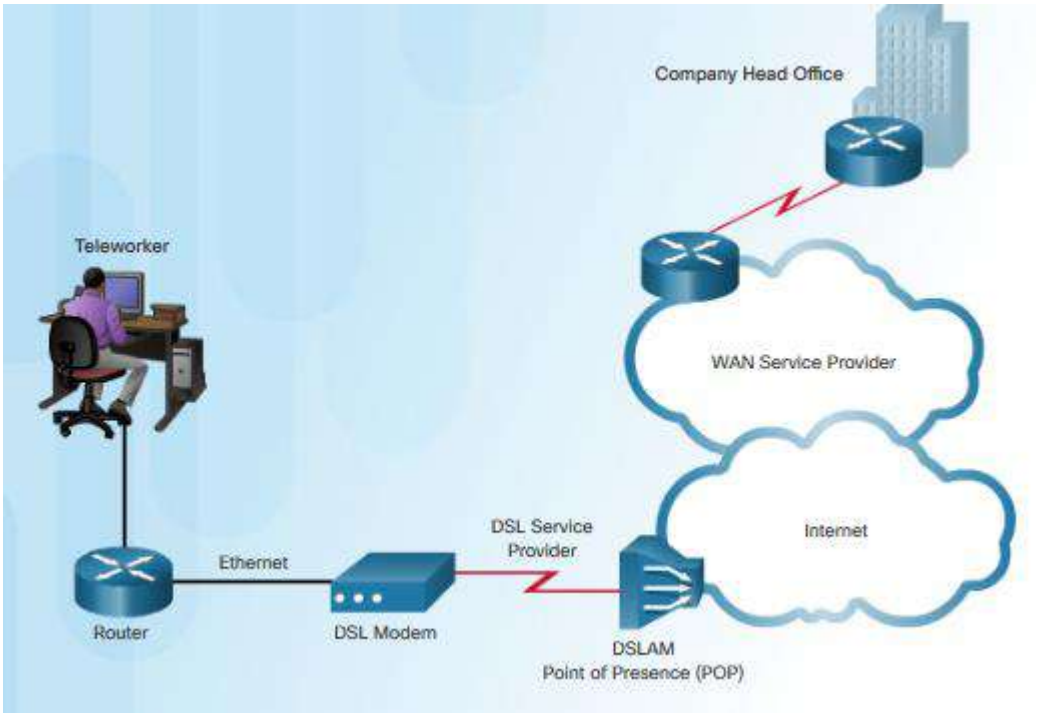
DSL

DSL technology is an always-on connection technology that uses existing twisted-pair telephone lines to transport high-bandwidth data, and provides IP services to subscribers. A DSL modem converts an Ethernet signal from the user device to a DSL signal, which is transmitted to the central office.

Multiple DSL subscriber lines are multiplexed into a single, high-capacity link using a DSL access multiplexer (DSLAM) at the provider location. DSLAMs incorporate TDM technology to aggregate many subscriber lines into a single medium, generally a T3 (DS3) connection. Current DSL technologies use sophisticated coding and modulation techniques to achieve fast data rates.

There is a wide variety of DSL types, standards, and emerging standards. DSL is now a popular choice for enterprise IT departments to support home workers. Generally, a subscriber cannot choose to connect to an enterprise network directly, but must first connect to an ISP, and then an IP connection is made through the Internet to the enterprise. Security risks are incurred in this process, but can be mediated with security measures.

The topology in the figure displays a sample DSL WAN connection.



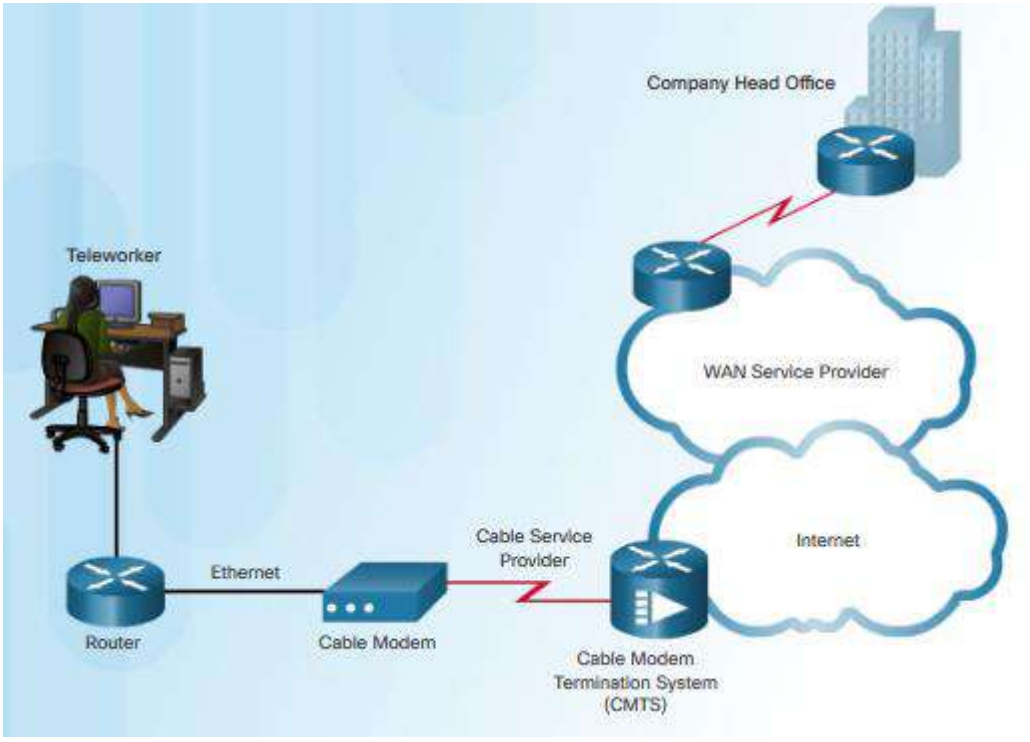
Cable

Coaxial cable is widely used in urban areas to distribute television signals. Network access is available from many cable television providers. This allows for greater bandwidth than the conventional

telephone local loop.

Cable modems provide an always-on connection and a simple installation. A subscriber connects a computer or LAN router to the cable modem, which translates the digital signals into the broadband frequencies used for transmitting on a cable television network. The local cable TV office, which is called the cable headend, contains the computer system and databases needed to provide Internet access. The most important component located at the headend is the cable modem termination system (CMTS), which sends and receives digital cable modem signals on a cable network and is necessary for providing Internet services to cable subscribers.

Cable modem subscribers must use the ISP associated with the service provider. All the local subscribers share the same cable bandwidth. As more users join the service, available bandwidth may drop below the expected rate.



Wireless

Wireless technology uses the unlicensed radio spectrum to send and receive data. The unlicensed spectrum is accessible to anyone who has a wireless router and wireless technology in the device they are using.

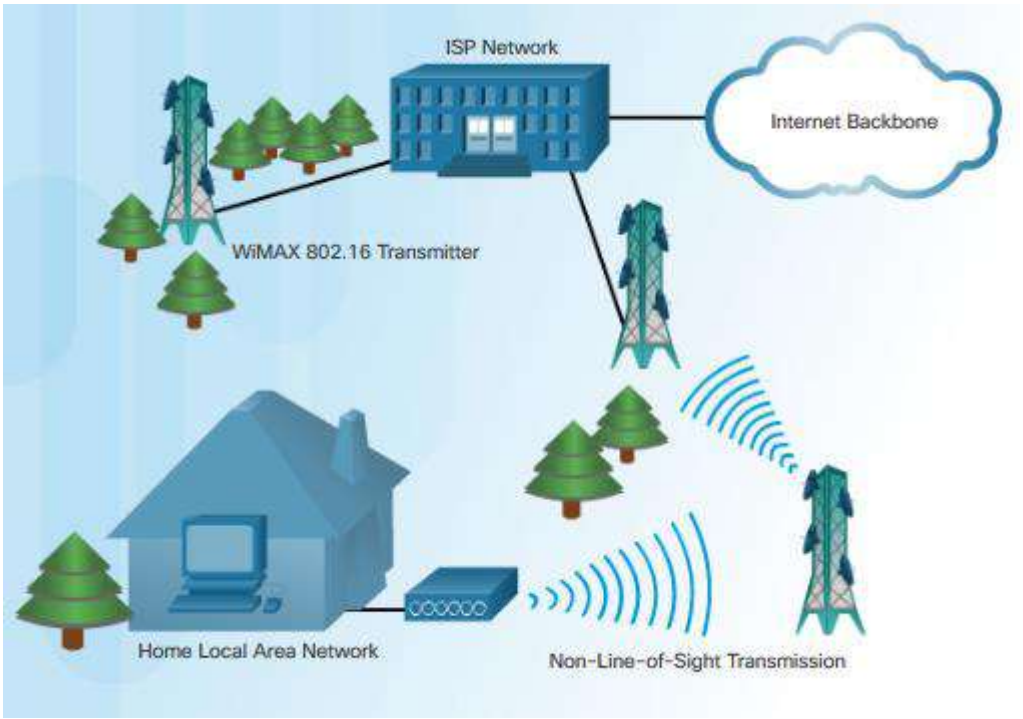
Until recently, one limitation of wireless access has been the need to be within the local transmission range (typically less than 100 feet) of a wireless router or a wireless modem that has a wired connection to the Internet. The following new developments in broadband wireless technology are changing this situation:

Municipal Wi-Fi - Many cities have begun setting up municipal wireless networks. Some of these networks provide high-speed Internet access for free or for substantially less than the price of other

broadband services. Others are for city use only, allowing police and fire departments and other city employees to do certain aspects of their jobs remotely. To connect to a municipal Wi-Fi, a subscriber typically needs a wireless modem, which provides a stronger radio and directional antenna than conventional wireless adapters. Most service providers provide the necessary equipment for free or for a fee, much like they do with DSL or cable modems.

WiMAX - Worldwide Interoperability for Microwave Access (WiMAX) is a new technology that is just beginning to come into use. It is described in the IEEE standard 802.16. WiMAX provides high-speed broadband service with wireless access and provides broad coverage like a cell phone network rather than through small Wi-Fi hotspots. WiMAX operates in a similar way to Wi-Fi, but at higher speeds, over greater distances, and for a greater number of users. It uses a network of WiMAX towers that are similar to cell phone towers. To access a WiMAX network, subscribers must subscribe to an ISP with a WiMAX tower within 30 miles of their location. They also need some type of WiMAX receiver and a special encryption code to get access to the base station.

Satellite Internet - Typically used by rural users where cable and DSL are not available. A VSAT provides two-way (upload and download) data communications. The upload speed is about one-tenth of the 500 kb/s download speed. Cable and DSL have higher download speeds, but satellite systems are about 10 times faster than an analog modem. To access satellite Internet services, subscribers need a satellite dish, two modems (uplink and downlink), and coaxial cables between the dish and the modem.



3G/4G Cellular

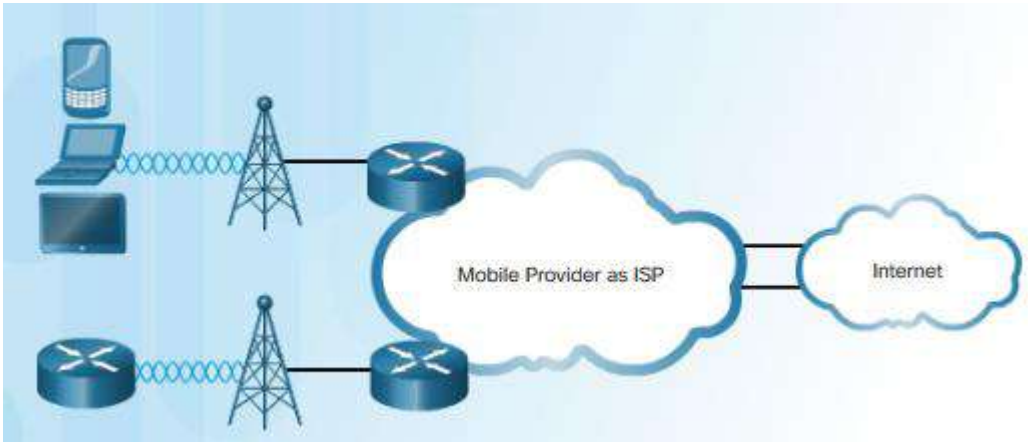
Increasingly, cellular service is another wireless WAN technology being used to connect users and remote locations where no other WAN access technology is available. Many users with smart phones and tablets can use cellular data to email, surf the web, download apps, and watch videos.

Phones, tablet computers, laptops, and even some routers can communicate through to the Internet using cellular technology. These devices use radio waves to communicate through a nearby mobile phone tower. The device has a small radio antenna, and the provider has a much larger antenna sitting at the top of a tower somewhere within miles of the phone.

These are two common cellular industry terms:

3G/4G Wireless - Abbreviation for 3rd generation and 4th generation cellular access. These technologies support wireless Internet access.

Long-Term Evolution (LTE) - Refers to a newer and faster technology and is considered to be part of fourth generation (4G) technology.



VPN Technology

Security risks are incurred when a teleworker or a remote office worker uses a broadband service to access the corporate WAN over the Internet. To address security concerns, broadband services provide capabilities for using VPN connections to a network device that accepts VPN connections, which is typically located at the corporate site.

A VPN is an encrypted connection between private networks over a public network, such as the Internet. Instead of using a dedicated Layer 2 connection, such as a leased line, a VPN uses virtual connections called VPN tunnels, which are routed through the Internet from the private network of the company to the remote site or employee host.

There are several benefits to using VPN:

Cost savings - VPNs enable organizations to use the global Internet to connect remote offices, and to connect remote users to the main corporate site. This eliminates expensive, dedicated WAN links and modem banks.

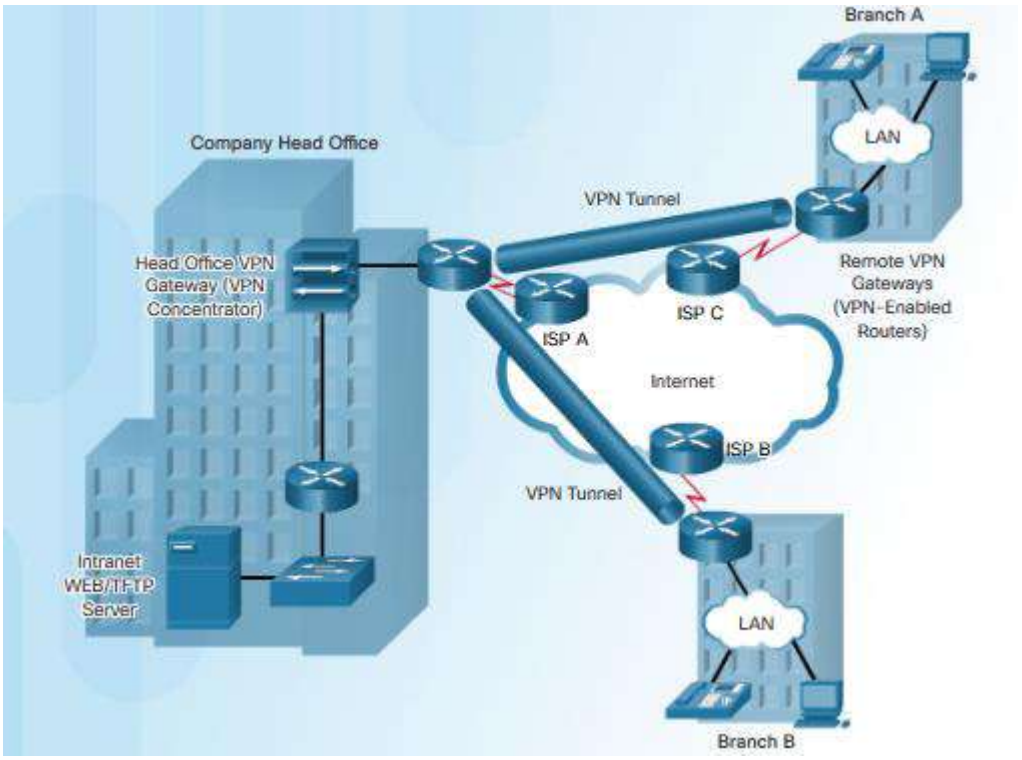
Security - VPNs provide the highest level of security by using advanced encryption and authentication protocols that protect data from unauthorized access.

Scalability - Because VPNs use the Internet infrastructure within ISPs and devices, it is easy to add new users. Corporations are able to add large amounts of capacity without adding significant infrastructure.

Compatibility with broadband technology - VPN technology is supported by broadband service providers such as DSL and cable. VPNs allow mobile workers and telecommuters to take advantage of their home high-speed Internet service to access their corporate networks. Business-grade, high-speed broadband connections can also provide a cost-effective solution for connecting remote offices.

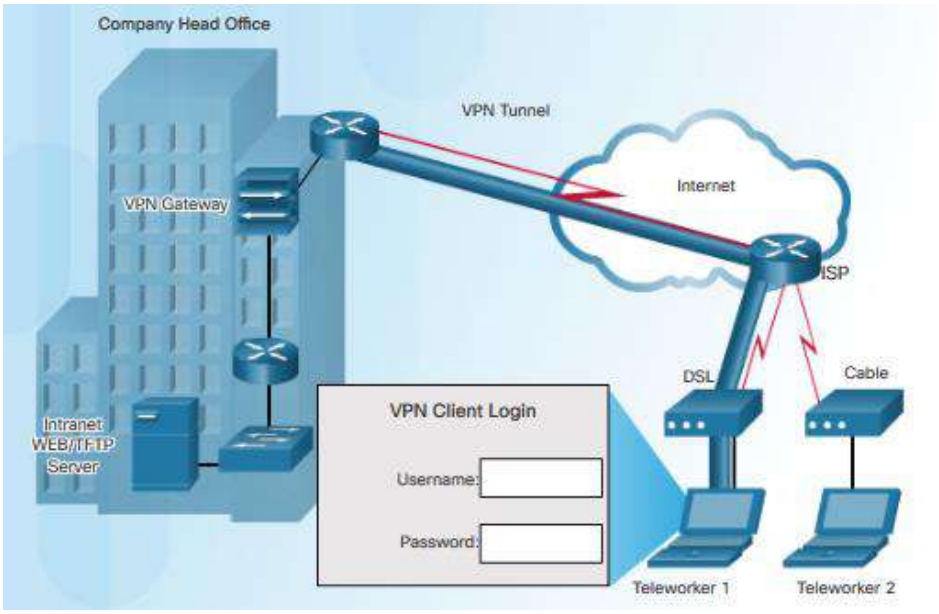
There are two types of VPN access:

Site-to-site VPNs - Site-to-site VPNs connect entire networks to each other; for example, they can connect a branch office network to a company headquarters network, as shown in Figure . Each site is equipped with a VPN gateway, such as a router, firewall, VPN concentrator, or security appliance. In the figure, a remote branch office uses a site-to-site-VPN to connect with the corporate head office.

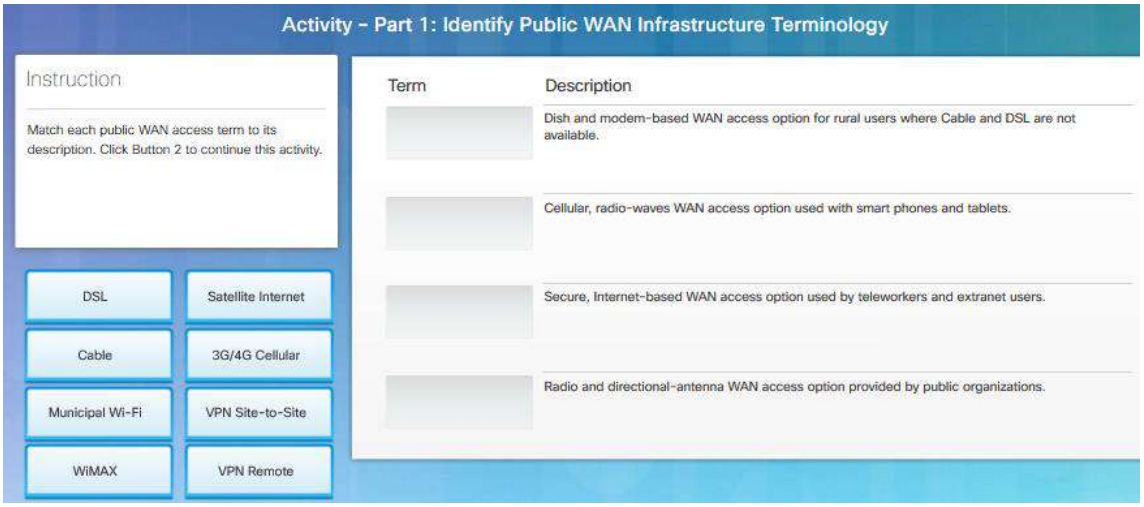


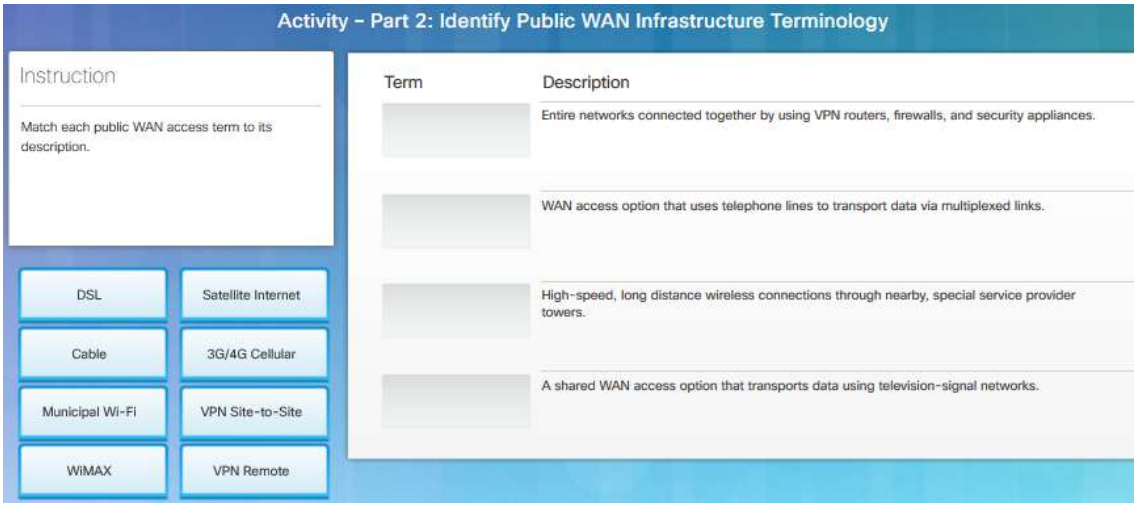
Remote-access VPNs

Remote-access VPNs enable individual hosts, such as telecommuters, mobile users, and extranet consumers, to access a company network securely over the Internet. Each host (Teleworker 1 and Teleworker 2) typically has VPN client software loaded or uses a web-based client, as shown in Figure .



Review questions





Choosing a WAN Link Connection

There are many important factors to consider when choosing an appropriate WAN connection. For a network administrator to decide which WAN technology best meets the requirements of their specific business, they must answer the following questions:

What is the purpose of the WAN?

There are a few issues to consider:

Will the enterprise connect local branches in the same city area, connect remote branches, or connect to a single branch?

Will the WAN be used to connect internal employees, or external business partners and customers, or all three?

Will the enterprise connect to customers, connect to business partners, connect to employees, or some combination of these?

Will the WAN provide authorized users limited or full access to the company intranet?

What is the geographic scope?

There are a few issues to consider:

Is the WAN local, regional, or global?

Is the WAN one-to-one (single branch), one-to-many branches, or many-to-many (distributed)?

What are the traffic requirements?

There are a few issues to consider:

What type of traffic must be supported (data only, VoIP, video, large files, streaming files)? This determines the quality and performance requirements.

What volume of traffic type (voice, video, or data) must be supported for each destination? This determines the bandwidth capacity required for the WAN connection to the ISP.

What Quality of Service is required? This may limit the choices. If the traffic is highly sensitive to latency and jitter, eliminate any WAN connection options that cannot provide the required quality.

What are the security requirements (data integrity, confidentiality, and security)? These are important factors if the traffic is of a highly confidential nature, or if it provides essential services, such as emergency response.

LEARNING UNIT 2- IMPLEMENT ROUTING AND POINT-TO-POINT PROTOCOLS

30 hours

Learning Outcomes:

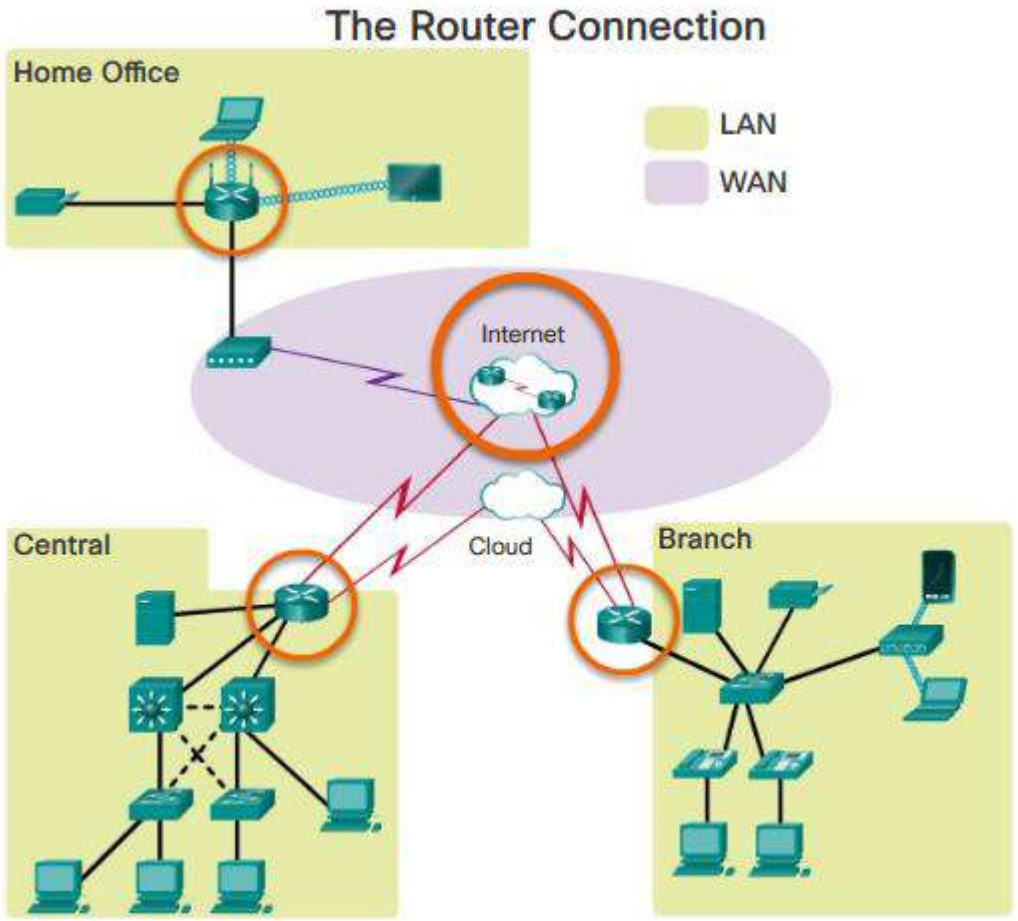
2.1. Apply static routing
2.2. Connect variety networks using EIGRP
2.3. Connect variety networks using OSPF
2.4. Connect networks using Border Gateway Protocol (BGP)
2.5. Implement point to point protocol (PPP)
2.6. Enable Management protocols

Why Routing?

How does clicking a link in a web browser return the desired information in mere seconds? Although there are many devices and technologies collaboratively working together to enable this, the primary device is the router. Stated simply, a router connects one network to another network.

Communication between networks would not be possible without a router determining the best path to the destination and forwarding traffic to the next router along that path. The router is responsible for the routing of traffic between networks.

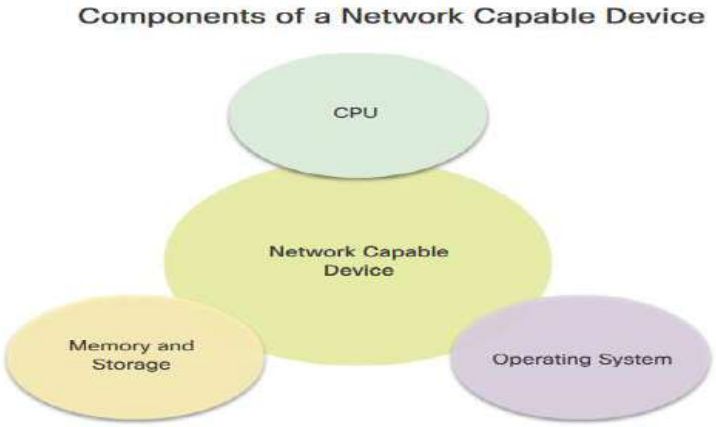
In the topology in the figure, the routers interconnect the networks at the different sites. When a packet arrives on a router interface, the router uses its routing table to determine how to reach the destination network. The destination of the IP packet might be a web server in another country or an email server on the local area network. It is the responsibility of routers to deliver those packets efficiently. The effectiveness of internetwork communications depends, to a large degree, on the ability of routers to forward packets in the most efficient way possible.



Routers Are Computers

Most network capable devices (e.g.., computers, tablets, and smartphones) require the following components to operate

- Central processing unit (CPU)
- Operating system (OS)
- Memory and storage (RAM, ROM, NVRAM, Flash, hard drive)



A router is essentially a specialized computer. It requires a CPU and memory to temporarily and permanently store data to execute operating system instructions, such as system initialization, routing

functions, and switching functions.

Note: Cisco devices use the Cisco Internetwork Operating System (IOS) as the system software.

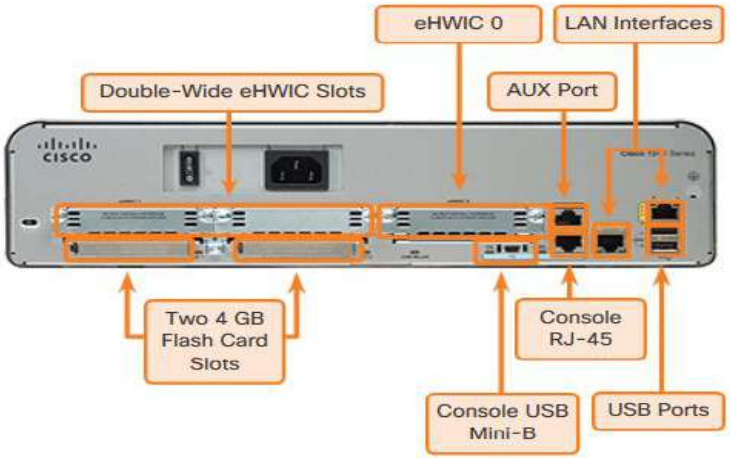
Router memory is classified as volatile or non-volatile. Volatile memory loses its content when the power is turned off, while non-volatile memory does not lose its content when the power is turned off.

Router Memory

Memory	Description
Random Access Memory (RAM)	Volatile memory that provides temporary storage for various applications and processes including: • Running IOS • Running configuration file • IP routing and ARP tables • Packet buffer
Read-Only Memory (ROM)	Non-volatile memory that provides permanent storage for: • Bootup instructions • Basic diagnostic software • Limited IOS in case the router cannot load the full featured IOS
Non-Volatile Random Access Memory (NVRAM)	Non-volatile memory that provides permanent storage for the: • Startup configuration file
Flash	Non-volatile memory that provides permament storage for: • IOS • Other system-related files

Unlike a computer, a router does not have video adapters or sound card adapters. Instead, routers have specialized ports and network interface cards to interconnect devices to other networks.

Back Panel of a Router



Routers Interconnect Networks

Most users are unaware of the presence of numerous routers on their own network or on the Internet. Users expect to be able to access web pages, send emails, and download music, regardless of whether

the server accessed is on their own network or on another network. Networking professionals know that it is the router that is responsible for forwarding packets from network to network, from the original source to the final destination.

A router connects multiple networks, which means that it has multiple interfaces that each belong to a different IP network. When a router receives an IP packet on one interface, it determines which interface to use to forward the packet to the destination. The interface that the router uses to forward the packet may be the final destination, or it may be a network connected to another router that is used to reach the destination network.

Each network that a router connects to typically requires a separate interface. These interfaces are used to connect a combination of both local-area networks (LANs) and wide-area networks (WANs). LANs are commonly Ethernet networks that contain devices, such as PCs, printers, and servers. WANs are used to connect networks over a large geographical area. For example, a WAN connection is commonly used to connect a LAN to the Internet service provider (ISP) network.

Routers Choose Best Paths

The primary functions of a router are to:

Determine the best path to send packets

Forward packets toward their destination

The router uses its routing table to determine the best path to use to forward a packet. When the router receives a packet, it examines the destination address of the packet and uses the routing table to search for the best path to that network. The routing table also includes the interface to be used to forward packets for each known network. When a match is found, the router encapsulates the packet into the data link frame of the outgoing or exit interface, and the packet is forwarded toward its destination.

It is possible for a router to receive a packet that is encapsulated in one type of data link frame, and to forward the packet out of an interface that uses a different type of data link frame. For example, a router may receive a packet on an Ethernet interface, but must forward the packet out of an interface configured with the Point-to-Point Protocol (PPP). The data link encapsulation depends on the type of interface on the router and the type of medium to which it connects. The different data link technologies that a router can connect to include Ethernet, PPP, Frame Relay, DSL, cable, and wireless (802.11, Bluetooth, etc.). Notice that it is the responsibility of the router to find the destination network in its routing table and forward the packet on toward its destination. Note: Routers use static routes and dynamic routing protocols to learn about remote networks and build their routing tables.

Packet Forwarding Mechanisms

Routers support three packet-forwarding mechanisms:

Process switching - An older packet forwarding mechanism still available for Cisco routers. When a packet arrives on an interface, it is forwarded to the control plane where the CPU matches the destination address with an entry in its routing table, and then determines the exit interface and forwards the packet.

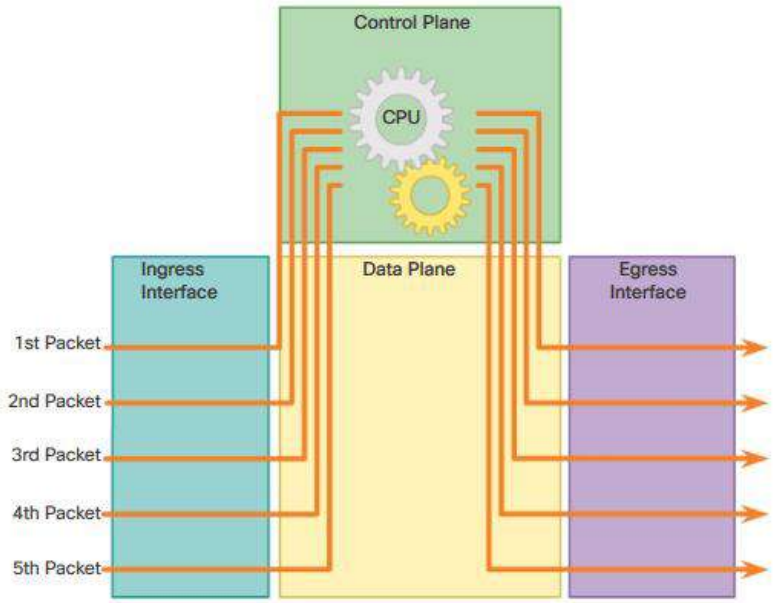
It is important to understand that the router does this for every packet, even if the destination is the same for a stream of packets. This process-switching mechanism is very slow and rarely implemented in modern networks.

Fast switching - This is a common packet forwarding mechanism which uses a fast-switching cache to store next-hop information. When a packet arrives on an interface, it is forwarded to the control plane where the CPU searches for a match in the fast-switching cache. If it is not there, it is process-switched and forwarded to the exit interface. The flow information for the packet is also stored in the fast-switching cache. If another packet going to the same destination arrives on an interface, the next-hop information in the cache is re-used without CPU intervention.

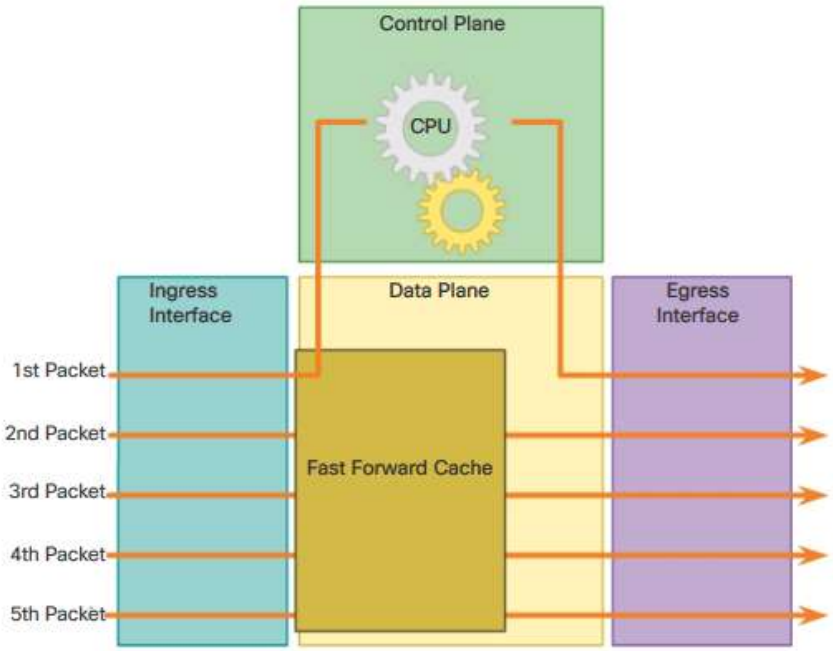
Cisco Express Forwarding (CEF) - CEF is the most recent and preferred Cisco IOS packet-forwarding mechanism. Like fast switching, CEF builds a Forwarding Information Base (FIB), and an adjacency table. However, the table entries are not packet-triggered like fast switching but change-triggered such as when something changes in the network topology. Therefore, when a network has converged, the FIB and adjacency tables contain all the information a router would have to consider when forwarding a packet. The FIB contains pre-computed reverse lookups, next hop information for routes including the interface and Layer 2 information. Cisco Express Forwarding is the fastest forwarding mechanism and the preferred choice on Cisco routers.

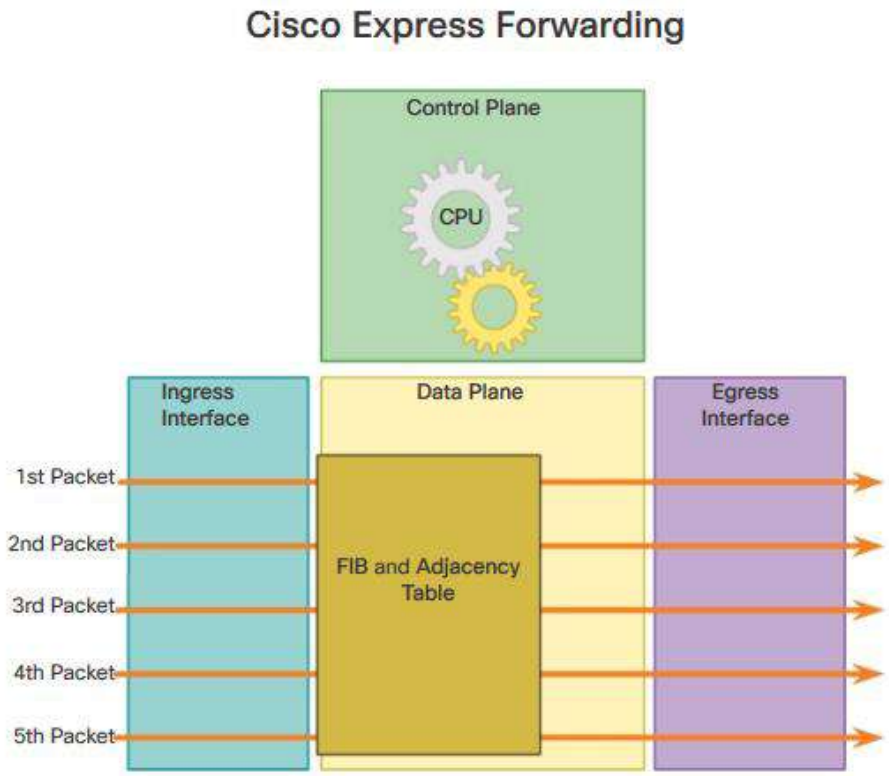
Assume that a traffic flow consisting of five packets are all going to the same destination. With process switching, each packet must be processed by the CPU individually. Contrast this with fast switching, as shown in Figure 2. With fast switching, notice how only the first packet of a flow is process-switched and added to the fast-switching cache. The next four packets are quickly processed based on the information in the fast-switching cache. Finally, in Figure 3, CEF builds the FIB and adjacency tables, after the network has converged. All five packets are quickly processed in the data plane. A common analogy used to describe the three packet-forwarding mechanisms is as follows: Process switching solves a problem by doing math long hand, even if it is the identical problem. Fast switching solves a problem by doing math long hand one time and remembering the answer for subsequent identical problems. CEF solves every possible problem ahead of time in a spreadsheet.

Process Switching



Fast Switching





Review questions

Describe the packet forward mechanism ?

Default Gateways

To enable network access, devices must be configured with IP address information to identify the appropriate:

- IP address - Identifies a unique host on a local network.
- Subnet mask - Identifies with which network subnet the host can communicate.
- Default gateway - Identifies the IP address of the router to send a packet to when the destination is not on the same local network subnet.

When a host sends a packet to a device that is on the same IP network, the packet is simply forwarded out of the host interface to the destination device.

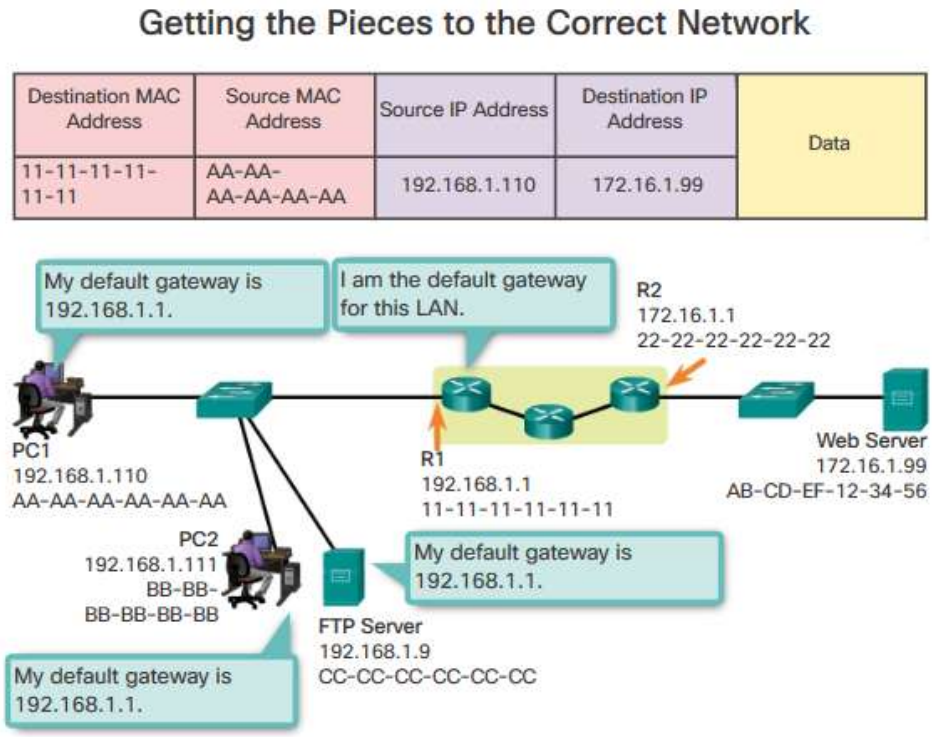
When a host sends a packet to a device on a different IP network, then the packet is forwarded to the default gateway, because a host device cannot communicate directly with devices outside of the local network. The default gateway is the destination that routes traffic from the local network to devices on remote networks. It is often used to connect a local network to the Internet.

The default gateway is usually the address of the interface on the router connected to the local network. The router maintains routing table entries of all connected networks as well as entries of remote networks, and determines the best path to reach those destinations.

For example, if PC1 sends a packet to the Web Server located at 176.16.1.99, it would discover that the

Web Server is not on the local network and it, therefore, must send the packet to the Media Access Control (MAC) address of its default gateway. The Packet protocol data unit (PDU) in the figure identifies the source and destination IP and MAC addresses.

Note: A router is also usually configured with its own default gateway. This is known as the Gateway of Last Resort.



Enable IP on a Switch

Network infrastructure devices require IP addresses to enable remote management. Using the device IP address, the network administrator can remotely connect to the device using Telnet, SSH, HTTP, or HTTPS.

A switch does not have a dedicated interface to which an IP address can be assigned. Instead, the IP address information is configured on a virtual interface called a switched virtual interface (SVI).

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.10.2 255.255.255.0
S1(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
S1(config-if)# exit
S1(config)#
S1(config)# ip default-gateway 192.168.10.1
S1(config)#
```

Configure an IPv4 Router Interface

One distinguishing feature between switches and routers is the type of interfaces supported by each. For example, Layer 2 switches support LANs and, therefore, have multiple FastEthernet or Gigabit Ethernet

ports.

Routers support LANs and WANs and can interconnect different types of networks; therefore, they support many types of interfaces. For example, G2 ISRs have one or two integrated Gigabit Ethernet interfaces and High-Speed WAN Interface Card (HWIC) slots to accommodate other types of network interfaces, including serial, DSL, and cable interfaces.

To be available, an interface must be:

Configured with an IP address and a subnet mask - Use the ip address *ip-address subnet-mask* interface configuration command.

Activated - By default, LAN and WAN interfaces are not activated (shutdown). To enable an interface, it must be activated using the no shutdown command. (This is similar to powering on the interface.) The interface must also be connected to another device (a hub, a switch, or another router) for the physical layer to be active.

Optionally, the interface could also be configured with a short description of up to 240 characters. It is good practice to configure a description on each interface. On production networks, the benefits of interface descriptions are quickly realized as they are helpful in troubleshooting and to identify a third party connection and contact information.

Depending on the type of interface, additional parameters may be required. For example, in the lab environment, the serial interface connecting to the serial cable end labeled DCE must be configured with the clock rate command.

Note: Accidentally using the clock rate command on a DTE interface generates a "%Error: This command applies only to DCE interface" informational message.

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
```

Configure an IPv6 Router Interface

Configuring an IPv6 interface is similar to configuring an interface for IPv4. Most IPv6 configuration and verification commands in the Cisco IOS are very similar to their IPv4 counterparts. In many cases, the only difference is the use of ipv6 in place of ip in commands.

An IPv6 interface must be:

Configured with IPv6 address and subnet mask - Use the ipv6 address *ipv6-address*/*prefix-length* [link-local | eui-64] interface configuration command.

Activated - The interface must be activated using the no shutdown command.

Note: An interface can generate its own IPv6 link-local address without having a global unicast address by using the ipv6 enable interface configuration command.

Unlike IPv4, IPv6 interfaces will typically have more than one IPv6 address. At a minimum, an IPv6

device must have an IPv6 link-local address but will most likely also have an IPv6 global unicast address. IPv6 also supports the ability for an interface to have multiple IPv6 global unicast addresses from the same subnet. The following commands can be used to statically create a global unicast or link-local IPv6 address:

ipv6 address *ipv6-address/prefix-length* - Creates a global unicast IPv6 address as specified.

ipv6 address *ipv6-address/prefix-length* eui-64 - Configures a global unicast IPv6 address with an interface identifier (ID) in the low-order 64 bits of the IPv6 address using the EUI-64 process.

ipv6 address *ipv6-address/prefix-length* link-local - Configures a static link-local address on the interface that is used instead of the link-local address that is automatically configured when the global unicast IPv6 address is assigned to the interface or enabled using the ipv6 enable interface command. Recall, the ipv6 enable interface command is used to automatically create an IPv6 link-local address whether or not an IPv6 global unicast address has been assigned.

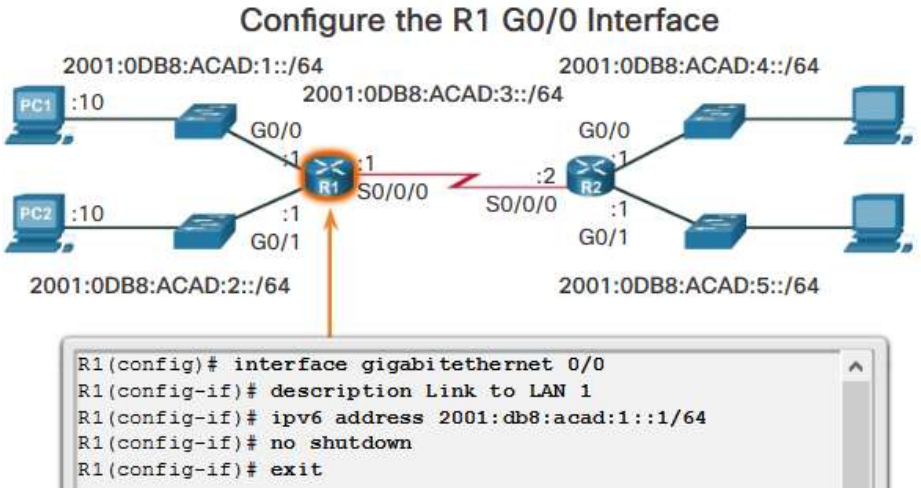
In the example topology shown in Figure 1, R1 must be configured to support the following IPv6 network addresses:

2001:0DB8:ACAD:0001:/64 or equivalently 2001:DB8:ACAD:1::/64

2001:0DB8:ACAD:0002:/64 or equivalently 2001:DB8:ACAD:2::/64

2001:0DB8:ACAD:0003:/64 or equivalently 2001:DB8:ACAD:3::/64

When the router is configured using the ipv6 unicast-routing global configuration command, the router begins sending ICMPv6 Router Advertisement messages out the interface. This enables a PC connected to the interface to automatically configure an IPv6 address and to set a default gateway without needing the services of a DHCPv6 server. Alternatively, a PC connected to the IPv6 network can have an IPv6 address manually configured, as shown in Figure 2. Notice that the default gateway address configured for PC1 is the IPv6 global unicast address of the R1 GigabitEthernet 0/0 interface.



```
R1(config)# interface serial 0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# clock rate 128000
R1(config-if)# no shutdown
R1(config-if)#
```

Configure an IPv4 Loopback Interface

Another common configuration of Cisco IOS routers is enabling a loopback interface.

The loopback interface is a logical interface internal to the router. It is not assigned to a physical port and can therefore never be connected to any other device. It is considered a software interface that is automatically placed in an "up" state, as long as the router is functioning.

The loopback interface is useful in testing and managing a Cisco IOS device because it ensures that at least one interface will always be available. For example, it can be used for testing purposes, such as testing internal routing processes, by emulating networks behind the router.

Additionally, the IPv4 address assigned to the loopback interface can be significant to processes on the router that use an interface IPv4 address for identification purposes, such as the Open Shortest Path First (OSPF) routing process. By enabling a loopback interface, the router will use the always available loopback interface address for identification, rather than an IP address assigned to a physical port that may go down.

Enabling and assigning a loopback address is simple:

Router(config)# **interface loopback** *number*

Router(config-if)# **ip address** *ip-address subnet-mask*

Router(config-if)# **exit**

Multiple loopback interfaces can be enabled on a router. The IPv4 address for each loopback interface must be unique and unused by any other interface.

Routing Decisions

A primary function of a router is to determine the best path to use to send packets. To determine the best path, the router searches its routing table for a network address that matches the destination IP address of the packet.

The routing table search results in one of three path determinations:

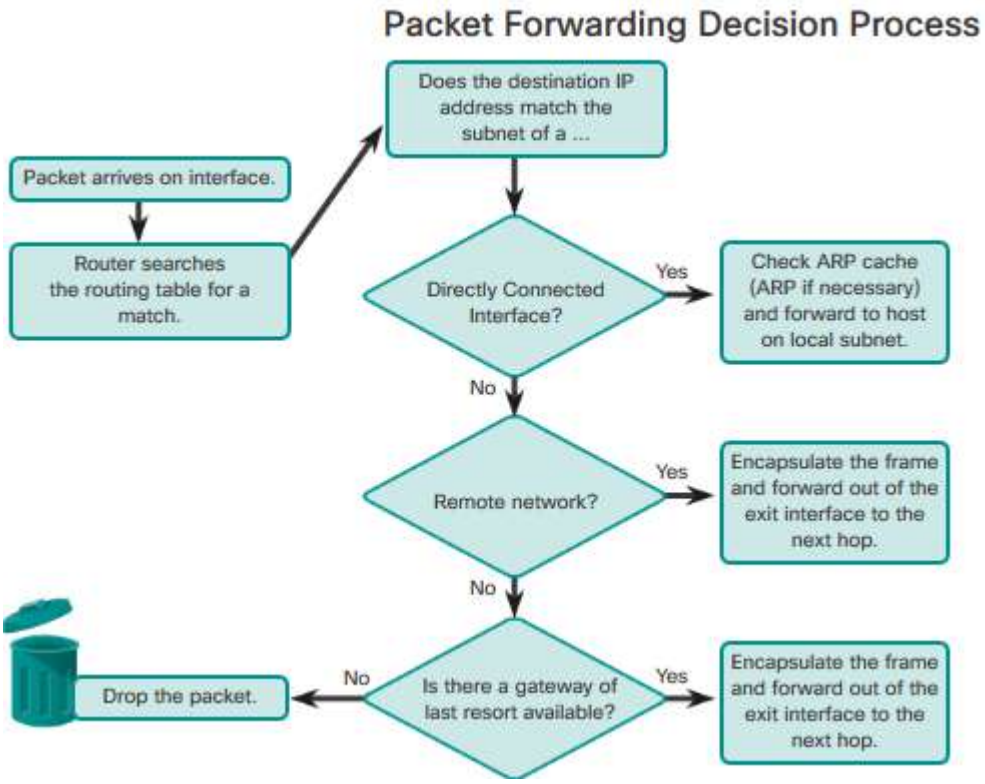
Directly connected network - If the destination IP address of the packet belongs to a device on a network that is directly connected to one of the interfaces of the router, that packet is forwarded directly to the destination device. This means that the destination IP address of the packet is a host address on the same network as the interface of the router.

Remote network - If the destination IP address of the packet belongs to a remote network, then the packet is forwarded to another router. Remote networks can only be reached by forwarding packets to another router.

No route determined - If the destination IP address of the packet does not belong to either a connected

or remote network, the router determines if there is a Gateway of Last Resort available. A Gateway of Last Resort is set when a default route is configured or learned on a router. If there is a default route, the packet is forwarded to the Gateway of Last Resort. If the router does not have a default route, then the packet is discarded.

The logic flowchart in the figure illustrates the router packet forwarding decision process.



Best Path

Determining the best path involves the evaluation of multiple paths to the same destination network and selecting the optimum or shortest path to reach that network. Whenever multiple paths to the same network exist, each path uses a different exit interface on the router to reach that network.

The best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network. A metric is the quantitative value used to measure the distance to a given network. The best path to a network is the path with the lowest metric.

Dynamic routing protocols typically use their own rules and metrics to build and update routing tables. The routing algorithm generates a value, or a metric, for each path through the network. Metrics can be based on either a single characteristic or several characteristics of a path. Some routing protocols can base route selection on multiple metrics, combining them into a single metric.

The following lists some dynamic protocols and the metrics they use:

Routing Information Protocol (RIP) - Hop count

Open Shortest Path First (OSPF) - Cisco's cost based on cumulative bandwidth from source to destination

Enhanced Interior Gateway Routing Protocol (EIGRP) - Bandwidth, delay, load, reliability

Load Balancing

What happens if a routing table has two or more paths with identical metrics to the same destination network?

When a router has two or more paths to a destination with equal cost metrics, then the router forwards the packets using both paths equally. This is called equal cost load balancing. The routing table contains the single destination network, but has multiple exit interfaces, one for each equal cost path. The router forwards packets using the multiple exit interfaces listed in the routing table.

If configured correctly, load balancing can increase the effectiveness and performance of the network. Equal cost load balancing can be configured to use both dynamic routing protocols and static routes.

Note: Only EIGRP supports unequal cost load balancing.

Administrative Distance

It is possible for a router to be configured with multiple routing protocols and static routes. If this occurs, the routing table may have more than one route source for the same destination network. For example, if both RIP and EIGRP are configured on a router, both routing protocols may learn of the same destination network. However, each routing protocol may decide on a different path to reach the destination based on that routing protocol's metrics. RIP chooses a path based on hop count, whereas EIGRP chooses a path based on its composite metric. How does the router know which route to use?

Cisco IOS uses what is known as the administrative distance (AD) to determine the route to install into the IP routing table. The AD represents the "trustworthiness" of the route; the lower the AD, the more trustworthy the route source. For example, a static route has an AD of 1, whereas an EIGRP-discovered route has an AD of 90. Given two separate routes to the same destination, the router chooses the route with the lowest AD. When a router has the choice of a static route and an EIGRP route, the static route takes precedence. Similarly, a directly connected route with an AD of 0 takes precedence over a static route with an AD of 1.

The figure lists various routing protocols and their associated ADs.

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

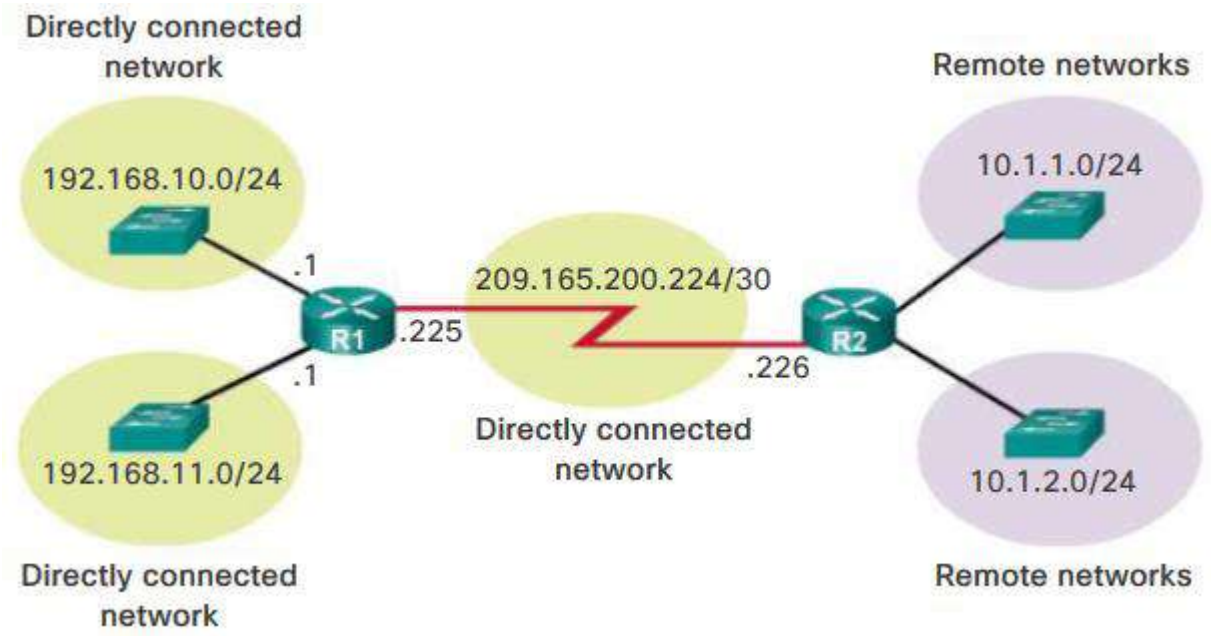
The Routing Table

The routing table of a router stores information about:

Directly connected routes - These routes come from the active router interfaces. Routers add a directly connected route when an interface is configured with an IP address and is activated.

Remote routes - These are remote networks connected to other routers. Routes to these networks can either be statically configured or dynamically learned through dynamic routing protocols.

Specifically, a routing table is a data file in RAM that is used to store route information about directly connected and remote networks. The routing table contains network or next hop associations. These associations tell a router that a particular destination can be optimally reached by sending the packet to a specific router that represents the next hop on the way to the final destination. The next hop association can also be the outgoing or exit interface to the next destination.



On a Cisco router, the show ip route command can be used to display the IPv4 routing table of a router. A router provides additional route information, including how the route was learned, how long the route has been in the table, and which specific interface to use to get to a predefined destination.

Entries in the routing table can be added as:

Local Route interfaces - Added when an interface is configured and active. This entry is only displayed in IOS 15 or newer for IPv4 routes and all IOS releases for IPv6 routes.

Directly connected interfaces - Added to the routing table when an interface is configured and active.

Static routes - Added when a route is manually configured and the exit interface is active.

Dynamic routing protocol - Added when routing protocols that dynamically learn about the network, such as EIGRP or OSPF, are implemented and networks are identified.

The sources of the routing table entries are identified by a code. The code identifies how the route was learned. For instance, common codes include:

- L - Identifies the address assigned to a router's interface. This allows the router to efficiently determine when it receives a packet for the interface instead of being forwarded.

- C - Identifies a directly connected network.
- S - Identifies a static route created to reach a specific network.
- D - Identifies a dynamically learned network from another router using EIGRP.
- - Identifies a dynamically learned network from another router using the OSPF routing protocol.

As a network administrator, it is imperative to know how to interpret the content of IPv4 and IPv6 routing tables. The figure displays an IPv4 routing table entry on R1 for the route to remote network 10.1.1.0.

The entry identifies the following information:

Route source - Identifies how the route was learned.

Destination network - Identifies the address of the remote network.

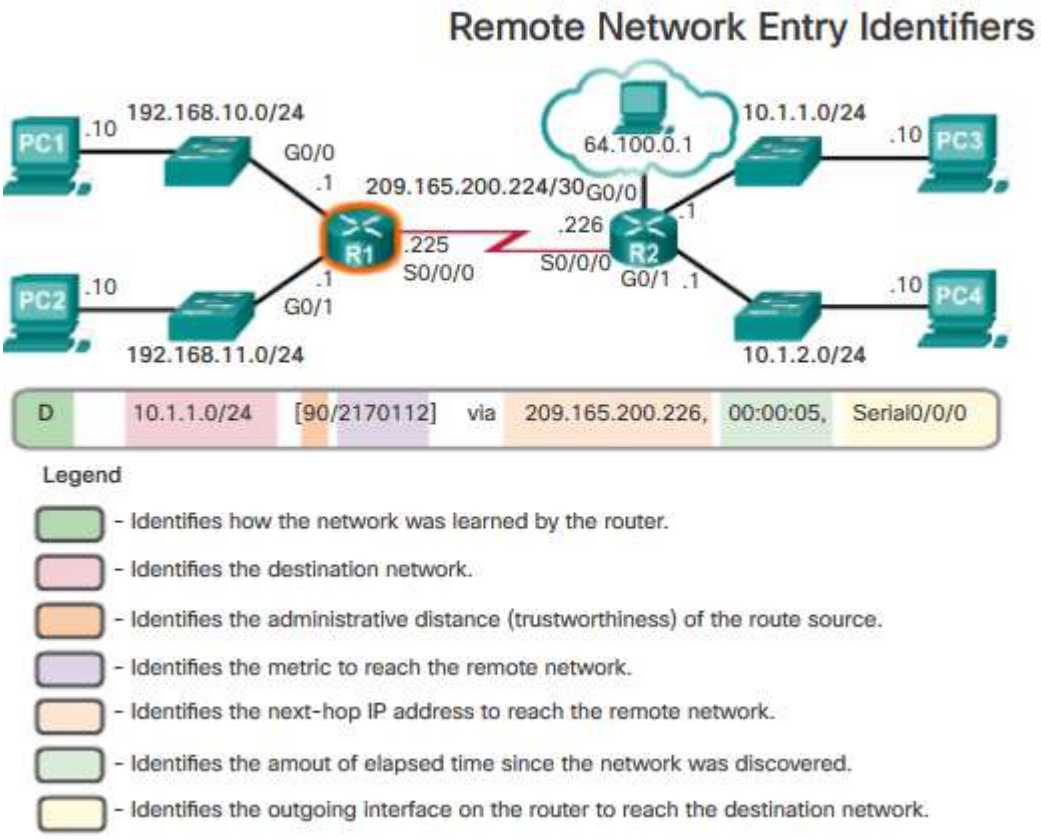
Administrative distance - Identifies the trustworthiness of the route source. Lower values indicate preferred route source.

Metric - Identifies the value assigned to reach the remote network. Lower values indicate preferred routes.

Next-hop - Identifies the IPv4 address of the next router to forward the packet to.

Route timestamp - Identifies how much time has passed since the route was learned.

Outgoing interface - Identifies the exit interface to use to forward a packet toward the final destination.



Review questions

See the practical attachment.

Learning Outcome 2.1: Apply static routing

Static Routes

Routing is at the core of every data network, moving information across an internetwork from source to destination. Routers are the devices responsible for the transfer of packets from one network to the next.

Routers learn about remote networks either dynamically, using routing protocols, or manually, or using static routes. In many cases, routers use a combination of both dynamic routing protocols and static routes. This chapter focuses on static routing.

Static routes are very common and do not require the same amount of processing and overhead as dynamic routing protocols.

In this chapter, sample topologies will be used to configure IPv4 and IPv6 static routes and to present troubleshooting techniques. In the process, several important IOS commands and the resulting output will be examined. An introduction to the routing table using both directly connected networks and static routes will be included.

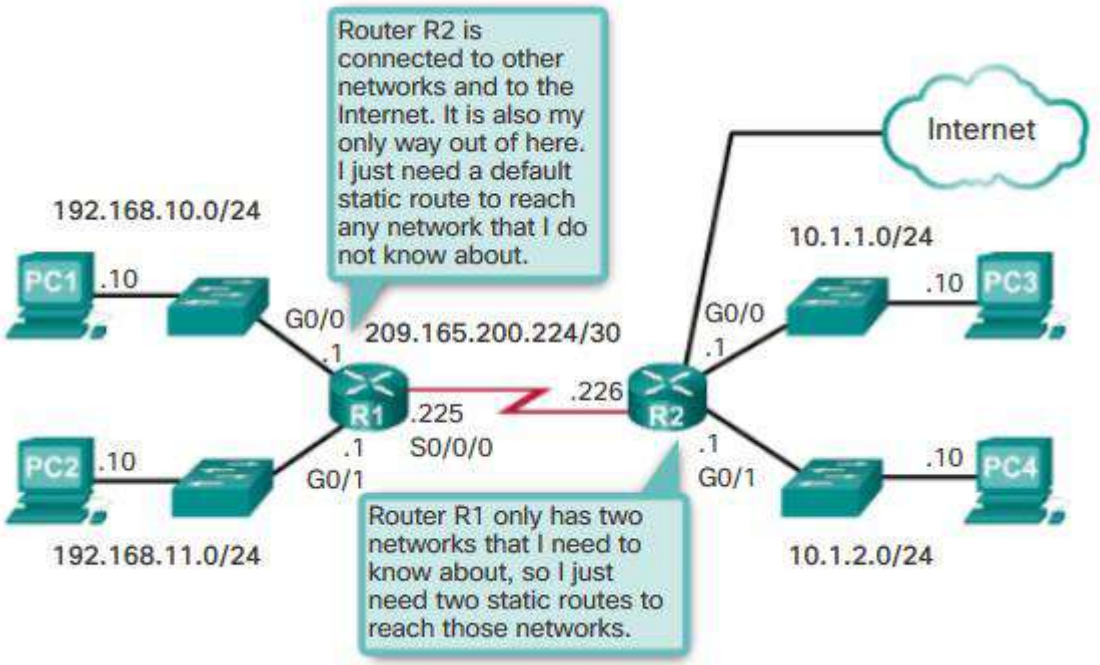
Reach Remote Networks

A router can learn about remote networks in one of two ways:

Manually - Remote networks are manually entered into the route table using static routes.

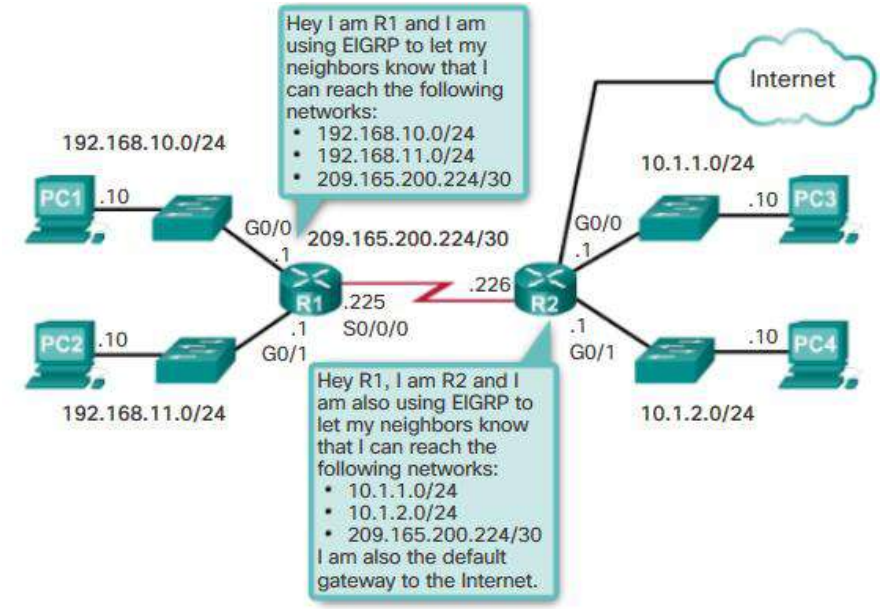
Dynamically - Remote routes are automatically learned using a dynamic routing protocol.

Figure provides a sample scenario of static routing.



A network administrator can manually configure a static route to reach a specific network. Unlike a dynamic routing protocol, static routes are not automatically updated and must be manually reconfigured any time the network topology changes. Figure provides a sample scenario of dynamic

routing using EIGRP.



Why Use Static Routing?

	Dynamic Routing	Static Routing
Configuration Complexity	Generally independent of the network size	Increases with network size
Topology Changes	Automatically adapts to topology changes	Administrator intervention required
Scaling	Suitable for simple and complex topologies	Suitable for simple topologies
Security	Less secure	More secure
Resource Usage	Uses CPU, memory, link bandwith	No extra resources needed
Predictability	Route depends on the current topology	Route to destination is always the same

Review questions

Activity - Identify the Advantages and Disadvantages of Static Routing

Instructions

Determine whether the static routing descriptors are advantages or disadvantages of static routing.

Click the appropriate field next to each descriptor to indicate your answers.

	Advantage	Disadvantage
Configuration complexity increases with network size.		
No extra resources (CPU, bandwidth, etc.) are needed.		
Topology changes will affect configuration.		
Route path to destination is always the same.		
Routing tables are small and maintenance is minimal.		
No automatic updates will be made to the routing table if topology changes.		

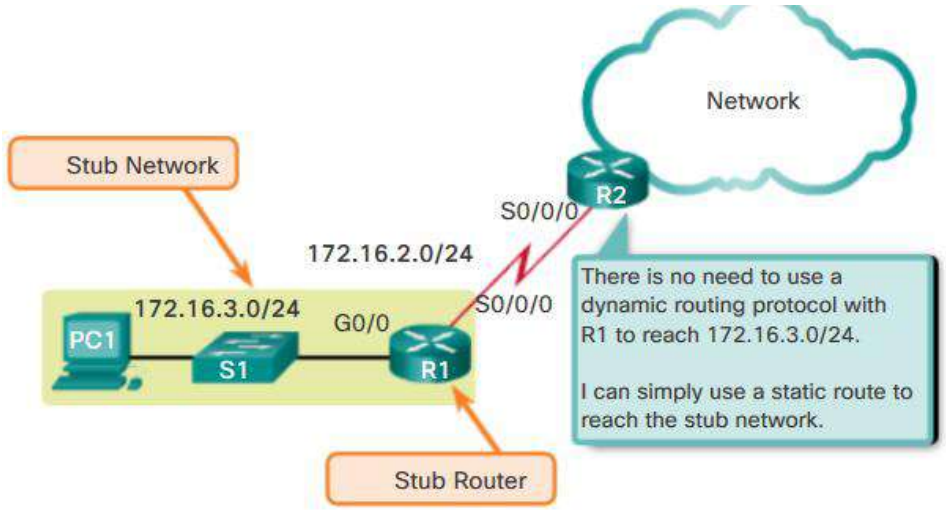
The following types of IPv4 and IPv6 static routes will be discussed:

- Standard static route
- Default static route
- Summary static route
- Floating static route
- Standard Static Route

Both IPv4 and IPv6 support the configuration of static routes. Static routes are useful when connecting to a specific remote network.

The figure shows that R2 can be configured with a static route to reach the stub network 172.16.3.0/24.

Note: The example is highlighting a stub network, but in fact, a static route can be used to connect to any network.



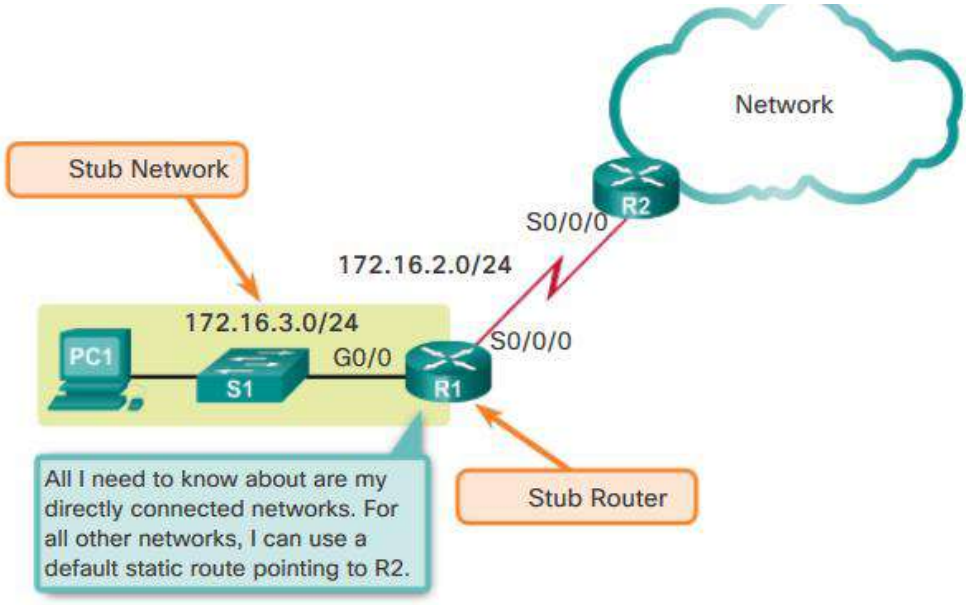
Default Static Route

A default route is a route that matches all packets and is used by the router if a packet does not match any other, more specific route in the routing table. A default route can be dynamically learned or statically configured. A default static route is simply a static route with 0.0.0.0/0 as the destination IPv4 address. Configuring a default static route creates a Gateway of Last Resort.

Default static routes are used:

When no other routes in the routing table match the packet destination IP address. In other words, when a more specific match does not exist. A common use is when connecting a company's edge router to the ISP network.When a router has only one other router to which it is connected. In this situation, the router is known as a stub router.

Refer to the figure for a stub network default route scenario.



Summary Static Route

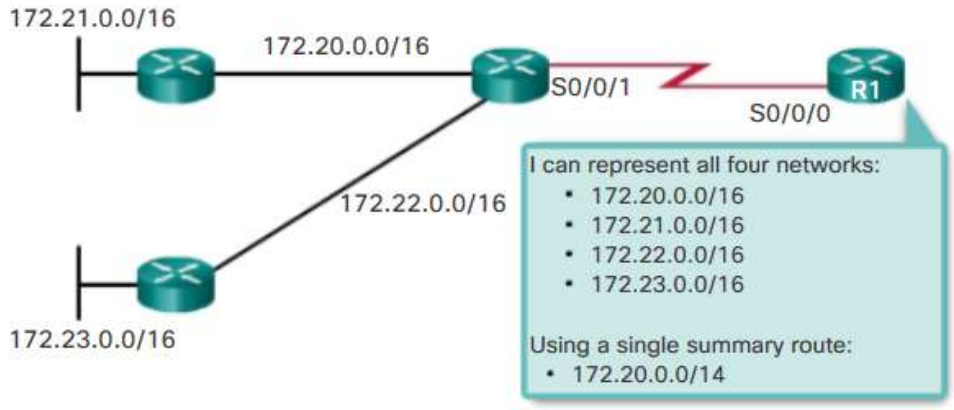
To reduce the number of routing table entries, multiple static routes can be summarized into a single static route if:

The destination networks are contiguous and can be summarized into a single network address.

The multiple static routes all use the same exit interface or next-hop IP address.

In the figure, R1 would require four separate static routes to reach the 172.20.0.0/16 to 172.23.0.0/16 networks. Instead, one summary static route can be configured and still provide connectivity to those networks.

Note: Refer to the Chapter Appendix for more information on calculating and configuring summary static routes.



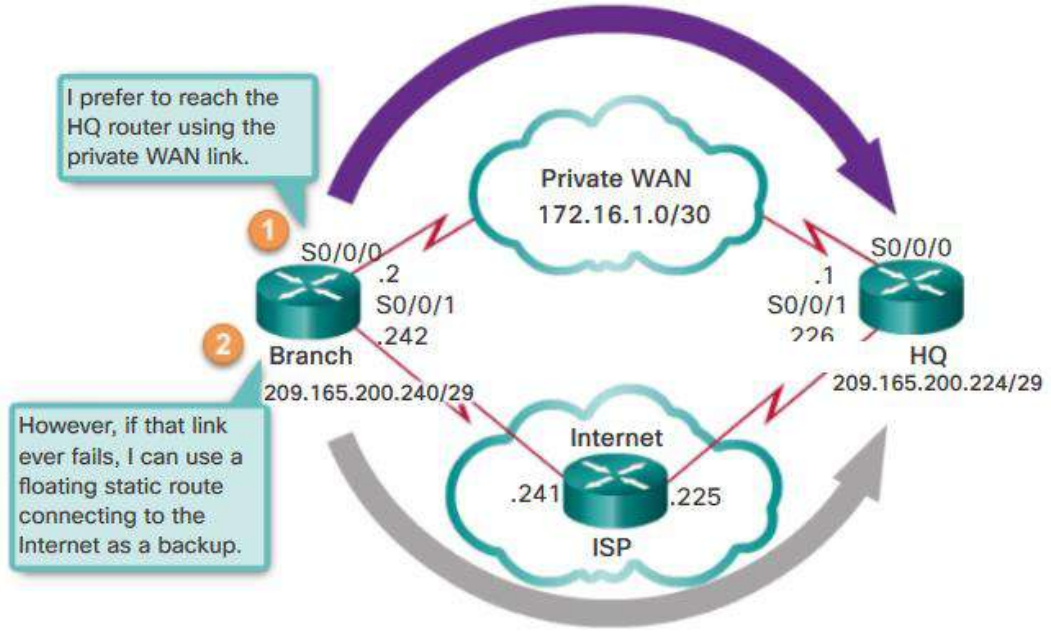
Floating Static Route

Another type of static route is a floating static route. Floating static routes are static routes that are used to provide a backup path to a primary static or dynamic route, in the event of a link failure. The floating static route is only used when the primary route is not available.

To accomplish this, the floating static route is configured with a higher administrative distance than the primary route. The administrative distance represents the trustworthiness of a route. If multiple paths to the destination exist, the router will choose the path with the lowest administrative distance.

For example, assume that an administrator wants to create a floating static route as a backup to an EIGRP-learned route. The floating static route must be configured with a higher administrative distance than EIGRP. EIGRP has an administrative distance of 90. If the floating static route is configured with an administrative distance of 95, the dynamic route learned through EIGRP is preferred to the floating static route. If the EIGRP-learned route is lost, the floating static route is used in its place.

In the figure, the Branch router typically forwards all traffic to the HQ router over the private WAN link. In this example, the routers exchange route information using EIGRP. A floating static route, with an administrative distance of 91 or higher, could be configured to serve as a backup route. If the private WAN link fails and the EIGRP route disappears from the routing table, the router selects the floating static route as the best path to reach the HQ LAN.



Ip route Command

Static routes are configured using the ip route global configuration command.

```
Router(config)# ip route network-address subnet-mask
{ip-address | exit-intf}
```

The following parameters are required to configure static routing:

network-address - Destination network address of the remote network to be added to the routing table, often this is referred to as the prefix.

subnet-mask - Subnet mask, or just mask, of the remote network to be added to the routing table. The subnet mask can be modified to summarize a group of networks.

One or both of the following parameters must also be used:

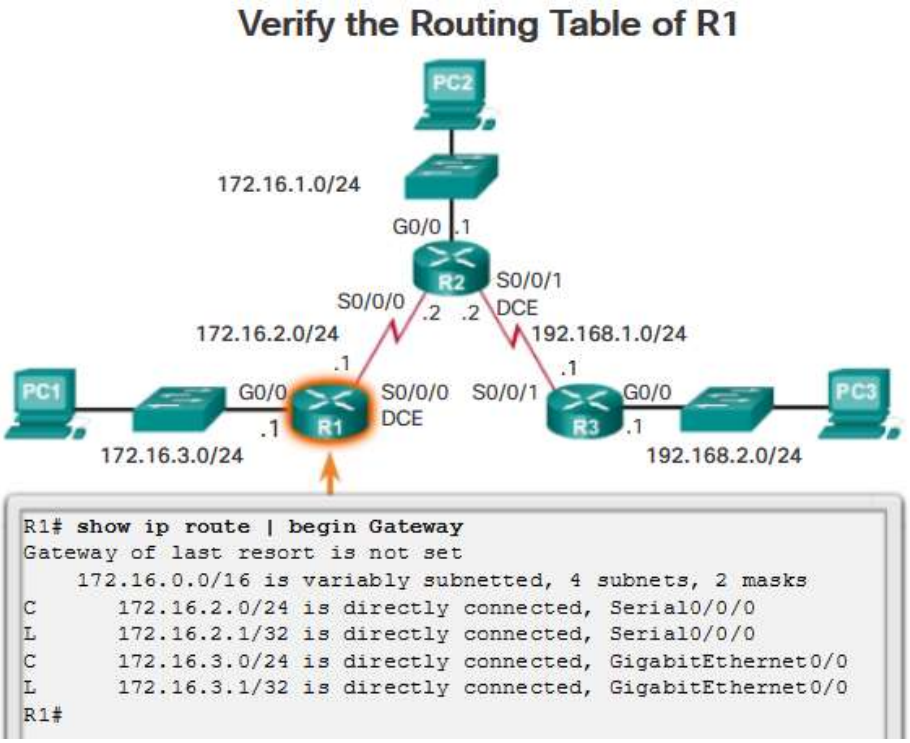
ip-address - The IP address of the connecting router to use to forward the packet to the remote destination network. Commonly referred to as the next hop.

exit-intf - The outgoing interface to use to forward the packet to the next hop.

The *distance* parameter is used to create a floating static route by setting an administrative distance that is higher than a dynamically learned route.

Next-Hop Options

In this example, Figures display the routing tables of R1, R2, and R3. Notice that each router has entries only for directly connected networks and their associated local addresses. None of the routers have any knowledge of any networks beyond their directly connected interfaces.



For example, R1 has no knowledge of networks:

172.16.1.0/24 - LAN on R2

192.168.1.0/24 - Serial network between R2 and R3

192.168.2.0/24 - LAN on R3

Figure 4 displays a successful ping from R1 to R2. Figure displays an unsuccessful ping to the R3 LAN. This is because R1 does not have an entry in its routing table for the R3 LAN network.

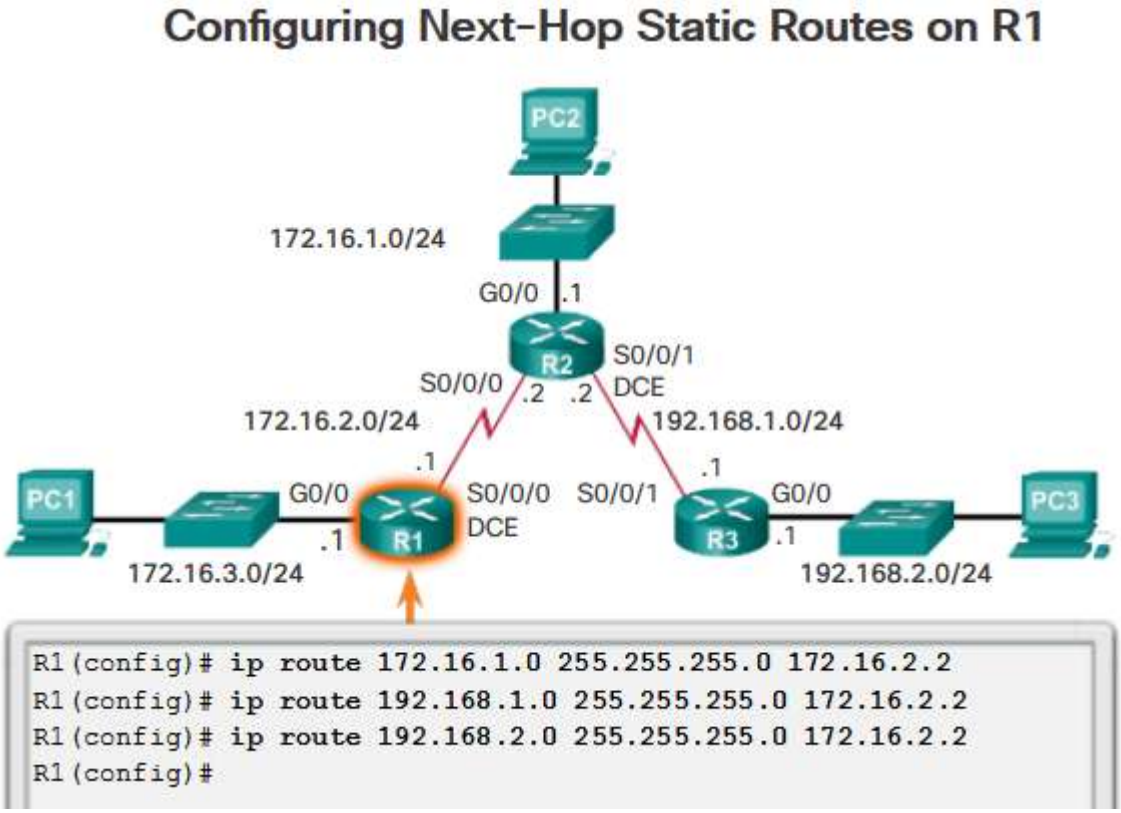
The next hop can be identified by an IP address, exit interface, or both. How the destination is specified creates one of the three following route types:

- Next-hop route - Only the next-hop IP address is specified
- Directly connected static route - Only the router exit interface is specified
- Fully specified static route - The next-hop IP address and exit interface are specified

Configure a Next-Hop Static Route

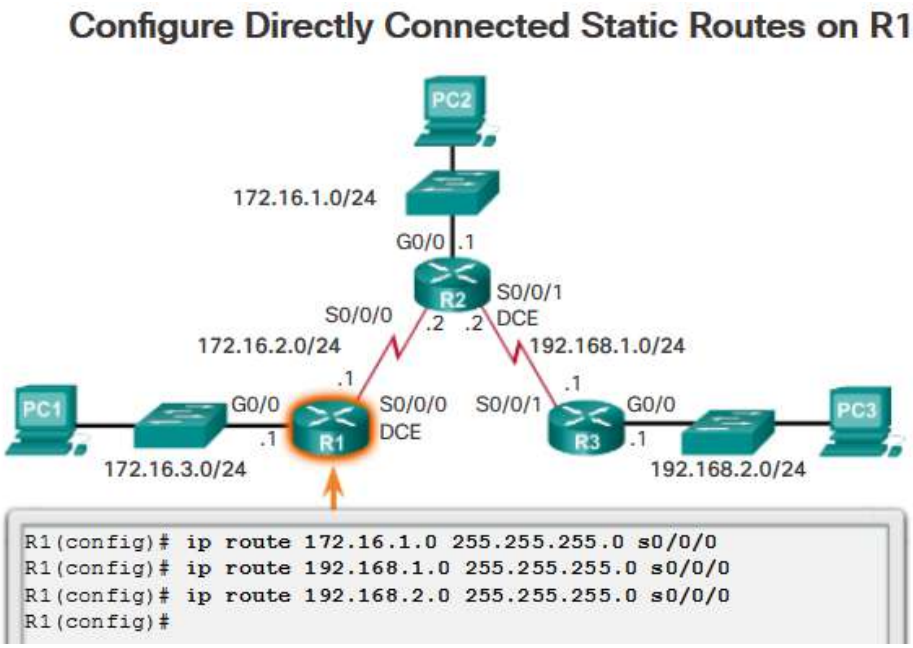
In a next-hop static route, only the next-hop IP address is specified. The exit interface is derived from the next hop. For example, in Figure 1, three next-hop static routes are configured on R1 using the IP address of the next hop, R2.

Before any packet is forwarded by a router, the routing table process must determine the exit interface to use to forward the packet. This is known as route resolvability.



Configure a Directly Connected Static Route

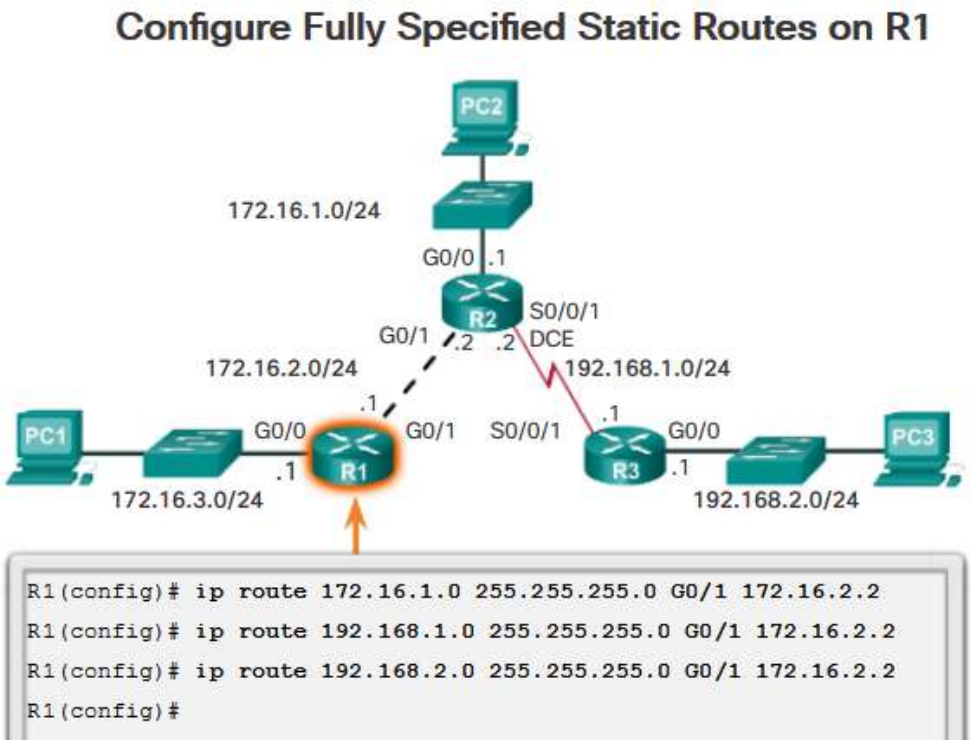
When configuring a static route, another option is to use the exit interface to specify the next-hop address.



Configure a Fully Specified Static Route

Fully Specified Static Route

In a fully specified static route, both the exit interface and the next-hop IP address are specified. This is another type of static route that is used in older IOSs, prior to CEF. This form of static route is used when the exit interface is a multi-access interface and it is necessary to explicitly identify the next hop. The next hop must be directly connected to the specified exit interface.



Verify a Static Route

Along withpingandtraceroute, useful commands to verify static routes include:

- show ip route
- show ip route static
- show ip route *network*

Default Static Route

Routers commonly use default routes that are either configured locally or learned from another router, using a dynamic routing protocol. A default route does not require any left-most bits to match between the default route and the destination IPv4 address. A default route is used when no other routes in the routing table match the destination IP address of the packet. In other words, if a more specific match does not exist, then the default route is used as the Gateway of Last Resort.

Default static routes are commonly used when connecting:

An edge router to a service provider network

A stub router (a router with only one upstream neighbor router)

As shown in the figure, the command syntax for a default static route is similar to any other static route, except that the network address is 0.0.0.0 and the subnet mask is 0.0.0.0.

Note: An IPv4 default static route is commonly referred to as a quad-zero route

```
Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}
```

Parameter	Description
0.0.0.0 0.0.0.0	Matches any network address.
ip-address	• Commonly referred to as the next-hop router's IP address. • Typically used when connecting to a broadcast media (i.e., Ethernet). • Commonly creates a recursive lookup.
exit-intf	• Use the outgoing interface to forward packets to the destination network. • Also referred to as a directly attached static route. • Typically used when connecting in a point-to-point configuration.

The ipv6 route Command

Static routes for IPv6 are configured using the ipv6 route global configuration command. Figure 1 shows the simplified version of the command syntax.

Most of parameters are identical to the IPv4 version of the command. An IPv6 static route can also be implemented as:

- Standard IPv6 static route
- Default IPv6 static route
- Summary IPv6 static route

- Floating IPv6 static route

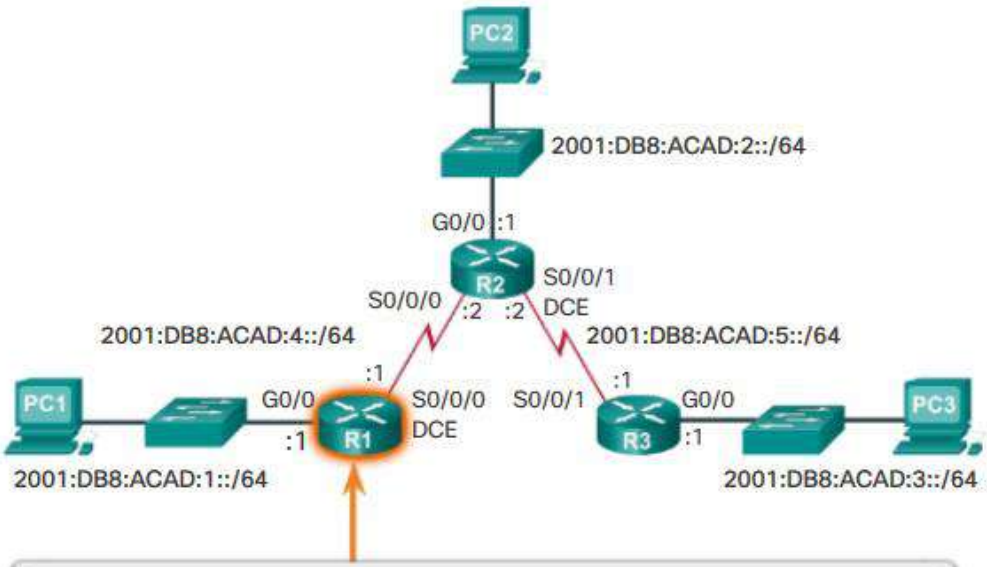
As with IPv4, these routes can be configured as recursive, directly connected, or fully specified.

The ipv6 unicast-routing global configuration command must be configured to enable the router to forward IPv6 packets. Figure displays the enabling of IPv6 unicast routing.

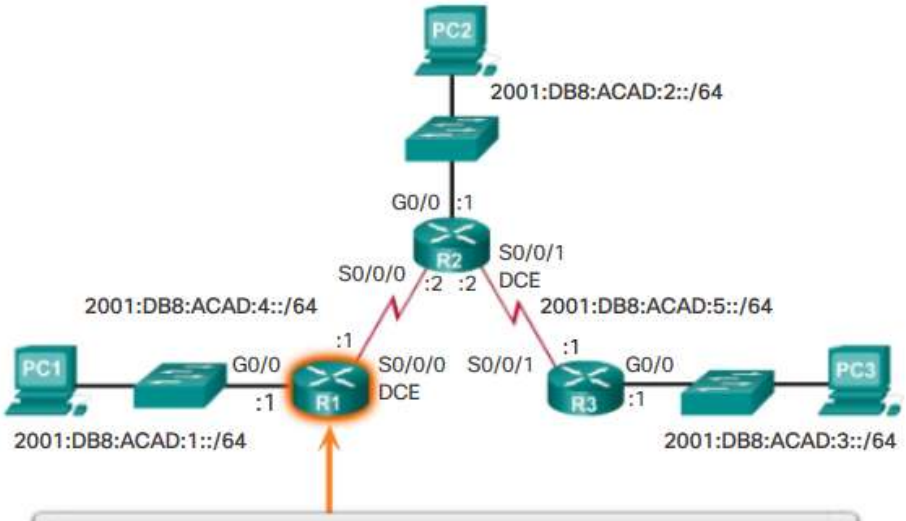
```
Router(config)# ipv6 route ipv6-prefix/ipv6-mask
{ipv6-address | exit-intf}
```

Parameter	Description
ipv6-prefix	Destination network address of the remote network to be added to the routing table.
prefix-length	Prefix length of the remote network to be added to the routing table.
ipv6-address	• Commonly referred to as the next-hop router's IP address. • Typically used when connecting to a broadcast media (i.e., Ethernet). • Commonly creates a recursive lookup.
exit-intf	• Use the outgoing interface to forward packets to the destination network. • Also referred to as a directly attached static route. • Typically used when connecting in a point-to-point configuration.

Enabling IPv6 Unicast Routing

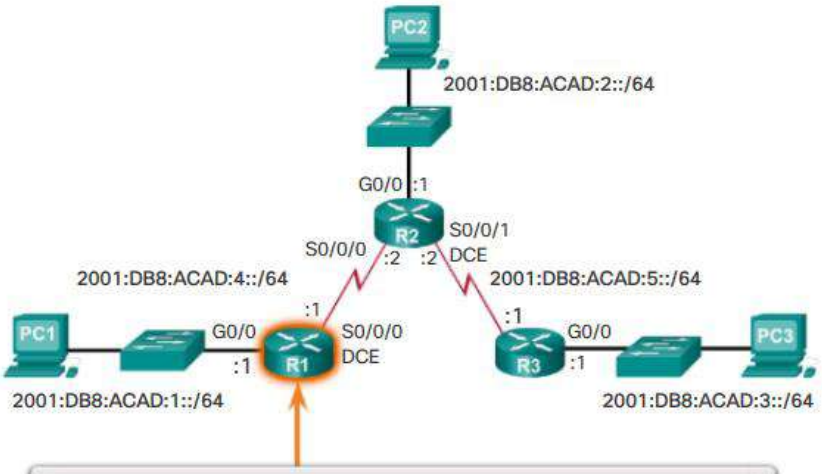


Configure Next-Hop Static IPv6 Routes




```
R1(config)# ipv6 route 2001:DB8:ACAD:2::/64 2001:DB8:ACAD:4::2
R1(config)# ipv6 route 2001:DB8:ACAD:5::/64 2001:DB8:ACAD:4::2
R1(config)# ipv6 route 2001:DB8:ACAD:3::/64 2001:DB8:ACAD:4::2
R1(config)#
```

Configure Directly Connected Static IPv6 Routes on R1




```
R1(config)# ipv6 route 2001:DB8:ACAD:2::/64 s0/0/0
R1(config)# ipv6 route 2001:DB8:ACAD:5::/64 s0/0/0
R1(config)# ipv6 route 2001:DB8:ACAD:3::/64 s0/0/0
R1(config)#
R1#
```

Configure Fully Specified Static IPv6 Routes on R1


```
R1(config)# ipv6 route 2001:db8:acad:2::/64 fe80::2
% Interface has to be specified for a link-local nexthop
R1(config)# ipv6 route 2001:db8:acad:2::/64 s0/0/0 fe80::2
R1(config)#
```

Verify IPv6 Static Routes

Along with ping and traceroute, useful commands to verify static routes include:

- show ipv6 route
- show ipv6 route static
- show ipv6 route network

Default Static IPv6 Route

A default route is a static route that matches all packets. Instead of routers storing routes for all of the networks in the Internet, they can store a single default route to represent any network that is not in the routing table. A default route does not require any left-most bits to match between the default route and the destination IPv6 address.

Routers commonly use default routes that are either configured locally, or learned from another router using a dynamic routing protocol. They are used when no other routes match the packet's destination IP address in the routing table. In other words, if a more specific match does not exist, then use the default route as the Gateway of Last Resort.

Default static routes are commonly used when connecting:

A company's edge router to a service provider network.A router with only an upstream neighbor router. The router has no other neighbors and is therefore, referred to as a stub router.

As shown in the figure, the command syntax for a default static route is similar to any other static route, except that the ipv6-prefix/prefix-length is::/0, which matches all routes.

The basic command syntax of a default static route is:

ipv6 route ::/0 {*ipv6-address* | *exit-intf*}

```
Router(config)# ipv6 route ::/0 {ipv6-address | exit-intf}
```

Parameter	Description
::/0	Matches any IPv6 prefix regardless of prefix length.
ipv6-address	• Commonly referred to as the next-hop router's IPv6 address. • Typically used when connecting to a broadcast media (i.e., Ethernet). • Commonly creates a recursive lookup.
exit-intf	• Use the outgoing interface to forward packets to the destination network. • Also referred to as a directly attached static route. • Typically used when connecting in a point-to-point configuration.

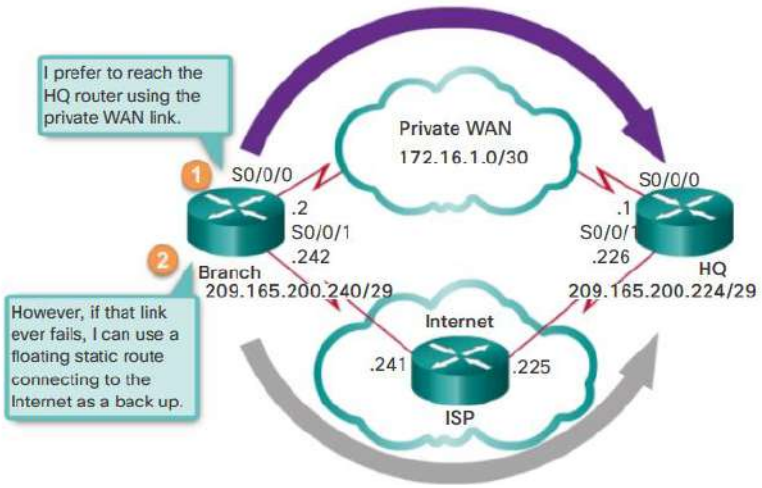
Floating Static Routes

Floating static routes are static routes that have an administrative distance greater than the administrative distance of another static route or dynamic routes. They are very useful when providing a backup to a primary link, as shown in the figure. By default, static routes have an administrative distance of 1, making them preferable to routes learned from dynamic routing protocols. For example, the administrative distances of some common dynamic routing protocols are:

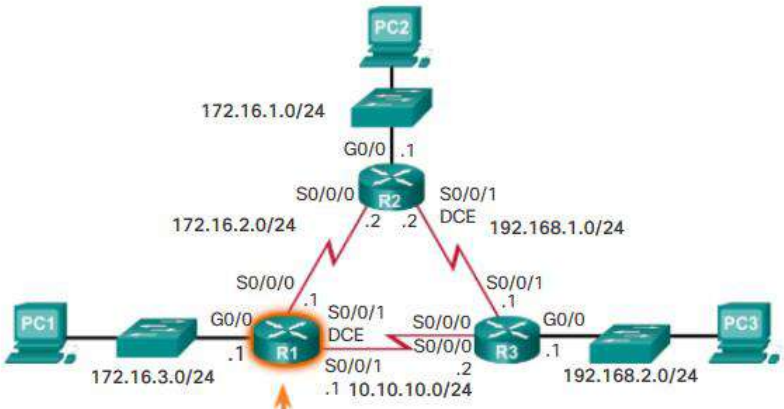
EIGRP = 90
IGRP = 100
OSPF = 110
IS-IS = 115
RIP = 120

The administrative distance of a static route can be increased to make the route less desirable than that of another static route or a route learned through a dynamic routing protocol. In this way, the static route "floats" and is not used when the route with the better administrative distance is active. However, if the preferred route is lost, the floating static route can take over, and traffic can be sent through this alternate route.

Why Configure a Floating Static Route?

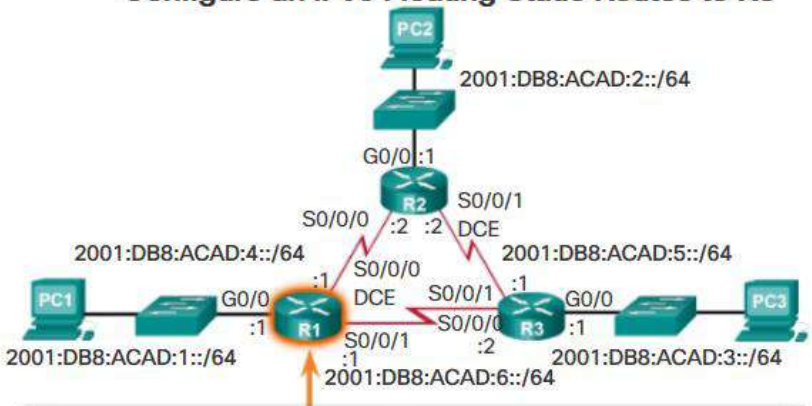


Configuring a Floating Static Route to R3




```
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
R1(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.2 5
R1(config)#
```

Configure an IPv6 Floating Static Routes to R3




```
R1(config)# ipv6 route ::/0 2001:db8:acad:4::2
R1(config)# ipv6 route ::/0 2001:db8:acad:6::2 5
R1(config)#
```

1. Why Routing?

2. What are the types of static routing?

3. specify the connection in which we use the type of static routing.

4. See the practical attachment.

Learning Outcome 2.2: Connect variety networks using EIGRP

Dynamic Routing

The data networks that we use in our everyday lives to learn, play, and work range from small, local networks to large, global internetworks. At home, a user may have a router and two or more computers. At work, an organization may have multiple routers and switches servicing the data communication needs of hundreds or even thousands of PCs.

Routers forward packets by using information in the routing table. Routes to remote networks can be learned by the router in two ways: static routes and dynamic routes.

In a large network with numerous networks and subnets, configuring and maintaining static routes between these networks requires a great deal of administrative and operational overhead. This operational overhead is especially cumbersome when changes to the network occur, such as a down link or implementing a new subnet. Implementing dynamic routing protocols can ease the burden of configuration and maintenance tasks and give the network scalability.

This chapter introduces dynamic routing protocols. It compares the use of static and dynamic routing. Then the implementation of dynamic routing using the Routing Information Protocol version 1 (RIPv1) and version 2 (RIPv2) is discussed. The chapter concludes with an in-depth look at the routing table.

Dynamic Routing Protocol Components

Routing protocols are used to facilitate the exchange of routing information between routers. A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the routing protocol's choice of best paths. The purpose of dynamic routing protocols includes:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available

The main components of dynamic routing protocols include:

Data structures - Routing protocols typically use tables or databases for its operations. This information is kept in RAM.

Routing protocol messages - Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network.

Algorithm - An algorithm is a finite list of steps used to accomplish a task. Routing protocols use algorithms for facilitating routing information and for best path determination.

Routing protocols allow routers to dynamically share information about remote networks and automatically offer this information to their own routing tables.

Routing protocols determine the best path, or route, to each network. That route is then offered to the routing table. The route will be installed in the routing table is there is not another routing source with a lower administrative distance. For example, a static route with an administrative distance of 1 will have precedence over the same network learned by a dynamic routing protocol. A primary benefit of dynamic routing protocols is that routers exchange routing information when there is a topology change. This exchange allows routers to automatically learn about new networks and also to find alternate paths when there is a link failure to a current network.

Advantages	Disadvantages
Suitable in all topologies where multiple routers are required.	Can be more complex to implement.
Generally independent of the network size.	Less secure. Additional configuration settings are required to secure.
Automatically adapts topology to reroute traffic if possible.	Route depends on the current topology.
	Requires additional CPU, RAM, and link bandwidth.

Classifying Routing Protocols

Dynamic routing protocols are used to facilitate the exchange of routing information between routers. A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the routing protocol's choice of best paths. The purpose of dynamic routing protocols includes:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available

Routing protocols can be classified into different groups according to their characteristics. Specifically, routing protocols can be classified by their:

Purpose - Interior Gateway Protocol (IGP) or Exterior Gateway Protocol (EGP)

Operation - Distance vector protocol, link-state protocol, or path-vector protocol

Behavior - Classful (legacy) or classless protocol

For example, IPv4 routing protocols are classified as follows:

RIPv1 (legacy) - IGP, distance vector, classful protocol

IGRP (legacy) - IGP, distance vector, classful protocol developed by Cisco (deprecated from 12.2 IOS and later)

RIPv2 - IGP, distance vector, classless protocol

EIGRP - IGP, distance vector, classless protocol developed by Cisco

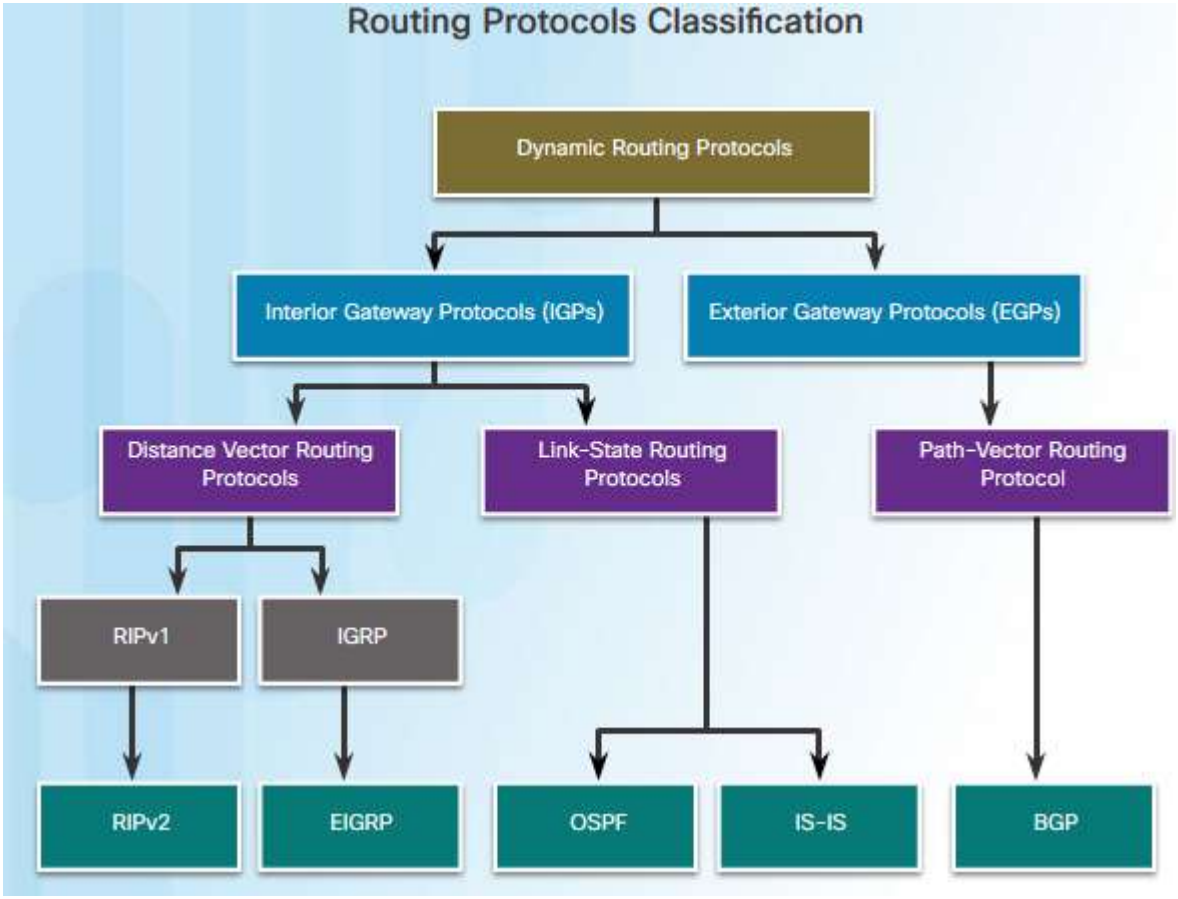
OSPF - IGP, link-state, classless protocol

IS-IS - IGP, link-state, classless protocol

BGP - EGP, path-vector, classless protocol

The classful routing protocols, RIPv1 and IGRP, are legacy protocols and are only used in older networks. These routing protocols have evolved into the classless routing protocols, RIPv2 and EIGRP, respectively. Link-state routing protocols are classless by nature.

The figure displays a hierarchical view of dynamic routing protocol classification.



IGP and EGP Routing Protocols

An autonomous system (AS) is a collection of routers under a common administration such as a company or an organization. An AS is also known as a routing domain. Typical examples of an AS are a company's internal network and an ISP's network.

The Internet is based on the AS concept; therefore, two types of routing protocols are required:

Interior Gateway Protocols (IGP) - Used for routing within an AS. It is also referred to as intra-AS routing. Companies, organizations, and even service providers use an IGP on their internal networks. IGPs include RIP, EIGRP, OSPF, and IS-IS.

Exterior Gateway Protocols (EGP) - Used for routing between ASes. It is also referred to as inter-AS routing. Service providers and large companies may interconnect using an EGP. The Border Gateway Protocol (BGP) is the only currently-viable EGP and is the official routing protocol used on the Internet.

Note: Because BGP is the only EGP available, the term EGP is rarely used; instead, most engineers simply refer to BGP.

The example in the figure provides simple scenarios highlighting the deployment of IGPs, BGP, and static routing:

ISP-1 - This is an AS and it uses IS-IS as the IGP. It interconnects with other autonomous systems and service providers using BGP to explicitly control how traffic is routed.

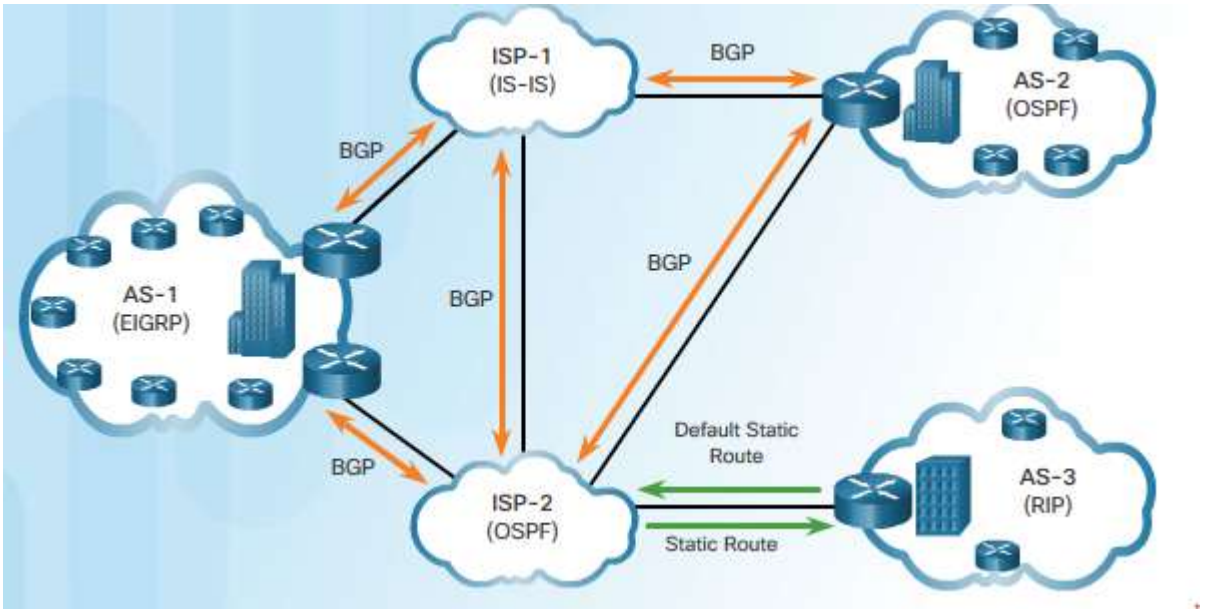
ISP-2 - This is an AS and it uses OSPF as the IGP. It interconnects with other autonomous systems and service providers using BGP to explicitly control how traffic is routed.

AS-1 - This is a large organization and it uses EIGRP as the IGP. Because it is multihomed (i.e., connects to two different service providers), it uses BGP to explicitly control how traffic enters and leaves the AS.

AS-2 - This is a medium-sized organization and it uses OSPF as the IGP. It is also multihomed; therefore, it uses BGP to explicitly control how traffic enters and leaves the AS.

AS-3 - This is a small organization with older routers within the AS; it uses RIP as the IGP. BGP is not required because it is single-homed (i.e., connects to one service provider). Instead, static routing is implemented between the AS and the service provider.

Note: BGP is beyond the scope of this course and is not discussed in detail.



Distance Vector Routing Protocols

Distance vector means that routes are advertised by providing two characteristics:

Distance - Identifies how far it is to the destination network and is based on a metric such as the hop count, cost, bandwidth, delay, and more.

Vector - Specifies the direction of the next-hop router or exit interface to reach the destination.

For example, in the figure, R1 knows that the distance to reach network 172.16.3.0/24 is one hop and that the direction is out of the interface S0/0/0 toward R2.

A router using a distance vector routing protocol does not have the knowledge of the entire path to a destination network. Distance vector protocols use routers as sign posts along the path to the final

destination. The only information a router knows about a remote network is the distance or metric to reach that network and which path or interface to use to get there. Distance vector routing protocols do not have a map of the network topology like other types of routing protocols do.

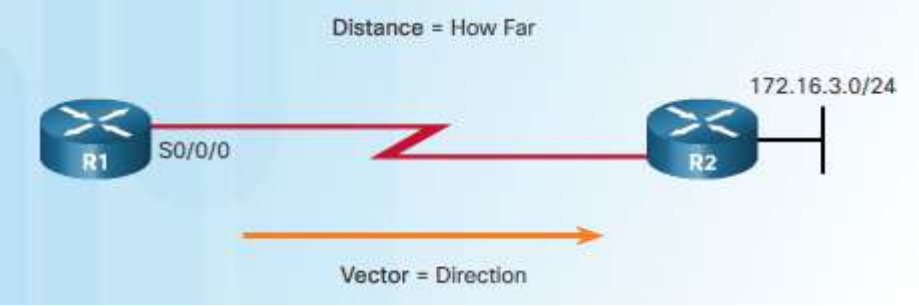
There are four distance vector IPv4 IGPs:

RIPv1 - First generation legacy protocol

RIPv2 - Simple distance vector routing protocol

IGRP - First generation Cisco proprietary protocol (obsolete and replaced by EIGRP)

EIGRP - Advanced version of distance vector routing

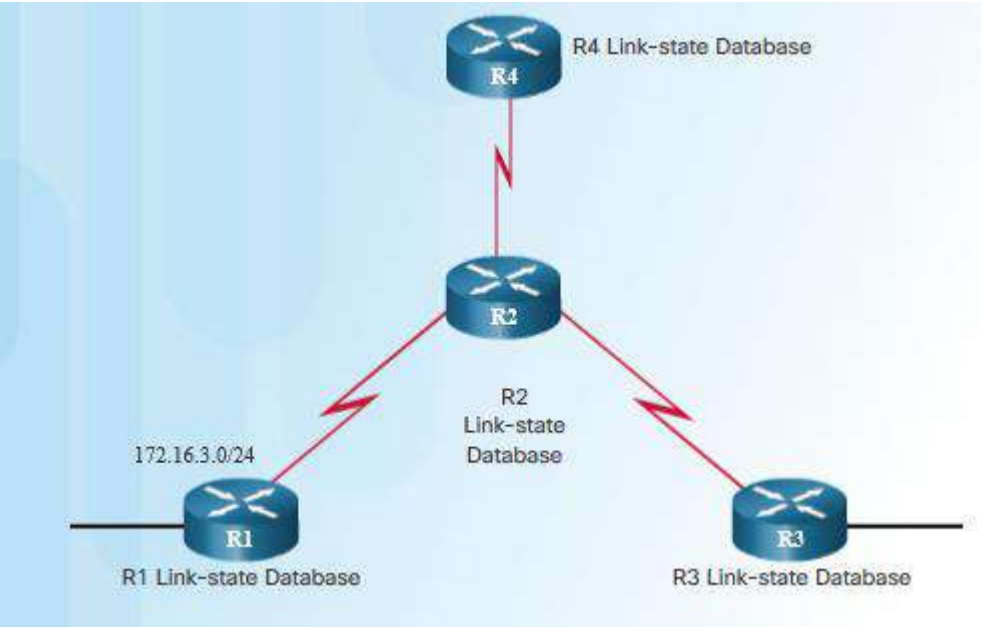


Link-State Routing Protocols

In contrast to distance vector routing protocol operation, a router configured with a link-state routing protocol can create a complete view or topology of the network by gathering information from all of the other routers.

To continue our analogy of sign posts, using a link-state routing protocol is like having a complete map of the network topology. The sign posts along the way from source to destination are not necessary, because all link-state routers are using an identical map of the network. A link-state router uses the link-state information to create a topology map and to select the best path to all destination networks in the topology.

Link-state routing protocols do not use periodic updates. In contrast, RIP-enabled routers send periodic updates of their routing information to their neighbors. After the routers have learned about all the required networks (achieved convergence), a link-state update is only sent when there is a change in the topology. For example, the link-state update in the animation is not sent until the 172.16.3.0 network goes down.



Outing Protocol Characteristics

Routing protocols can be compared based on the following characteristics:

Speed of Convergence - Speed of convergence defines how quickly the routers in the network topology share routing information and reach a state of consistent knowledge. The faster the convergence, the more preferable the protocol. Routing loops can occur when inconsistent routing tables are not updated due to slow convergence in a changing network.

Scalability - Scalability defines how large a network can become, based on the routing protocol that is deployed. The larger the network is, the more scalable the routing protocol needs to be.

Classful or Classless (Use of VLSM) - Classful routing protocols do not include the subnet mask and cannot support VLSM. Classless routing protocols include the subnet mask in the updates. Classless routing protocols support VLSM and better route summarization.

Resource Usage - Resource usage includes the requirements of a routing protocol such as memory space (RAM), CPU utilization, and link bandwidth utilization. Higher resource requirements necessitate more powerful hardware to support the routing protocol operation, in addition to the packet forwarding processes.

Implementation and Maintenance - Implementation and maintenance describes the level of knowledge that is required for a network administrator to implement and maintain the network based on the routing protocol deployed.

The table in the figure summarizes the characteristics of each routing protocol.

	Distance Vector				Link State	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Speed of Convergence	Slow	Slow	Slow	Fast	Fast	Fast
Scalability - Size of Network	Small	Small	Small	Large	Large	Large
Use of VLSM	No	Yes	No	Yes	Yes	Yes
Resource Usage	Low	Low	Low	Medium	High	High
Implementation and Maintenance	Simple	Simple	Simple	Complex	Complex	Complex

Routing Protocol Metrics

There are cases when a routing protocol learns of more than one route to the same destination. To select the best path, the routing protocol must be able to evaluate and decide between the available paths. This is accomplished through the use of routing metrics.

A metric is a measurable value that is assigned by the routing protocol to different routes based on the usefulness of that route. In situations where there are multiple paths to the same remote network, the routing metrics are used to determine the overall "cost" of a path from source to destination. Routing protocols determine the best path based on the route with the lowest cost.

Different routing protocols use different metrics. The metric used by one routing protocol is not comparable to the metric used by another. As a result, two different routing protocols might choose different paths to the same destination.

The following lists some dynamic protocols and the metrics they use:

- Routing Information Protocol (RIP) - Hop count
- Open Shortest Path First (OSPF) - Cisco's cost based on cumulative bandwidth from source to destination
- Enhanced Interior Gateway Routing Protocol (EIGRP) – Minimum bandwidth, delay, load, reliability, and maximum transmission unit (MTU).

Dynamic Routing Protocol Operation

All routing protocols are designed to learn about remote networks and to quickly adapt whenever there is a change in the topology. The method that a routing protocol uses to accomplish this depends upon the algorithm it uses and the operational characteristics of that protocol.

In general, the operations of a dynamic routing protocol can be described as follows:

1. The router sends and receives routing messages on its interfaces.

2. The router shares routing messages and routing information with other routers that are using the same routing protocol.

3. Routers exchange routing information to learn about remote networks.

4. When a router detects a topology change, the routing protocol can advertise this change to otherrouters.

Cold Start

When a router powers up, it knows nothing about the network topology. It does not even know that there are devices on the other end of its links. The only information that a router has is from its own saved configuration file stored in NVRAM. After a router boots successfully, it applies the saved configuration. If the IP addressing is configured correctly, then the router initially discovers its own directly connected networks.

Network Discovery

After initial boot up and discovery, the routing table is updated with all directly connected networks and the interfaces those networks reside on.

If a routing protocol is configured, the next step is for the router to begin exchanging routing updates to learn about any remote routes.

The router sends an update packet out all interfaces that are enabled on the router. The update contains the information in the routing table, which currently is all directly connected networks.

At the same time, the router also receives and processes similar updates from other connected routers. Upon receiving an update, the router checks it for new network information. Any networks that are not currently listed in the routing table are added.

Exchanging the Routing Information

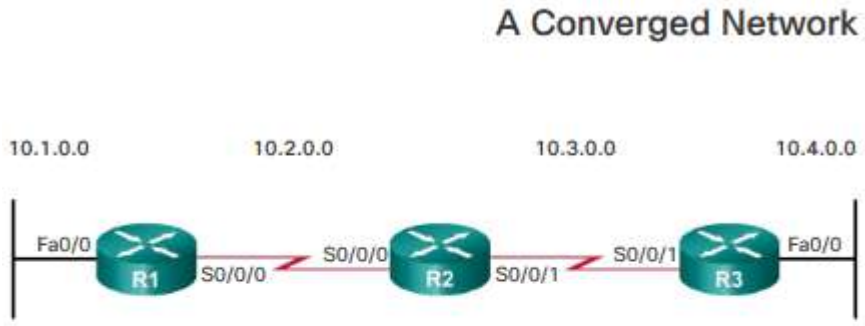
At this point the routers have knowledge about their own directly connected networks and about the connected networks of their immediate neighbors. Continuing the journey toward convergence, the routers exchange the next round of periodic updates. Each router again checks the updates for new information.

Achieving Convergence

The network has converged when all routers have completed and accurate information about the entire network, as shown in the figure. Convergence time is the time it takes routers to share information, calculate best paths, and update their routing tables. A network is not completely operable until the network has converged; therefore, most networks require short convergence times.

Convergence is both collaborative and independent. The routers share information with each other but must independently calculate the impacts of the topology change on their own routes. Because they develop an agreement with the new topology independently, they are said to converge on this consensus. Convergence properties include the speed of propagation of routing information and the calculation of optimal paths. The speed of propagation refers to the amount of time it takes for routers within the network to forward routing information.

Routing protocols can be rated based on the speed to convergence, the faster the convergence, the better the routing protocol. Generally, older protocols, such as RIP, are slow to converge, whereas modern protocols, such as EIGRP and OSPF, converge more quickly.



10.1.0.0	Fa0/0	0	10.2.0.0	S0/0/0	0	10.3.0.0	S0/0/1	0
10.2.0.0	S0/0/0	0	10.3.0.0	S0/0/1	0	10.4.0.0	Fa0/0	0
10.3.0.0	S0/0/0	1	10.1.0.0	S0/0/0	1	10.2.0.0	S0/0/1	1
10.4.0.0	S0/0/0	2	10.4.0.0	S0/0/1	1	10.1.0.0	S0/0/1	2

Distance Vector Algorithm

At the core of the distance vector protocol is the routing algorithm. The algorithm is used to calculate the best paths and then send that information to the neighbors.

The algorithm used for the routing protocols defines the following processes:

- Mechanism for sending and receiving routing information
- Mechanism for calculating the best paths and installing routes in the routing table
- Mechanism for detecting and reacting to topology changes

Different routing protocols use different algorithms to install routes in the routing table, send updates to neighbors, and make path determination decisions. For example:

RIP uses the Bellman-Ford algorithm as its routing algorithm. It is based on two algorithms developed in 1958 and 1956 by Richard Bellman and Lester Ford, Jr.

IGRP and EIGRP use the Diffusing Update Algorithm (DUAL) routing algorithm developed by Dr. J.J. Garcia-Luna-Aceves at SRI International.

Routing Information Protocol

The Routing Information Protocol (RIP) was a first generation routing protocol for IPv4 originally specified in RFC 1058. It is easy to configure, making it a good choice for small networks.

RIPv1 has the following key characteristics:

Routing updates are broadcasted (255.255.255.255) every 30 seconds.

The hop count is used as the metric for path selection.

A hop count greater than 15 hops is deemed infinite (too far). That 15th hop router would not propagate the routing update to the next router.

In 1993, RIPv1 was updated to a classless routing protocol known as RIP version 2 (RIPv2). RIPv2

included the following improvements:

Classless routing protocol - It supports VLSM and CIDR, because it includes the subnet mask in the routing updates.

Increased efficiency - It forwards updates to multicast address 224.0.0.9, instead of the broadcast address 255.255.255.255.

Reduced routing entries - It supports manual route summarization on any interface.

Secure - It supports an authentication mechanism to secure routing table updates between neighbors.

RIP updates are encapsulated into a UDP segment, with both source and destination port numbers set to UDP port 520.

In 1997, the IPv6 enabled version of RIP was released. RIPng is based on RIPv2. It still has a 15 hop limitation and the administrative distance is 120.

Enhanced Interior-Gateway Routing Protocol

The Interior Gateway Routing Protocol (IGRP) was the first proprietary IPv4 routing protocol developed by Cisco in 1984. It used the following design characteristics:

Bandwidth, delay, load, and reliability are used to create a composite metric.

Routing updates are broadcast every 90 seconds, by default.

Maximum limit of 255 hops

In 1992, IGRP was replaced by Enhanced IGRP (EIGRP). Like RIPv2, EIGRP also introduced support for VLSM and CIDR. EIGRP increases efficiency, reduces routing updates, and supports secure message exchange.

EIGRP also introduced:

Bounded triggered updates - It does not send periodic updates. Only routing table changes are propagated, whenever a change occurs. This reduces the amount of load the routing protocol places on the network. Bounded triggered updates means that EIGRP only sends to the neighbors that need it. It uses less bandwidth, especially in large networks with many routes.

Hello keepalive mechanism - A small Hello message is periodically exchanged to maintain adjacencies with neighboring routers. This requires a very low usage of network resources during normal operation, as compared to periodic updates.

Maintains a topology table - Maintains all the routes received from neighbors (not only the best paths) in a topology table. DUAL can insert backup routes into the EIGRP topology table.

Rapid convergence - In most cases, it is the fastest IGP to converge because it maintains alternate routes, enabling almost instantaneous convergence. If a primary route fails, the router can use the already identified alternate route. The switchover to the alternate route is immediate and does not involve interaction with other routers.

Multiple network layer protocol support - EIGRP uses Protocol Dependent Modules (PDM), which means that it is the only protocol to include support for protocols other than IPv4 and IPv6, such as

legacy IPX and AppleTalk.

Routing Table Terms

A dynamically built routing table provides a great deal of information, as shown in the figure. Therefore, it is crucial to understand the output generated by the routing table. Special terms are applied when discussing the contents of a routing table.

The Cisco IP routing table is not a flat database. The routing table is actually a hierarchical structure that is used to speed up the lookup process when locating routes and forwarding packets. Within this structure, the hierarchy includes several levels.

Routes are discussed in terms of:

- Ultimate route
- Level 1 route
- Level 1 parent route
- Level 2 child routes
- Ultimate Route

An ultimate route is a routing table entry that contains either a next-hop IPv4 address or an exit interface. Directly connected, dynamically learned, and local routes are ultimate routes.

In the figure, the highlighted areas are examples of ultimate routes. Notice that all of these routes specify either a next-hop IPv4 address or an exit interface.

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/0
L        172.16.1.1/32 is directly connected, GigabitEthernet0/0
R        172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12,
         Serial0/0/0
R        172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12,
          Serial0/0/0
R        172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12,
         Serial0/0/0
```

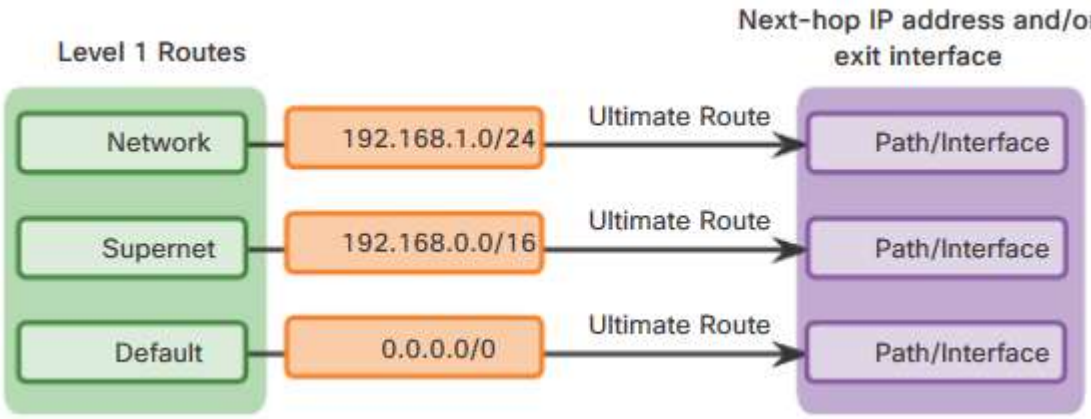
Level 1 Route

A level 1 route is a route with a subnet mask equal to or less than the classful mask of the network address. Therefore, a level 1 route can be a:

Network route - A network route that has a subnet mask equal to that of the classful mask.

Supernet route - A supernet route is a network address with a mask less than the classful mask, for example, a summary address.

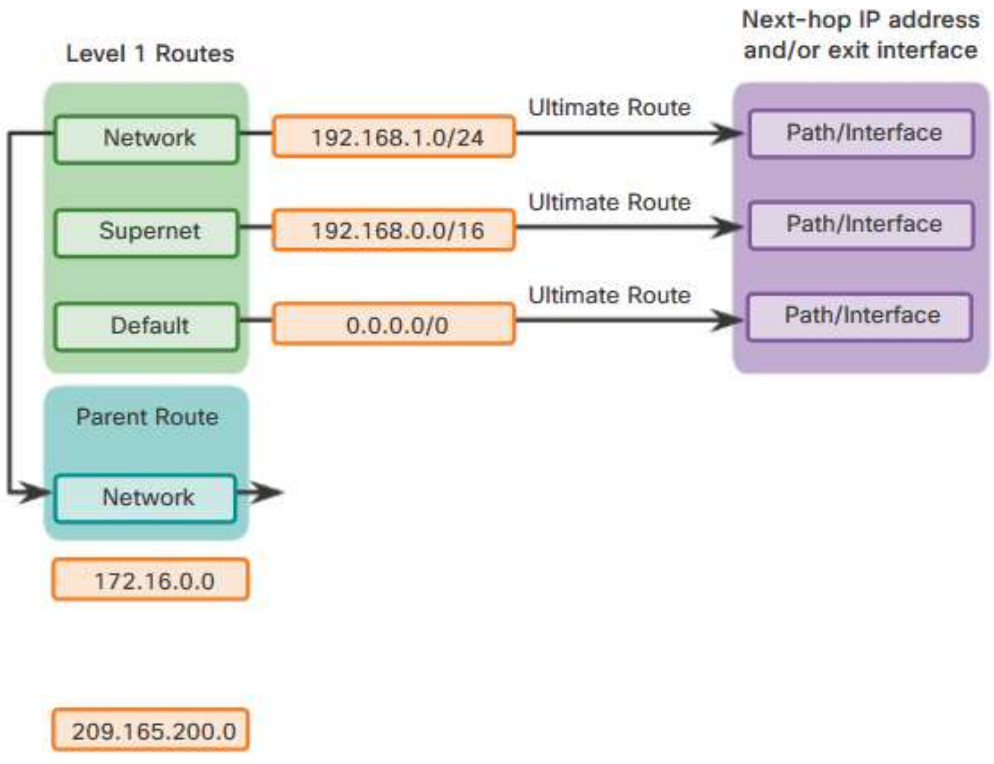
Default route - A default route is a static route with the address 0.0.0.0/0.




```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network
0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3
masks
C        172.16.1.0/24 is directly connected,
GigabitEthernet0/0
L        172.16.1.1/32 is directly connected,
GigabitEthernet0/0
R        172.16.2.0/24 [120/1] via 209.165.200.226,
00:00:12, Serial0/0/0
R        172.16.3.0/24 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R        172.16.4.0/28 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R     192.168.0.0/16 [120/2] via 209.165.200.226,
00:00:03, Serial0/0/0
```

Level 1 Parent Route

As illustrated in Figure 1, the 172.16.0.0 and 209.165.200.0 routes are level 1 parent routes. A parent route is a level 1 network route that is subnetted. A parent route can never be an ultimate route.

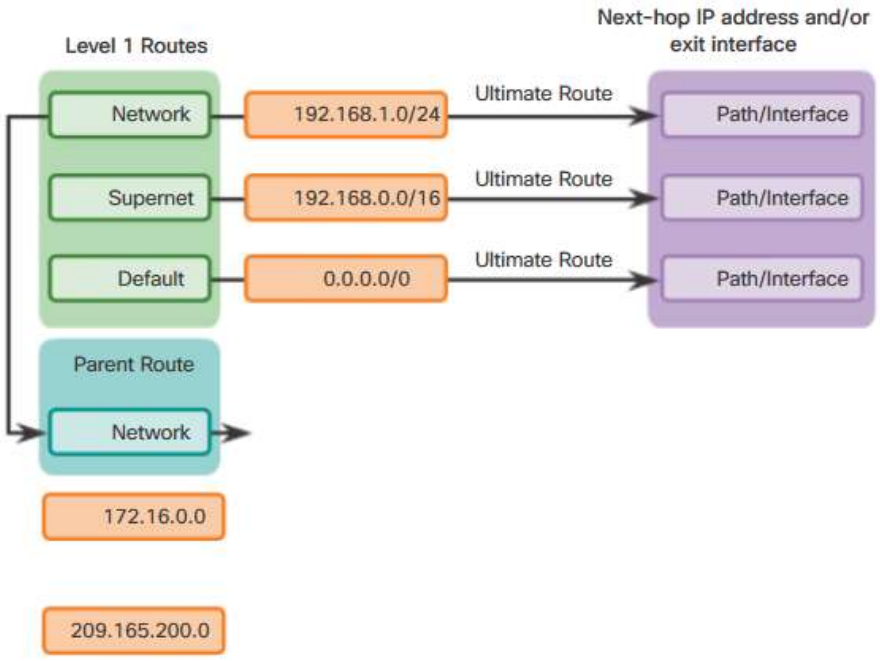



```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network
0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                is directly connected, Serial0/0/1

172.16.0.0/16 is variably subnetted, 5 subnets,
 3 masks
```

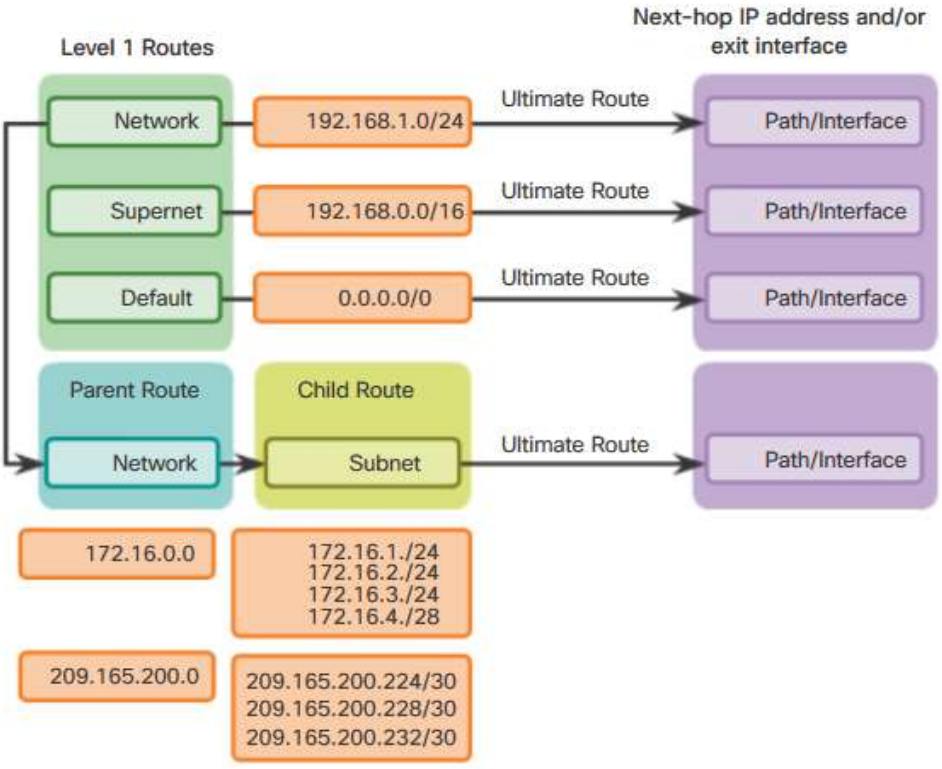
Level 2 Child Route

A level 2 child route is a route that is a subnet of a classful network address. As illustrated in Figure , a level 1 parent route is a level 1 network route that is subnetted.

Level 2 Child Route



Child Routes are Ultimate Routes



```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network
0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3
masks
C        172.16.1.0/24 is directly connected,
GigabitEthernet0/0
L        172.16.1.1/32 is directly connected,
GigabitEthernet0/0
R        172.16.2.0/24 [120/1] via 209.165.200.226,
 00:00:12, Serial0/0/0
R        172.16.3.0/24 [120/2] via 209.165.200.226,
 00:00:12, Serial0/0/0
R        172.16.4.0/28 [120/2] via 209.165.200.226,
 00:00:12, Serial0/0/0
R     192.168.0.0/16 [120/2] via 209.165.200.226,
00:00:03, Serial0/0/0
```

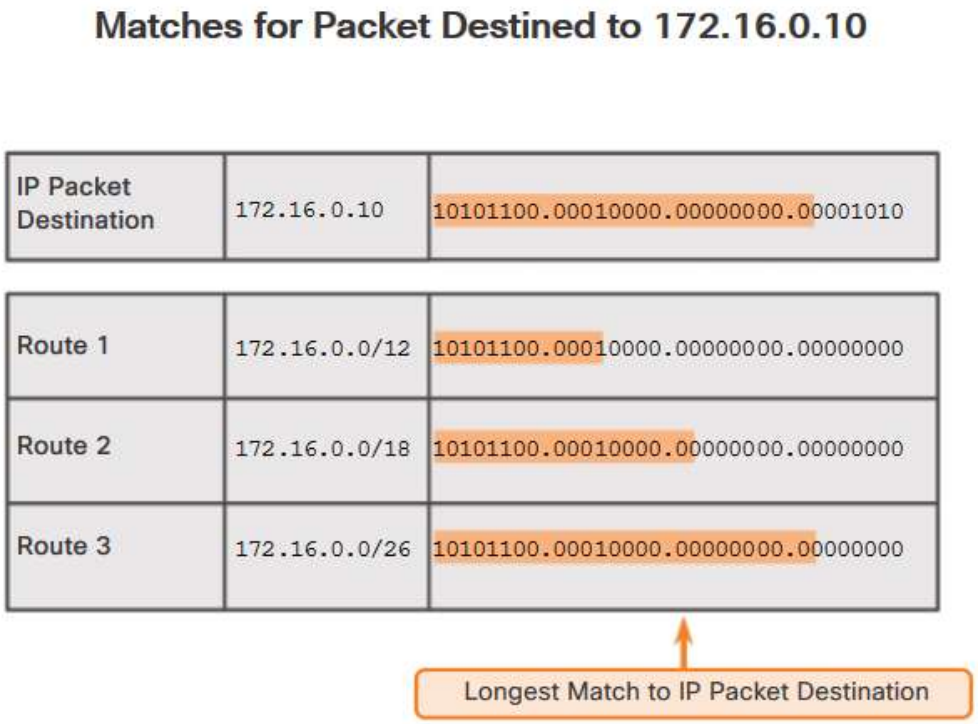
Best Route = Longest Match

What is meant by the router must find the best match in the routing table? Best match is equal to the longest match.

For there to be a match between the destination IPv4 address of a packet and a route in the routing table, a minimum number of far left bits must match between the IPv4 address of the packet and the route in the routing table. The subnet mask of the route in the routing table is used to determine the minimum number of far left bits that must match. Remember that an IPv4 packet only contains the IPv4 address and not the subnet mask.

The best match is the route in the routing table that has the most number of far left matching bits with the destination IPv4 address of the packet. The route with the greatest number of equivalent far left bits, or the longest match, is always the preferred route.

In the figure, a packet is destined for 172.16.0.10. The router has three possible routes that match this packet: 172.16.0.0/12, 172.16.0.0/18, and 172.16.0.0/26. Of the three routes, 172.16.0.0/26 has the longest match and is chosen to forward the packet. Remember, for any of these routes to be considered a match there must be at least the number of matching bits indicated by the subnet mask of the route.



Routing Table Entries

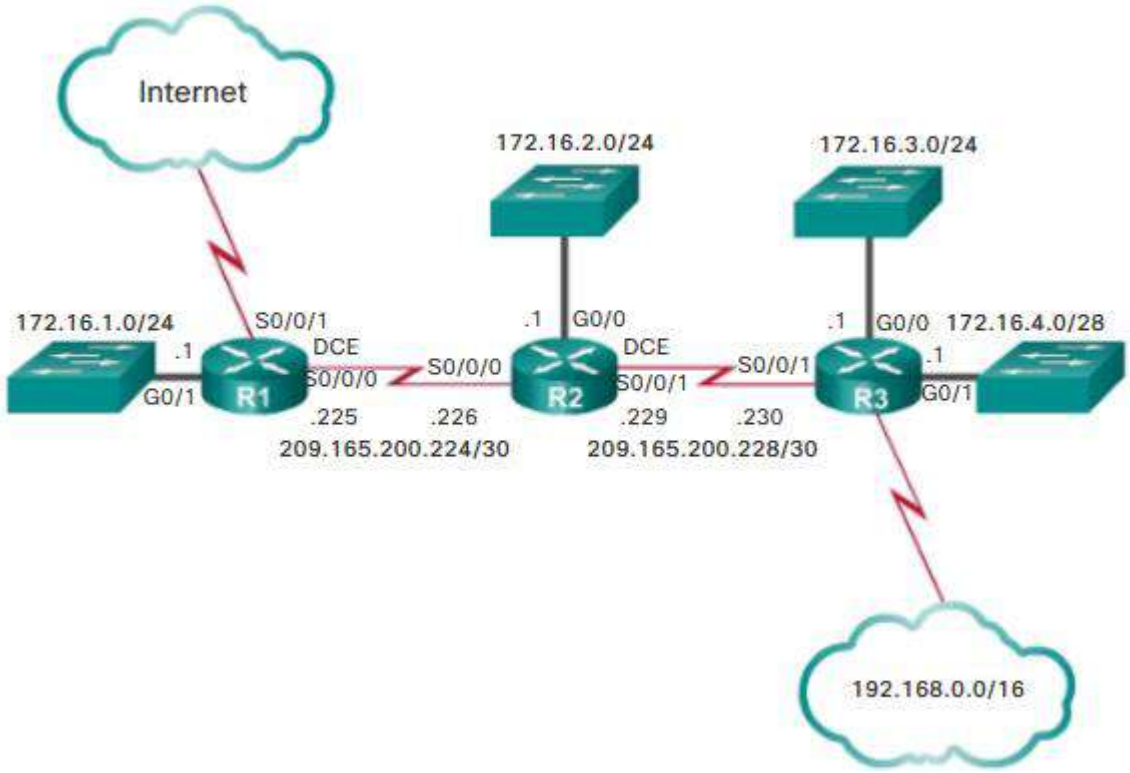
The topology displayed in Figure is used as the reference topology for this section. Notice that in the topology:

R1 is the edge router that connects to the Internet; therefore, it is propagating a default static route to R2 and R3.

R1, R2, and R3 contain discontiguous networks separated by another classful network.

R3 is also introducing a 192.168.0.0/16 supernet route.

Note: The routing table hierarchy in Cisco IOS was originally implemented with the classful routing scheme. Although the routing table incorporates both classful and classless addressing, the overall structure is still built around this classful scheme.



Directly Connected Entries

As highlighted in Figure 1, the routing table of R1 contains three directly connected networks. Notice that two routing table entries are automatically created when an active router interface is configured with an IP address and subnet mask.

Figure 2 displays one of the routing table entries on R1 for the directly connected network 172.16.1.0. These entries were automatically added to the routing table when the GigabitEthernet 0/0 interface was configured and activated. The entries contain the following information:

Route source - Identifies how the route was learned. Directly connected interfaces have two route source codes. C identifies a directly connected network. Directly connected networks are automatically created whenever an interface is configured with an IP address and activated. L identifies that this is a local route. Local routes are automatically created whenever an interface is configured with an IP address and activated.

Destination network - The address of the remote network and how that network is connected.

Outgoing interface - Identifies the exit interface to use when forwarding packets to the destination network.

A router typically has multiple interfaces configured. The routing table stores information about both directly connected and remote routes. As with directly connected networks, the route source identifies how the route was learned. For instance, common codes for remote networks include:

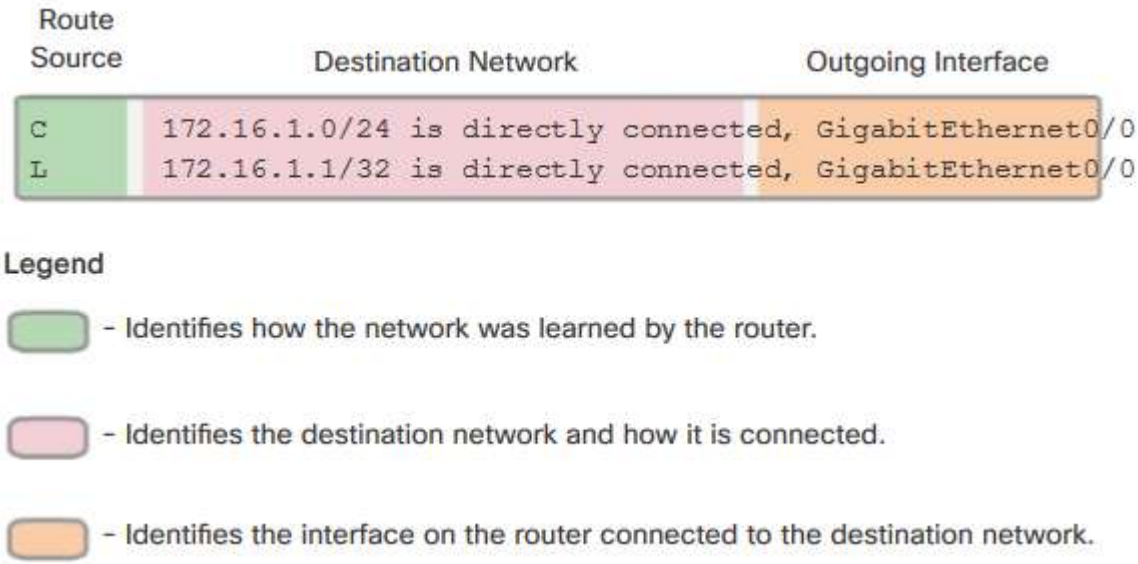
S - Identifies that the route was manually created by an administrator to reach a specific network. This is known as a static route.

D - Identifies that the route was learned dynamically from another router using the EIGRP routing

protocol.

O - Identifies that the route was learned dynamically from another router using the OSPF routing protocol.

R - Identifies that the route was learned dynamically from another router using the RIP routing protocol.



Remote Network Entries

The figure displays an IPv4 routing table entry on R1 for the route to remote network 172.16.4.0 on R3. The entry identifies the following information:

Route source - Identifies how the route was learned.

Destination network - Identifies the address of the remote network.

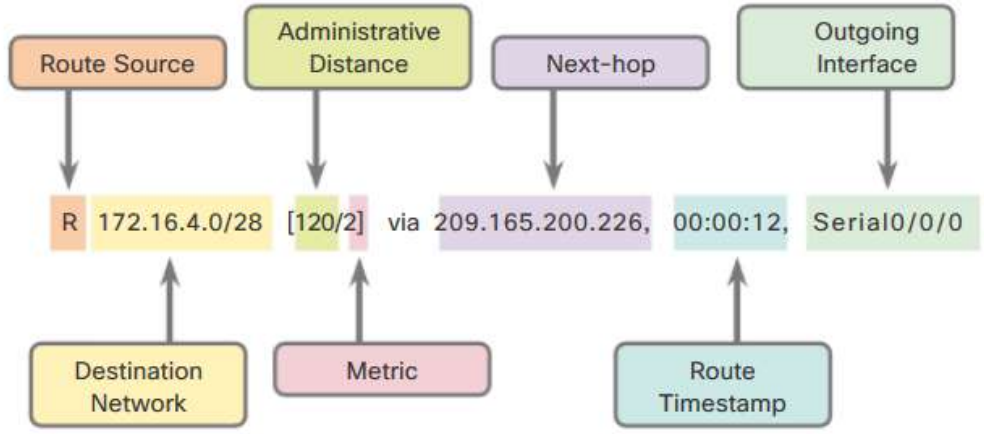
Administrative distance (AD) - Identifies the trustworthiness of the route source. The AD for static routes is 1 and the AD for connected routes is 0. Dynamic routing protocols have an AD higher than 1 depending upon the protocol.

Metric - Identifies the value assigned to reach the remote network. Lower values indicate preferred routes. The metric for static and connected routes is 0.

Next hop - Identifies the IPv4 address of the next router to forward the packet to.

Route timestamp - Identifies from when the route was last heard.

Outgoing interface - Identifies the exit interface to use to forward a packet toward the final destination.



IPv6 Routing Table Entries

Components of the IPv6 routing table are very similar to the IPv4 routing table. For instance, it is populated using directly connected interfaces, static routes, and dynamically learned routes.

Because IPv6 is classless by design, all routes are effectively level 1 ultimate routes. There is no level 1 parent of level 2 child routes.

The topology displayed in the figure is used as the reference topology for this section. Notice that in the topology:

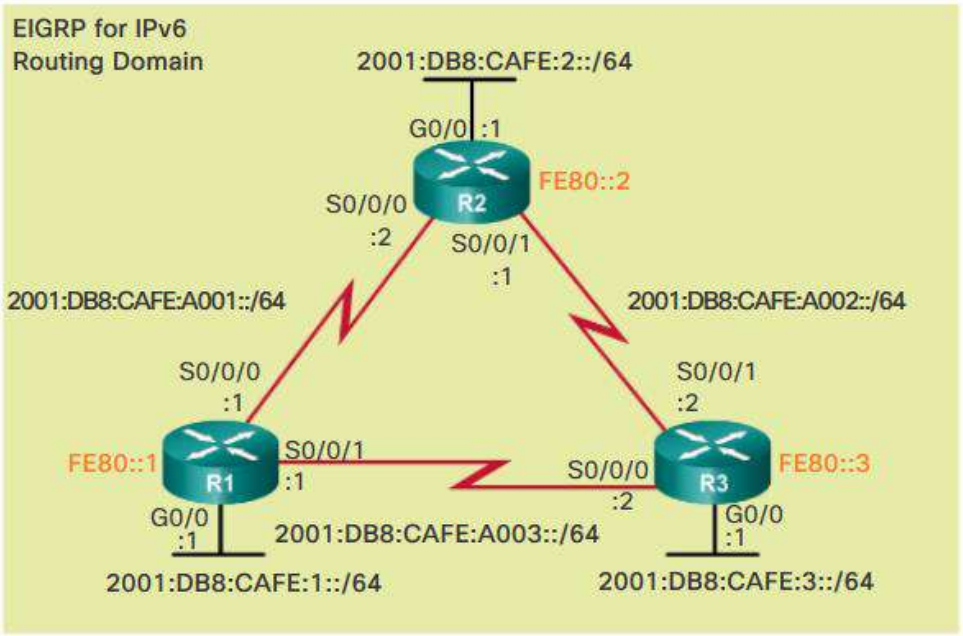
R1, R2, and R3 are configured in a full mesh topology. All routers have redundant paths to various networks.

R2 is the edge router and connects to the ISP; however, a default static route is not being advertised.

EIGRP for IPv6 has been configured on all three routers.

Note: Although EIGRP for IPv6 is used to populate the routing tables, the operation and configuration of EIGRP is beyond the scope of this course.

Reference IPv6 Topology



The FE80 address represents the link-local address assigned to each router.

Directly Connected Entries

Although, the command output is displayed slightly differently than in the IPv4 version, it still contains the relevant route information.

The three entries were added when the interfaces were configured and activated.

Directly connected route entries display the following information:

Route source - Identifies how the route was learned. Directly connected interfaces have two route source codes (C identifies a directly connected network while L identifies that this is a local route.)

Directly connected network - The IPv6 address of the directly connected network.

Administrative distance - Identifies the trustworthiness of the route source. IPv6 uses the same distances as IPv4. A value of 0 indicates the best, most trustworthy source.

Metric - Identifies the value assigned to reach the remote network. Lower values indicate preferred routes.

Outgoing interface - Identifies the exit interface to use when forwarding packets to the destination network.

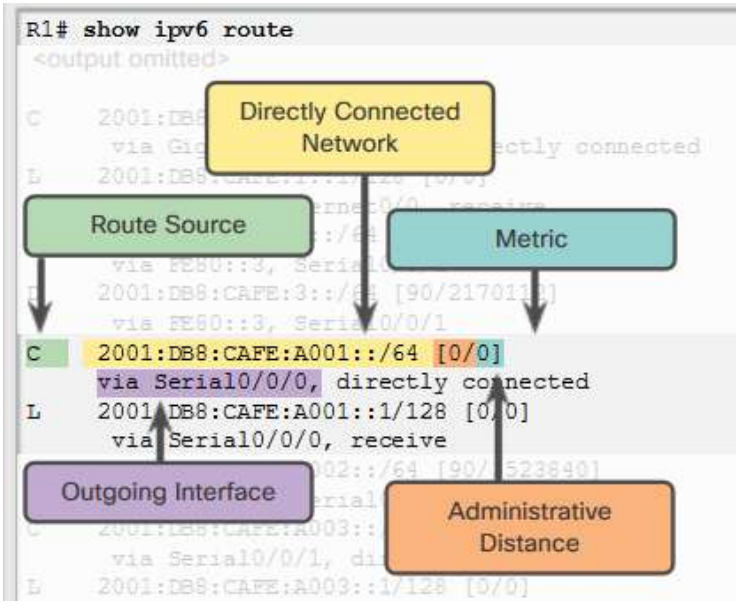
Note: The serial links have reference bandwidths configured to observe how EIGRP metrics select the best route. The reference bandwidth is not a realistic representation of modern networks. It is used only to provide a visual depiction of link speed.

Directly Connected Routes on R1

```
R1# show ipv6 route
<output omitted>

C   2001:DB8:CAFE:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:CAFE:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
D   2001:DB8:CAFE:2::/64 [90/3524096]
     via FE80::3, Serial0/0/1
D   2001:DB8:CAFE:3::/64 [90/2170112]
     via FE80::3, Serial0/0/1
C   2001:DB8:CAFE:A001::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:CAFE:A001::1/128 [0/0]
     via Serial0/0/0, receive
D   2001:DB8:CAFE:A002::/64 [90/3523840]
     via FE80::3, Serial0/0/1
C   2001:DB8:CAFE:A003::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:CAFE:A003::1/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

IPv6 Routing Table of R1

```
R1# show ipv6 route
<output omitted>

C   2001:DB8:CAFE:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:CAFE:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
D   2001:DB8:CAFE:2::/64 [90/3524096]
     via FE80::3, Serial0/0/1
D   2001:DB8:CAFE:3::/64 [90/2170112]
     via FE80::3, Serial0/0/1
C   2001:DB8:CAFE:A001::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:CAFE:A001::1/128 [0/0]
     via Serial0/0/0, receive
D   2001:DB8:CAFE:A002::/64 [90/3523840]
     via FE80::3, Serial0/0/1
C   2001:DB8:CAFE:A003::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:CAFE:A003::1/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```



Remote IPv6 Network Entries

Figure 1 highlights the routing table entries for the three remote networks (i.e., R2 LAN, R3 LAN, and

the link between R2 and R3). The three entries were added by the EIGRP.

Figure 2 displays a routing table entry on R1 for the route to remote network 2001:DB8:CAFE:3::/64 on R3. The entry identifies the following information:

Route source - Identifies how the route was learned. Common codes include O (OSPF), D (EIGRP), R (RIP), and S (Static route).

Destination network - Identifies the address of the remote IPv6 network.

Administrative distance - Identifies how trustworthiness of the route source. IPv6 uses the same distances as IPv4.

Metric - Identifies the value assigned to reach the remote network. Lower values indicate preferred routes.

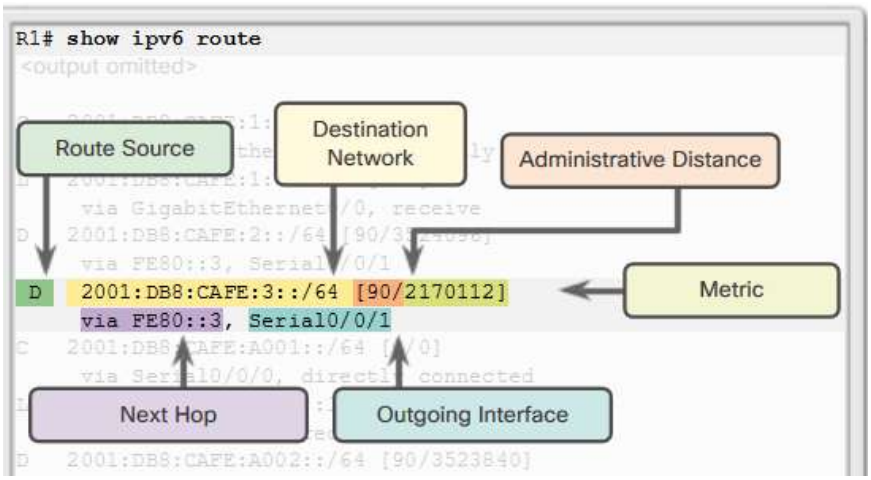
Next hop - Identifies the IPv6 address of the next router to forward the packet to.

Outgoing interface - Identifies the exit interface to use to forward a packet toward the final destination.

When an IPv6 packet arrives on a router interface, the router examines the IPv6 header and identifies the destination IPv6 address. The router then proceeds through the following router lookup process.

The router examines level 1 network routes for the best match with the destination address of the IPv6 packet. Just like IPv4, the longest match is the best match. For example, if there are multiple matches in the routing table, the router chooses the route with the longest match. A match is made by matching the far left bits of the packet's destination IPv6 address with the IPv6 prefix and prefix-length in the IPv6 routing table.

```
R1# show ipv6 route
 <output omitted>

C   2001:DB8:CAFE:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:CAFE:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
D   2001:DB8:CAFE:2::/64 [90/3524096]
     via FE80::3, Serial0/0/1
D   2001:DB8:CAFE:3::/64 [90/2170112]
     via FE80::3, Serial0/0/1
C   2001:DB8:CAFE:A001::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:CAFE:A001::1/128 [0/0]
     via Serial0/0/0, receive
D   2001:DB8:CAFE:A002::/64 [90/3523840]
     via FE80::3, Serial0/0/1
C   2001:DB8:CAFE:A003::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:CAFE:A003::1/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```



Review questions

See the practical attachment

EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance vector routing protocol developed by Cisco Systems. As the name suggests, EIGRP is an enhancement of another Cisco routing protocol IGRP (Interior Gateway Routing Protocol). IGRP is an older classful, distance vector routing protocol, now obsolete since IOS 12.3.

EIGRP includes features found in link-state routing protocols. EIGRP is suited for many different topologies and media. In a well-designed network, EIGRP can scale to include multiple topologies and can provide extremely quick convergence times with minimal network traffic.

Features of EIGRP

EIGRP was initially released in 1992 as a proprietary protocol available only on Cisco devices. However, in 2013, Cisco released a basic functionality of EIGRP as an open standard to the IETF, as an informational RFC. This means that other networking vendors can now implement EIGRP on their equipment to interoperate with both Cisco and non-Cisco routers running EIGRP. However, advanced features of EIGRP, such as EIGRP stub, needed for the Dynamic Multipoint Virtual Private Network (DMVPN) deployment, will not be released to the IETF. As an informational RFC, Cisco will continue to maintain control of EIGRP.

EIGRP includes features of both link-state and distance vector routing protocols. However, EIGRP is still based on the key distance vector routing protocol principle, in which information about the rest of the network is learned from directly connected neighbors.

EIGRP is an advanced distance vector routing protocol that includes features not found in other distance vector routing protocols like RIP and IGRP.

In Cisco IOS Release 15.0(1)M, Cisco introduced a new EIGRP configuration option called named EIGRP. Named EIGRP enables the configuration of EIGRP for both IPv4 and IPv6 under a single configuration mode. This helps eliminate configuration complexity that occurs when configuring EIGRP for both IPv4 and IPv6. Named EIGRP is beyond the scope of this course.

Features of EIGRP include:

Diffusing Update Algorithm - As the computational engine that drives EIGRP, the Diffusing Update Algorithm (DUAL) resides at the center of the routing protocol. DUAL guarantees loop-free and backup paths throughout the routing domain. Using DUAL, EIGRP stores all available backup routes for destinations so that it can quickly adapt to alternate routes when necessary.

Establishing Neighbor Adjacencies - EIGRP establishes relationships with directly connected routers that are also enabled for EIGRP. Neighbor adjacencies are used to track the status of these neighbors.

Reliable Transport Protocol - The Reliable Transport Protocol (RTP) is unique to EIGRP and provides delivery of EIGRP packets to neighbors. RTP and the tracking of neighbor adjacencies set the stage for DUAL.

Partial and Bounded Updates - EIGRP uses the terms partial and bounded when referring to its updates.

Unlike RIP, EIGRP does not send periodic updates and route entries do not age out. The term partial means that the update only includes information about the route changes, such as a new link or a link becoming unavailable. The term bounded refers to the propagation of partial updates that are sent only to those routers that the changes affect. This minimizes the bandwidth that is required to send EIGRP updates.

Equal and Unequal Cost Load Balancing - EIGRP supports equal cost load balancing and unequal cost load balancing, which allows administrators to better distribute traffic flow in their networks.

Note: The term "hybrid routing" protocol may be used in some older documentation to define EIGRP. However, this term is misleading because EIGRP is not a hybrid between distance vector and link-state routing protocols. EIGRP is solely a distance vector routing protocol; therefore, Cisco no longer uses this term to refer to it.

Protocol Dependent Modules

EIGRP has the capability for routing different protocols, including IPv4 and IPv6. EIGRP does so by using protocol-dependent modules (PDMs). PDMs were also used to support the now obsolete Novell IPX and Apple Computer's AppleTalk network layer protocols.

PDMs are responsible for network layer protocol-specific tasks. An example is the EIGRP module that is responsible for sending and receiving EIGRP packets that are encapsulated in IPv4. This module is also responsible for parsing EIGRP packets and informing DUAL of the new information that is received. EIGRP asks DUAL to make routing decisions, but the results are stored in the IPv4 routing table.

PDMs are responsible for the specific routing tasks for each network layer protocol, including:

- Maintaining the neighbor and topology tables of EIGRP routers that belong to that protocol suite
- Building and translating protocol-specific packets for DUAL
- Interfacing DUAL to the protocol-specific routing table
- Computing the metric and passing this information to DUAL
- Implementing filtering and access lists
- Performing redistribution functions to and from other routing protocols
- Redistributing routes that are learned by other routing protocols

When a router discovers a new neighbor, it records the neighbor's address and interface as an entry in the neighbor table. One neighbor table exists for each protocol-dependent module, such as IPv4. EIGRP also maintains a topology table. The topology table contains all destinations that are advertised by neighboring routers. There is also a separate topology table for each PDM.

Reliable Transport Protocol

EIGRP was designed as a network layer independent routing protocol. Because of this design, EIGRP cannot use the services of UDP or TCP. Instead, EIGRP uses the Reliable Transport Protocol (RTP) for the delivery and reception of EIGRP packets. This allows EIGRP to be flexible and can be used for

protocols other than those from the TCP/IP protocol suite, such as the now obsolete IPX and AppleTalk protocols.

Authentication

Like other routing protocols, EIGRP can be configured for authentication. RIPv2, EIGRP, OSPF, IS-IS, and BGP can each be configured to authenticate their routing information.

It is a good practice to authenticate transmitted routing information. Doing so ensures that routers only accept routing information from other routers that have been configured with the same password or authentication information.

Note: Authentication does not encrypt the EIGRP routing updates.

EIGRP Packet Types

EIGRP uses five different packet types, some in pairs. EIGRP packets are sent using either RTP reliable or unreliable delivery and can be sent as a unicast, multicast, or sometimes both. EIGRP packet types are also called EIGRP packet formats or EIGRP messages.

The five EIGRP packet types include:

Hello packets - Used for neighbor discovery and to maintain neighbor adjacencies.

Sent with unreliable delivery

Multicast (on most network types)

Update packets - Propagates routing information to EIGRP neighbors.

Sent with reliable delivery

Unicast or multicast

Acknowledgment packets - Used to acknowledge the receipt of an EIGRP message that was sent using reliable delivery.

Sent with unreliable delivery

Unicast

Query packets - Used to query routes from neighbors.

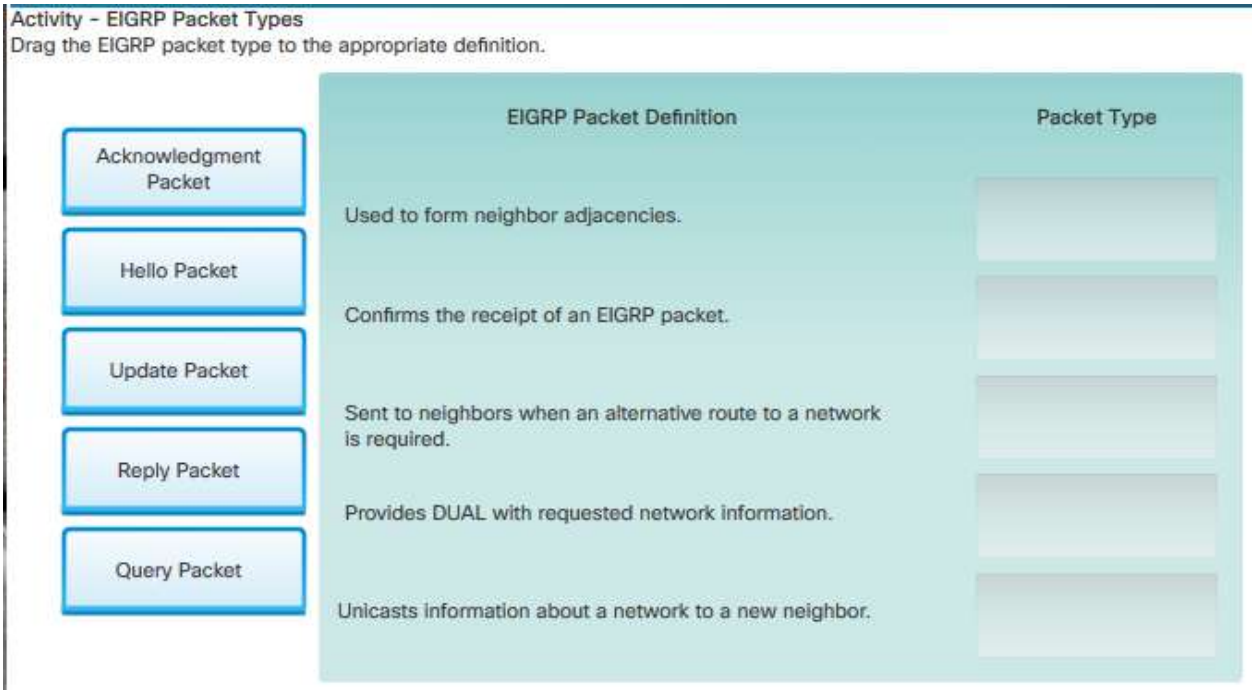
Sent with reliable delivery

Unicast or multicast

Reply packets - Sent in response to an EIGRP query.

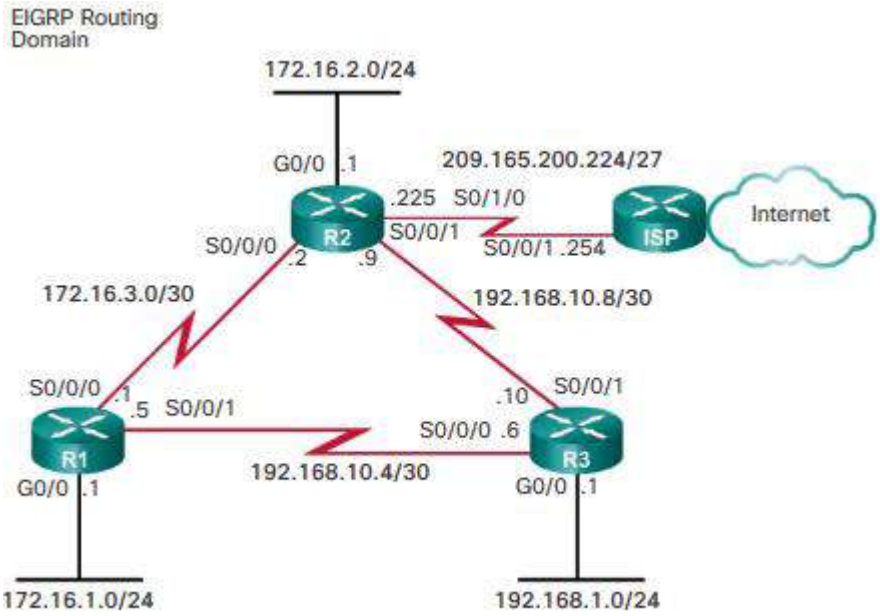
Sent with reliable delivery

Unicast



EIGRP Network Topology

Figure 1 displays the topology that is used in this chapter to configure EIGRP for IPv4.



The routers in the topology have a starting configuration that includes addresses on the interfaces. There is currently no static routing or dynamic routing configured on any of the routers.

Autonomous System Numbers

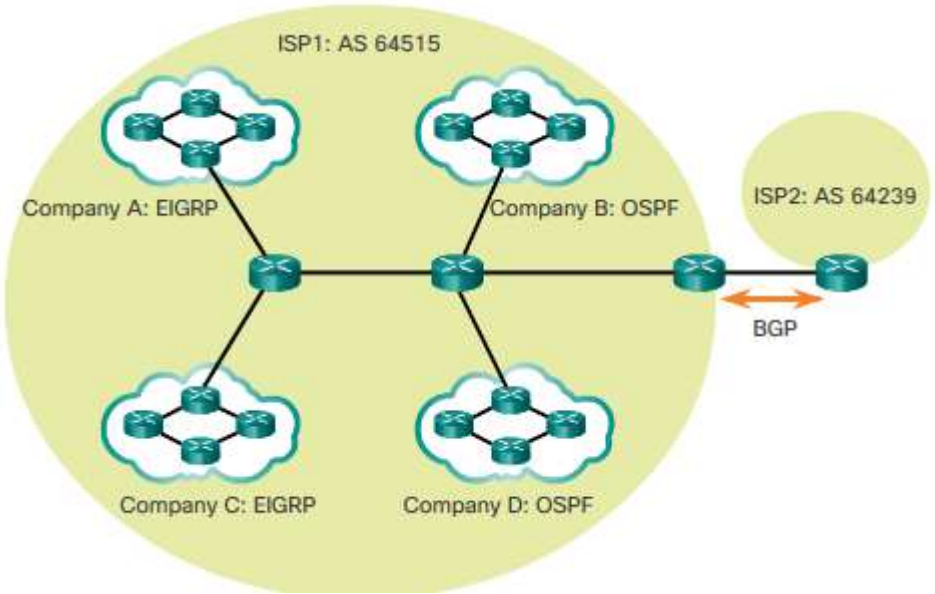
EIGRP uses the router eigrp *autonomous-system* command to enable the EIGRP process. The autonomous system number referred to in the EIGRP configuration is not associated with the Internet Assigned Numbers Authority (IANA) globally assigned autonomous system numbers used by external routing protocols.

So what is the difference between the IANA globally assigned autonomous system number and the EIGRP autonomous system number?

An IANA globally assigned autonomous system is a collection of networks under the administrative control of a single entity that presents a common routing policy to the Internet. In the figure, companies A, B, C, and D are all under the administrative control of ISP1. ISP1 presents a common routing policy for all of these companies when advertising routes to ISP2.

The guidelines for the creation, selection, and registration of an autonomous system are described in RFC 1930. Global autonomous system numbers are assigned by IANA, the same authority that assigns IP address space. The local regional Internet registry (RIR) is responsible for assigning an autonomous system number to an entity from its block of assigned autonomous system numbers. Prior to 2007, assigned autonomous system numbers were 16-bit numbers ranging from 0 to 65,535. Today, 32-bit autonomous system numbers are assigned thereby increasing the number of available autonomous system numbers to over 4 billion.

Usually, only Internet Service Providers (ISPs), Internet backbone providers, and large institutions connecting to other entities require an autonomous system number. These ISPs and large institutions use the exterior gateway routing protocol, Border Gateway Protocol (BGP), to propagate routing information. BGP is the only routing protocol that uses an actual autonomous system number in its configuration.

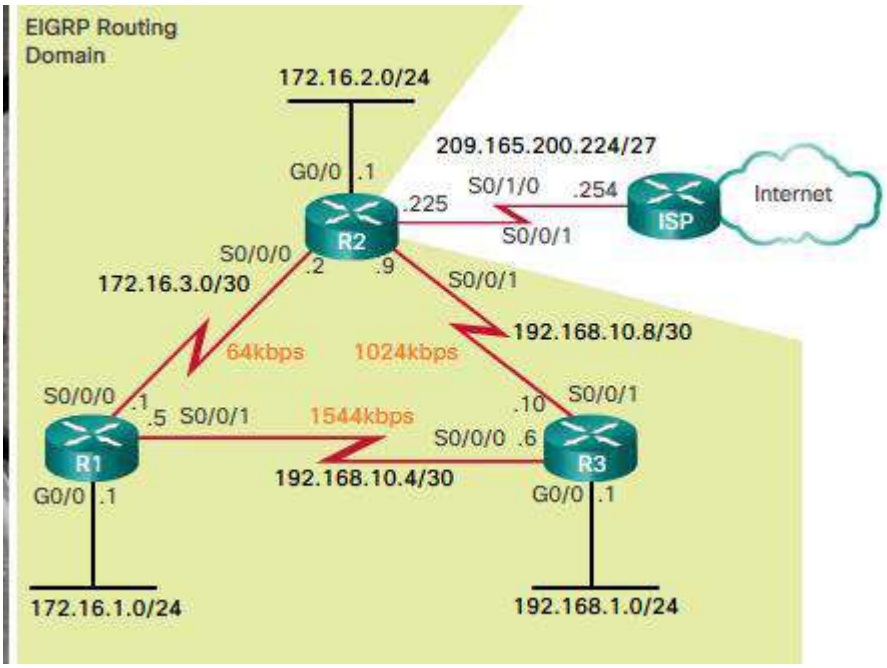


The vast majority of companies and institutions with IP networks do not need an autonomous system number, because they are controlled by a larger entity, such as an ISP. These companies use interior gateway protocols, such as RIP, EIGRP, OSPF, and IS-IS to route packets within their own networks. They are one of many independent and separate networks within the autonomous system of the ISP. The ISP is responsible for the routing of packets within its autonomous system and between other autonomous systems.

The autonomous system number used for EIGRP configuration is only significant to the EIGRP routing domain. It functions as a process ID to help routers keep track of multiple running instances of EIGRP. This is required because it is possible to have more than one instance of EIGRP running on a network. Each instance of EIGRP can be configured to support and exchange routing updates for different networks.

The router eigrp Command

The Cisco IOS includes the processes to enable and configure several different types of dynamic routing protocols. The router global configuration mode command is used to begin the configuration of any dynamic routing protocol. The topology shown in Figure 1 is used to demonstrate this command.



As shown in Figure 2, when followed by a question mark (?), the router global configuration mode command lists of all the available routing protocols supported by this specific IOS release running on the router.

```
R1# conf t
Enter configuration commands, one per line. End with
CNTL/Z.
R1(config)# router ?
   bgp       Border Gateway Protocol (BGP)
   eigrp     Enhanced Interior Gateway Routing Protocol
             (EIGRP)
   isis      ISO IS-IS
   iso-igrp  IGRP for OSI networks
   mobile    Mobile routes
   odr       On Demand stub Routes
   ospf      Open Shortest Path First (OSPF)
   ospfv3    OSPFv3
   rip       Routing Information Protocol (RIP)

R1(config)# router
```

The following global configuration mode command is used to enter the router configuration mode for EIGRP and begin the configuration of the EIGRP process:

Router(config)# **router eigrp** *autonomous-system*

The *autonomous-system* argument can be assigned to any 16-bit value between the number 1 and 65,535. All routers within the EIGRP routing domain must use the same autonomous system number.

Figure 3 shows the configuration of the EIGRP process on routers R1, R2, and R3. Notice that the prompt changes from a global configuration mode prompt to router configuration mode.

```
R1(config)# router eigrp 1
R1(config-router)#
```

```
R2(config)# router eigrp 1
R2(config-router)#
```

```
R3(config)# router eigrp 1
R3(config-router)#
```

In this example, 1 identifies this particular EIGRP process running on this router. To establish neighbor adjacencies, EIGRP requires all routers in the same routing domain to be configured with the same autonomous system number. In Figure 3, that same EIGRP is enabled on all three routers using the same autonomous system number of 1.

Note: EIGRP and OSPF can support multiple instances of the routing protocol. However, this multiple routing protocol implementation is not usually needed or recommended.

The router eigrp *autonomous-system* command does not start the EIGRP process itself. The router does not start sending updates. Rather, this command only provides access to configure the EIGRP settings. To completely remove the EIGRP routing process from a device, use the no router eigrp *autonomous-system* global configuration mode command, which stops the EIGRP process and removes all existing EIGRP router configurations.

EIGRP Router ID

The EIGRP router ID is used to uniquely identify each router in the EIGRP routing domain.

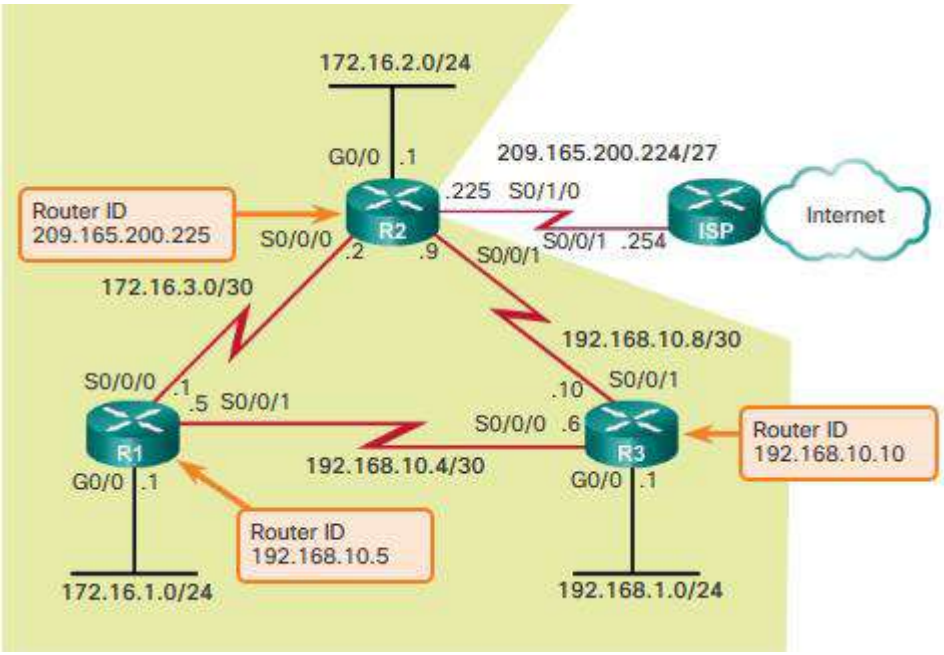
The router ID is used in both EIGRP and OSPF routing protocols. However, the role of the router ID is more significant in OSPF. In EIGRP IPv4 implementations, the use of the router ID is not that apparent. EIGRP for IPv4 uses the 32-bit router ID to identify the originating router for redistribution of external routes. The need for a router ID becomes more evident in the discussion of EIGRP for IPv6. While the router ID is necessary for redistribution, the details of EIGRP redistribution are beyond the scope of this curriculum. For purposes of this curriculum, it is only necessary to understand what the router ID is and how it is determined.

To determine its router ID, a Cisco IOS router will use the following three criteria in order:

1. Use the address configured with the eigrp router-id *ipv4-address* router configuration mode command.

2. If the router ID is not configured, choose the highest IPv4 address of any of its loopback interfaces.
3. If no loopback interfaces are configured, choose the highest active IPv4 address of any of its physical interfaces.

If the network administrator does not explicitly configure a router ID using the eigrp router-id command, EIGRP generates its own router ID using either a loopback or physical IPv4 address. A loopback address is a virtual interface and is automatically in the up state when configured. The interface does not need to be enabled for EIGRP, meaning that it does not need to be included in one of the EIGRP network commands. However, the interface must be in the up/up state.



Using the criteria described above, the figure shows the default EIGRP router IDs that are determined by the routers' highest active IPv4 address.

Note: The eigrp router-id command is used to configure the router ID for EIGRP. Some versions of IOS will accept the command router-id, without first specifying eigrp. The running-config, however, will display eigrp router-id regardless of which command is used.

Configuring the EIGRP Router ID

The eigrp router-id *ipv4-address* router configuration command is the preferred method used to configure the EIGRP router ID. This method takes precedence over any configured loopback or physical interface IPv4 addresses. The command syntax is:

Note: The IPv4 address used to indicate the router ID is actually any 32-bit number displayed in dotted-decimal notation.

The *ipv4-address* router ID can be configured with any IPv4 address except 0.0.0.0 and 255.255.255.255. The router ID should be a unique 32-bit number in the EIGRP routing domain; otherwise, routing inconsistencies can occur.

```
R1(config)# router eigrp 1
R1(config-router)# eigrp router-id 1.1.1.1
R1(config-router)#
```

```
R2(config)# router eigrp 1
R2(config-router)# eigrp router-id 2.2.2.2
R2(config-router)#
```

Figure 1 shows the configuration of the EIGRP router ID for routers R1 and R2.

If a router ID is not explicitly configured, then the router would use its highest IPv4 address configured on a loopback interface. The advantage of using a loopback interface is that unlike physical interfaces, loopbacks cannot fail. There are no actual cables or adjacent devices on which the loopback interface depends for being in the up state. Therefore, using a loopback address for the router ID can provide a more consistent router ID than using an interface address.

If the eigrp router-id command is not used and loopback interfaces are configured, EIGRP chooses the highest IPv4 address of any of its loopback interfaces. The following commands are used to enable and configure a loopback interface:

Router(config)# **interface loopback** *number*

Router(config-if)# **ip address** *ipv4-address subnet-mask*

Verifying the EIGRP Process

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is n
  set
  Incoming update filter list for all interfaces is n
  set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 1.1.1.1

    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
```

Figure 2 shows the show ip protocols output for R1, including its router ID. The show ip protocols command displays the parameters and current state of any active routing protocol processes, including both EIGRP and OSPF. The show ip protocols command displays different types of output specific to each routing protocol.

The network Command

EIGRP router configuration mode allows for the configuration of the EIGRP routing protocol. Figure 1 shows that R1, R2, and R3 all have networks that should be included within a single EIGRP routing domain. To enable EIGRP routing on an interface, use the network *ipv4-network-address* router configuration mode command. The *ipv4-network-address* is the classful network address for each directly connected network.

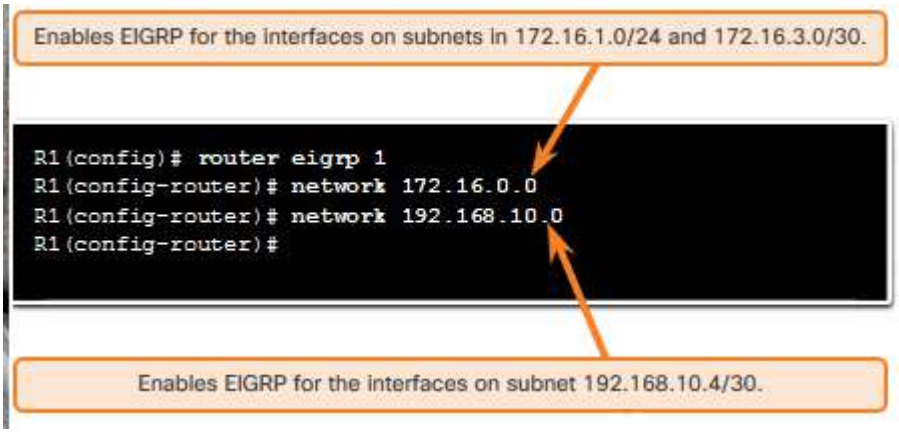
The network command has the same function as in all IGP routing protocols. The network command in EIGRP:

Enables any interface on this router that matches the network address in the network router configuration mode command to send and receive EIGRP updates.The network of the interfaces is included in EIGRP routing updates.

Figure 2 shows the network commands required to configure EIGRP on R1. In the figure, a single classful network statement, network 172.16.0.0, is used on R1 to include both interfaces in subnets 172.16.1.0/24 and 172.16.3.0/30. Notice that only the classful network address is used.

Figure 3 shows the network command used to enable EIGRP on R2's interfaces for subnets 172.16.1.0/24 and 172.16.2.0/24. When EIGRP is configured on R2's S0/0/0 interface, DUAL sends a notification message to the console stating that a neighbor adjacency with another EIGRP router on that interface has been established. This new adjacency happens automatically because both R1 and R2 use the same autonomous system number (i.e., 1), and both routers now send updates on their interfaces in the 172.16.0.0 network.

DUAL automatically generates the notification message because the eigrp log-neighbor-changes router configuration mode command is enabled by default. Specifically, the command helps verify neighbor adjacencies during configuration of EIGRP and displays any changes in EIGRP neighbor adjacencies, such as when an EIGRP adjacency has been added or removed.




```
R2(config)# router eigrp 1
R2(config-router)# network 172.16.0.0
R2(config-router)#
*Feb 28 17:51:42.543: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1:
Neighbor 172.16.3.1 (Serial0/0/0) is up: new adjacency
R2(config-router)#
```

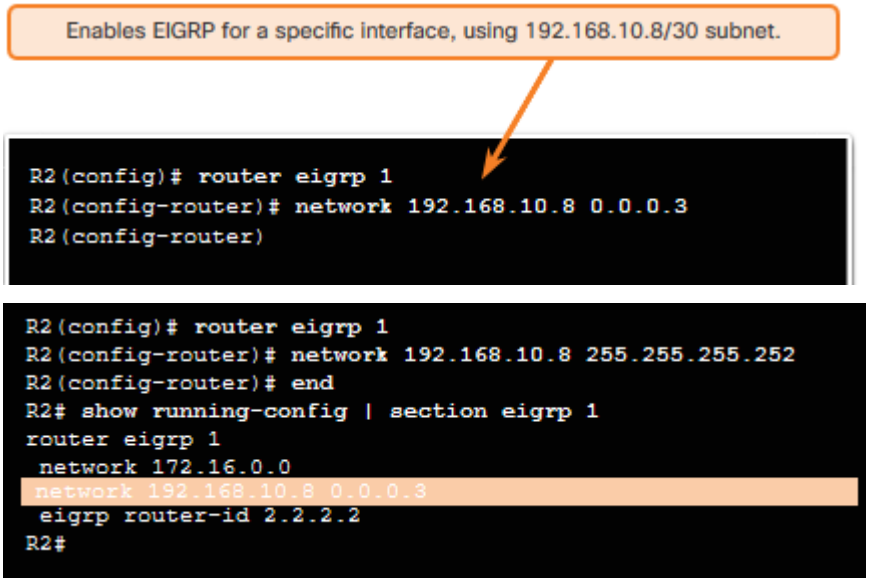
The network Command and Wildcard Mask

By default, when using the network command and an IPv4 network address, such as 172.16.0.0, all interfaces on the router that belong to that classful network address are enabled for EIGRP. However, there may be times when the network administrator does not want to include all interfaces within a network when enabling EIGRP. For example, in Figure 1, assume that an administrator wants to enable EIGRP on R2, but only for the subnet 192.168.10.8 255.255.255.252, on the S0/0/1 interface.

To configure EIGRP to advertise specific subnets only, use the *wildcard-mask* option with the network command:

Router(config-router)# **network** *network-address* [*wildcard-mask*]

A wildcard mask is similar to the inverse of a subnet mask. In a subnet mask, binary 1s are significant while binary 0s are not. In a wildcard mask, binary 0s are significant, while binary 1s are not. For example, the inverse of subnet mask 255.255.255.252 is 0.0.0.3.



Calculating a wildcard mask may seem daunting at first but it's actually pretty easy to do. To calculate the inverse of the subnet mask, subtract the subnet mask from 255.255.255.255 as follows:

255.255.255.255

\- 255.255.255.252

---

0. 0. 0. 3 Wildcard mask

Figure 2 continues the EIGRP network configuration of R2. The network 192.168.10.8 0.0.0.3 command specifically enables EIGRP on the S0/0/1 interface, a member of the 192.168.10.8 255.255.255.252 subnet.

Configuring a wildcard mask is the official command syntax of the EIGRP network command. However, the Cisco IOS versions also accepts a subnet mask to be used instead. For example, Figure 3 configures the same S0/0/1 interface on R2, but this time using a subnet mask in the network command.

Notice in the output of the show running-config command, the IOS converted the subnet mask command to its wildcard mask.

Passive Interface

As soon as a new interface is enabled within the EIGRP network, EIGRP attempts to form a neighbor adjacency with any neighboring routers to send and receive EIGRP updates.

At times it may be necessary, or advantageous, to include a directly connected network in the EIGRP routing update, but not allow any neighbor adjacencies off of that interface to form. The passive-interface command can be used to prevent the neighbor adjacencies. There are two primary reasons for enabling the passive-interface command:

To suppress unnecessary update traffic, such as when an interface is a LAN interface, with no other routers connected

To increase security controls, such as preventing unknown rogue routing devices from receiving EIGRP updates

```
R1(config)# router eigrp 1
R1(config-router)# passive-interface gigabitethernet 0/0
```

```
R3(config)# router eigrp 1
R3(config-router)# passive-interface gigabitethernet 0/0
```

Verifying EIGRP: Examining Neighbors

Before EIGRP can send or receive any updates, routers must establish adjacencies with their neighbors. EIGRP routers establish adjacencies with neighbor routers by exchanging EIGRP Hello packets.

Use the show ip eigrp neighbors command to view the neighbor table and verify that EIGRP has established an adjacency with its neighbors. For each router, you should be able to see the IPv4 address of the adjacent router and the interface that this router uses to reach that EIGRP neighbor. Using this topology, each router has two neighbors listed in the neighbor table.

The column headers in the show ip eigrp neighbors command output identify the following:

H - Lists the neighbors in the order that they were learned.

Address - IPv4 address of the neighbor.

Interface - Local interface on which this Hello packet was received.

Hold - Current hold time. When a Hello packet is received, this value is reset to the maximum hold time for that interface, and then counts down to zero. If zero is reached, the neighbor is considered down.

Uptime - Amount of time since this neighbor was added to the neighbor table.

Smooth Round Trip Timer (SRTT) and Retransmission Timeout (RTO) - Used by RTP to manage reliable EIGRP packets.

Queue Count - Should always be zero. If more than zero, then EIGRP packets wait to be sent.

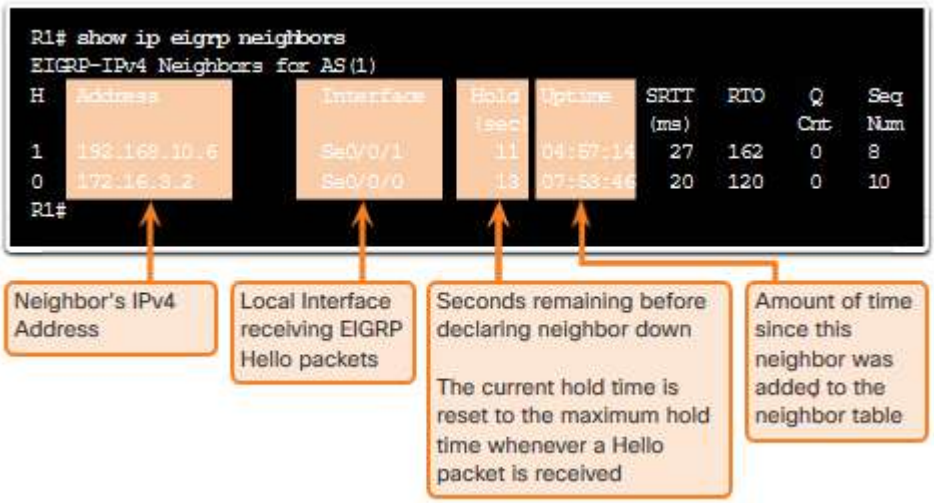
Sequence Number - Used to track updates, queries, and reply packets.

The show ip eigrp neighbors command is very useful for verifying and troubleshooting EIGRP.

If a neighbor is not listed after adjacencies have been established with a router's neighbors, check the local interface to ensure it is activated with the show ip interface brief command. If the interface is active, try to ping the IPv4 address of the neighbor. If the ping fails, it means that the neighbor interface is down and must be activated. If the ping is successful and EIGRP still does not see the router as a neighbor, examine the following configurations:

Are both routers configured with the same EIGRP autonomous system number?

Is the directly connected network included in the EIGRP network statements?



EIGRP Composite Metric

By default, EIGRP uses the following values in its composite metric to calculate the preferred path to a network:

Bandwidth - The slowest bandwidth among all of the outgoing interfaces, along the path from source to destination.

Delay - The cumulative (sum) of all interface delay along the path (in tens of microseconds).

The following values can be used, but are not recommended, because they typically result in frequent recalculation of the topology table:

Reliability - Represents the worst reliability between the source and destination, which is based on keepalives.

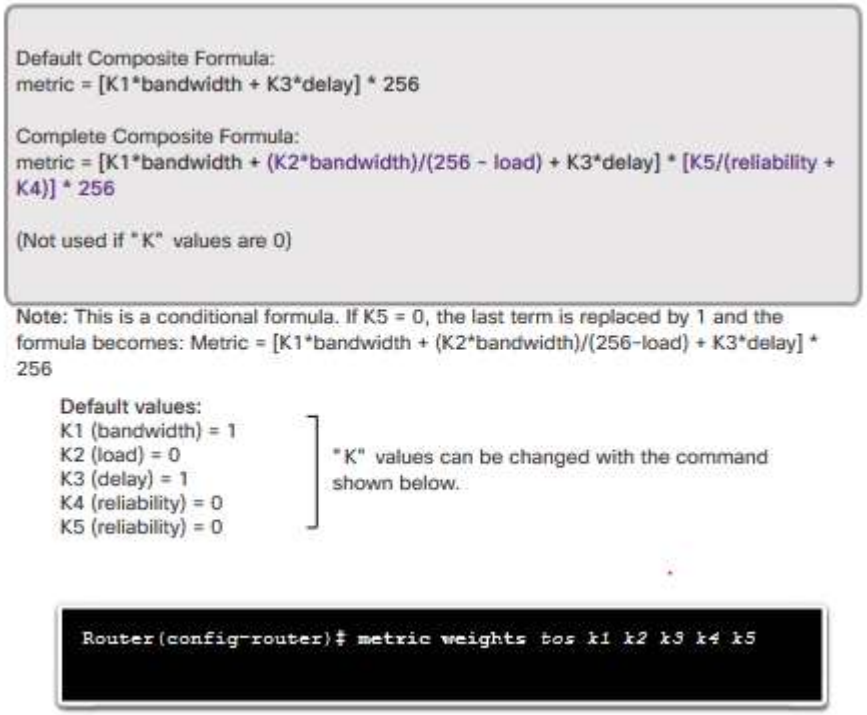
Load - Represents the worst load on a link between the source and destination, which is computed based on the packet rate and the configured bandwidth of the interface.

Note: Although the MTU is included in the routing table updates, it is not a routing metric used by EIGRP.

The Composite Metric

Figure 1 shows the composite metric formula used by EIGRP. The formula consists of values K1 to K5,

known as EIGRP metric weights. K1 and K3 represent bandwidth and delay, respectively. K2 represents load, and K4 and K5 represent reliability. By default, K1 and K3 are set to 1, and K2, K4, and K5 are set to 0. The result is that only the bandwidth and delay values are used in the computation of the default composite metric. EIGRP for IPv4 and EIGRP for IPv6 use the same formula for the composite metric.



The metric calculation method (*k* values) and the EIGRP autonomous system number must match between EIGRP neighbors. If they do not match, the routers do not form an adjacency.

The default *k* values can be changed with the metric weights router configuration mode command:

Router(config-router)# **metric weights** *tos k1 k2 k3 k4 k5*

Note: Modifying the metric weights value is generally not recommended and beyond the scope of this course. However, its relevance is important in establishing neighbor adjacencies. If one router has modified the metric weights and another router has not, an adjacency does not form.

Verifying the *k* Values

The show ip protocols command is used to verify the *k* values. The command output for R1 is shown in Figure 2. Notice that the *k* values on R1 are set to the default.

Bandwidth Metric

The bandwidth metric is a static value used by some routing protocols, such as EIGRP and OSPF, to calculate their routing metric. The bandwidth is displayed in kilobits per second (kb/s).

On older routers, the serial link bandwidth metric defaults to 1544 kb/s. This is the bandwidth of a T1 connection. On newer routers, such as the Cisco 4321, serial link bandwidth defaults to the clock rate used on the link. The serial links in topology in Figure 1 have been configured with the bandwidths that will be used in this section.

Note: The bandwidths used in this topology were chosen to help explain the calculation of the routing

protocol metrics and the process of best path selection. These bandwidth values do not reflect the more common types of connections found in today's networks.

Always verify bandwidth with the show interfaces command. The default value of the bandwidth may or may not reflect the actual physical bandwidth of the interface. If actual bandwidth of the link differs from the default bandwidth value, the bandwidth value should be modified.

Configuring the Bandwidth Parameter

Because both EIGRP and OSPF use bandwidth in default metric calculations, a correct value for bandwidth is very important to the accuracy of routing information.

Use the following interface configuration mode command to modify the bandwidth metric:

Router(config-if)# **bandwidth** *kilobits-bandwidth-value*

Use the no bandwidth command to restore the default value.

The link between R1 and R2 has a bandwidth of 64 kb/s, and the link between R2 and R3 has a bandwidth of 1,024 kb/s. The figure shows the configurations used on all three routers to modify the bandwidth on the appropriate serial interfaces. Modify the bandwidth metric on both sides of the link to ensure proper routing in both directions.

Verifying the Bandwidth Parameter

Use the show interfaces command to verify the new bandwidth parameters.

Modifying the bandwidth value does not change the actual bandwidth of the link. The bandwidth command only modifies the bandwidth metric used by routing protocols, such as EIGRP and OSPF.

```
R1(config)# interface s 0/0/0
R1(config-if)# bandwidth 64
```

```
R2(config)# interface s 0/0/0
R2(config-if)# bandwidth 64
R2(config-if)# exit
R2(config)# interface s 0/0/1
R2(config-if)# bandwidth 1024
```

```
R3(config)# interface s 0/0/1
R3(config-if)# bandwidth 1024
```

DUAL Concepts

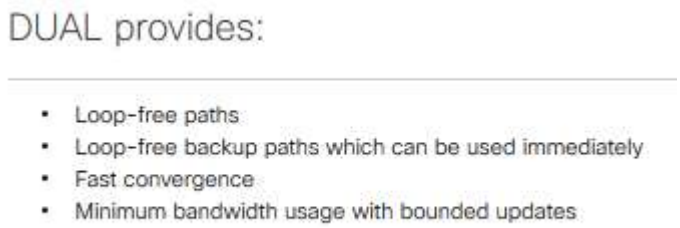
EIGRP uses the Diffusing Update Algorithm (DUAL) to provide the best loop-free path and loop-free backup paths.

DUAL uses several terms, which are discussed in more detail throughout this section:

- Successor
- Feasible Distance (FD)
- Feasible Successor (FS)

- Reported Distance (RD) or Advertised Distance (AD)
- Feasible Condition or Feasibility Condition (FC)

These terms and concepts are at the center of the loop avoidance mechanism of DUAL.



Introduction to DUAL

EIGRP uses the DUAL convergence algorithm. Convergence is critical to a network to avoid routing loops.

Routing loops, even temporary ones, can be detrimental to network performance. Distance vector routing protocols, such as RIP, prevent routing loops with hold-down timers and split horizon. Although EIGRP uses both of these techniques, it uses them somewhat differently; the primary way that EIGRP prevents routing loops is with the DUAL algorithm.

The DUAL algorithm is used to obtain loop-freedom at every instance throughout a route computation. This allows all routers involved in a topology change to synchronize at the same time. Routers that are not affected by the topology changes are not involved in the recomputation. This method provides EIGRP with faster convergence times than other distance vector routing protocols.

The decision process for all route computations is done by the DUAL Finite State Machine (FSM). An FSM is a workflow model, similar to a flow chart, which is composed of the following:

- A finite number of stages (states)
- Transitions between those stages

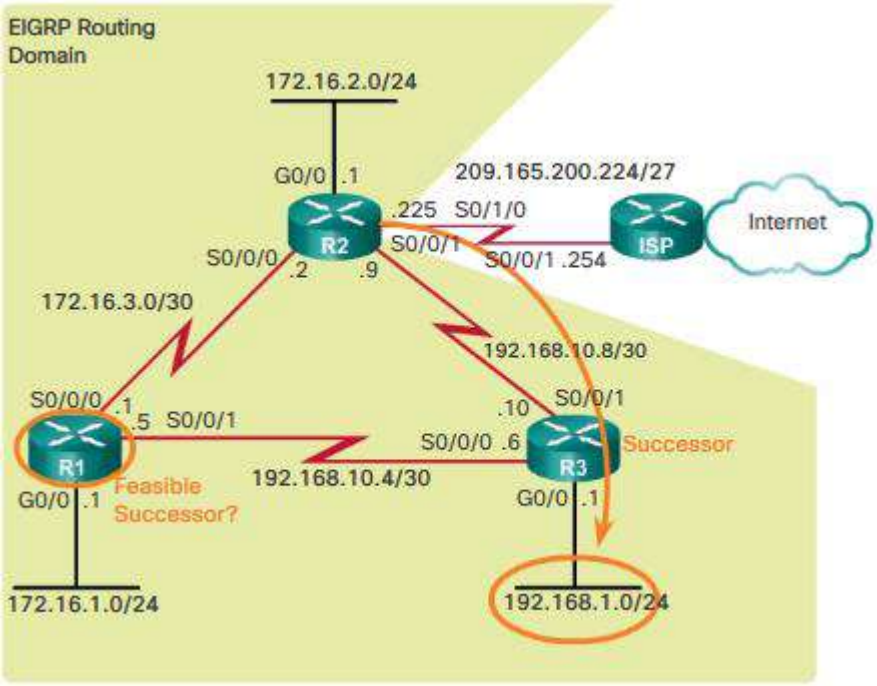
Operations

The DUAL FSM tracks all routes and uses EIGRP metrics to select efficient, loop-free paths, and to identify the routes with the least-cost path to be inserted into the routing table.

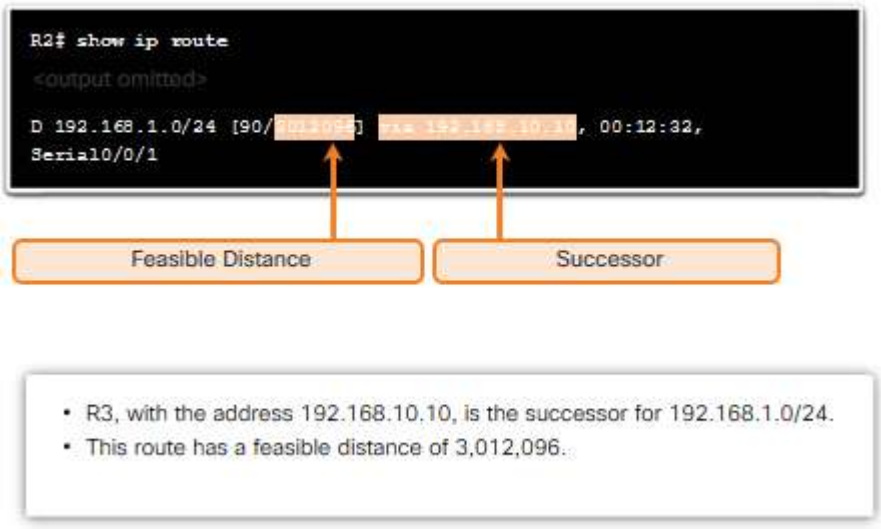
Recomputation of the DUAL algorithm can be processor-intensive. EIGRP avoids recomputation whenever possible by maintaining a list of backup routes that DUAL has already determined to be loop-free. If the primary route in the routing table fails, the best backup route is immediately added to the routing table.

Successor and Feasible Distance

Figure 1 shows the topology for this topic. A successor is a neighboring router that is used for packet forwarding and is the least-cost route to the destination network. The IP address of a successor is shown in a routing table entry right after the word via.



FD is the lowest calculated metric to reach the destination network. FD is the metric listed in the routing table entry as the second number inside the brackets. As with other routing protocols, this is also known as the metric for the route.



- R3, with the address 192.168.10.10, is the successor for 192.168.1.0/24.
- This route has a feasible distance of 3,012,096.

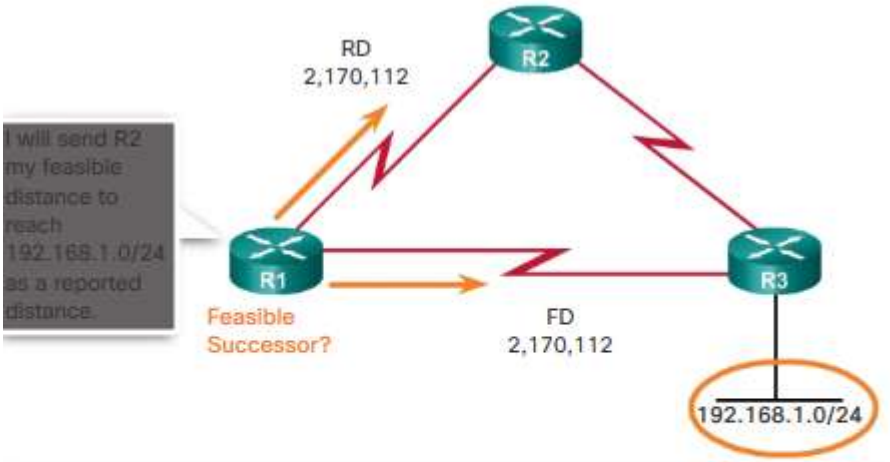
Examining the routing table for R2 in Figure 2, notice that EIGRP's best path for the 192.168.1.0/24 network is through router R3, and that the feasible distance is 3,012,096. This is the metric that was calculated in the previous topic.

Feasible Successors, Feasibility Condition, and Reported Distance

DUAL can converge quickly after a change in the topology because it can use backup paths to other networks without recomputing DUAL. These backup paths are known as Feasible Successors (FSs).

An FS is a neighbor that has a loop-free backup path to the same network as the successor, and it satisfies the Feasibility Condition (FC). R2's successor for the 192.168.1.0/24 network is R3, providing the best

path or lowest metric to the destination network. Notice in Figure 1, that R1 provides an alternative path, but is it an FS? Before R1 can be an FS for R2, R1 must first meet the FC.



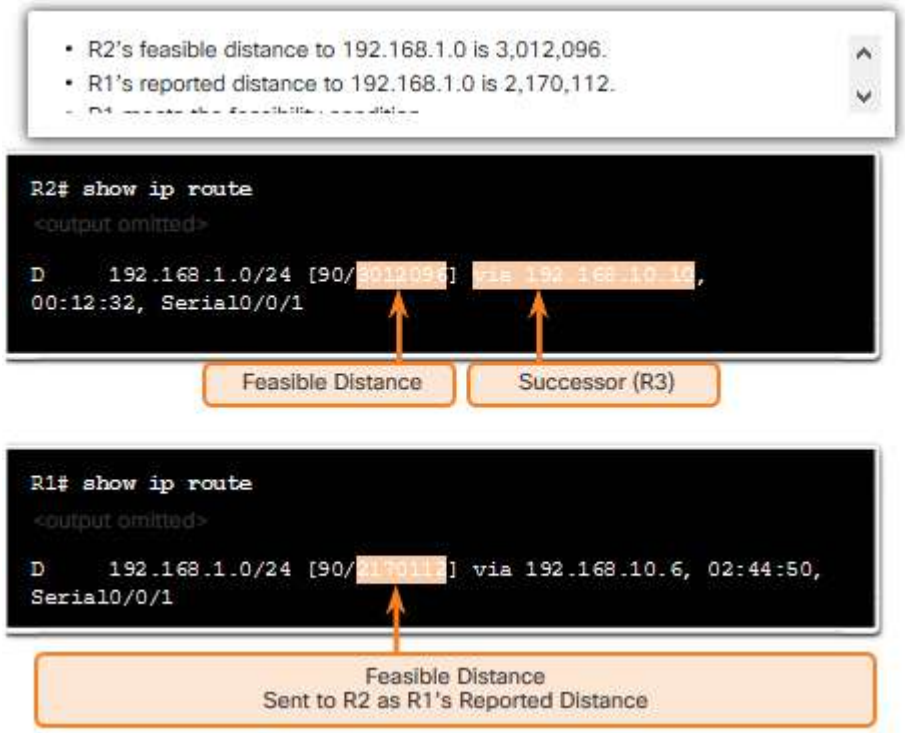

```
R1# show ip route
<output omitted>

D     192.168.1.0/24 [90/2170112] via 192.168.10.6, 02:44:50,
Serial0/0/1
```

The FC is met when a neighbor's Reported Distance (RD) to a network is less than the local router's feasible distance to the same destination network. If the reported distance is less, it represents a loop-free path. The reported distance is simply an EIGRP neighbor's feasible distance to the same destination network. The reported distance is the metric that a router reports to a neighbor about its own cost to that network.

In Figure 2, R1's feasible distance to 192.168.1.0/24 is 2,170,112.

R1 reports to R2 that its FD to 192.168.1.0/24 is 2,170,112.

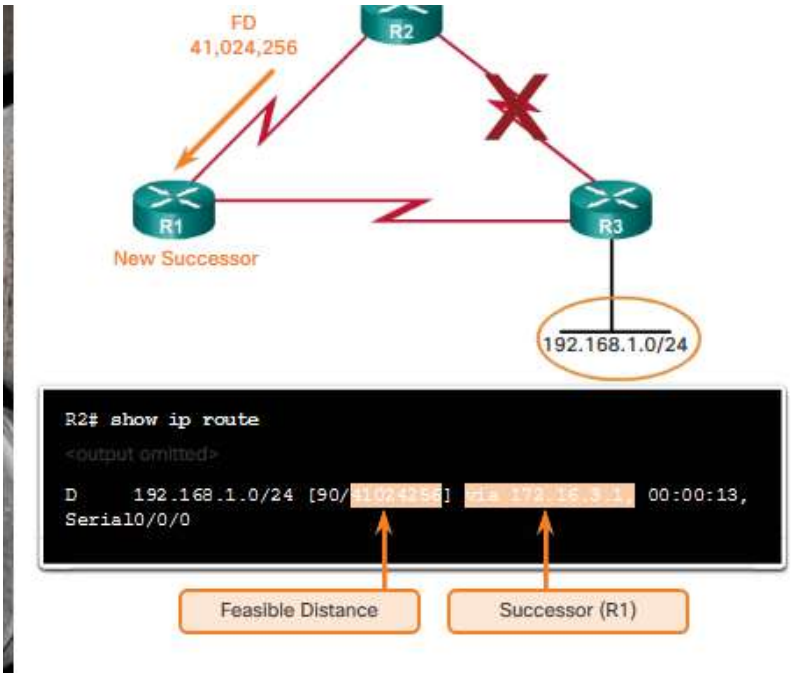
From R2's perspective, 2,170,112 is R1's RD.



R2 uses this information to determine if R1 meets the FC and, therefore, can be an FS.

As shown in Figure 3, because the RD of R1 (2,170,112) is less than R2's own FD (3,012,096), R1 meets the FC.

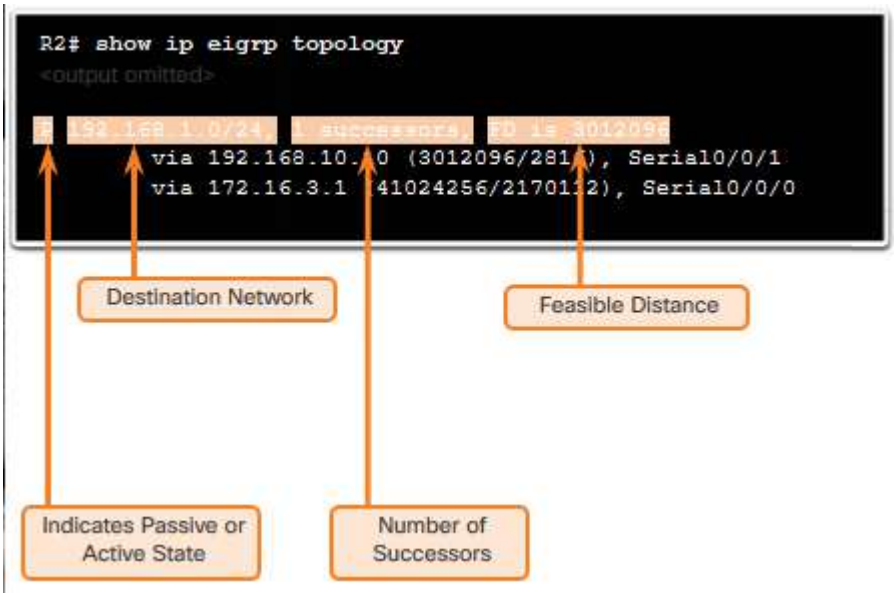
R1 is now an FS for R2 to the 192.168.1.0/24 network.



If there is a failure in R2's path to 192.168.1.0/24 via R3 (successor), then R2 immediately installs the path via R1 (FS) in its routing table. R1 becomes the new successor for R2's path to this network,

Topology Table: show ip eigrp topology Command (Cont.)

As shown in Figure 1, the first line in the topology table displays:



P - Route in the passive state. When DUAL is not performing its diffusing computations to determine a path for a network, the route is in a stable mode, known as the passive state. If DUAL recalculates or searches for a new path, the route is in an active state and displays an A. All routes in the topology table should be in the passive state for a stable routing domain.

192.168.1.0/24 - Destination network that is also found in the routing table.

1 successors - Displays the number of successors for this network. If there are multiple equal cost paths to this network, there are multiple successors.

FD is 3012096 - FD, the EIGRP metric to reach the destination network. This is the metric displayed in the IP routing table.

As shown in Figure 2, the first subentry in the output shows the successor:

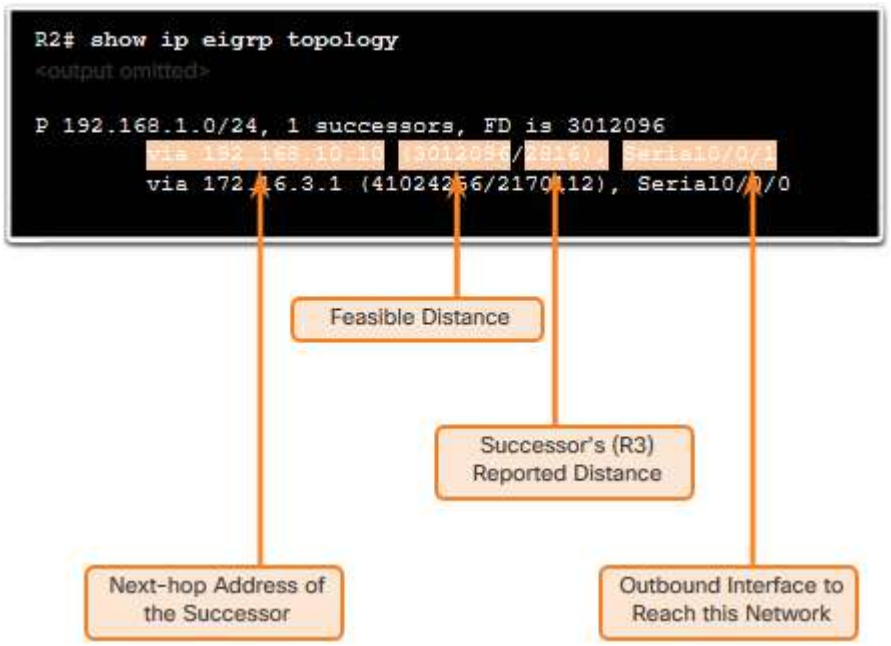
via 192.168.10.10 - Next-hop address of the successor, R3. This address is shown in the routing table.

3012096 - FD to 192.168.1.0/24. It is the metric shown in the IP routing table.

2816 - RD of the successor and is R3's cost to reach this network.

Serial 0/0/1 - Outbound interface used to reach this network, also shown in the routing table.

As shown in Figure 3, the second subentry shows the FS, R1 (if there is not a second entry, then there are no FSs):

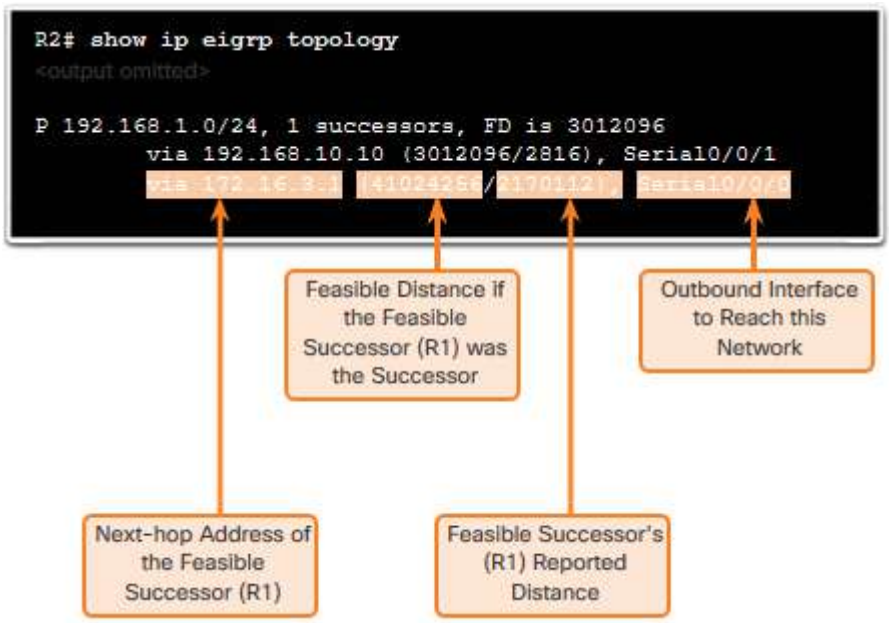


via 172.16.3.1 - Next-hop address of the FS, R1.

41024256 - R2's new FD to 192.168.1.0/24, if R1 became the new successor and would be the new metric displayed in the IP routing table.

2170112 - RD of the FS, or R1's metric to reach this network. RD must be less than the current FD of 3,012,096 to meet the FC.

Serial 0/0/0 - This is the outbound interface used to reach FS, if this router becomes the successor.



Review questions

See the practical attachment

EIGRP for IPv6

Similar to its IPv4 counterpart, EIGRP for IPv6 exchanges routing information to populate the IPv6 routing table with remote prefixes. EIGRP for IPv6 was made available in Cisco IOS, Release 12.4(6)T.

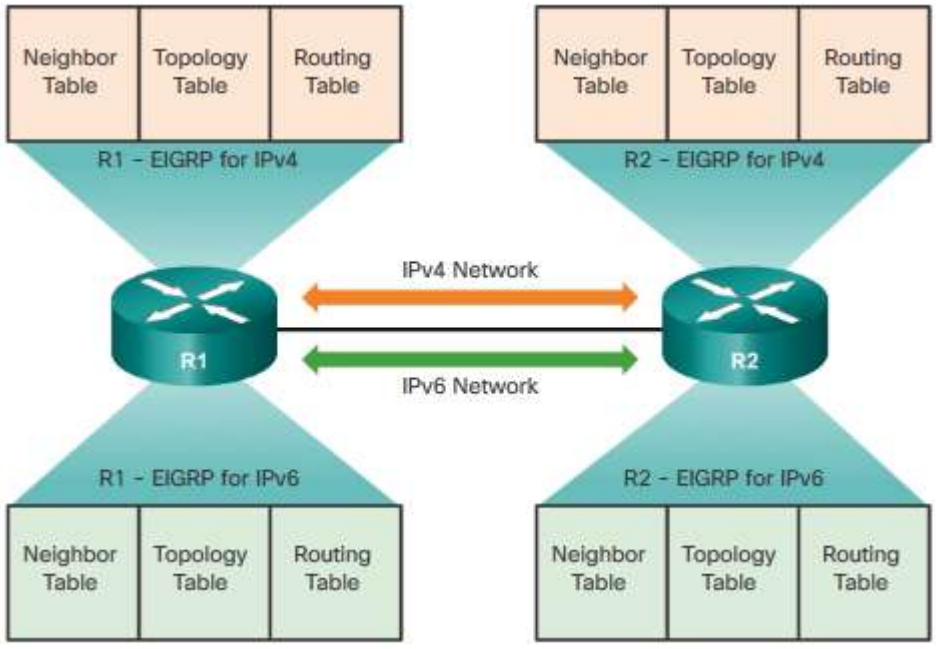
Note: In IPv6, the network address is referred to as the prefix and the subnet mask is called the prefix length.

EIGRP for IPv4 runs over the IPv4 network layer, communicating with other EIGRP IPv4 peers, and advertising only IPv4 routes. EIGRP for IPv6 has the same functionality as EIGRP for IPv4, but uses IPv6 as the network layer transport, communicating with EIGRP for IPv6 peers and advertising IPv6 routes.

EIGRP for IPv6 also uses DUAL as the computation engine to guarantee loop-free paths and backup paths throughout the routing domain.

As with all IPv6 routing protocols, EIGRP for IPv6 has separate processes from its IPv4 counterpart. The processes and operations are basically the same as in the IPv4 routing protocol; however, they run independently. EIGRP for IPv4 and EIGRP for IPv6 each have separate EIGRP neighbor tables, EIGRP topology tables, and IP routing tables, as shown in the figure. EIGRP for IPv6 is a separate protocol-dependent module (PDM).

The EIGRP for IPv6 configuration and verification commands are very similar to those used in EIGRP for IPv4. These commands are described later in this section.



Compare EIGRP for IPv4 and IPv6

The following is a comparison of the main features of EIGRP for IPv4 and EIGRP for IPv6:

Advertised routes - EIGRP for IPv4 advertises IPv4 networks; whereas, EIGRP for IPv6 advertises IPv6 prefixes.

Distance vector - Both EIGRP for IPv4 and IPv6 are advanced distance vector routing protocols. Both protocols use the same administrative distances.

Convergence technology - EIGRP for IPv4 and IPv6 both use the DUAL algorithm. Both protocols use the same DUAL techniques and processes, including successor, FS, FD, and RD.

Metric - Both EIGRP for IPv4 and IPv6 use bandwidth, delay, reliability, and load for their composite metric. Both routing protocols use the same composite metric and use only bandwidth and delay, by default.

Transport protocol - The Reliable Transport Protocol (RTP) is responsible for guaranteed delivery of EIGRP packets to all neighbors for both protocols, EIGRP for IPv4 and IPv6.

Update messages - Both EIGRP for IPv4 and IPv6 send incremental updates when the state of a destination changes. The terms, partial and bounded, are used when referring to updates for both protocols.

Neighbor discovery mechanism - EIGRP for IPv4 and EIGRP for IPv6 use a simple Hello mechanism to learn about neighboring routers and form adjacencies.

Source and destination addresses - EIGRP for IPv4 sends messages to the multicast address 224.0.0.10. These messages use the source IPv4 address of the outbound interface. EIGRP for IPv6 sends its messages to the multicast address FF02::A. EIGRP for IPv6 messages are sourced using the IPv6 link-local address of the exit interface.

Authentication - EIGRP for IPv4 and EIGRP for IPv6 use Message Digest 5 (MD5) authentication. Named EIGRP also supports the stronger SHA256 algorithm.

Router ID - Both EIGRP for IPv4 and EIGRP for IPv6 use a 32-bit number for the EIGRP router ID. The 32-bit router ID is represented in dotted-decimal notation and is commonly referred to as an IPv4 address. If the EIGRP for IPv6 router has not been configured with an IPv4 address, the eigrp router-id command must be used to configure a 32-bit router ID. The process for determining the router ID is the same for both EIGRP for IPv4 and IPv6.

	EIGRP for IPv4	EIGRP for IPv6
Advertised Routes	IPv4 networks	IPv6 prefixes
Distance Vector	Yes	Yes
Convergence Technology	DUAL	DUAL
Metric	Bandwidth and delay by default, reliability and load are optional	Bandwidth and delay by default, reliability and load are optional
Transport Protocol	RTP	RTP
Update Messages	Incremental, partial, and bounded updates	Incremental, partial, and bounded updates
Neighbor Discovery	Hello packets	Hello packets
Source and Destination Addresses	IPv4 source address and 224.0.0.10 IPv4 multicast destination address	IPv6 link-local source address and FF02::A IPv6 multicast destination address
Authentication	MD5, SHA256	MD5, SHA256
Router ID	32-bit router ID	32-bit router ID

IPv6 Link-local Addresses

Routers running a dynamic routing protocol, such as EIGRP exchange messages between neighbors on the same subnet or link. Routers only need to send and receive routing protocol messages with their directly connected neighbors. These messages are always sent from the source IP address of the router that is doing the forwarding.

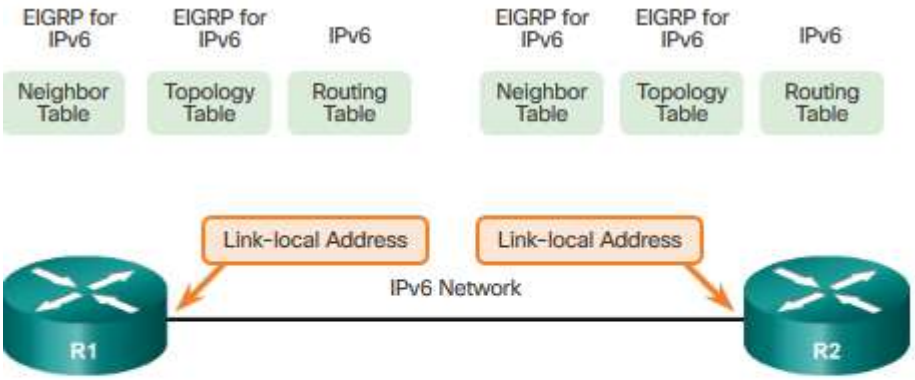
IPv6 link-local addresses are ideal for this purpose. An IPv6 link-local address enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet). Packets with a source or destination link-local address cannot be routed beyond the link from where the packet originated.

EIGRP for IPv6 messages are sent using:

Source IPv6 address - This is the IPv6 link-local address of the exit interface.

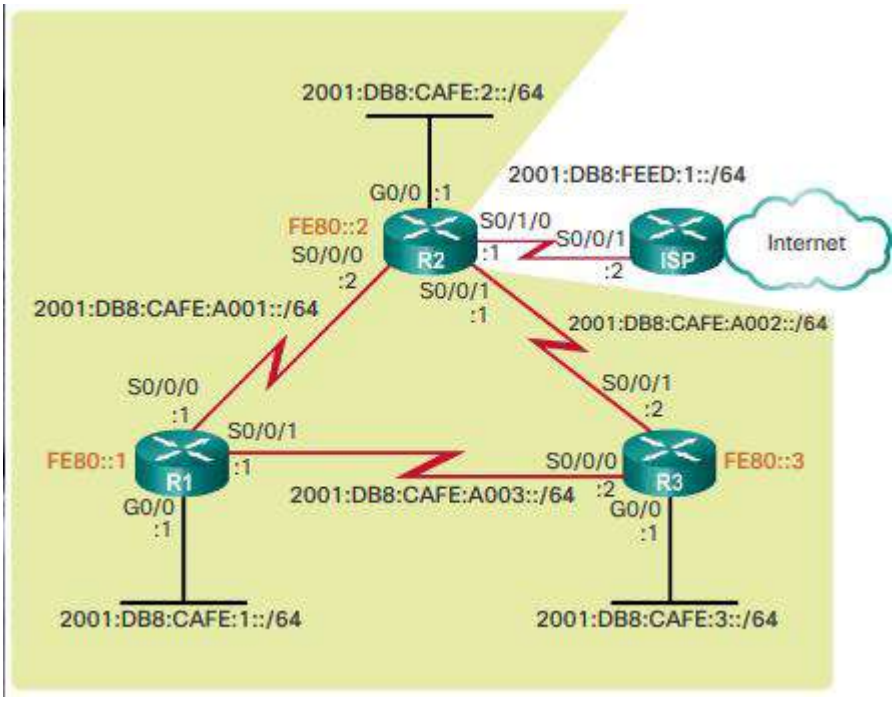
Destination IPv6 address - When the packet needs to be sent to a multicast address, it is sent to the IPv6 multicast address FF02::A, the all-EIGRP-routers with link-local scope. If the packet can be sent as a unicast address, it is sent to the link-local address of the neighboring router.

Note: IPv6 link-local addresses are in the FE80::/10 range. The /10 indicates that the first 10 bits are 1111 1110 10xx xxxx, which results in the first hextet having a range of 1111 1110 1000 0000 (FE80) to 1111 1110 1011 1111 (FEBF).



Configuring IPv6 Link-local Addresses

Link-local addresses are automatically created when an IPv6 global unicast address is assigned to the interface. Global unicast addresses are not required on an interface; however, IPv6 link-local addresses are, as shown in Figure 1.



Unless configured manually, Cisco routers create the link-local address using FE80::/10 prefix and the EUI-64 process. EUI-64 involves using the 48-bit Ethernet MAC address, inserting FFFE in the middle and flipping the seventh bit. For serial interfaces, Cisco uses the MAC address of an Ethernet interface. A router with several serial interfaces can assign the same link-local address to each IPv6 interface, because link-local addresses only need to be local on the link.

Link-local addresses created using the EUI-64 format, or in some cases random interface IDs, make it difficult to recognize and remember those addresses. Because IPv6 routing protocols use IPv6 link-local addresses for unicast addressing and next hop address information in the routing table, it is common practice to make it an easily recognizable address. Configuring the link-local address manually provides the ability to create an address that is recognizable and easier to remember.

Link-local addresses can be configured manually using the same interface configuration mode command used to create IPv6 global unicast addresses, but with different parameters:

Router(config-if)# **ipv6 address** *link-local-address* **link-local**

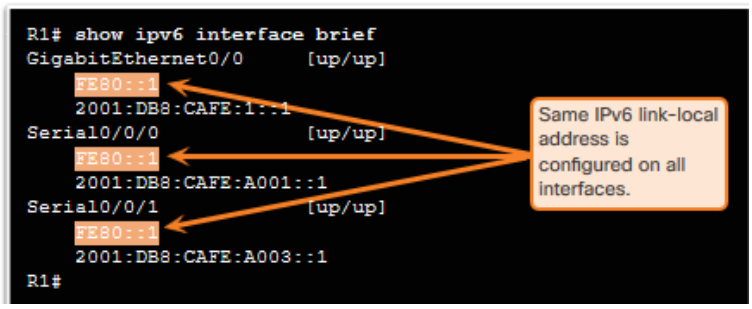
A link-local address has a prefix within the range FE80 to FEBF. When an address begins with this hextet (16-bit segment), the link-local keyword must follow the address.

```
R1(config)# interface s 0/0/0
R1(config-if)# ipv6 address fe80::1 ?
  link-local  Use link-local address

R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface s 0/0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface g 0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)#
```

Figure 2 shows the configuration of a link-local address using the ipv6 address interface configuration mode command. The link-local address FE80::1 is used to make it easily recognizable as belonging to router R1. The same IPv6 link-local address is configured on all of R1's interfaces. FE80::1 can be configured on each link because it only has to be unique on that link.

```
R2(config)# interface s 0/0/0
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# exit
R2(config)# interface s 0/0/1
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# exit
R2(config)# interface s 0/1/0
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# exit
R2(config)# interface g 0/0
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)#
```

Similar to R1, in Figure 3, router R2 is configured with FE80::2 as the IPv6 link-local address on all of its interfaces.



Configuring the EIGRP for IPv6 Routing Process

The ipv6 unicast-routing global configuration mode command enables IPv6 routing on the router. This command is required before any IPv6 routing protocol can be configured. This command is not required to configure IPv6 addresses on the interfaces but is necessary for the router to be enabled as an IPv6 router.

EIGRP for IPv6

```
R1(config)# ipv6 router eigrp 2
% IPv6 routing not enabled
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 router eigrp 2
R1(config-rtr)#
```

The following global configuration mode command is used to enter router configuration mode for EIGRP for IPv6:

Router(config)# **ipv6 router eigrp** *autonomous-system*

Similar to EIGRP for IPv4, the *autonomous-system* value must be the same on all routers in the routing domain. In Figure 1, the EIGRP for IPv6 routing process could not be configured until IPv6 routing was enabled with the ipv6 unicast-routing global configuration mode command.

Configuring the Router ID

```
R1(config)# ipv6 router eigrp 2
R1(config-rtr)# eigrp router-id 1.0.0.0
R1(config-rtr)#
```

As shown in Figure 2, the eigrp router-id command is used to configure the router ID. EIGRP for IPv6 uses a 32 bit value for the router ID. To obtain that value, EIGRP for IPv6 uses the same process as EIGRP for IPv4. The eigrp router-id command takes precedence over any loopback or physical interface IPv4 addresses. If an EIGRP for IPv6 router does not have any active interfaces with an IPv4 address, then the eigrp router-id command is required.

The router ID should be a unique 32-bit number in the EIGRP for IP routing domain; otherwise, routing inconsistencies can occur.

Note: The eigrp router-id command is used to configure the router ID for EIGRP. Some versions of IOS will accept the command router-id, without first specifying eigrp. The running-config, however, will

display eigrp router-id regardless of which command is used.

By default, the EIGRP for IPv6 process is in a shutdown state. The no shutdown command is required to activate the EIGRP for IPv6 process, as shown in Figure 3.

```
R1(config)# ipv6 router eigrp 2
R1(config-rtr)# eigrp router-id 1.0.0.0
R1(config-rtr)# no shutdown
R1(config-rtr)#
```

This command is not required for EIGRP for IPv4. Although, EIGRP for IPv6 is enabled, neighbor adjacencies and routing updates cannot be sent and received until EIGRP is activated on the appropriate interfaces.

Both the no shutdown command and a router ID are required for the router to form neighbor adjacencies.

```
R2(config)# ipv6 unicast-routing
R2(config)# ipv6 router eigrp 2
R2(config-rtr)# eigrp router-id 2.0.0.0
R2(config-rtr)# no shutdown
R2(config-rtr)#
```

Figure 4 shows the complete EIGRP for IPv6 configuration for router R2. The show ipv6 interface brief command is used to verify the IPv6 link-local and global unicast addresses on all interfaces.

The ipv6 eigrp Interface Command

EIGRP for IPv6 uses a different method to enable an interface for EIGRP. Instead of using the network router configuration mode command to specify matching interface addresses, EIGRP for IPv6 is configured directly on the interface.

Use the following interface configuration mode command to enable EIGRP for IPv6 on an interface:

Router(config-if)# ipv6 eigrp *autonomous-system*

The *autonomous-system* value must be the same as the autonomous system number used to enable the EIGRP routing process. Similar to the network command used in EIGRP for IPv4, the ipv6 eigrp interface command:

Enables the interface to form adjacencies and send or receive EIGRP for IPv6 updates.Includes the prefix (network) of this interface in EIGRP for IPv6 routing updates.

Figure 1 shows the configuration to enable EIGRP for IPv6 on routers R1 and R2 interfaces. Notice the message following the serial 0/0/0 interface in R2:

```
R1(config)# interface g0/0
R1(config-if)# ipv6 eigrp 2
R1(config-if)# exit
R1(config)# interface s 0/0/0
R1(config-if)# ipv6 eigrp 2
R1(config-if)# exit
R1(config)# interface s 0/0/1
R1(config-if)# ipv6 eigrp 2
R1(config-if)#
```

```
R2(config)# interface g 0/0
R2(config-if)# ipv6 eigrp 2
R2(config-if)# exit
R2(config)# interface s 0/0/0
R2(config-if)# ipv6 eigrp 2
R2(config-if)# exit
%DUAL-5-NBRCHANGE: EIGRP-IPv6 2: Neighbor FE80::1
(Serial0/0/0) is up: new adjacency
R2(config)# interface s 0/0/1
R2(config-if)# ipv6 eigrp 2
R2(config-if)#
```

%DUAL-5-NBRCHANGE: EIGRP-IPv6 2: Neighbor FE80::1 (Serial0/0/0) is up: new adjacency

This message indicates that R2 has now formed an EIGRP-IPv6 adjacency with the neighbor at link-local address FE80::1. Because static link-local addresses were configured on all three routers, it is easy to determine that this adjacency is with router R1 (FE80::1).

```
R1(config)# ipv6 router eigrp 2
R1(config-rtr)# passive-interface gigabitethernet 0/0
R1(config-rtr)# end

R1# show ipv6 protocols

IPv6 Routing Protocol is "eigrp 2"
EIGRP-IPv6 Protocol for AS(2)
<output omitted>

  Interfaces:
    Serial0/0/0
    Serial0/0/1
    GigabitEthernet0/0 (passive)
  Redistribution:
    None
R1#
```

Passive Interface with EIGRP for IPv6

The same passive-interface command used for IPv4 is used to configure an interface as passive with EIGRP for IPv6. The show ipv6 protocols command is used to verify the configuration.

IPv6 Neighbor Table

Similar to EIGRP for IPv4, before any EIGRP for IPv6 updates can be sent or received, routers must establish adjacencies with their neighbors.

Use the show ipv6 eigrp neighbors command to view the neighbor table and verify that EIGRP for IPv6 has established an adjacency with its neighbors. The output shown in Figure 2 displays the IPv6 link-local address of the adjacent neighbor and the interface that this router uses to reach that EIGRP

neighbor. Using meaningful link-local addresses makes it easy to recognize the neighbors R2 at FE80::2 and R3 at FE80::3.

The column headers in the show ipv6 eigrp neighbors command output identify the following:

- H - Lists the neighbors in the order they were learned.
- Address - IPv6 link-local address of the neighbor.
- Interface - Local interface on which this Hello packet was received.
- Hold - Current hold time. When a Hello packet is received, this value is reset to the maximum hold time for that interface and then counts down to zero. If zero is reached, the neighbor is considered down.
- Uptime - Amount of time since this neighbor was added to the neighbor table.

SRTT and RTO - Used by RTP to manage reliable EIGRP packets.

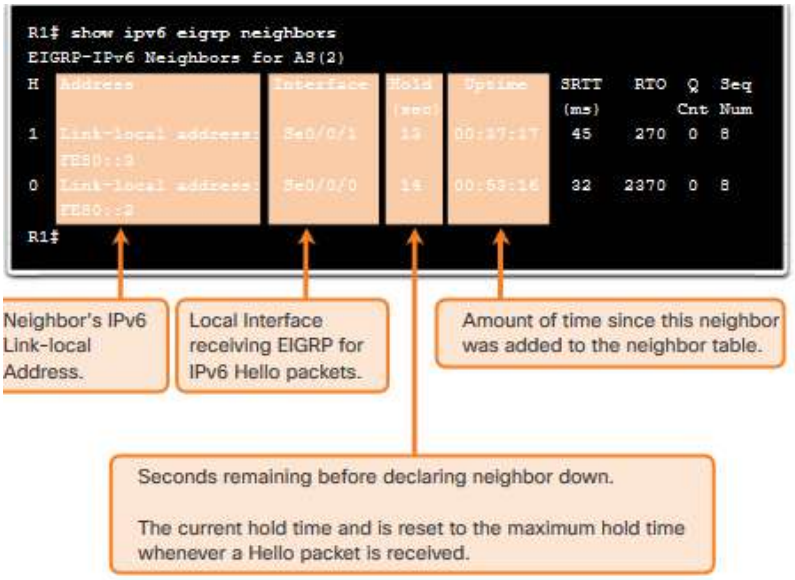
Queue Count - Should always be zero. If it is more than zero, then EIGRP packets are waiting to be sent.

Sequence Number - Used to track updates, queries, and reply packets.

The show ipv6 eigrp neighbors command is useful for verifying and troubleshooting EIGRP for IPv6. If an expected neighbor is not listed, ensure that both ends of the link are up/up using the show ipv6 interface brief command. The same requirements exist for establishing neighbor adjacencies with EIGRP for IPv6 as it does for IPv4. If both sides of the link have active interfaces, check to see:

Are both routers configured with the same EIGRP autonomous system number?

Is the interface enabled for EIGRP for IPv6 with the correct autonomous system number?



Review questions

See the practical attachment

Learning Outcome 2.3: Connect networks using OSPF

Evolution of OSPF

	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector		Link-State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP

As shown in Figure 1, OSPF version 2 (OSPFv2) is available for IPv4 while OSPF version 3 (OSPFv3) is available for IPv6.

The initial development of OSPF began in 1987 by the Internet Engineering Task Force (IETF) OSPF Working Group. At that time, the Internet was largely an academic and research network funded by the U.S. government.

In 1989, the specification for OSPFv1 was published in RFC 1131. Two implementations were written. One implementation was developed to run on routers and the other to run on UNIX workstations. The latter implementation became a widespread UNIX process known as GATED. OSPFv1 was an experimental routing protocol and was never deployed.

In 1991, OSPFv2 was introduced in RFC 1247 by John Moy. OSPFv2 offered significant technical improvements over OSPFv1. It is classless by design; therefore, it supports VLSM and CIDR.

At the same time the OSPF was introduced, ISO was working on a link-state routing protocol of their own, Intermediate System-to-Intermediate System (IS-IS). IETF chose OSPF as their recommended Interior Gateway Protocol (IGP).

In 1998, the OSPFv2 specification was updated in RFC 2328, which remains the current RFC for OSPF.

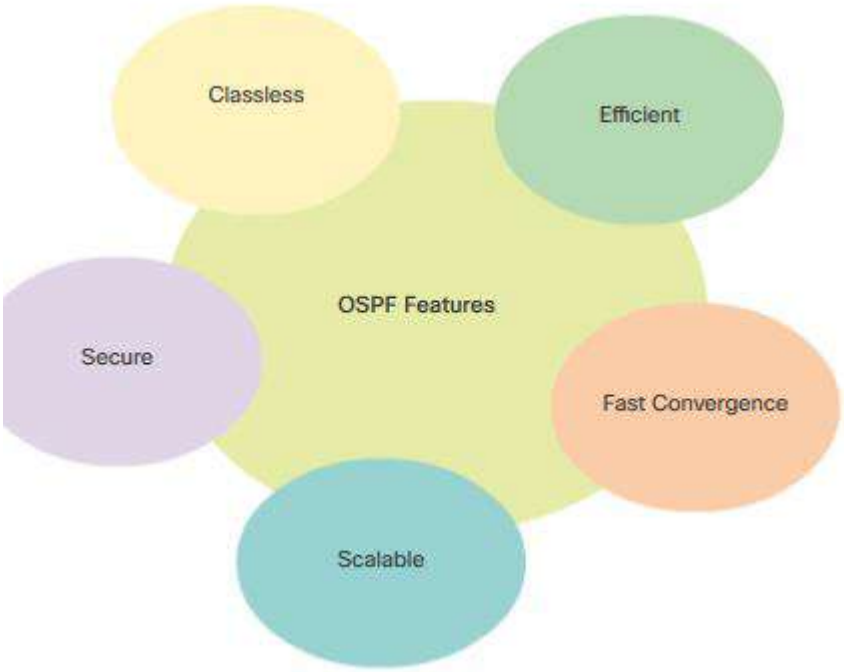
In 1999, OSPFv3 for IPv6 was published in RFC 2740. OSPF for IPv6, created by John Moy, Rob Coltun, and Dennis Ferguson, is not only a new protocol implementation for IPv6, but also a major rewrite of the operation of the protocol.

In 2008, OSPFv3 was updated in RFC 5340 as OSPF for IPv6.

In 2010, the support of the Address Families (AF) feature in OSPFv3 was introduced with RFC 5838. The use of address families allows a routing protocol to support both IPv4 and IPv6 within a single unified configuration process. OSPFv3 with address families is beyond the scope of this curriculum.

Note: In this chapter, unless explicitly identified as OSPFv2 or OSPFv3, the term OSPF is used to indicate concepts that are shared by both.

Features of OSPF



OSPF features, as shown in Figure 1, include:

Classless - OSPFv2 is classless by design; therefore, it supports IPv4 VLSM and CIDR.

Efficient - Routing changes trigger routing updates (no periodic updates). It uses the SPF algorithm to choose the best path.

Fast convergence - It quickly propagates network changes.

Scalable - It works well in small and large network sizes. Routers can be grouped into areas to support a hierarchical system.

Secure - OSPFv2 supports Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) authentication. OSPFv3 uses Internet Protocol Security (IPsec) to add authentication for OSPFv3 packets. When authentication is enabled, OSPF routers only accept encrypted routing updates from peers with the same pre-shared password.

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

Administrative distance (AD) is the trustworthiness (or preference) of the route source. OSPF has a default administrative distance of 110. As shown in Figure 2, OSPF has a lower number (making it a preferred routing protocol over IS-IS and RIP) on Cisco devices.

Components of OSPF

All routing protocols share similar components. They all use routing protocol messages to exchange route information. The messages help build data structures, which are then processed using a routing algorithm.

The three main components of the OSPF routing protocol include:

Data Structures

Database	Table	Description
Adjacency Database	Neighbor Table	• List of all neighbor routers to which a router has established bidirectional communication. • This table is unique for each router. • Can be viewed using the `show ip ospf neighbor` command.
Link-state Database (LSDB)	Topology Table	• Lists information about all other routers in the network. • The database represents the network topology. • All routers within an area have identical LSDB. • Can be viewed using the `show ip ospf database` command.
Forwarding Database	Routing Table	• List of routes generated when an algorithm is run on the link-state database. • Each router's routing table is unique and contains information on how and where to send packets to other routers. • Can be viewed using the `show ip route` command.

OSPF creates and maintains three databases: (see Figure 1).

Adjacency database - Creates the neighbor table.

Link-state database (LSDB) - Creates the topology table.

Forwarding database - Creates the routing table.

These tables contain a list of neighboring routers to exchange routing information with and are kept and

maintained in RAM.

Routing Protocol Messages

Layer 3 devices (such as routers) running OSPF exchange messages to convey routing information using five types of packets. These packets, as shown in Figure 2, are:

- Hello packet
- Database description packet
- Link-state request packet
- Link-state update packet
- Link-state acknowledgment packet

These packets are used to discover neighboring routers and also to exchange routing information to maintain accurate information about the network.

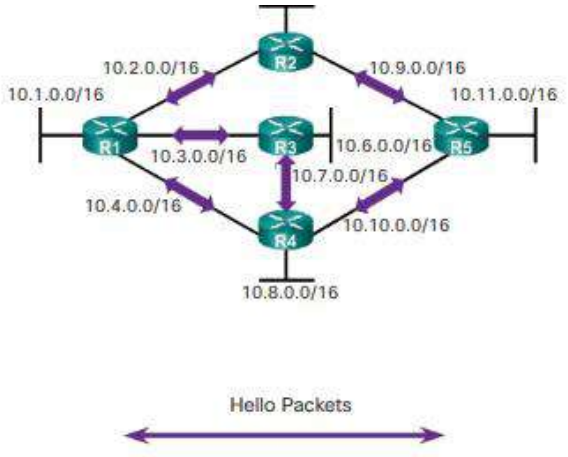
Algorithm

The router builds the topology table using results of calculations based on the Dijkstra SPF algorithm. The SPF algorithm is based on the cumulative cost to reach a destination.

The SPF algorithm creates an SPF tree by placing each router at the root of the tree and calculating the shortest path to each node. The SPF tree is then used to calculate the best routes. OSPF places the best routes into the forwarding database, which is used to make the routing table.

Link-State Operation

To maintain routing information, OSPF routers complete the following generic link-state routing process to reach a state of convergence:



1. Establish Neighbor Adjacencies - OSPF-enabled routers must recognize each other on the network before they can share information. An OSPF-enabled router sends Hello packets out all OSPF-enabled interfaces to determine if neighbors are present on those links. If a neighbor is present, the OSPF-enabled router attempts to establish a neighbor adjacency with that neighbor.

2. Exchange Link-State Advertisements- After adjacencies are established, routers then exchange link-state advertisements (LSAs). LSAs contain the state and cost of each directly connected link. Routers

flood their LSAs to adjacent neighbors. Adjacent neighbors receiving the LSA immediately flood the LSA to other directly connected neighbors, until all routers in the area have all LSAs.

3. Build the Topology Table - After LSAs are received, OSPF-enabled routers build the topology table (LSDB) based on the received LSAs. This database eventually holds all the information about the topology of the network.

4. Execute the SPF Algorithm - Routers then execute the SPF algorithm. The gears in the figure are used to indicate the execution of the SPF algorithm. The SPF algorithm creates the SPF tree.

From the SPF tree, the best paths are offered to the IP routing table. The route will be inserted into the routing table unless there is a route source to the same network with a lower administrative distance, such as a static route. Routing decisions are made based on the entries in the routing table.

Single-Area and Multiarea OSPF

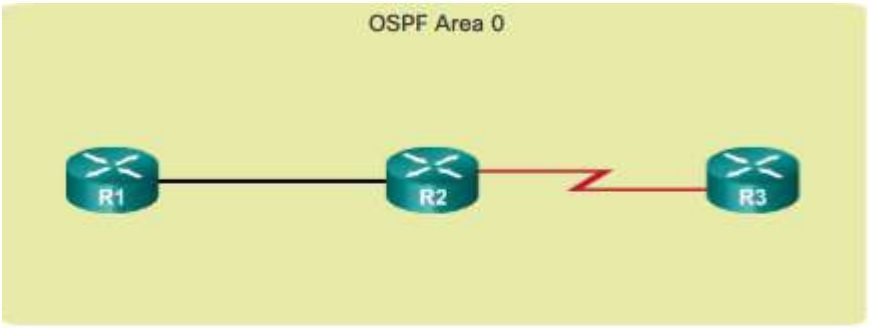
To make OSPF more efficient and scalable, OSPF supports hierarchical routing using areas. An OSPF area is a group of routers that share the same link-state information in their LSDBs.

OSPF can be implemented in one of two ways:

Single-Area OSPF - In Figure 1, all routers are in one area called the backbone area (area 0).

Multiarea OSPF - In Figure 2, OSPF is implemented using multiple areas, in a hierarchal fashion. All areas must connect to the backbone area (area 0). Routers interconnecting the areas are referred to as Area Border Routers (ABRs).

With multiarea OSPF, OSPF can divide one large routing domain into smaller areas, to support hierarchical routing. With hierarchical routing, routing still occurs between the areas (interarea routing), while many of the processor intensive routing operations, such as recalculating the database, are kept within an area.



- Area 0 is also called the backbone area.
- Single-Area OSPF is useful in smaller networks with few routers.

For instance, any time a router receives new information about a topology change within the area (including the addition, deletion, or modification of a link) the router must rerun the SPF algorithm, create a new SPF tree, and update the routing table. The SPF algorithm is CPU-intensive and the time

it takes for calculation depends on the size of the area.

Note: Routers in other areas receive messages regarding topology changes, but these routers only update the routing table, not rerun the SPF algorithm.

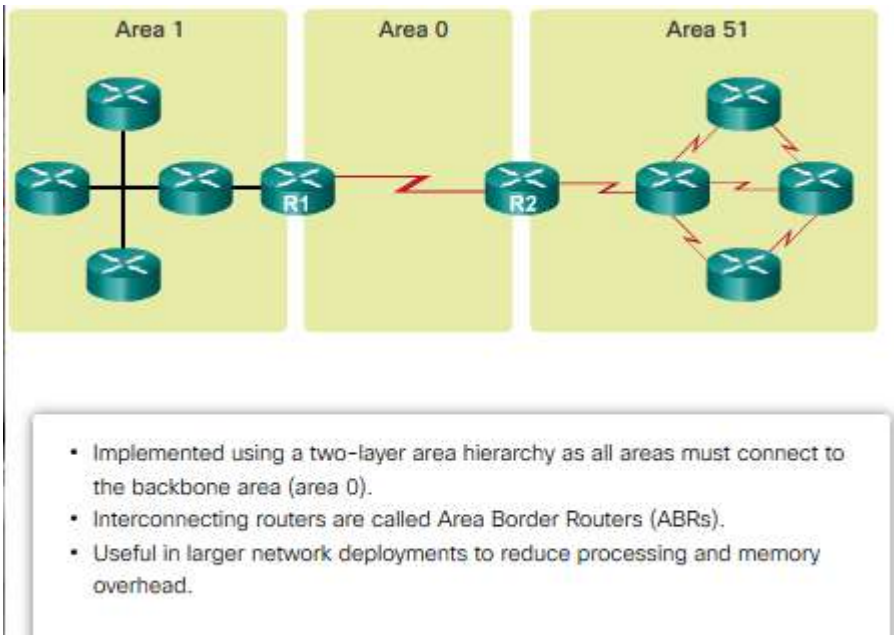
Too many routers in one area would make the LSDBs very large and increase the load on the CPU. Therefore, arranging routers into areas effectively partitions a potentially large database into smaller and more manageable databases.

The hierarchical-topology design options with multiarea OSPF can offer these advantages:

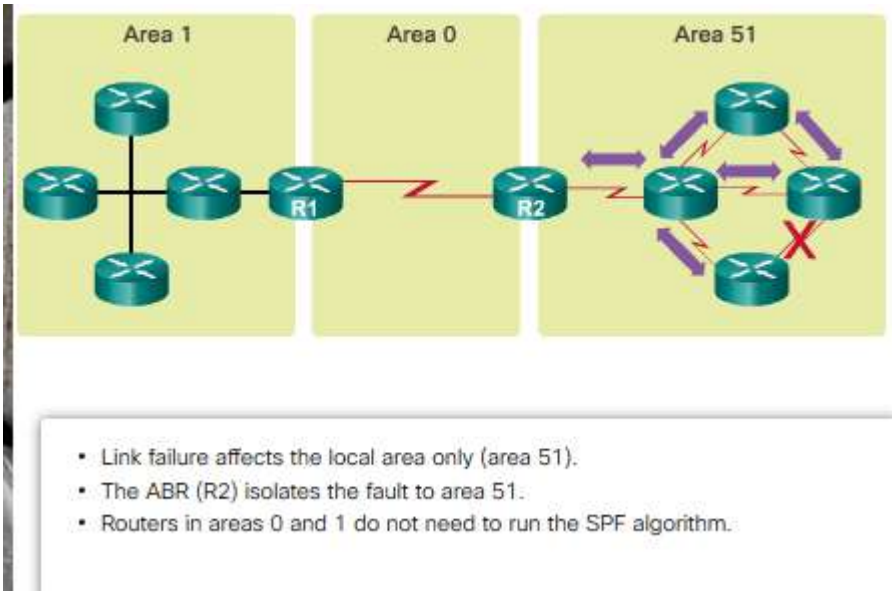
Smaller routing tables - Fewer routing table entries because network addresses can be summarized between areas. Route summarization is not enabled by default.

Reduced link-state update overhead - Designing multiarea OSPF with smaller areas minimizes processing and memory requirements.

Reduced frequency of SPF calculations - Localizes the impact of a topology change within an area. For instance, it minimizes routing update impact because LSA flooding stops at the area boundary.



For example, R2 is an ABR for area 51. As an ABR, it would summarize the area 51 routes into area 0. When one of the summarized links fails, LSAs are exchanged within area 51 only. Routers in area 51 must rerun the SPF algorithm to identify the best routes. However, the routers in area 0 and area 1 do not receive any updates; therefore, they do not execute the SPF algorithm.



Types of OSPF Packets

OSPF uses link-state packets (LSPs) to establish and maintain neighbor adjacencies and exchange routing updates.

The figure shows the five different types of LSPs used by OSPFv2. OSPFv3 has similar packet types. Each packet serves a specific purpose in the OSPF routing process:

Type 1: Hello packet - Used to establish and maintain adjacency with other OSPF routers.

Type 2: Database Description (DBD) packet - Contains an abbreviated list of the sending router's LSDB and is used by receiving routers to check against the local LSDB. The LSDB must be identical on all link-state routers within an area to construct an accurate SPF tree.

Type 3: Link-State Request (LSR) packet - Receiving routers can then request more information about any entry in the DBD by sending an LSR.

Type 4: Link-State Update (LSU) packet - Used to reply to LSRs and to announce new information. LSUs contain seven different types of LSAs.

Type 5: Link-State Acknowledgment (LSAck) packet - When an LSU is received, the router sends an LSAck to confirm receipt of the LSU. The LSAck data field is empty.

Type	Packet Name	Description
1	Hello	Discovers neighbors and builds adjacencies between them
2	Database Description (DBD)	Checks for database synchronization between routers
3	Link-State Request (LSR)	Requests specific link-state records from router to router
4	Link-State Update (LSU)	Sends specifically requested link-state records
5	Link-State Acknowledgment (LSAck)	Acknowledges the other packet types

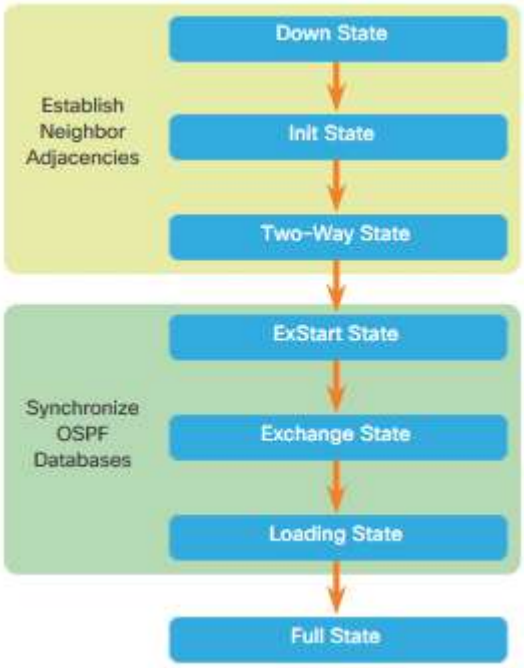
OSPF Operational States

When an OSPF router is initially connected to a network, it attempts to:

- Create adjacencies with neighbors
- Exchange routing information
- Calculate the best routes
- Reach convergence

OSPF progresses through several states while attempting to reach convergence:

- Down state
- Init state
- Two-Way state
- ExStart state
- Exchange state
- Loading state
- Full state



OSPF DR and BDR

Why is a DR and BDR election necessary?

Multiaccess networks can create two challenges for OSPF regarding the flooding of LSAs:

Creation of multiple adjacencies - Ethernet networks could potentially interconnect many OSPF routers over a common link. Creating adjacencies with every router is unnecessary and undesirable. It would lead to an excessive number of LSAs exchanged between routers on the same network.

Extensive flooding of LSAs - Link-state routers flood their LSAs any time OSPF is initialized, or when there is a change in the topology. This flooding can become excessive.

To understand the problem with multiple adjacencies, we must study a formula:
For any number of routers (designated as *n*) on a multiaccess network, there are $n(n-1)/2$ adjacencies.

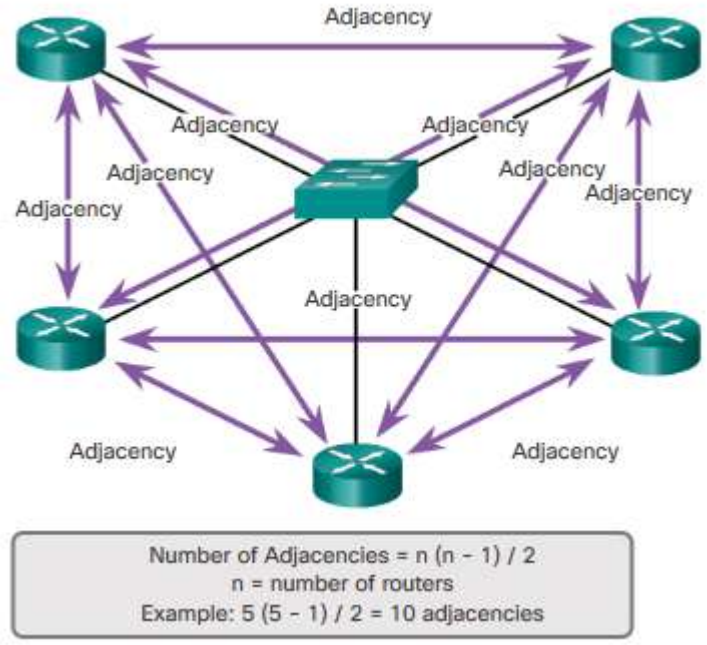


Figure 1 shows a simple topology of five routers, all of which are attached to the same multiaccess Ethernet network. Without some type of mechanism to reduce the number of adjacencies, collectively these routers would form 10 adjacencies:
$5(5-1)/2 = 10$
This may not seem like much, but as routers are added to the network, the number of adjacencies increases dramatically, as shown in Figure 2.

Routers	Adjacencies
n	n (n - 1) / 2
5	10
10	45
20	190
100	4,950

To understand the problem of extensive flooding of LSAs, play the animation in Figure 3. In the animation, R2 sends out an LSA. This event triggers every other router to also send out an LSA. Not shown in the animation are the required acknowledgments sent for every LSA received. If every router in a multiaccess network had to flood and acknowledge all received LSAs to all other routers on that same multiaccess network, the network traffic would become quite chaotic.

The solution to managing the number of adjacencies and the flooding of LSAs on a multiaccess network is the DR. On multiaccess networks, OSPF elects a DR to be the collection and distribution point for

LSAs sent and received. A BDR is also elected in case the DR fails. All other routers become DROTHERs. A DROTHER is a router that is neither the DR nor the BDR.

Note: The DR is only used for the dissemination of LSAs. The router will still use the best next-hop router indicated in the routing table for the forwarding of all other packets.

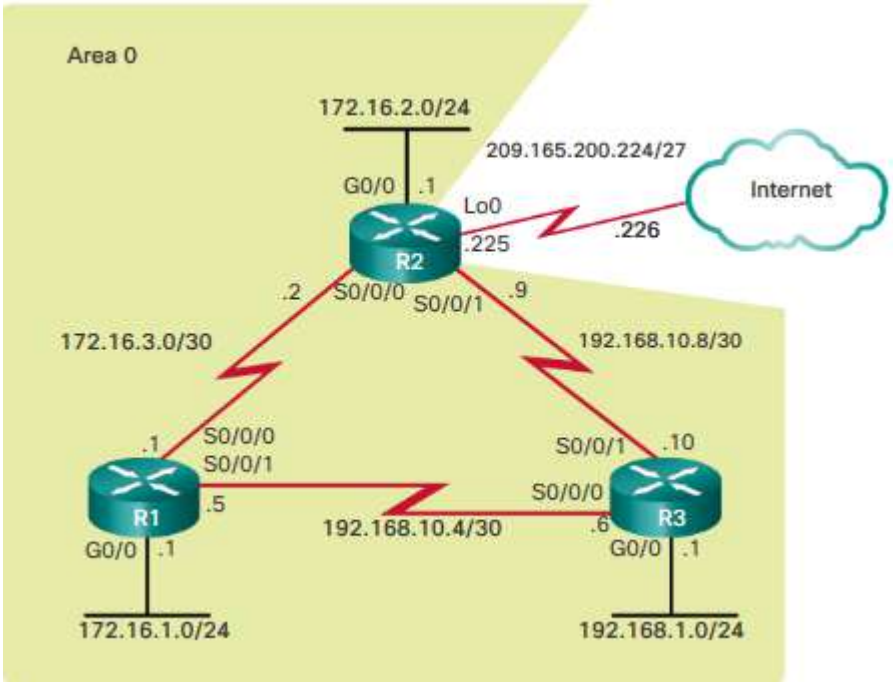
OSPF Network Topology

Introduced in 1991, OSPFv2 is a link-state routing protocol for IPv4. OSPF was designed as an alternative to another IPv4 routing protocol, RIP.

The figure shows the topology used for configuring OSPFv2 in this section. The types of serial interfaces and their associated bandwidths may not necessarily reflect the more common types of connections found in networks today. The bandwidths of the serial links used in this topology were chosen to help explain the calculation of the routing protocol metrics and the process of best path selection.

The routers in the topology have a starting configuration, including interface addresses. There is currently no static routing or dynamic routing configured on any of the routers. All interfaces on routers R1, R2, and R3 (except the loopback on R2) are within the OSPF backbone area. The ISP router is used as the routing domain's gateway to the Internet.

Note: In this topology the loopback interface is used to simulate the WAN link to the Internet.



Router OSPF Configuration Mode

OSPFv2 is enabled using the router ospf *process-id* global configuration mode command. The *process-id* value represents a number between 1 and 65,535 and is selected by the network administrator. The *process-id* value is locally significant, which means that it does not have to be the same value on the

other OSPF routers to establish adjacencies with those neighbors.

```
R1(config)# router ospf 10
R1(config-router)# ?
Router configuration commands:
  auto-cost               Calculate OSPF interface cost
                          according to bandwidth
  network                 Enable routing on an IP network
  no                      Negate a command or set its defaults
  passive-interface       Suppress routing updates on an
                          interface
  priority                OSPF topology priority
  router-id               router-id for this OSPF process
```

Figure provides an example of entering router OSPFv2 configuration mode on R1.

Note: The list of commands has been altered to display only the commands that are used in this chapter.

Router IDs

Every router requires a router ID to participate in an OSPF domain. The router ID can be defined by an administrator or automatically assigned by the router. The router ID is used by the OSPF-enabled router to:

Uniquely identify the router - The router ID is used by other routers to uniquely identify each router within the OSPF domain and all packets that originate from them.

Participate in the election of the DR - In a multiaccess LAN environment, the election of the DR occurs during initial establishment of the OSPF network. When OSPF links become active, the routing device configured with the highest priority is elected the DR. Assuming there is no priority configured, or there is a tie, then the router with the highest router ID is elected the DR. The routing device with the second highest router ID is elected the BDR.

But how does the router determine the router ID? As illustrated in the figure, Cisco routers derive the router ID based on one of three criteria, in the following preferential order:

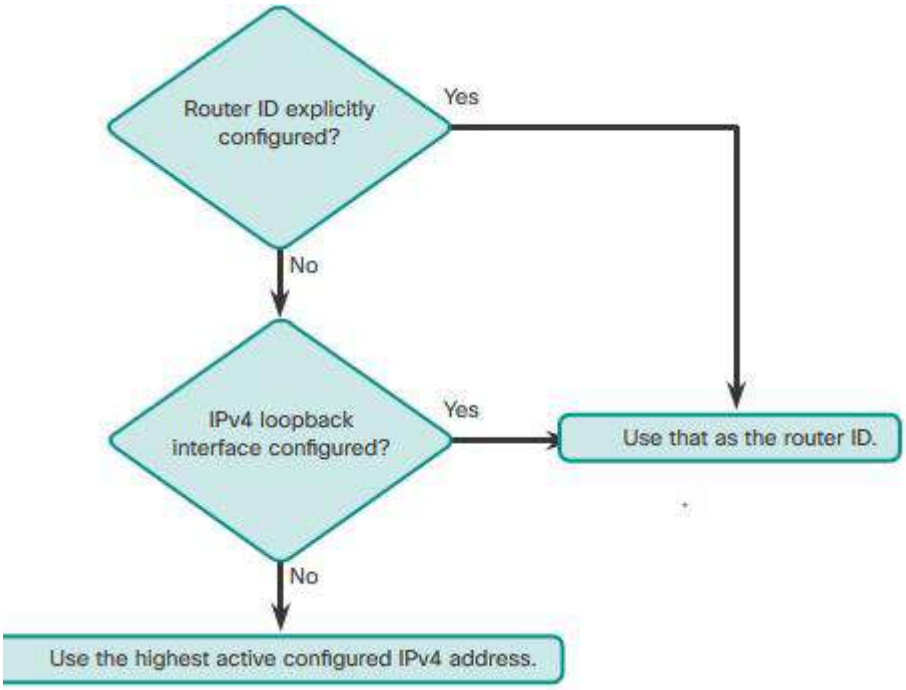
The router ID is explicitly configured using the OSPF router-id *rid* router configuration mode command. The *rid* value is any 32-bit value expressed as an IPv4 address. This is the recommended method to assign a router ID.

If the router ID is not explicitly configured, the router chooses the highest IPv4 address of any of configured loopback interfaces. This is the next best alternative to assigning a router ID.

If no loopback interfaces are configured, then the router chooses the highest active IPv4 address of any of its physical interfaces. This is the least recommended method because it makes it more difficult for administrators to distinguish between specific routers.

If the router uses the highest IPv4 address for the router ID, the interface does not need to be OSPF-enabled. This means that the interface address does not need to be included in one of the OSPF*network* commands for the router to use that IPv4 address as the router ID. The only requirement is that the interface is active and in the up state.

Note: The router ID looks like an IPv4 address, but it is not routable and, therefore, is not included in the routing table, unless the OSPF routing process chooses an interface (physical or loopback) that is appropriately defined by a network command.




```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# end
R1#
*Mar 25 19:50:36.595: %SYS-5-CONFIG_I: Configured from
R1#
R1# show ip protocols
*** IP Routing is NSF aware ***
```

Modifying a Router ID

Sometimes a router ID needs to be changed, for example, when a network administrator establishes a new router ID scheme for the network. However, after a router selects a router ID, an active OSPFv2 router does not allow the router ID to be changed until the router is reloaded or the OSPFv2 process cleared.

```
R1(config)#
R1(config-router)#
% OSPF: Reload or use "clear ip ospf process" command, for
 this to take effect
R1(config-router)#
R1#
*Mar 25 19:46:09.711: %SYS-5-CONFIG_I: Configured from
console by console
```

Clearing the OSPF process is the preferred method to reset the router ID.

The OSPFv2 routing process is cleared using the clear ip ospf process privileged EXEC mode command. This forces OSPFv2 on R1 to transition to the Down and Init states. Notice the adjacency

change messages from full to down and then from loading to full. The show ip protocols command verifies that the router ID has changed.

```
R1#
Reset ALL OSPF processes? [no]:
R1#
*Mar 25 19:46:22.423: %OSPF-5-ADJCHG: Process 10, Nbr
3.3.3.3 on Serial0/0/1 from FULL to DOWN, Neighbor Down:
 Interface down or detached
*Mar 25 19:46:22.423: %OSPF-5-ADJCHG: Process 10, Nbr
2.2.2.2 on Serial0/0/0 from FULL to DOWN, Neighbor Down:
 Interface down or detached
*Mar 25 19:46:22.475: %OSPF-5-ADJCHG: Process 10, Nbr
3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done
*Mar 25 19:46:22.475: %OSPF-5-ADJCHG: Process 10, Nbr
2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done
R1#
R1#
  Router ID 1.1.1.1
R1#
```

Enabling OSPF on Interfaces

The network command determines which interfaces participate in the routing process for an OSPFv2 area. Any interfaces on a router that match the network address in the network command are enabled to send and receive OSPF packets. The network command also indicates the network (or subnet) address for the interface is included in OSPF routing updates.

The basic command syntax is network *network-address wildcard-mask* area *area-id*.

The area *area-id* syntax refers to the OSPF area. When configuring single-area OSPFv2, the network command must be configured with the same *area-id* value on all routers. Although any area ID can be used, it is good practice to use an area ID of 0 with single-area OSPFv2. This convention makes it easier if the network is later altered to support multiarea OSPFv2.

```
R1(config)# router ospf 10
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
R1(config-router)# network 172.16.3.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0
R1(config-router)#
```

Passive Interface

By default, OSPF messages are forwarded out all OSPF-enabled interfaces. However, these messages really only need to be sent out interfaces connecting to other OSPF-enabled routers.

Refer to the topology in the figure. OSPFv2 messages are forwarded out of all three routers G0/0 interface even though no OSPFv2 neighbor exists on that LAN. Sending out unneeded messages on a LAN affects the network in three ways:

Inefficient Use of Bandwidth - Available bandwidth is consumed transporting unnecessary messages. Messages are multicasted; therefore, switches are also forwarding the messages out all ports.

Inefficient Use of Resources - All devices on the LAN must process the message and eventually discard the message.

Increased Security Risk - Advertising updates on a broadcast network is a security risk. OSPF messages

can be intercepted with packet sniffing software. Routing updates can be modified and sent back to the router, corrupting the routing table with false metrics that misdirect traffic.

OSPF Metric = Cost

Recall that a routing protocol uses a metric to determine the best path of a packet across a network. A metric gives indication of the overhead that is required to send packets across a certain interface. OSPF uses cost as a metric. A lower cost indicates a better path than a higher cost.

The cost of an interface is inversely proportional to the bandwidth of the interface. Therefore, a higher bandwidth indicates a lower cost. More overhead and time delays equal a higher cost. Therefore, a 10-Mb/s Ethernet line has a higher cost than a 100-Mb/s Ethernet line.

The formula used to calculate the OSPF cost is:

Cost = *reference bandwidth* / *interface bandwidth*

The default reference bandwidth is 10^8 (100,000,000); therefore, the formula is:

Cost = 100,000,000 bps / *interface bandwidth in bps*

Refer to the table in the figure for a breakdown of the cost calculation. Notice that FastEthernet, Gigabit Ethernet, and 10 GigE interfaces share the same cost, because the OSPF cost value must be an integer. Consequently, because the default reference bandwidth is set to 100 Mb/s, all links that are faster than Fast Ethernet also have a cost of 1.

Interface Type	Reference Bandwidth in bps		Default Bandwidth in bps	Cost
10 Gigabit Ethernet 10 Gbps	100,000,000	÷	10,000,000,000	1
Gigabit Ethernet 1 Gbps	100,000,000	÷	1,000,000,000	1
Fast Ethernet 100 Mbps	100,000,000	÷	100,000,000	1
Ethernet 10 Mbps	100,000,000	÷	10,000,000	10
Serial 1.544 Mbps	100,000,000	÷	1,544,000	64
Serial 128 kbps	100,000,000	÷	128,000	781
Serial 64 kbps	100,000,000	÷	64,000	1562

Same Cost due to reference bandwidth

OSPF Accumulates Costs

The cost of an OSPF route is the accumulated value from one router to the destination network.

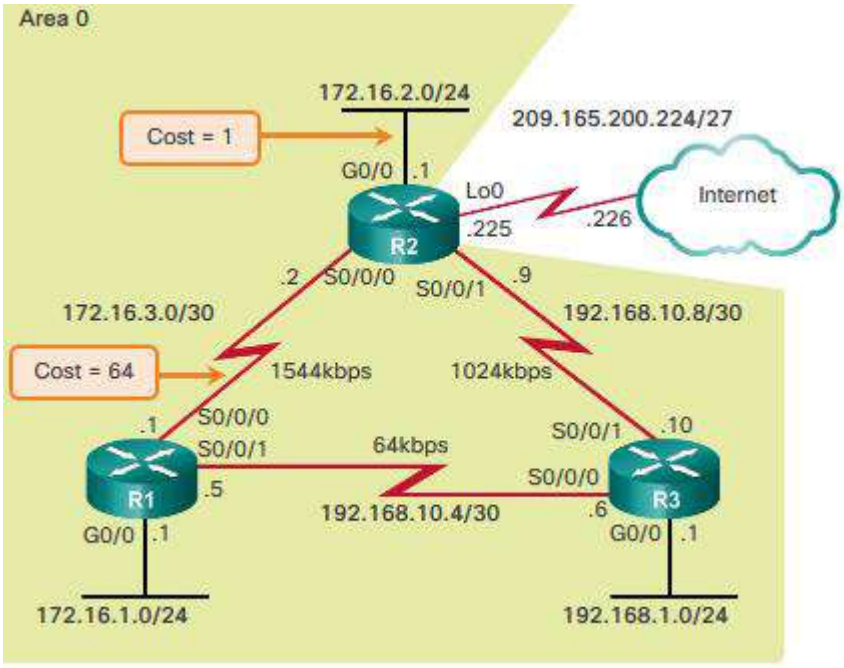
For example, in Figure 1, the cost to reach the R2 LAN 172.16.2.0/24 from R1 should be as follows:

Serial link from R1 to R2 cost = 64

Gigabit Ethernet link on R2 cost = 1

Total cost to reach 172.16.2.0/24 = 65

The routing table of R1 in Figure 2 confirms that the metric to reach the R2 LAN is a cost of 65.




```
R1# show ip route | include 172.16.2.0
O        172.16.2.0/24 [110/65] via 172.16.3.2, 03:39:07,
         Serial0/0/0
R1#
R1# show ip route 172.16.2.0
Routing entry for 172.16.2.0/24
  Known via "ospf 10", distance 110, metric 65, type intra
  area
  Last update from 172.16.3.2 on Serial0/0/0, 03:39:15 ago
  Routing Descriptor Blocks:
  * 172.16.3.2, from 2.2.2.2, 03:39:15 ago, via Serial0/0/0
      Route metric is 65, traffic share count is 1
R1#
```

Adjusting the Reference Bandwidth

OSPF uses a reference bandwidth of 100 Mb/s for any links that are equal to or faster than a fast Ethernet connection. Therefore, the cost assigned to a fast Ethernet interface with an interface bandwidth of 100 Mb/s would equal 1.

Cost = *100,000,000 bps* / *100,000,000* = *1*

While this calculation works for fast Ethernet interfaces, it is problematic for links that are faster than 100 Mb/s; because the OSPF metric only uses integers as its final cost of a link. If something less than an integer is calculated, OSPF rounds up to the nearest integer. For this reason, from the OSPF perspective, an interface with an interface bandwidth of 100 Mb/s (a cost of 1) has the same cost as an interface with a bandwidth of 100 Gb/s (a cost of 1).

To assist OSPF in making the correct path determination, the reference bandwidth must be changed to a higher value to accommodate networks with links faster than 100 Mb/s.

Adjusting the Reference Bandwidth

Changing the reference bandwidth does not actually affect the bandwidth capacity on the link; rather, it simply affects the calculation used to determine the metric. To adjust the reference bandwidth, use the auto-cost reference-bandwidth *Mb/s* router configuration command. This command must be configured on every router in the OSPF domain. Notice that the value is expressed in Mb/s; therefore, to adjust the costs for:

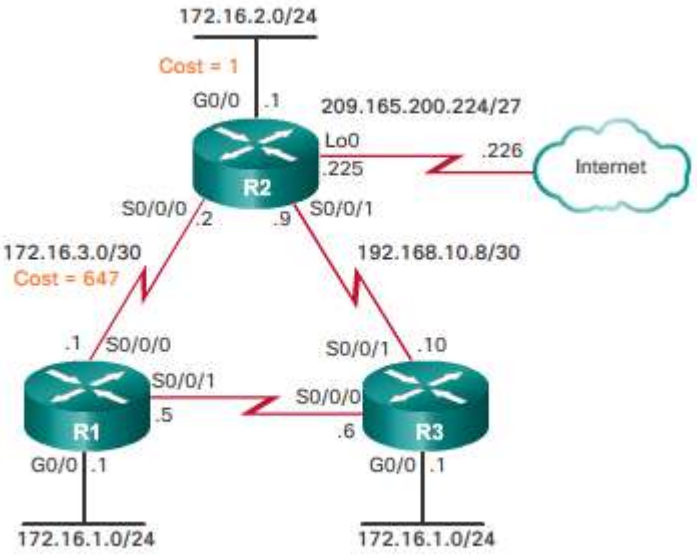
Gigabit Ethernet -auto-cost reference-bandwidth 1000

10 Gigabit Ethernet -auto-cost reference-bandwidth 10000

To return to the default reference bandwidth, use the auto-cost reference-bandwidth 100 command.

. Although the metric values increase, OSPF makes better choices because it can now distinguish between FastEthernet and Gigabit Ethernet links.

The reference bandwidth should be adjusted anytime there are links faster than FastEthernet (100 Mb/s).



Note: The costs represent whole numbers that have been rounded down.

If all routers have been configured to accommodate the Gigabit Ethernet link with the auto-cost reference-bandwidth 1000 router configuration command. The new accumulated cost to reach the R2 LAN 172.16.2.0/24 from R1:

Serial link from R1 to R2 cost = 647

Gigabit Ethernet link on R2 cost = 1

Total cost to reach 172.16.2.0/24 = 648

Use the show ip ospf interface s0/0/0 command to verify the current OSPFv2 cost assigned to the R1 serial 0/0/0 interface, as shown in Figure 4. Notice how it displays a cost of 647.

The routing table of R1 in Figure 5 confirms that the metric to reach the R2 LAN is a cost of 648.

Interface Type	Reference Bandwidth in bps		Default Bandwidth in bps	Cost
10 Gigabit Ethernet 10 Gbps	1,000,000,000	÷	10,000,000,000	1
Gigabit Ethernet 1 Gbps	1,000,000,000	÷	1,000,000,000	1
Fast Ethernet 100 Mbps	1,000,000,000	÷	100,000,000	10
Ethernet 10 Mbps	1,000,000,000	÷	10,000,000	100
Serial 1.544 Mbps	1,000,000,000	÷	1,544,000	647
Serial 128 kbps	1,000,000,000	÷	128,000	7812
Serial 64 kbps	1,000,000,000	÷	64,000	15625

Review questions

See the practical attachment

OSPFv3

OSPFv3 is the OSPFv2 equivalent for exchanging IPv6 prefixes. Recall that in IPv6, the network address is referred to as the prefix and the subnet mask is called the prefix-length.

Similar to its IPv4 counterpart, OSPFv3 exchanges routing information to populate the IPv6 routing table with remote prefixes, as shown in the figure.

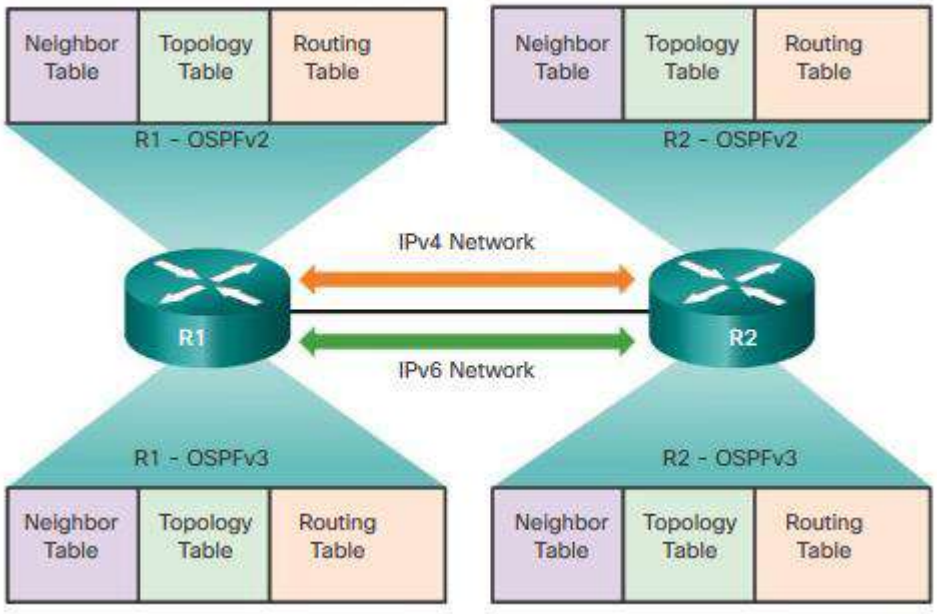
Note: With the OSPFv3 Address Families feature, OSPFv3 includes support for both IPv4 and IPv6. OSPF Address Families is beyond the scope of this curriculum.

OSPFv2 runs over the IPv4 network layer, communicating with other OSPF IPv4 peers, and advertising only IPv4 routes.

OSPFv3 has the same functionality as OSPFv2, but uses IPv6 as the network layer transport, communicating with OSPFv3 peers and advertising IPv6 routes. OSPFv3 also uses the SPF algorithm as the computation engine to determine the best paths throughout the routing domain.

As with all IPv6 routing protocols, OSPFv3 has separate processes from its IPv4 counterpart. The processes and operations are basically the same as in the IPv4 routing protocol, but run independently. OSPFv2 and OSPFv3 each have separate adjacency tables, OSPF topology tables, and IP routing tables, as shown in the figure.

The OSPFv3 configuration and verification commands are similar those used in OSPFv2.



Similarities Between OSPFv2 to OSPFv3

As shown in the figure, the following are similarities between OSPFv2 and OSPFv3:

Link-state - OSPFv2 and OSPFv3 are both classless link-state routing protocols.

Routing algorithm - OSPFv2 and OSPFv3 use the SPF algorithm to make routing decisions.

Metric - The RFCs for both OSPFv2 and OSPFv3 define the metric as the cost of sending packets out

the interface. OSPFv2 and OSPFv3 can be modified using the auto-cost reference-bandwidth *ref-bw* router configuration mode command. The command only influences the OSPF metric where it was configured. For example, if this command was entered for OSPFv3, it does not affect the OSPFv2 routing metrics.

Areas - The concept of multiple areas in OSPFv3 is the same as in OSPFv2. Multiareas that minimize link-state flooding and provide better stability with the OSPF domain.

OSPF packet types - OSPFv3 uses the same five basic packet types as OSPFv2 (Hello, DBD, LSR, LSU, and LSAck).

Neighbor discovery mechanism - The neighbor state machine, including the list of OSPF neighbor states and events, remains unchanged. OSPFv2 and OSPFv3 use the Hello mechanism to learn about neighboring routers and form adjacencies. However, in OSPFv3, there is no requirement for matching subnets to form neighbor adjacencies. This is because neighbor adjacencies are formed using IPv6 link-local addresses, not IPv6 global unicast addresses.

DR/BDR election process - The DR/BDR election process remains unchanged in OSPFv3.

Router ID - Both OSPFv2 and OSPFv3 use a 32-bit number for the router ID represented in dotted-decimal notation. Typically this is an IPv4 address. The OSPF router-id command must be used to configure the router ID. The process in determining the 32-bit Router ID is the same in both protocols. Use an explicitly-configured router ID; otherwise, the highest loopback or configured active IPv4 address becomes the router ID.

OSPFv2 and OSPFv3	
Link-State	Yes
Routing Algorithm	SPF
Metric	Cost
Areas	Supports the same two-level hierarchy
Packet Types	Same Hello, DBD, LSR, LSU, and LSAck packets
Neighbor Discovery	Transitions through the same states using Hello packets
DR and BDR	Function and election process is the same
Router ID	32-bit router ID: determined by the same process in both protocols

Differences Between OSPFv2 and OSPFv3

The figure shows the differences between OSPFv2 and OSPFv3:

Advertises - OSPFv2 advertises IPv4 routes, whereas OSPFv3 advertises routes for IPv6.

Source address - OSPFv2 messages are sourced from the IPv4 address of the exit interface. In OSPFv3, OSPF messages are sourced using the link-local address of the exit interface.

All OSPF router multicast addresses - OSPFv2 uses 224.0.0.5; whereas, OSPFv3 uses FF02::5.

DR/BDR multicast address - OSPFv2 uses 224.0.0.6; whereas, OSPFv3 uses FF02::6.

Advertise networks - OSPFv2 advertises networks using the network router configuration command;

whereas, OSPFv3 uses the ipv6 ospf *process-id* area *area-id* interface configuration command.

IP unicast routing - Enabled, by default, in IPv4; whereas, the ipv6 unicast-routing global configuration command must be configured.

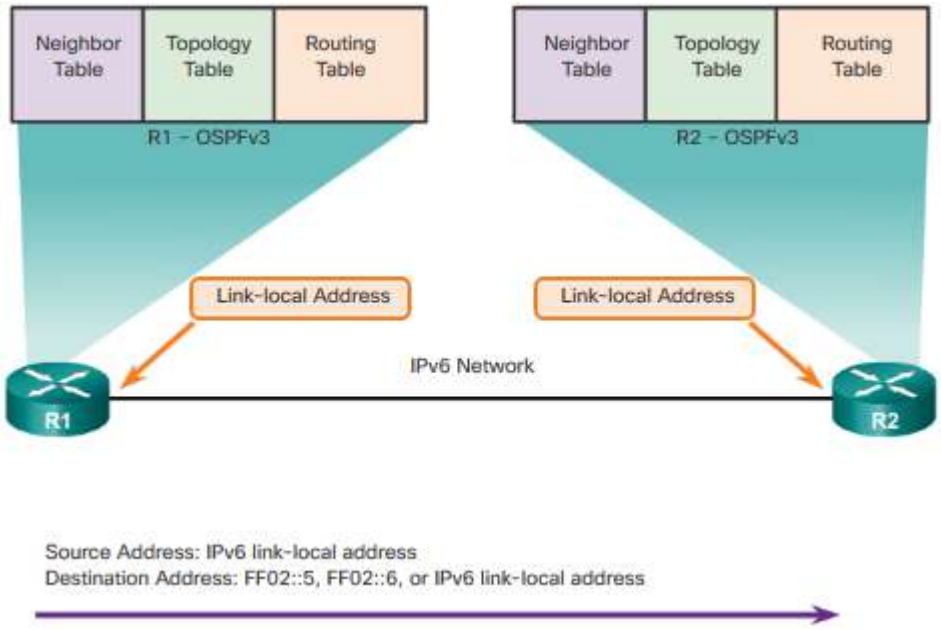
Authentication - OSPFv2 uses either plaintext authentication, MD5, or HMAC-SHA authentication. OSPFv3 uses IPsec to add authentication for OSPFv3 packets.

	OSPFv2	OSPFv3
Advertises	IPv4 networks	IPv6 prefixes
Source Address	IPv4 source address	IPv6 link-local address
Destination Address	Choice of: • Neighbor IPv4 unicast address • 224.0.0.5 all-OSPF-routers multicast address • 224.0.0.6 DR/BDR multicast address	Choice of: • Neighbor IPv6 link-local address • FF02::5 all-OSPFv3-routers multicast address • FF02::6 DR/BDR multicast address
Advertise Networks	Configured using the `network` router configuration command	Configured using the `ipv6 ospf process-id area area-id` interface configuration command
IP Unicast Routing	IPv4 unicast routing is enabled by default.	IPv6 unicast forwarding is not enabled by default. The `ipv6 unicast-routing` global configuration command must be configured.
Authentication	Plain text and MD5	IPv6 authentication

Link-Local Addresses

Routers running a dynamic routing protocol, such as OSPF, exchange messages between neighbors on the same subnet or link. Routers only need to send and receive routing protocol messages with their directly connected neighbors. These messages are always sent from the source IP address of the router doing the forwarding.

IPv6 link-local addresses are ideal for this purpose. An IPv6 link-local address enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet). Packets with a source or destination link-local address cannot be routed beyond the link from where the packet originated.

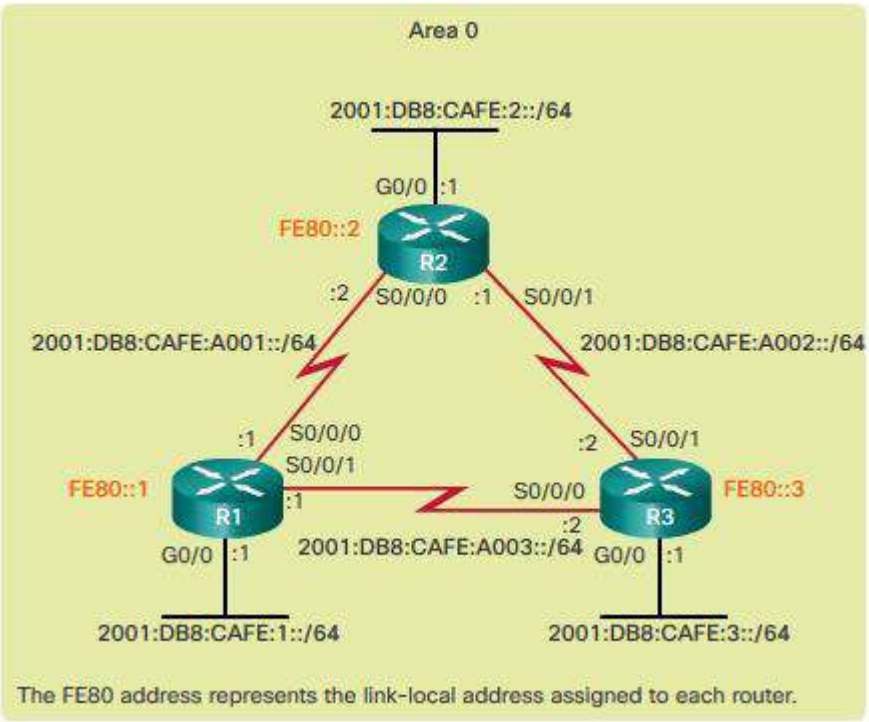


OSPFv3 Network Topology

Figure 1 displays the network topology that is used to configure OSPFv3.

Figure 2 shows IPv6 unicast routing and the configuration of the global unicast addresses of R1, as identified in the reference topology. Assume that the interfaces of R2 and R3 have also been configured with their global unicast addresses, as identified in the referenced topology.

In this topology, none of the routers have IPv4 addresses configured. A network with router interfaces configured with IPv4 and IPv6 addresses is referred to as dual-stacked. A dual-stacked network can have OSPFv2 and OSPFv3 simultaneously-enabled.



```
R1(config)# ipv6 unicast-routing
R1(config)#
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# description R1 LAN
R1(config-if)# ipv6 address 2001:DB8:CAFE:1::1/64
R1(config-if)# no shut
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ipv6 address 2001:DB8:CAFE:A001::1/64
R1(config-if)# clock rate 128000
R1(config-if)# no shut
R1(config-if)#
R1(config-if)# interface Serial0/0/1
R1(config-if)# description Link to R3
R1(config-if)# ipv6 address 2001:DB8:CAFE:A003::1/64
R1(config-if)# no shut
R1(config-if)# end
R1#
```

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface Serial0/0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface Serial0/0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)#
```

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)#
*Mar 29 11:21:53.739: %OSPFv3-4-NORTRID: Process OSPFv3-1-
IPv6 could not pick a router-id, please configure manuall
R1(config-rtr)#
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)#
R1(config-rtr)# auto-cost reference-bandwidth 1000
% OSPFv3-1-IPv6:  Reference bandwidth is changed. Please
ensure reference bandwidth is consistent across all routers.
R1(config-rtr)#
R1(config-rtr)# end
R1#
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Number of areas: 0 normal, 0 stub, 0 nssa
  Redistribution:
    None
R1#
```

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/1
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# end
R1#
R1# show ipv6 ospf interfaces brief
Interface  PID   Area     Intf ID  Cost   State  Nbrs F/C
Se0/0/1    10     0         7      15625  P2P    0/0
Se0/0/0    10     0         6      647    P2P    0/0
Gi0/0      10     0         3       1     WAIT   0/0
R1#
```

Multiarea OSPF

Multiarea OSPF is used to divide a large OSPF network. Too many routers in one area increase the load on the CPU and create a large link-state database. In this chapter, directions are provided to effectively partition a large single area into multiple areas. Area 0, used in a single-area OSPF, is known as the backbone area.

Multiarea OSPF

When a large OSPF area is divided into smaller areas, this is called multiarea OSPF. Multiarea OSPF is useful in larger network deployments to reduce processing and memory overhead.

For instance, any time a router receives new information about the topology, as with additions, deletions, or modifications of a link, the router must rerun the SPF algorithm, create a new SPF tree, and update the routing table. The SPF algorithm is CPU-intensive and the time it takes for calculation depends on the size of the area. Too many routers in one area make the LSDB larger and increase the load on the CPU. Therefore, arranging routers into areas effectively partitions one potentially large database into smaller and more manageable databases.

Multiarea OSPF requires a hierarchical network design. The main area is called the backbone area (area 0) and all other areas must connect to the backbone area. With hierarchical routing, routing still occurs between the areas (interarea routing). However, the CPU intensive routing operation of recalculating the SPF algorithm is done only for routes within an area. A change in one area does not cause an SPF algorithm recalculation in other areas.

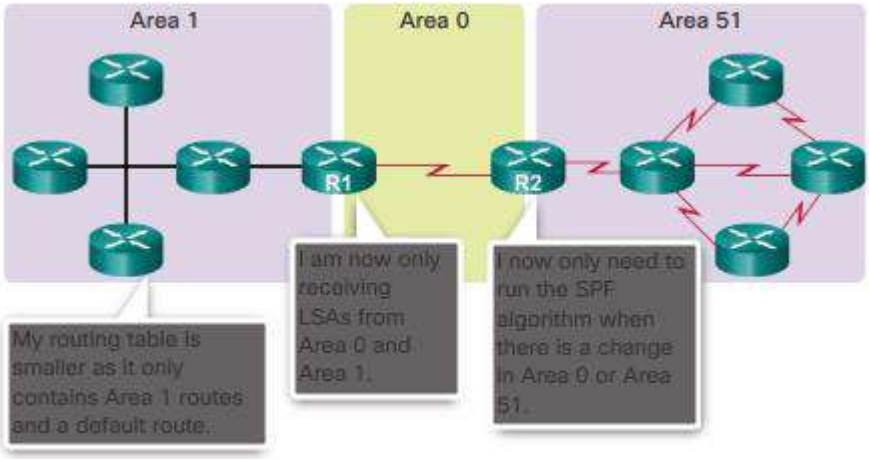
As illustrated in Figure 1, the hierarchical-topology possibilities of multiarea OSPF have these advantages:

Smaller routing tables - There are fewer routing table entries as network addresses can be summarized between areas. Also, routers in an area may only receive a default route for destination outside their area. For example, R1 summarizes the routes from area 1 to area 0 and R2 summarizes the routes from area 51 to area 0. R1 and R2 also propagate a default static route to area 1 and area 51.

Reduced link-state update overhead - Minimizes processing and memory requirements, because there

are fewer routers exchanging LSAs with detailed topology information.

Reduced frequency of SPF calculations - Localizes impact of a topology change within an area. For instance, it minimizes routing update impact, because LSA flooding stops at the area boundary.



OSPF Two-Layer Area Hierarchy

Multiarea OSPF is implemented in a two-layer area hierarchy:

Backbone (Transit) area - An OSPF area whose primary function is the fast and efficient movement of IP packets. Backbone areas interconnect with other OSPF area types. Generally, end users are not found within a backbone area. The backbone area is also called OSPF area 0. Hierarchical networking defines area 0 as the core to which all other areas directly connect (Figure 1).

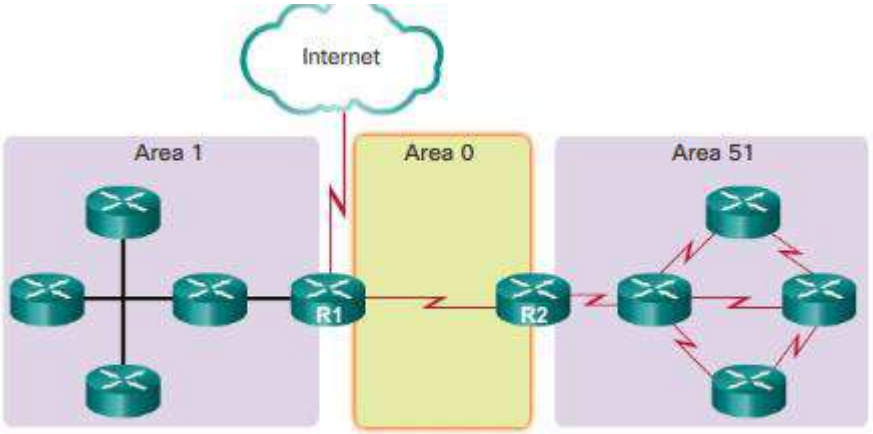
Regular (Non-backbone) area - Connects users and resources. Regular areas are usually set up along functional or geographical groupings. By default, a regular area does not allow traffic from another area to use its links to reach other areas. All traffic from other areas must cross a transit area (Figure 2).

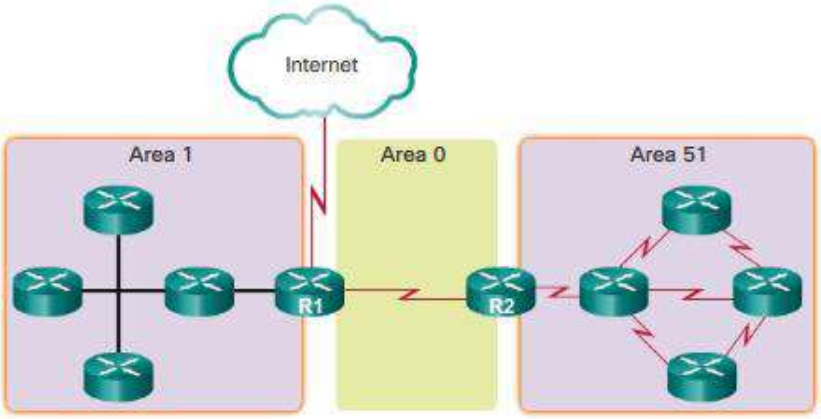
Note: A regular area can have a number of subtypes, including a standard area, stub area, totally stubby area, and not-so-stubby area (NSSA). Stub, totally stubby, and NSSAs are beyond the scope of this chapter.

OSPF enforces this rigid two-layer area hierarchy. The underlying physical connectivity of the network must map to the two-layer area structure, with all non-backbone areas attaching directly to area 0. All traffic moving from one area to another area must traverse the backbone area. This traffic is referred to as interarea traffic.

The optimal number of routers per area varies based on factors such as network stability, but Cisco recommends the following guidelines:

- An area should have no more than 50 routers.
- A router should not be in more than three areas.
- Any single router should not have more than 60 neighbors.



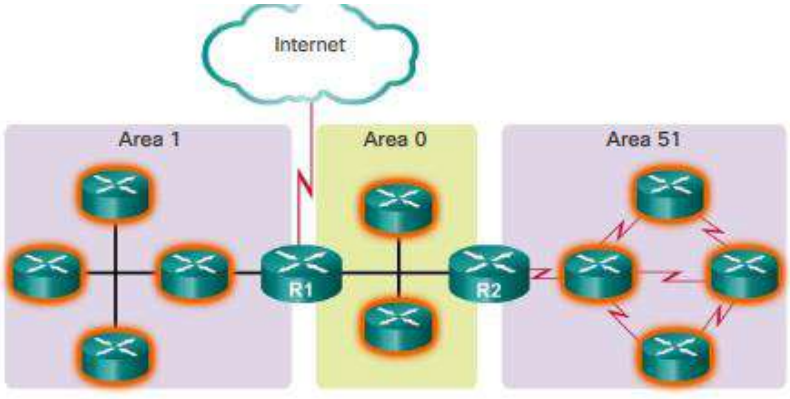


Types of OSPF Routers

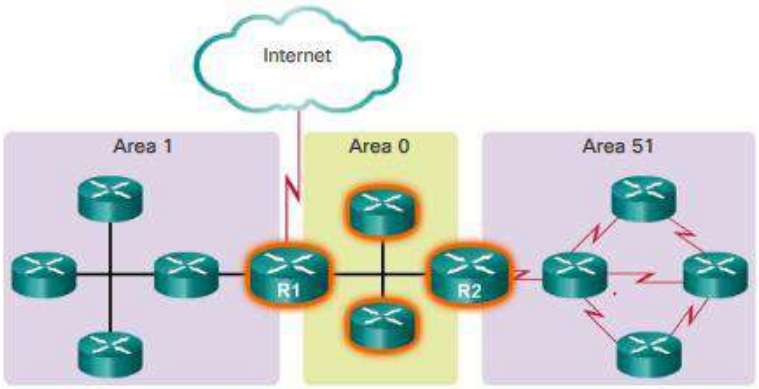
OSPF routers of different types control the traffic that goes in and out of areas. The OSPF routers are categorized based on the function they perform in the routing domain.

There are four different types of OSPF routers:

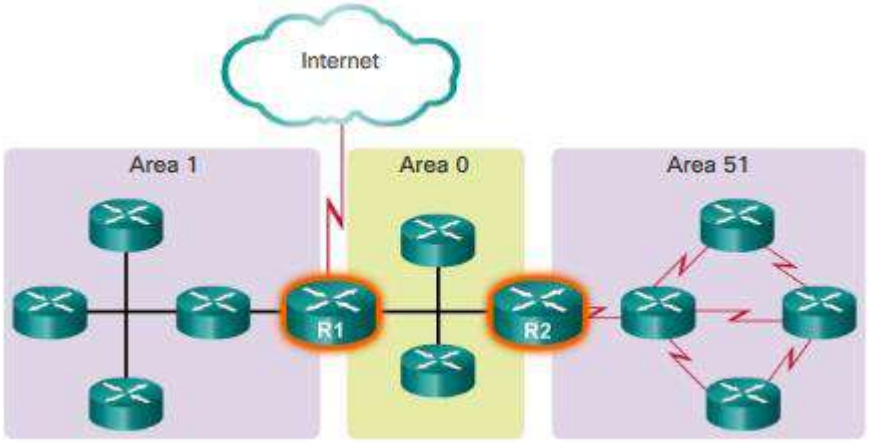
Internal router – This is a router that has all of its interfaces in the same area. All internal routers in an area have identical LSDBs.



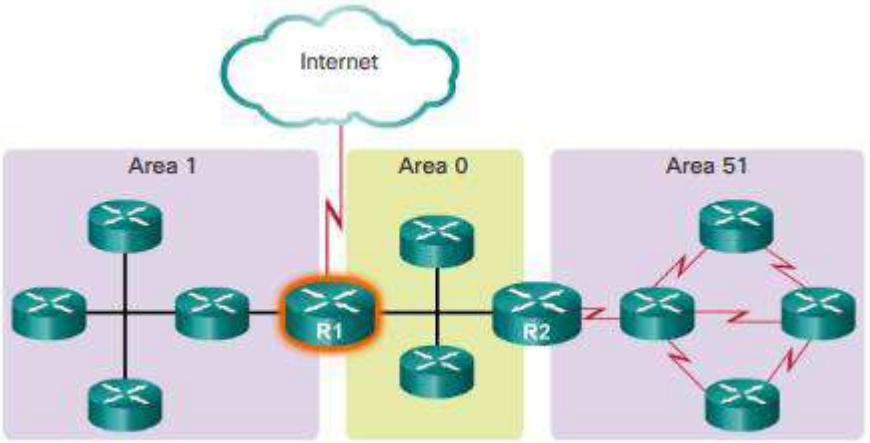
Backbone router – This is a router in the backbone area. The backbone area is set to area 0



Area Border Router (ABR) – This is a router that has interfaces attached to multiple areas. It must maintain separate LSDBs for each area it is connected to, and can route between areas. ABRs are exit points for the area, which means that routing information destined for another area can get there only via the ABR of the local area. ABRs can be configured to summarize the routing information from the LSDBs of their attached areas. ABRs distribute the routing information into the backbone. The backbone routers then forward the information to the other ABRs. In a multiarea network, an area can have one or more ABRs.



Autonomous System Boundary Router (ASBR) – This is a router that has at least one interface attached to an external internetwork. An external network is a network that is not part of this OSPF routing domain. For example, a network connection to an ISP. An ASBR can import external network information to the OSPF network, and vice versa, using a process called route redistribution .



Redistribution in multiarea OSPF occurs when an ASBR connects different routing domains (e.g., EIGRP and OSPF) and configures them to exchange and advertise routing information between those routing domains. A static route, including a default route, can also be redistributed as an external route into the OSPF routing domain.

A router can be classified as more than one router type. For example, if a router connects to area 0 and area 1, and in addition maintains routing information for external networks, it falls under three different classifications: a backbone router, an ABR, and an ASBR.

OSPF LSA Types

LSAs are the building blocks of the OSPF LSDB. Individually, they act as database records and provide specific OSPF network details. In combination, they describe the entire topology of an OSPF network or area.

LSA Type	Description
1	Router LSA
2	Network LSA
3 and 4	Summary LSAs
5	AS External LSA
6	Multicast OSPF LSA
7	Defined for NSSAs
8	External Attributes LSA for Border Gateway Protocol (BGP)
9, 10, or 11	Opaque LSAs

The RFCs for OSPF currently specify up to 11 different LSA types (Figure 1). However, any implementation of multiarea OSPF must support the first five LSAs: LSA 1 to LSA 5 . The focus of this topic is on these first five LSAs.

LSA Type	Description
1	Router LSA
2	Network LSA
3 and 4	Summary LSAs
5	AS External LSA

Each router link is defined as an LSA type. The LSA includes a link ID field that identifies, by network number and mask, the object to which the link connects. Depending on the type, the link ID has different meanings. LSAs differ on how they are generated and propagated within the routing domain.
Note: OSPFv3 includes additional LSA types.

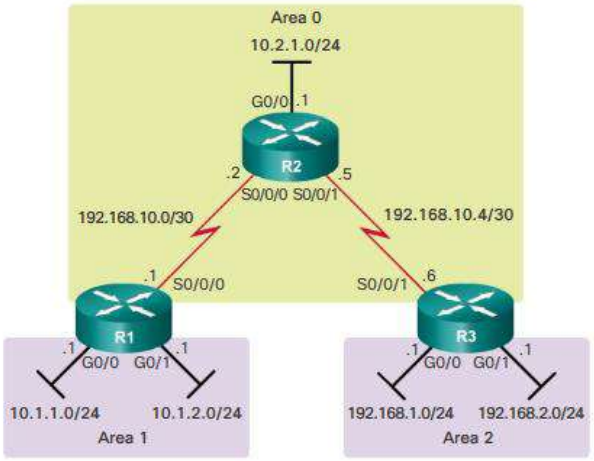
Implementing Multiarea OSPF

OSPF can be implemented as single-area or multiarea. The type of OSPF implementation chosen depends on the specific network design requirements and existing topology.
There are 4 steps to implementing multiarea OSPF, as displayed in the figure.
Steps 1 and 2 are part of the planning process.
Step 1. Gather the network requirements and parameters - Gather the network requirements and parameters - This includes determining the number of host and network devices, the IP addressing scheme (if already implemented), the size of the routing domain, the size of the routing tables, the risk of topology changes, whether existing routers can support OSPF, and other network characteristics.
Step 2. Define the OSPF parameters - Based on information gathered during Step 1, the network administrator must determine if single-area or multiarea OSPF is the preferred implementation. If multiarea OSPF is selected, there are several considerations the network administrator must take into account while determining the OSPF parameters, to include:
IP addressing plan - This governs how OSPF can be deployed and how well the OSPF deployment might scale. A detailed IP addressing plan, along with the IP subnetting information, must be created. A good IP addressing plan should enable the usage of OSPF multiarea design and summarization. This plan more easily scales the network, as well as optimizes OSPF behavior and the propagation of LSA.
OSPF areas - Dividing an OSPF network into areas decreases the LSDB size and limits the propagation of link-state updates when the topology changes. The routers that are to be ABRs and ASBRs must be identified, as are those ABRs or ASBRs that are to perform any summarization or redistribution.
Network topology - This consists of links that connect the network equipment and belong to different OSPF areas in a multiarea OSPF design. Network topology is important to determine primary and backup links. Primary and backup links are defined by the changing OSPF cost on interfaces. A detailed network topology plan should also be used to determine the different OSPF areas, ABR, and ASBR as well as summarization and redistribution points, if multiarea OSPF is used.
Step 3. Configure the multiarea OSPF implementation based on the parameters.
Step 4. Verify the multiarea OSPF implementation based on the parameters.

Configuring Multiarea OSPFv2

Figure 1 displays the reference multiarea OSPF topology. In this example:
R1 is an ABR because it has interfaces in area 1 and an interface in area 0.
R2 is an internal backbone router because all of its interfaces are in area 0.
R3 is an ABR because it has interfaces in area 2 and an interface in area 0.

Note: This topology is not a typical multiarea OSPF routing domain but is used to show an example configuration.



There are no special commands required to implement this multiarea OSPF network. A router simply becomes an ABR when it has two network statements in different areas.

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 10.1.1.1 0.0.0.0 area 1
R1(config-router)# network 10.1.2.1 0.0.0.0 area 1
R1(config-router)# network 192.168.10.1 0.0.0.0 area 0
R1(config-router)# end
R1#
```

As shown in Figure 2, R1 is assigned the router ID 1.1.1.1. This example enables OSPF on the two LAN interfaces in area 1. The serial interface is configured as part of OSPF area 0. Because R1 has interfaces connected to two different areas, it is an ABR.

Upon completion of the R2 configuration, notice the informational messages informing of the adjacency with R1 (1.1.1.1).

Upon completion of the R3 configuration, notice the informational messages informing of an adjacency with R2 (2.2.2.2). Also notice how the IPv4 addressing scheme used for the router ID makes it easy to identify the neighbor.

Note: The inverse wildcard masks used to configure R2 and R3 purposely differ to demonstrate the two alternatives to entering network statements. The interface method used for R3 is simpler because the wildcard mask is always 0.0.0.0 and does not need to be calculated.

Configuring Multiarea OSPFv3

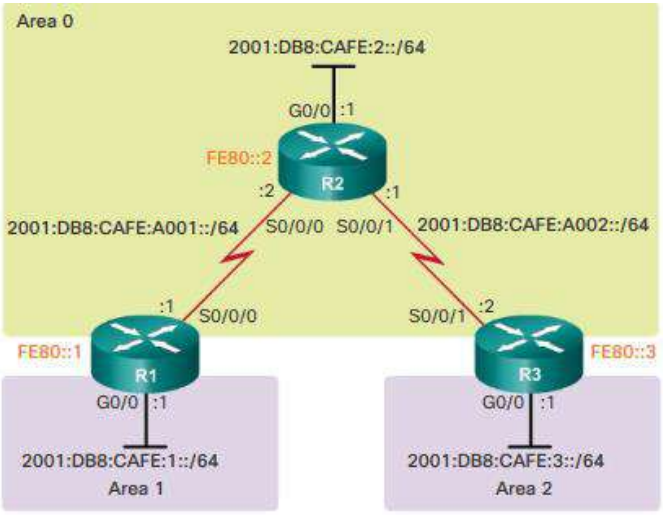
Like OSPFv2, implementing the multiarea OSPFv3 topology in Figure 1 is simple. There are no special commands required. A router simply becomes an ABR when it has two interfaces in different areas.

For example in Figure 2, R1 is assigned the router ID 1.1.1.1. The example also enables OSPF on the LAN interface in area 1 and the serial interface in area 0. Because R1 has interfaces connected to two different areas, it becomes an ABR.

Use the Syntax Checker in Figure 3 to configure multiarea OSPFv3 on R2 and on R3.

Upon completion of the R2 configuration, notice the message that there is an adjacency with R1 (1.1.1.1).

Upon completion of the R3 configuration, notice the message that there is an adjacency with R2 (2.2.2.2).




```
R1(config)# ipv6 router ospf 10
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# exit
R1(config)#
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 ospf 10 area 1
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)# end
R1#
```

Verifying Multiarea OSPFv2

The same verification commands used to verify single-area OSPFv2 also can be used to verify the multiarea OSPF topology in the figure:

show ip ospf neighbor

show ip ospf

show ip ospf interface

Commands that verify specific multiarea OSPFv2 information include:

show ip protocols

show ip ospf interface brief

show ip route ospf

show ip ospf database

Note: For the equivalent OSPFv3 command, simply substitute ip with ipv6.

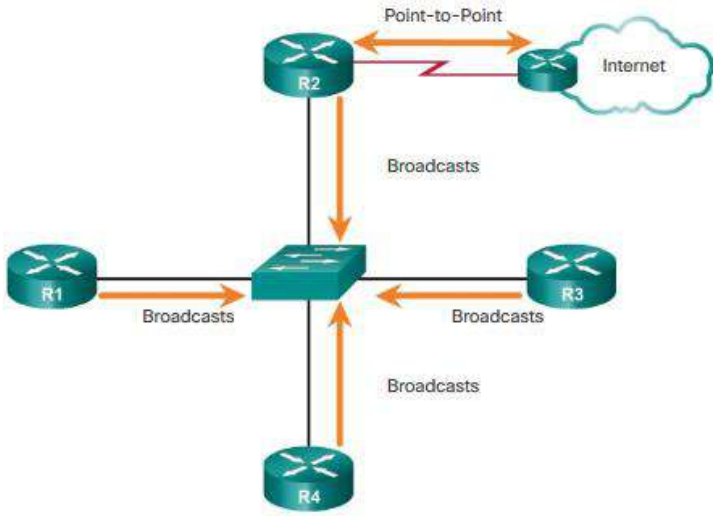
OSPF Network Types

To configure OSPF adjustments, start with a basic implementation of the OSPF routing protocol.

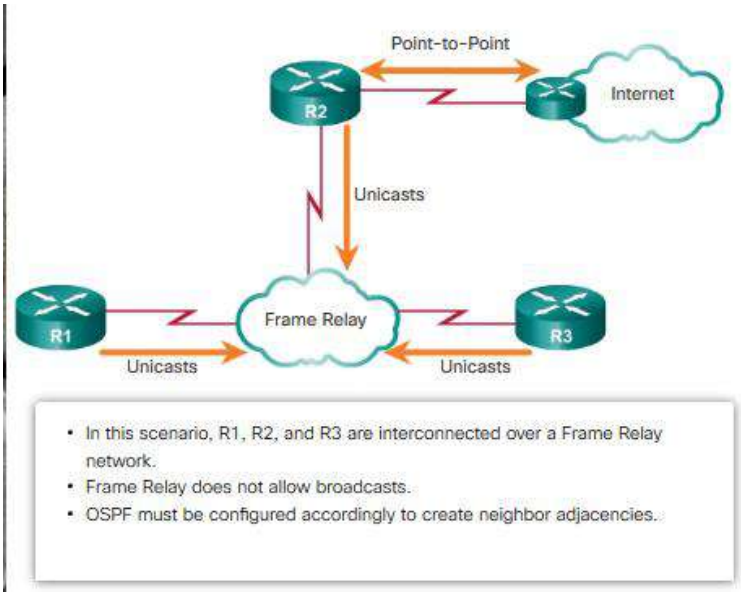
OSPF defines five network types, as shown in Figures 1 to 5:

Point-to-point - Two routers interconnected over a common link. No other routers are on the link. This is often the configuration in WAN links. (Figure 1)

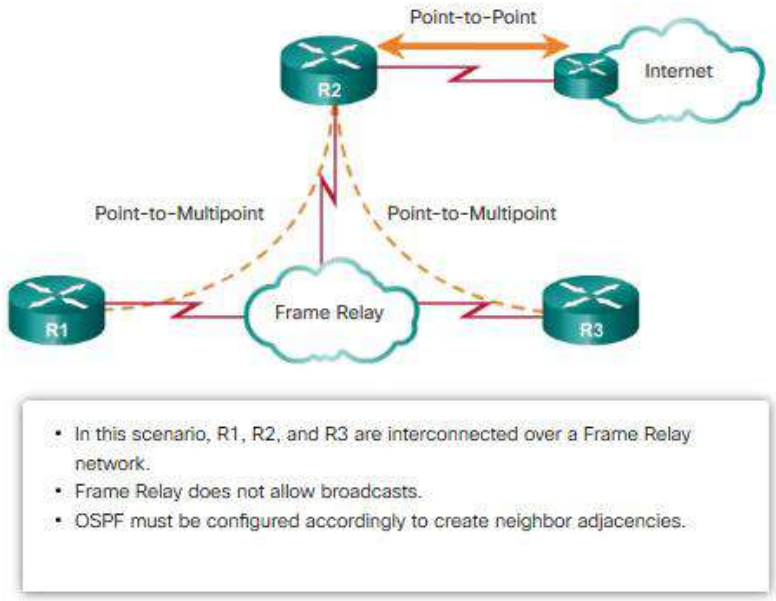
Broadcast multiaccess - Multiple routers interconnected over an Ethernet network. (Figure 2)



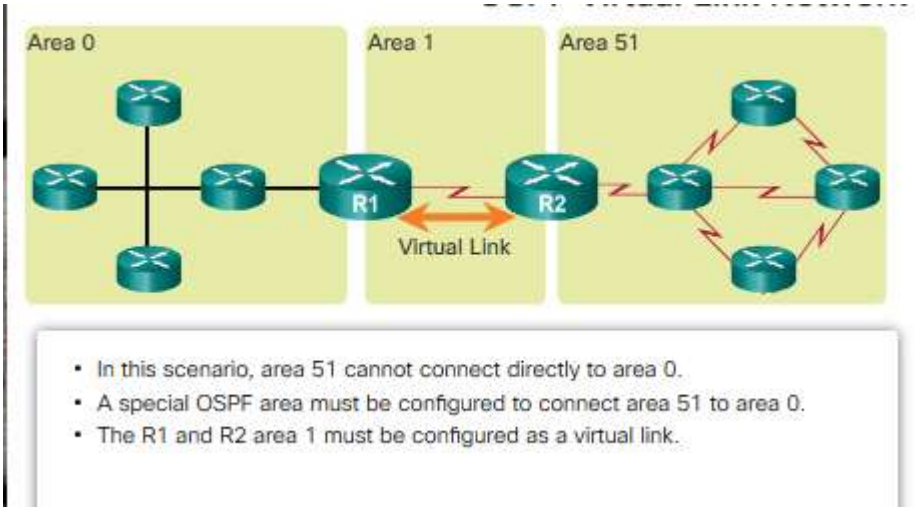
Nonbroadcast multiaccess (NBMA) - Multiple routers interconnected in a network that does not allow broadcasts, such as Frame Relay. (Figure 3)



Point-to-multipoint - Multiple routers interconnected in a hub-and-spoke topology over an NBMA network. Often used to connect branch sites (spokes) to a central site (hub). (Figure 4)



Virtual links - Special OSPF network used to interconnect distant OSPF areas to the backbone area. (Figure 5)



A multiaccess network is a network with multiple devices on the same shared media, which are sharing communications. Ethernet LANs are the most common example of broadcast multiaccess networks. In broadcast networks, all devices on the network see all broadcast and multicast frames. They are multiaccess networks because there may be numerous hosts, printers, routers, and other devices that are all members of the same network.

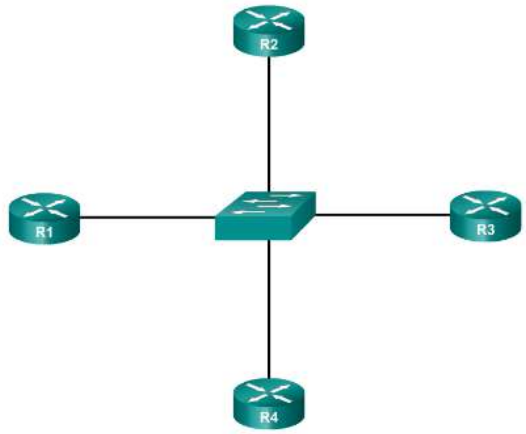
Challenges in Multiaccess Networks

Multiaccess networks can create two challenges for OSPF regarding the flooding of LSAs:

Creation of multiple adjacencies - Ethernet networks could potentially interconnect many OSPF routers over a common link. Creating adjacencies with every router is unnecessary and undesirable. This would lead to an excessive number of LSAs exchanged between routers on the same network.

Extensive flooding of LSAs - Link-state routers flood their link-state packets when OSPF is initialized,

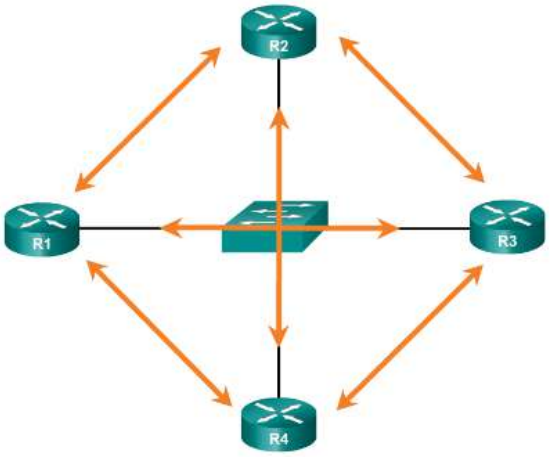
or when there is a change in the topology. This flooding can become excessive.



The following formula can be used to calculate the number of required adjacencies. The number of adjacencies required for any number of routers (designated as *n*) on a multiaccess network is:

$n(n-1)/2$

Figure 1 shows a simple topology of four routers, all of which are attached to the same multiaccess Ethernet network. Without some type of mechanism to reduce the number of adjacencies, collectively these routers would form six adjacencies: 4 (4 - 1) / 2 = 6, as shown in Figure 2. Figure 3 shows that as routers are added to the network, the number of adjacencies increases dramatically.



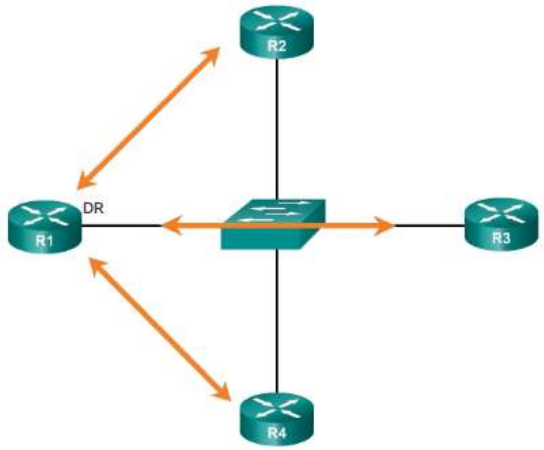
Routers n	Adjacencies n (n - 1) / 2
4	6
5	10
10	45
20	190
50	1225

OSPF Designated Router

The solution to managing the number of adjacencies and the flooding of LSAs on a multiaccess network is the DR. On multiaccess networks, OSPF elects a DR to be the collection and distribution point for LSAs sent and received. A BDR is also elected in case the DR fails. The BDR listens passively to this

exchange and maintains a relationship with all the routers. If the DR stops producing Hello packets, the BDR promotes itself and assumes the role of DR.

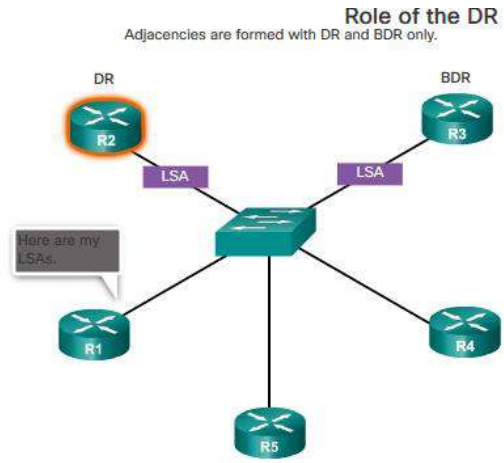
All other non-DR or BDR routers become DROTHER (a router that is neither the DR nor the BDR).



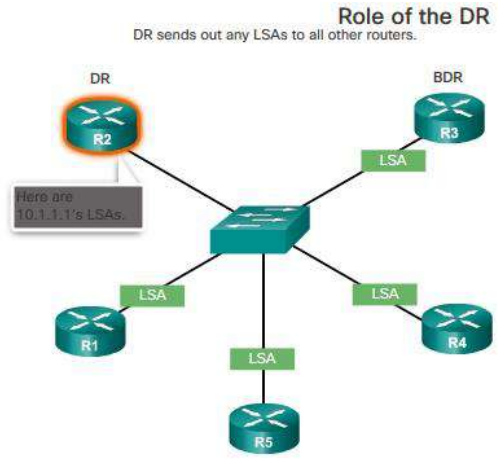
In Figure 1, R1 has been elected as the designated router for the Ethernet LAN interconnecting R2, R3, and R4. Notice how the number of adjacencies has been reduced to 3.

Routers on a multiaccess network elect a DR and BDR. DROTHERs only form full adjacencies with the DR and BDR in the network. Instead of flooding LSAs to all routers in the network, DROTHERs only send their LSAs to the DR and BDR using the multicast address 224.0.0.6 (all DR routers).

Note: The DR is used only for the distribution of LSAs. Packets are routed according the each of the routers' individual routing tables.



R1 sends LSAs to the DR. The BDR also listens. The DR is responsible for forwarding the LSAs from R1 to all other routers. The DR uses the multicast address 224.0.0.5 (all OSPF routers). The end result is that there is only one router doing all of the flooding of all LSAs in the multiaccess network.



Note: DR/BDR elections only occur in multiaccess networks and do not occur in point-to-point networks.

Default DR/BDR Election Process

How do the DR and BDR get elected? The OSPF DR and BDR election decision is based on the following criteria, in sequential order:

1. The routers in the network elect the router with the highest interface priority as the DR. The router with the second highest interface priority is elected as the BDR. The priority can be configured to be any number between 0 – 255. The higher the priority, the likelier the router will be selected as the DR. If the priority is set to 0, the router is not capable of becoming the DR. The default priority of multiaccess broadcast interfaces is 1. Therefore, unless otherwise configured, all routers have an equal priority value and must rely on another tie breaking method during the DR/BDR election.

2. If the interface priorities are equal, then the router with the highest router ID is elected the DR. The router with the second highest router ID is the BDR.

Recall that the router ID is determined in one of three ways:

The router ID can be manually configured.

If no router IDs are configured, the router ID is determined by the highest loopback IPv4 address.

If no loopback interfaces are configured, the router ID is determined by the highest active IPv4 address.

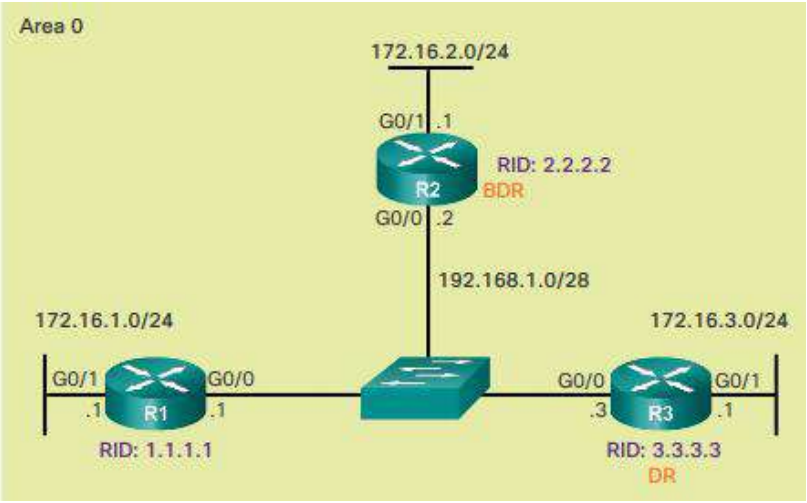
Note: In an IPv6 network, if there are no IPv4 addresses configured on the router, then the router ID must be manually configured with therouter-id *rid*command; otherwise, OSPFv3 does not start.

In the figure, all Ethernet router interfaces have a default priority of 1. As a result, based on the selection criteria listed above, the OSPF router ID is used to elect the DR and BDR. R3 with the highest router ID becomes the DR; and R2, with the second highest router ID, becomes the BDR.

Note: Serial interfaces have default priorities set to 0; therefore, they do not elect DR and BDRs.

The DR and BDR election process takes place as soon as the first router with an OSPF-enabled interface is active on the multiaccess network. This can happen when the preconfigured OSPF routers are powered on, or when OSPF is activated on the interface.. The election process only takes a few seconds. If all of the routers on the multiaccess network have not finished booting, it is possible that a router with

a lower router ID becomes the DR. (This can be a lower-end router that takes less time to boot.)



DR/BDR Election Process

OSPF DR and BDR elections are not pre-emptive. If a new router with a higher priority or higher router ID is added to the network after the DR and BDR election, the newly added router does not take over the DR or the BDR role. This is because those roles have already been assigned. The addition of a new router does not initiate a new election process.

After the DR is elected, it remains the DR until one of the following events occurs:

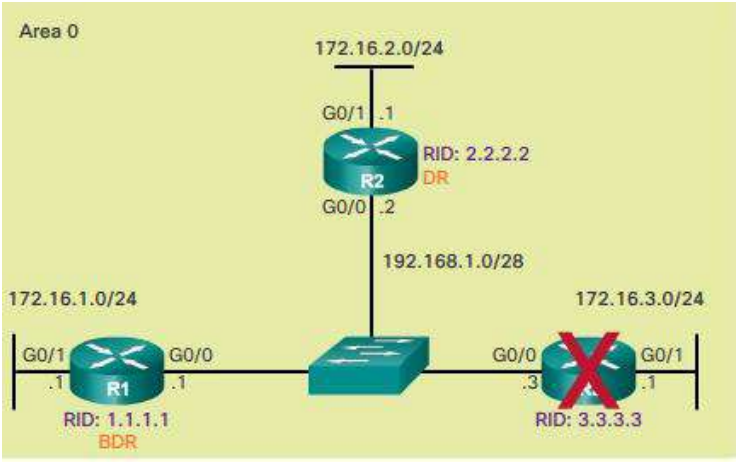
The DR fails

The OSPF process on the DR fails or is stopped

The multiaccess interface on the DR fails or is shutdown

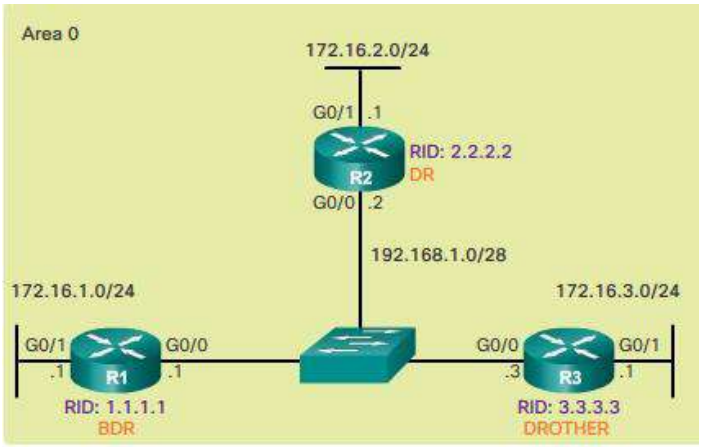
If the DR fails, the BDR is automatically promoted to DR. This is the case even if another DROTHER with a higher priority or router ID is added to the network after the initial DR/BDR election. However, after a BDR is promoted to DR, a new BDR election occurs and the DROTHER with the higher priority or router ID is elected as the new BDR.

Figures 1 to 4 illustrate various scenarios relating to the DR and BDR election process.

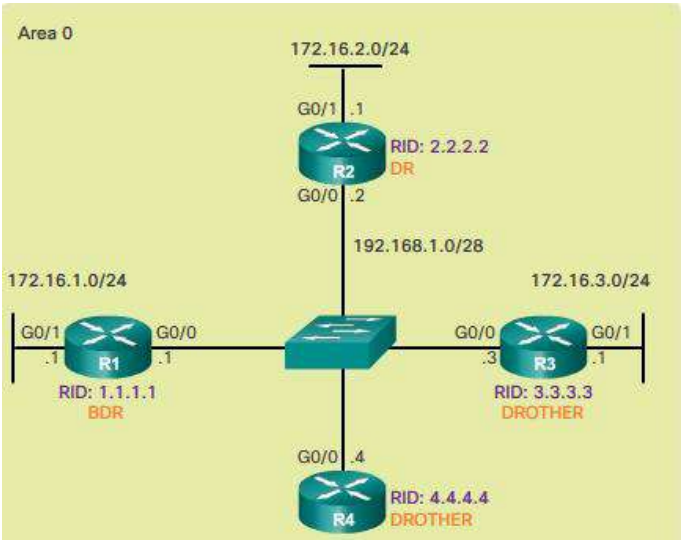


In Figure 1, the current DR (R3) fails; therefore, the pre-elected BDR (R2) assumes the role of DR. Subsequently, an election is held to choose a new BDR. Because R1 is the only DROTHER, it is elected

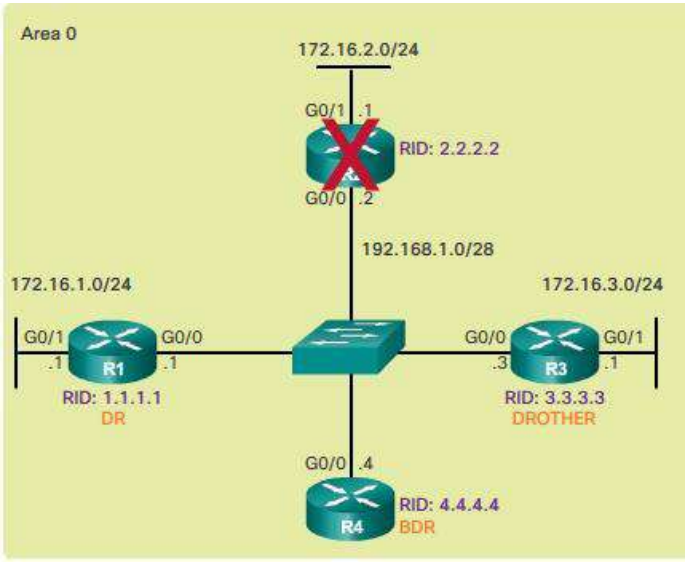
as the BDR.



In Figure 2, R3 has re-joined the network after several minutes of being unavailable. Because the DR and BDR already exist, R3 does not take over either role; instead, it becomes a DROTHER.



In Figure 3, a new router (R4) with a higher router ID is added to the network. DR (R2) and BDR (R1) retain the DR and BDR roles. R4 automatically becomes a DROTHER.

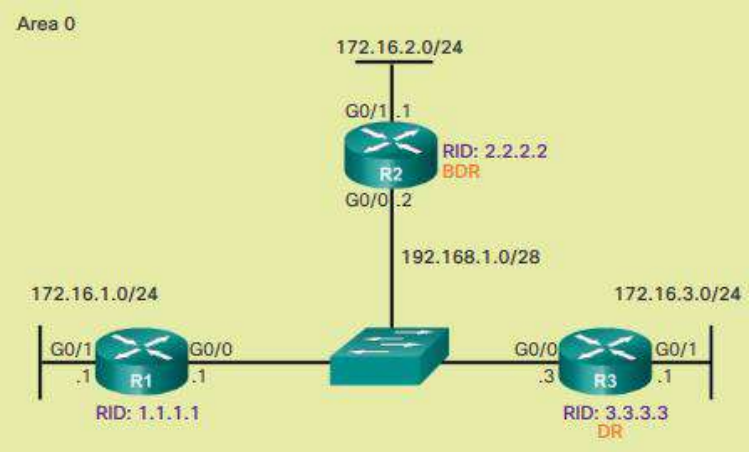


In Figure 4, R2 has failed. The BDR (R1) automatically becomes the DR and an election process selects R4 as the BDR because it has the higher router ID.

The OSPF Priority

The DR becomes the focal point for the collection and distribution of LSAs; therefore, this router must have sufficient CPU and memory capacity to handle the workload. It is possible to influence the DR/BDR election process through configurations.

If the interface priorities are equal on all routers, the router with the highest router ID is elected the DR. It is possible to configure the router ID to manipulate the DR/BDR election. However, this process only works if there is a stringent plan for setting the router ID on all routers. In large networks, this can be cumbersome.



Instead of relying on the router ID, it is better to control the election by setting interface priorities. Priorities are an interface-specific value, which means it provides better control on a multiaccess network. This also allows a router to be the DR in one network and a DROTHER in another.

To set the priority of an interface, use the following commands:

ip ospf priority *value* - OSPFv2 interface command

ipv6 ospf priority *value* - OSPFv3 interface command

The *value* can be:

0 - Does not become a DR or BDR.

1 – 255 - The higher the priority value, the more likely the router becomes the DR or BDR on the interface.

In the figure, all routers have an equal OSPF priority because the priority value defaults to 1 for all router interfaces. Therefore, the router ID is used to determine the DR (R3) and BDR (R2). Changing the priority value on an interface from 1 to a higher value, would enable the router to become a DR or BDR router during the next election.

If the interface priority is configured after OSPF is enabled, the administrator must shut down the OSPF process on all routers, and then re-enable the OSPF process, to force a new DR/BDR election.

Propagating a Default Static Route in OSPFv2

Propagating a Default Static Route

With OSPF, the router connected to the Internet is used to propagate a default route to other routers in the OSPF routing domain. This router is sometimes called the edge, the entrance, or the gateway router. However, in OSPF terminology, the router located between an OSPF routing domain and a non-OSPF network is also called the autonomous system boundary router (ASBR).

In Figure 1, R2 is single-homed to a service provider. Therefore, all that is required for R2 to reach the Internet is a default static route to the service provider.

Note: In this example, a loopback interface with IPv4 address 209.165.200.225 is used to simulate the connection to the service provider.

To propagate a default route, the edge router (R2) must be configured with:

A default static route using the ip route 0.0.0.0 0.0.0.0 {*ip-address* | *exit-intf*} command.

The default-information originate router configuration mode command. This instructs R2 to be the source of the default route information and propagate the default static route in OSPF updates.

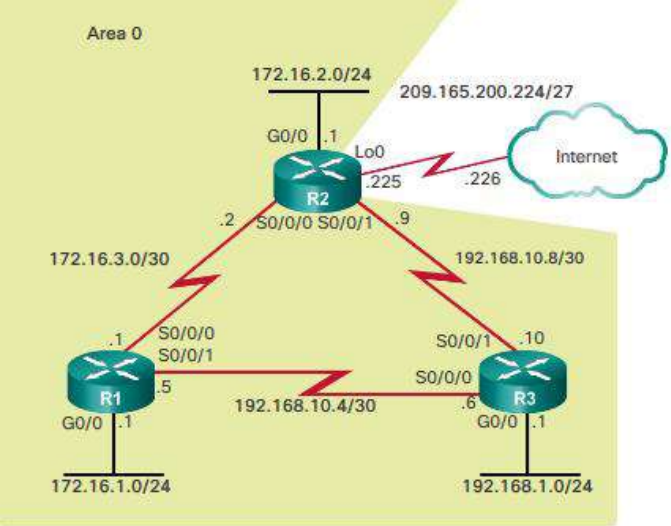


Figure 2 shows how to configure an IPv4 default static route to the service provider and have it propagate in OSPFv2.

```
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.226
R2(config)#
R2(config)# router ospf 10
R2(config-router)# default-information originate
R2(config-router)# end
R2#
```

Review questions

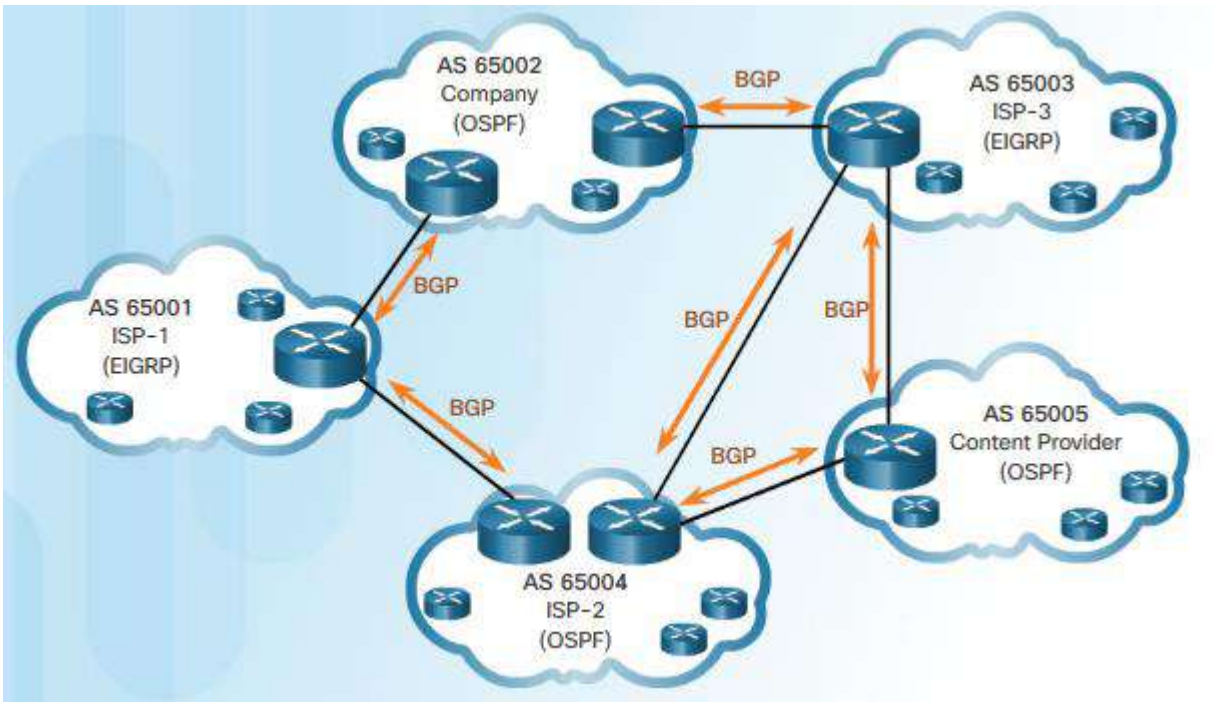
See the practical attachment

Learning Outcome 2.4: Connect networks using Border Gateway Protocol (BGP)

IGP and EGP Routing Protocols

RIP, EIGRP and OSPF are Interior Gateway Protocols (IGPs). ISPs and their customers, such as corporations and other enterprises, usually use an IGP to route traffic within their networks. IGPs are used to exchange routing information within a company network or an autonomous system (AS).

Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) used for the exchange of routing information between autonomous systems, such as ISPs, companies, and content providers (e.g., YouTube, Netflix, etc.).



In BGP, every AS is assigned a unique 16-bit or 32-bit AS number which uniquely identifies it on the Internet. An example of how IGPs are used is shown in the figure.

Note: There are also private AS numbers. However, private AS numbers are beyond the scope of this course.

Internal routing protocols use a specific metric, such as OSPF's cost, for determining the best paths to destination networks. BGP does not use a single metric like IGPs. BGP routers exchange several path attributes including a list of AS numbers (hop by hop) necessary to reach a destination network. For example, in Figure 1 AS 65002 may use the AS-path of 65003 and 65005 to reach a network within the content provider AS 65005. BGP is known as a path vector routing protocol.

Note: AS-path is one of several attributes that may be used by BGP to determine best path. However, path attributes and BGP best path determination are beyond the scope of this course.

BGP updates are encapsulated over TCP on port 179. Therefore, BGP inherits the connection-oriented properties of TCP, which ensures that BGP updates are transmitted reliably.

IGP routing protocols are used to route traffic within the same organization and administered by a single organization. In contrast, BGP is used to route between networks administered by two different organizations. BGP is used by an AS to advertise its networks and in some cases, networks that it learned about from other autonomous systems, to the rest of the Internet.

eBGP and iBGP

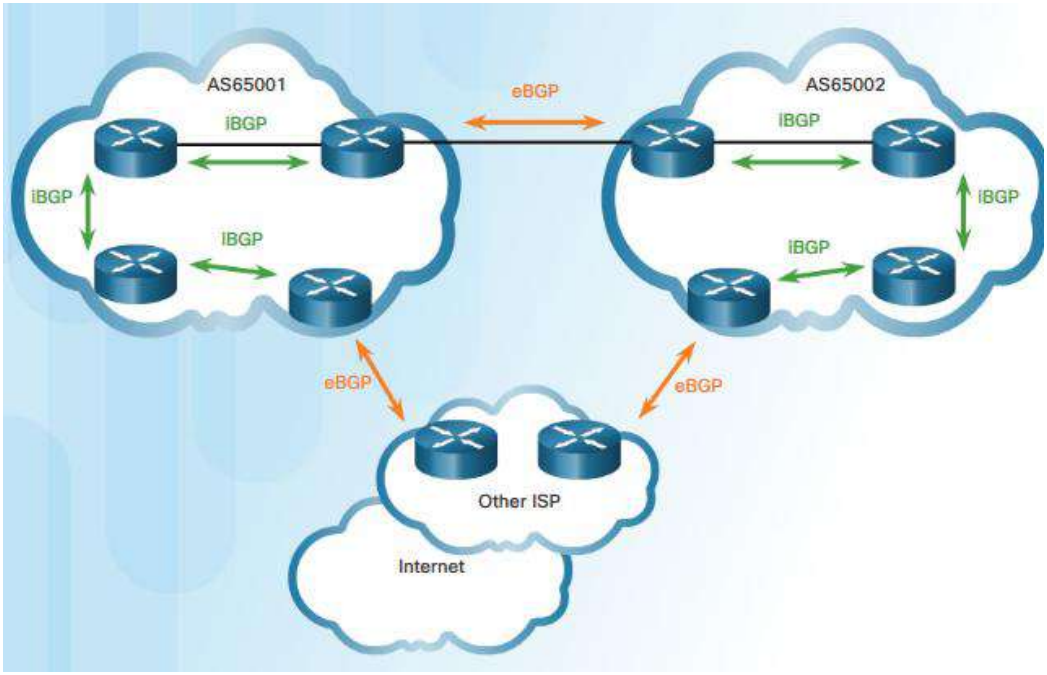
Two routers exchanging BGP routing information are known as BGP peers. As shown in the figure, there are two types of BGP:

External BGP (eBGP) – External BGP is the routing protocol used between routers in different autonomous systems.

Internal BGP (iBGP) - Internal BGP is the routing protocol used between routers in the same AS.

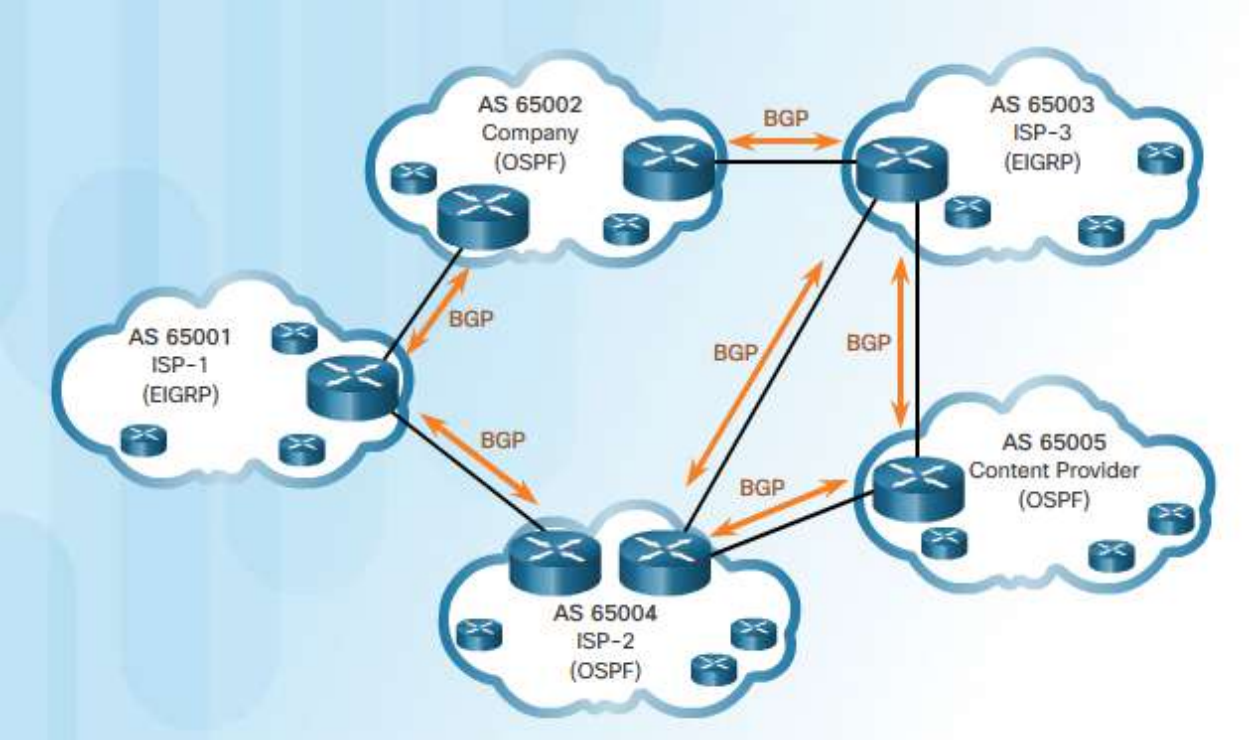
This course focuses on eBGP only.

Note: There are some differences in how BGP operates depending on whether the two routers are eBGP peers or iBGP peers. However, these differences are beyond the scope of this course.



When to use BGP

The use of BGP is most appropriate when an AS has connections to multiple autonomous systems. This is known as multi-homed. Each AS in the figure is multi-homed because each AS has connections to at least two other autonomous systems or BGP peers.



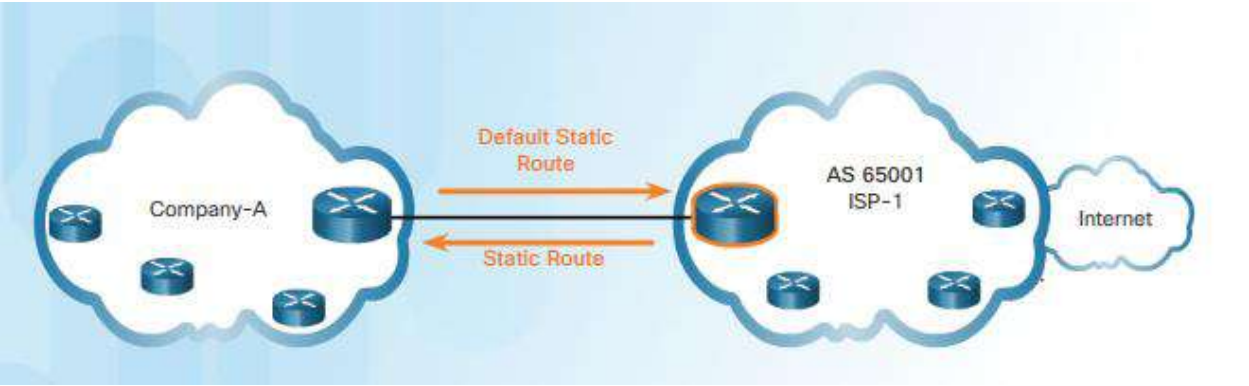
Before running BGP, it is important that the network administrator has a good understanding of BGP. A misconfiguration of a BGP router could have negative effects throughout the entire Internet.

When not to use BGP

BGP should not be used when at least one of the following conditions exist:

There is a single connection to the Internet or another AS. This is known as single-homed. In this case, Company-A may run an IGP with the ISP or, Company-A and the ISP will each use static routes, as shown in the figure. Although it is recommended only in unusual situations, for the purposes of this course, you will configure single-homed BGP.

When there is a limited understanding of BGP. A misconfiguration of a BGP router can have far reaching affects beyond the local AS, negatively impacting routers throughout the Internet.

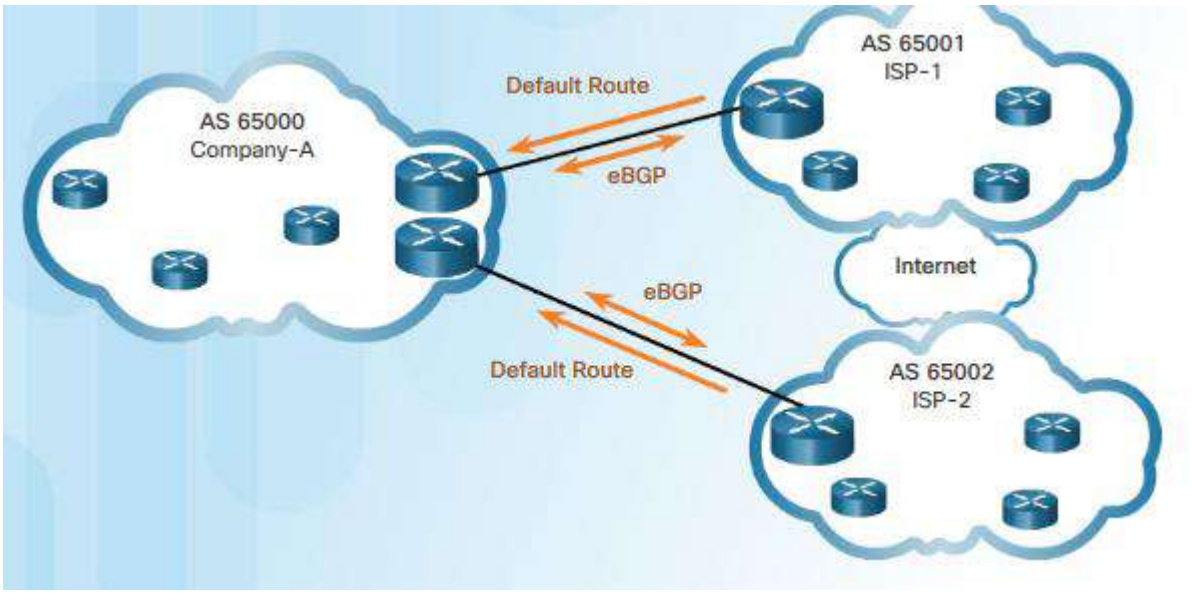


Note: There are some single-homed situations where BGP may be appropriate, such as the need for a specific routing policy. However, routing policies are beyond the scope of this course.

BGP Options

BGP is used by autonomous systems to advertise networks that originated within their AS or in the case of ISPs, the networks that originated from other autonomous systems.

For example, a company connecting to their ISP using BGP would advertise their network addresses to their ISP. The ISP would then advertise these networks to other ISPs (BGP peers). Eventually, all other autonomous systems on the Internet would learn about the networks initially originated by the company.

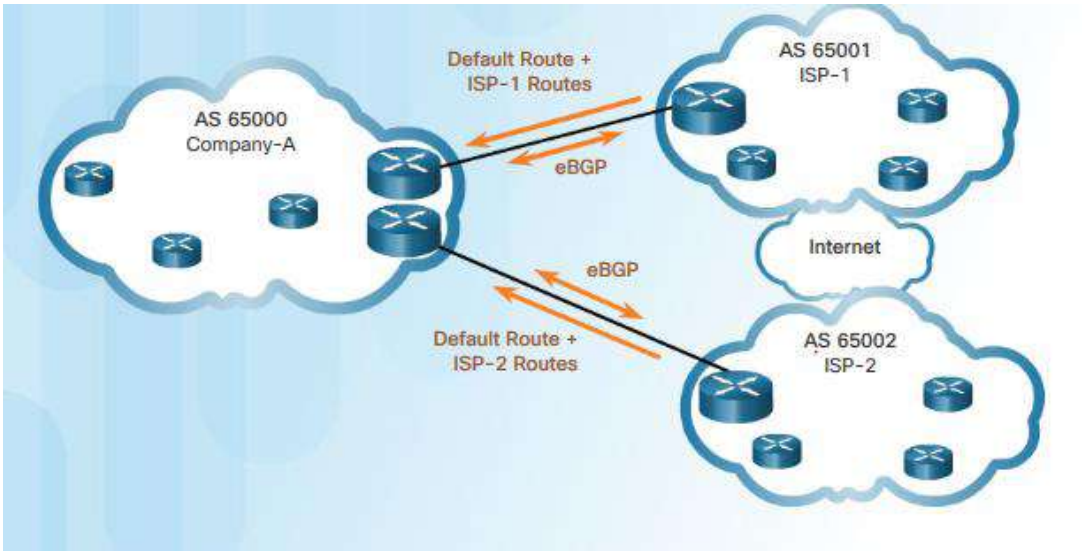


There are three common ways an organization can choose to implement BGP in a multi-homed environment:

Default Route Only

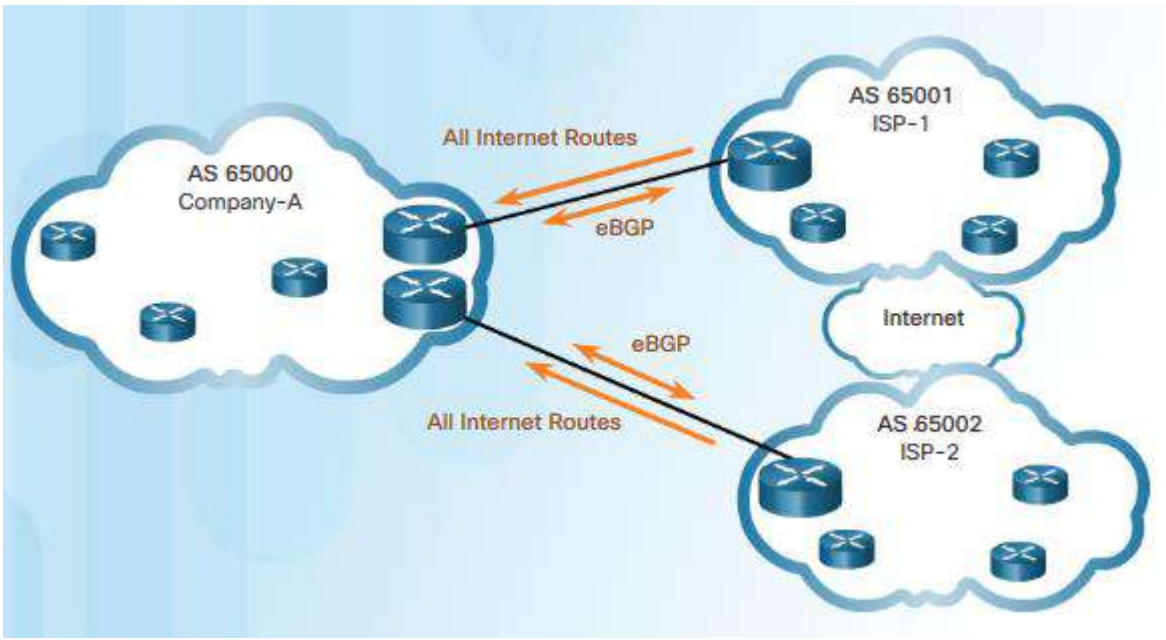
ISPs advertise a default route to Company-A, as shown in Figure 1. The arrows indicate that the default is configured on the ISPs, not on the Company-A. This is the simplest method to implement BGP. However, because the company only receives a default route from both ISPs, sub-optimal routing may occur. For example, Company-A may choose to use ISP-1's default route when sending packets to a destination network in ISP-2's AS.

Default Route and ISP Routes



ISPs advertise their default route and their network to Company-A, as shown in Figure 2. This option allows Company-A to forward traffic to the appropriate ISP for networks advertised by that ISP. For example, Company-A would choose ISP-1 for networks advertised by ISP-1. For all other networks, one of the two default routes can be used, which means sub-optimal routing may still occur for all other Internet routes.

All Internet Routes



ISPs advertise all Internet routes to Company-A, as shown in Figure 3. Because Company-A receives all Internet routes from both ISPs, Company-A can determine which ISP to use as the best path to forward traffic for any network. Although this solves the issue of sub-optimal routing, the Company-A's BGP router must contain all Internet routes, which would currently include routes to over 550,000 networks.

Steps to Configure eBGP

To implement eBGP for this course, you will need to complete the following tasks:

Step 1: Enable BGP routing.

Step 2: Configure BGP neighbor(s) (peering).

Step 3: Advertise network(s) originating from this AS.

The figure lists the command syntax and a description for basic eBGP configuration.

Command	Description
`Router(config)# router bgp as-number`	Enables a BGP routing process, and places the router in router configuration mode.
`Router(config-router)# neighbor ip-address remote-as as-number`	Specifies a BGP neighbor. The as-number is the neighbor's AS number.
`Router(config-router)# network network-address [mask network-mask]`	Advertises a network address to an eBGP neighbor as being originated by this AS. The network-mask is the subnet mask of the network.

BGP Sample Configuration

In this a single-homed BGP topology, Company-A in AS 65000 uses eBGP to advertise its 198.133.219.0/24 network to ISP-1 at AS 65001. ISP-1 advertises a default route in its eBGP updates to Company-A.

Note: BGP is usually not necessary in single-homed AS. It is used here to provide a simple configuration example.

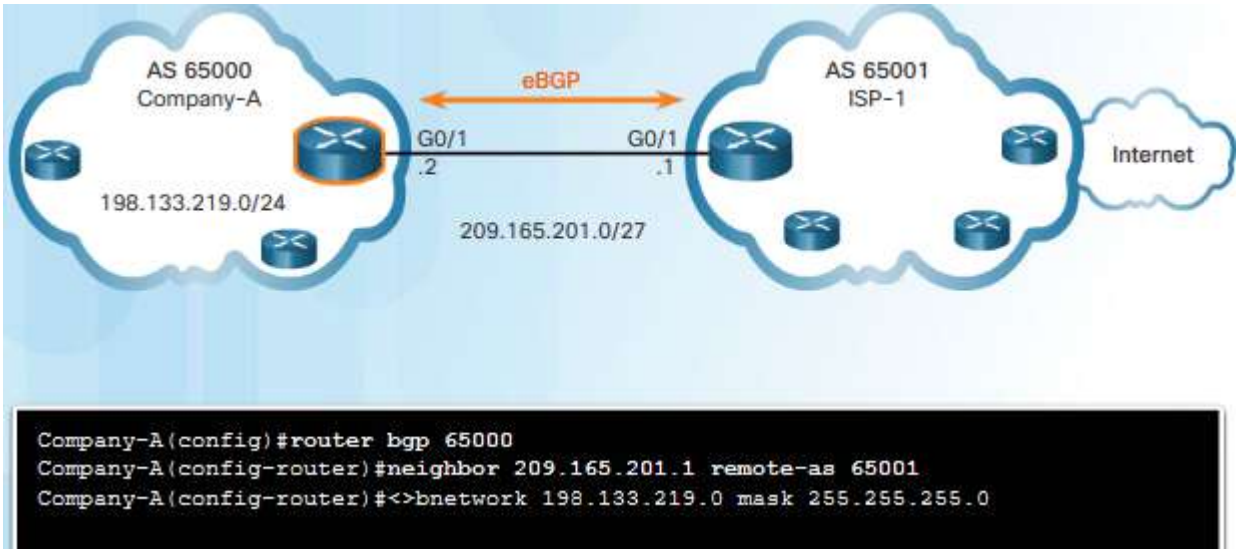


Figure 1 shows the BGP configuration for Company-A. Customers typically use private IPv4 address space for internal devices within their own network. Using NAT, the Company-A router translates these private IPv4 addresses to one of its public IPv4 addresses, advertised by BGP to the ISP.

The router bgp command enables BGP and identifies the AS number for Company-A. A router can belong to only a single AS, so only a single BGP process can run on a router.

The neighbor command identifies the BGP peer and its AS number. Notice that the ISP AS number is different than the Company-A AS number. This informs the BGP process that the neighbor is in a different AS and is therefore, an external BGP neighbor.

The mask option must be used when the network advertised is different than its classful equivalent. In this example, the 198.133.219.0/24 is equivalent to a class C network. Class C networks have a /24 subnet mask, so in this case the mask option is not required. If Customer-A was advertising the 198.133.0.0/16 network, then the mask option would be required. Otherwise BGP would advertise the network with a /24 classful mask.

The network command enters the *network-address* into the local BGP table. The BGP table contains all routes learned via BGP or advertised using BGP. eBGP will then advertise the *network-address* to its eBGP neighbors.

Note: In contrast to an IGP protocol, the *network-address* used in the network command does not have to be a directly connected network. The router only needs to have a route to this network in its routing table.

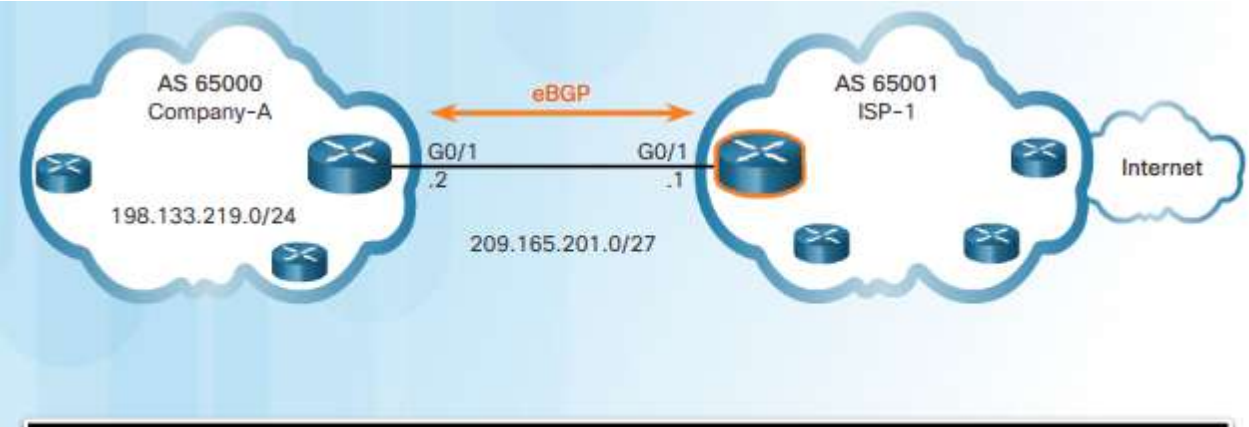


Figure 2 shows the BGP configuration for ISP-1.

The eBGP commands on the ISP-1 router are similar to the configuration on Company-A. Notice how the network 0.0.0.0 command is used to advertise a default network to Company-A.

Verify eBGP

Three commands can be used to verify eBGP, as shown in Figure 1.

Command	Description
`Router# show ip route`	Verify routes advertised by the BGP neighbor are present in the IPv4 routing table.
`Router# show ip bgp`	Verify that received and advertised IPv4 networks are in the BGP table.
`Router# show ip bgp summary`	Verify IPv4 BGP neighbors and other BGP information.

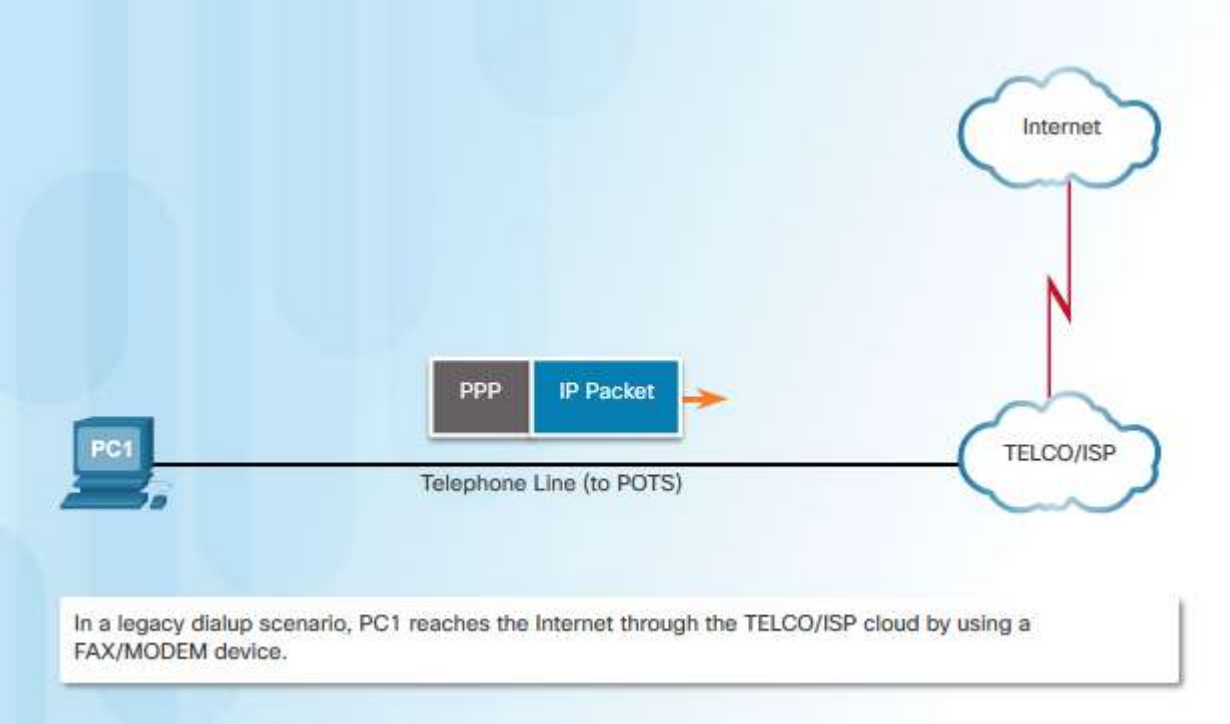
Review questions

See the practical attachment

Learning Outcome 2.5: Implementation of Point-to-Point Protocol (PPP)

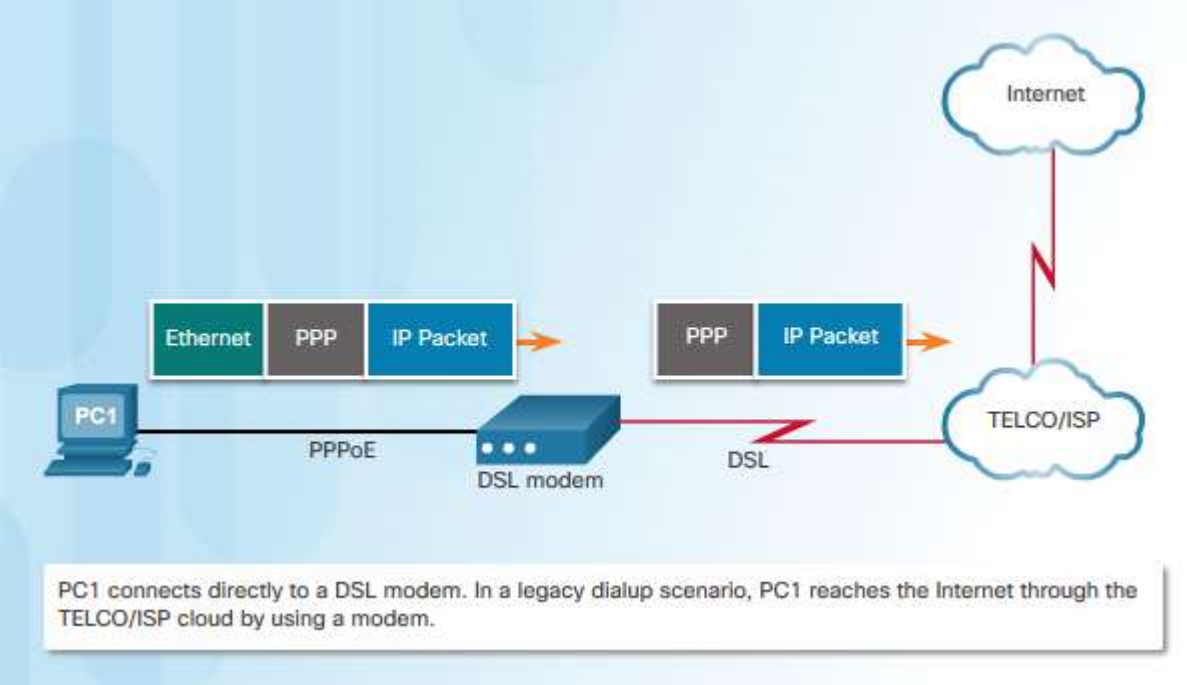
PPPoE Motivation

In addition to understanding the various technologies available for broadband Internet access, it is also important to understand the underlying data link layer protocol used by the ISP to form a connection.



A commonly used data link layer protocol by ISPs is PPP. PPP can be used on all serial links including those links created with dial-up analog and ISDN modems. To this day, the link from a dialup user to an ISP, using analog modems, likely uses PPP. Figure 1 shows a basic representation of that analog dial connection with PPP.

Additionally, ISPs often use PPP as the data link protocol over broadband connections. There are several reasons for this. First, PPP supports the ability to assign IP addresses to remote ends of a PPP link. With PPP enabled, ISPs can use PPP to assign each customer one public IPv4 address. More importantly, PPP supports CHAP authentication. ISPs often want to use CHAP to authenticate customers because during authentication, ISPs can check accounting records to determine whether the customer's bill is paid, prior to letting the customer connect to the Internet.



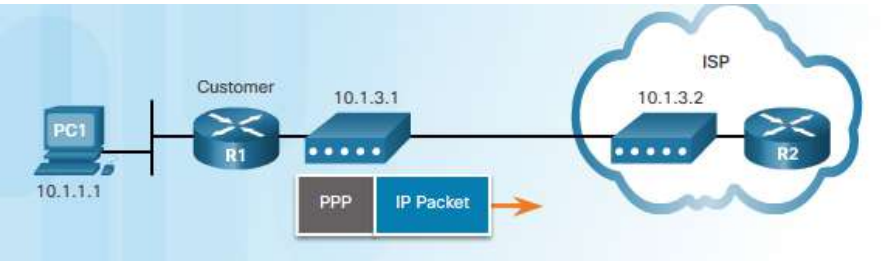
These technologies came to market in the following order, with varying support for PPP:

1. Analog modems for dialup that could use PPP and CHAP
2. ISDN for dialup that could use PPP and CHAP
3. DSL, which did not create a point-to-point link and could not support PPP and CHAP

ISPs value PPP because of the authentication, accounting, and link management features. Customers appreciate the ease and availability of the Ethernet connection. However, Ethernet links do not natively support PPP. PPP over Ethernet (PPPoE) provides a solution to this problem. As shown in Figure 2, PPPoE allows the sending of PPP frames encapsulated inside Ethernet frames.

PPPoE Concepts

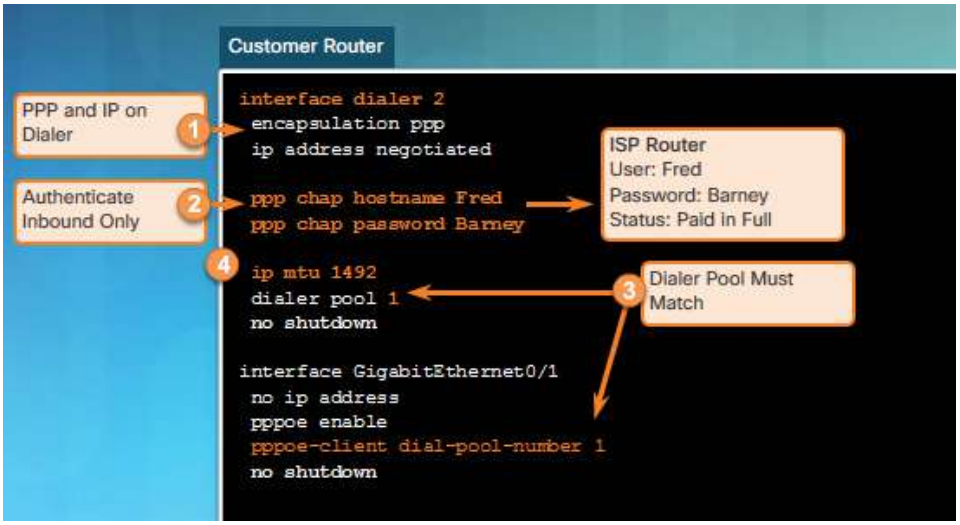
As shown in the figure, the customer's router is usually connected to a DSL modem using an Ethernet cable. PPPoE creates a PPP tunnel over an Ethernet connection. This allows PPP frames to be sent across the Ethernet cable to the ISP from the customer's router. The modem converts the Ethernet frames to PPP frames by stripping the Ethernet headers. The modem then transmits these PPP frames on the ISP's DSL network.



PPPoE Configuration

With the ability to send and receive PPP frames between the routers, the ISP could continue to use the same authentication model as with analog and ISDN. To make it all work, the client and ISP routers

need additional configuration, including PPP configuration, as shown in Figure 1. To understand the configuration, consider the following:



1. To create a PPP tunnel, the configuration uses a dialer interface. A dialer interface is a virtual interface. The PPP configuration is placed on the dialer interface, not the physical interface. The dialer interface is created using the interface dialer *number* command. The client can configure a static IP address, but will more likely be automatically assigned a public IP address by the ISP.

2. The PPP CHAP configuration usually defines one-way authentication; therefore, the ISP authenticates the customer. The hostname and password configured on the customer router must match the hostname and password configured on the ISP router. Notice in the figure that the CHAP username and password match the settings on the ISP router.

3. The physical Ethernet interface that connects to the DSL modem is then enabled with the command pppoe enable that enables PPPoE and links the physical interface to the dialer interface. The dialer interface is linked to the Ethernet interface with the dialer pool and pppoe-client commands, using the same number. The dialer interface number does not have to match the dialer pool number.

The ISP router has been configured with the following parameters:

- **Username: customer2222**
- **Password: ConnectMe**

Configure the virtual dialer interface 5 in the following order:

- **Create the virtual dialer 5 interface**
- **Set the encapsulation to PPP**
- **Negotiate the IP address from the ISP**
- **Reduce the MTU to 1492 to accomodate the PPP headers**
- **Create dialer pool 5**
- **Enforce chap authentication, use the username provided by the ISP**
- **Assign the chap password provided by the ISP**
- **Activate the interface**

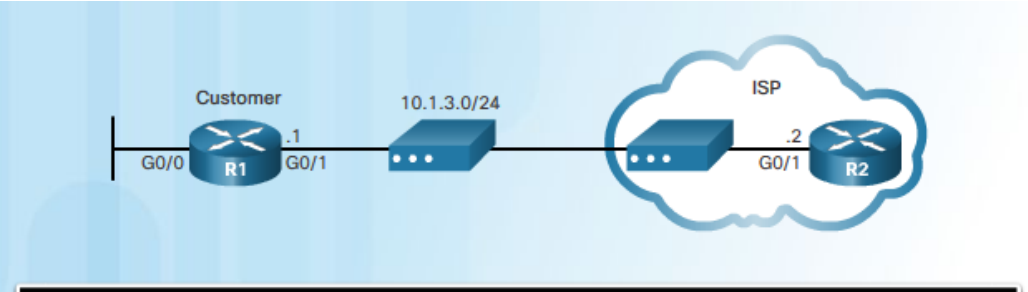
```
R1(config)#
```

4. The maximum transmission unit (MTU) should be set down to 1492, versus the default of 1500, to accommodate the PPPoE headers.

PPPoE Verification

The customer's router is connected to the ISP router using DSL. Both routers have been configured for PPPoE. The show ip interface brief command is issued on R1 to verify the IPv4 address automatically assigned to the dialer interface by the ISP router.

The show interface dialer command on R1, verifies the MTU and PPP encapsulation configured on the dialer interface.




```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         unassigned      YES unset  up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                unassigned      YES unset  administratively down down
Dialer2                    10.1.3.1        YES IPCP   up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Virtual-Access2            unassigned      YES unset  up                    up
R1#
```

Notice that two /32 host routes for 10.0.0.0 have been installed in R1's routing table. The first host route is for the address assigned to the dialer interface. The second host route is the IPv4 address of the ISP. The installation of these two host routes is the default behavior for PPPoE.

The show pppoe session command is used to display information about currently active PPPoE sessions. The output displays the local and remote Ethernet MAC addresses of both routers. The Ethernet MAC addresses can be verified by using the show interfaces command on each router.

Review questions

See the practical attachment

Learning Outcome 2.6: Enable Management protocols

In this chapter, you will explore the tools network administrators can use for device discovery, device management, and device maintenance. Cisco Discovery Protocol (CDP) and Link Layer Discover Protocol (LLDP) are both capable of discovering information about directly connected devices.

Network Time Protocol (NTP) can be effectively used to synchronize the time across all your networking devices, which is especially important when trying to compare log files from different devices. Those log files are generated by the syslog protocol. Syslog messages can be captured and sent to a syslog server to aid in device management tasks.

Device maintenance includes ensuring that Cisco IOS images and configuration files are backed up in a safe location in the event that the device memory is corrupted or erased, either maliciously or inadvertently. Maintenance also includes keeping the IOS image up to date. The device maintenance section of the chapter includes topics for file maintenance, image management, and software licensing.

CDP Overview

Cisco Discovery Protocol (CDP) is a Cisco proprietary Layer 2 protocol that is used to gather information about Cisco devices which share the same data link. CDP is media and protocol independent and runs on all Cisco devices, such as routers, switches, and access servers.

The device sends periodic CDP advertisements to connected devices, as shown in the figure. These advertisements share information about the type of device that is discovered, the name of the devices, and the number and type of the interfaces.

Because most network devices are connected to other devices, CDP can assist in network design decisions, troubleshooting, and making changes to equipment. CDP can also be used as a network discovery tool to determine the information about the neighboring devices. This information gathered from CDP can help build a logical topology of a network when documentation is missing or lacking in detail.

Configure and Verify CDP

For Cisco devices, CDP is enabled by default. For security reasons, it may be desirable to disable CDP on a network device globally, or per interface. With CDP, an attacker can gather valuable insight about the network layout, such as IP addresses, IOS versions, and types of devices.

To verify the status of CDP and display information about CDP, enter the show cdp command, as displayed in Example 1.

```
Router# show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
```

To enable CDP globally for all the supported interfaces on the device, enter cdp run in the global configuration mode. CDP can be disabled for all the interfaces on the device with the no cdp run command in the global configuration mode.

To disable CDP on a specific interface, such as the interface facing an ISP, enter no cdp enable in the interface configuration mode. CDP is still enabled on the device; however, no more CDP advertisements will be sent out that interface. To enable CDP on the specific interface again, enter cdp enable, as shown in Figure 2.

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# cdp enable
```

Figure 3 shows CDP disabled globally using the command no cdp run and re-enabled using the cdp run command.

```
Router(config)# no cdp run
Router(config)# exit
Router# show cdp
% CDP is not enabled
Router# conf t
Router(config)# cdp run
```

To verify the status of CDP and display a list of neighbors, use the show cdp neighbors command in the privileged EXEC mode. The show cdp neighbors command displays important information about the CDP neighbors. Currently, this device does not have any neighbors because it is not physically connected to any devices, as indicated by the results of the show cdp neighbors command displayed in Figure 4.

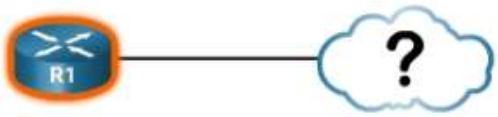
```
Router# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

Total cdp entries displayed : 0
```

Use the show cdp interface command to display the interfaces that are CDP enabled on a device. The status of each interface is also displayed. Figure 5 shows that five interfaces are CDP enabled on the router with only one active connection to another device.

```
Router# show cdp interface
Embedded-Service-Engine0/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0/0/0 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0/0/1 is administratively down, line protocol is down
  Encapsulation HDLC
```

Discover Devices Using CDP

With CDP enabled on the network, the show cdp neighbors command can be used to determine the network layout.




```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S1               Gig 0/1           122              S I   WS-C2960- Fas 0/5
                                                                    .
```

For example, consider the lack of documentation in the topology shown in Figure 1. No information is available regarding the rest of the network. The show cdp neighbors command provides helpful information about each CDP neighbor device, including the following:

Device identifiers - The host name of the neighbor device (S1)

Port identifier - The name of the local and remote port (Gig 0/1 and Fas 0/5, respectively)

Capabilities list - Whether the device is a router or a switch (S for switch; I for IGMP is beyond scope for this course)

Platform - The hardware platform of the device (WS-C2960 for Cisco 2960 switch)

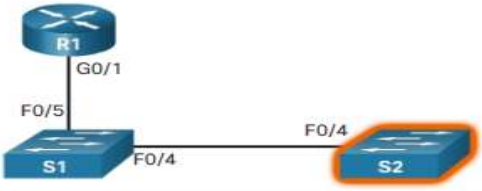
If more information is needed, the show cdp neighbors detail command can also provide information, such as the neighbors' IOS version and IPv4 address, as displayed in Figure 2.


```
R1# show cdp neighbors detail
-------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.2
Platform: cisco WS-C2960-24TT-L,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/1,  Port ID (outgoing port): FastEthernet0/5
Holdtime : 136 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
```

By accessing S1 either remotely through SSH or physically through the console port, a network administrator can determine the other devices connected to S1, as displayed in the output of the show cdp neighbors in Figure 3.


```
S1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S2               Fas 0/4           158              S I   WS-C2960- Fas 0/4
R1               Fas 0/5           136            R B S I CISCO1941 Gig 0/1
```

Another switch, S2, is revealed in the output. The network administrator then accesses S2 and displays the CDP neighbors, as shown in Figure 4.



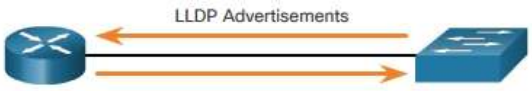

```
S2# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S1               Fas 0/4           173              S I   WS-C2960- Fas 0/4
```

The only device connected to S2 is S1. Therefore, there are no more devices to discover in the topology.

The network administrator can now update the documentation to reflect the discovered devices.

LLDP Overview

Cisco devices also support Link Layer Discovery Protocol (LLDP), which is a vendor-neutral neighbor discovery protocol similar to CDP. LLDP works with network devices, such as routers, switches, and wireless LAN access points. This protocol advertises its identity and capabilities to other devices and receives the information from a physically connected Layer 2 device.



Cisco devices support sending vendor-neutral LLDP advertisements to connected devices.

Configure and Verify LLDP

Depending on the device, LLDP may be enabled by default. To enable LLDP globally on a Cisco network device, enter the lldp run command in the global configuration mode. To disable LLDP, enter the no lldp run command in the global configuration mode.

Similar to CDP, LLDP can be configured on specific interfaces. However, LLDP must be configured separately to transmit and receive LLDP packets, as shown in Figure 1.

To verify LLDP has been enabled on the device, enter the show lldp command in the privileged EXEC mode.

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch# show lldp

Global LLDP Information:
    Status: ACTIVE
    LLDP advertisements are sent every 30 seconds
    LLDP hold time advertised is 120 seconds
    LLDP interface reinitialisation delay is 2 seconds
```

Discover Devices Using LLDP

With LLDP enabled, device neighbors can be discovered using the show lldp neighbors command. For example, consider the lack of documentation in the topology shown in Figure 1.


```
S1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
R1                  Fa0/5          99         R               Gi0/1
S2                  Fa0/4          120        B               Fa0/4

Total entries displayed: 2
```

The network administrator only knows that S1 is connected to two devices. Using the show lldp neighbors command, the network administrator discovers that S1 has a router and a switch as a neighbors.

Note: The letter B under capability for S2 represents a Bridge. For this output, the word bridge can also mean switch. From the results of show lldp neighbors, a topology from switch S1 can be constructed as depicted in Figure 2.


```
S1# show lldp neighbors detail
------------------------------------------------
Chassis id: fc99.4775.c3e0
Port id: Gi0/1
Port Description: GigabitEthernet0/1
System Name: R1

System Description:
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.4(3)M2,
  RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Fri 06-Feb-15 17:01 by prod_rel_team

Time remaining: 101 seconds
System Capabilities: B,R
Enabled Capabilities: R
```

When more details about the neighbors are needed, the show lldp neighbors detail command can provide information, such as the neighbors' IOS version, IP address, and device capability.

Setting the System Clock

The software clock on a router or switch starts when the system boots and is the primary source of time for the system. It is important to synchronize the time across all devices on the network because all aspects of managing, securing, troubleshooting, and planning networks require accurate timestamping. When the time is not synchronized between devices, it will be impossible to determine the order of the events and the cause of an event.

Typically, the date and time settings on a router or switch can be set using one of two methods:

Manually configure the date and time, as shown in the figure

Configure the Network Time Protocol (NTP)

As a network grows, it becomes difficult to ensure that all infrastructure devices are operating with synchronized time. Even in a smaller network environment, the manual method is not ideal. If a router reboots, how will it get an accurate date and timestamp?

A better solution is to configure the NTP on the network. This protocol allows routers on the network to synchronize their time settings with an NTP server. A group of NTP clients that obtain time and date information from a single source have more consistent time settings. When NTP is implemented in the network, it can be set up to synchronize to a private master clock or it can synchronize to a publicly available NTP server on the Internet.

NTP uses UDP port 123 and is documented in RFC 1305.

NTP Operation

NTP networks use a hierarchical system of time sources. Each level in this hierarchical system is called a stratum. The stratum level is defined as the number of hop counts from the authoritative source. The synchronized time is distributed across the network using NTP. The figure displays a sample NTP network.

NTP servers arranged in three levels showing the three strata. Stratum 1 is connected to Stratum 0 clocks.

Stratum 0

An NTP network gets the time from authoritative time sources. These authoritative time sources, also referred to as stratum 0 devices, are high-precision timekeeping devices assumed to be accurate and with little or no delay associated with them. Stratum 0 devices are represented by the clock in the figure.

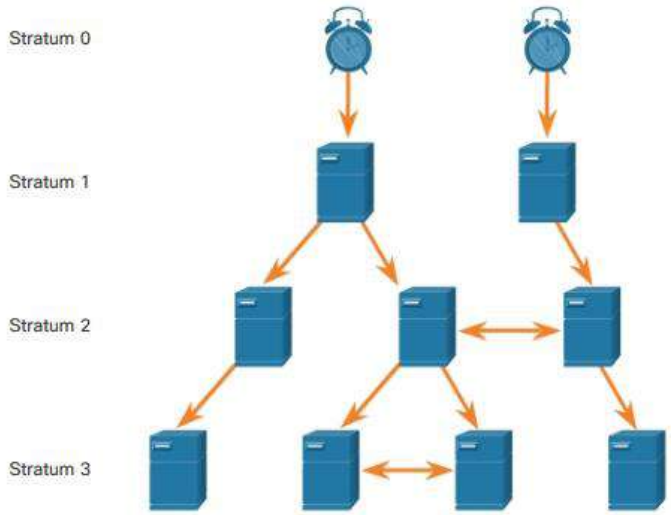
Stratum 1

The stratum 1 devices are directly connected to the authoritative time sources. They act as the primary network time standard.

Stratum 2 and Lower

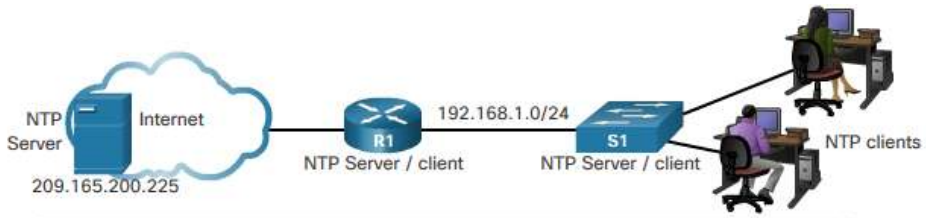
The stratum 2 servers are connected to stratum 1 devices through network connections. Stratum 2 devices, such as NTP clients, synchronize their time using the NTP packets from stratum 1 servers. They could also act as servers for stratum 3 devices.

Smaller stratum numbers indicate that the server is closer to the authorized time source than larger stratum numbers. The larger the stratum number, the lower the stratum level. The max hop count is 15. Stratum 16, the lowest stratum level, indicates that a device is unsynchronized. Time servers on the same stratum level can be configured to act as a peer with other time servers on the same stratum level for backup or verification of time.



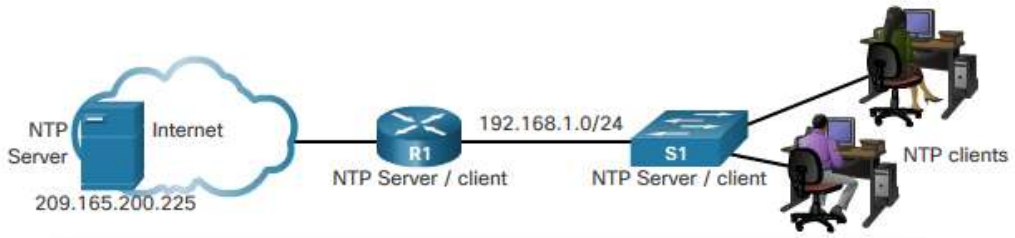
Configure and Verify NTP

Before NTP is configured on the network, the show clock command displays the current time on the software clock. With the detail option, the time source is also displayed.




```
R1# show clock detail
20:55:10.207 UTC Fri Dec 11 2015
Time source is user configuration
R1(config)# ntp server 209.165.200.225
R1(config)# end
R1# show clock detail
21:01:34.563 UTC Fri Dec 11 2015
Time source is NTP
```

As shown in Figure 1, the software clock has been manually configured. Use the ntp server *ip-address* command in global configuration mode to configure 209.165.200.225 as the NTP server for R1. To verify the time source is set to NTP, use the show clock detail command again.




```
R1# show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   c
*~209.165.200.225 .GPS.           1     61     64   377  0.481   7.480  4.2
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configure

R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**19
ntp uptime is 589900 (1/100 of seconds), resolution is 4016
```

As shown in Figure 2, use the show ip ntp associations and show ntp status commands to verify that R1 is synchronized with the NTP server at 209.165.200.225. Notice that R1 is synchronized with a stratum 1 NTP server at 209.165.200.225, which is synchronized with a GPS clock. The show ntp status command displays that R1 is now a stratum 2 device synchronized with the NTP server at 209.165.220.225.


```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations

  address         ref clock       st   when   poll reach  delay  offset
*~192.168.1.1     209.165.200.225  2     12     64   377  1.066  13.616
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ config

S1# Cshow ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2088 Hz, precision is 2*
reference time is DA08904B.3269C655 (13:31:55.196 PST Tue Dec 1 2015)
clock offset is 18.7764 msec, root delay is 102.42 msec
root dispersion is 38.03 msec, peer dispersion is 3.74 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.00000392
```

The clock on S1 is configured to synchronize to R1, as shown in Figure 3. Output from the show ntp associations command verifies that the clock on S1 is now synchronized with R1 at 192.168.1.1 via NTP. R1 is a stratum 2 device and NTP server to S1. Now S1 is a stratum 3 device that can provide NTP service to other devices in the network, such as end devices.

Introduction to Syslog

When certain events occur on a network, networking devices have trusted mechanisms to notify the administrator with detailed system messages. These messages can be either non-critical or significant. Network administrators have a variety of options for storing, interpreting, and displaying these messages, and for being alerted to those messages that could have the greatest impact on the network infrastructure.

The most common method of accessing system messages is to use a protocol called syslog.

Syslog is a term used to describe a standard. It is also used to describe the protocol developed for that standard. The syslog protocol was developed for UNIX systems in the 1980s, but was first documented as RFC 3164 by IETF in 2001. Syslog uses UDP port 514 to send event notification messages across IP networks to event message collectors, as illustrated in the figure.

Many networking devices support syslog, including: routers, switches, application servers, firewalls, and other network appliances. The syslog protocol allows networking devices to send their system messages across the network to syslog servers.

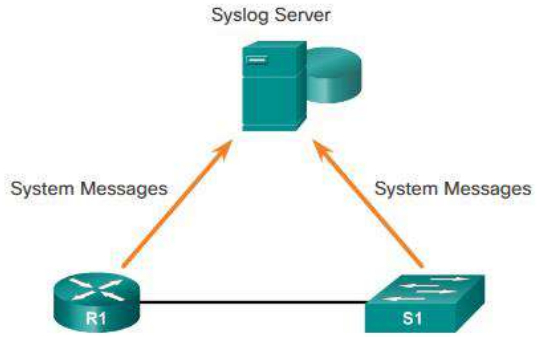
There are several different syslog server software packages for Windows and UNIX. Many of them are freeware.

The syslog logging service provides three primary functions:

The ability to gather logging information for monitoring and troubleshooting

The ability to select the type of logging information that is captured

The ability to specify the destinations of captured syslog messages



Syslog Operation

On Cisco network devices, the syslog protocol starts by sending system messages and debug output to a local logging process internal to the device. How the logging process manages these messages and outputs is based on device configurations. For example, syslog messages may be sent across the network to an external syslog server. These messages can be retrieved without the need of accessing the actual device. Log messages and outputs stored on the external server can be pulled into various reports for easier reading.

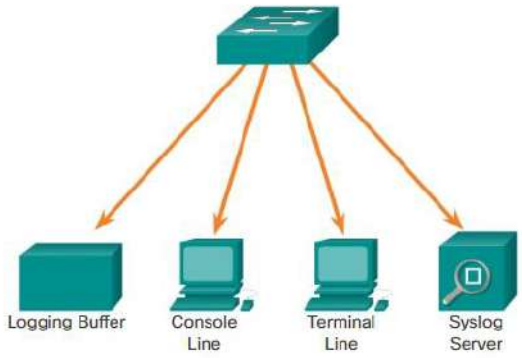
Alternatively, syslog messages may be sent to an internal buffer. Messages sent to the internal buffer are only viewable through the CLI of the device.

Finally, the network administrator may specify that only certain types of system messages are sent to various destinations. For example, the device may be configured to forward all system messages to an external syslog server. However, debug-level messages are forwarded to the internal buffer and are only accessible by the administrator from the CLI.

As shown in the figure, popular destinations for syslog messages include:

- Logging buffer (RAM inside a router or switch)
- Console line
- Terminal line
- Syslog server

It is possible to remotely monitor system messages by viewing the logs on a syslog server, or by accessing the device through Telnet, SSH, or through the console port.



Syslog Message Format

Cisco devices produce syslog messages as a result of network events. Every syslog message contains a severity level and a facility.

The smaller numerical levels are the more critical syslog alarms. The severity level of the messages can be set to control where each type of message is displayed (i.e. on the console or the other destinations).

Severity Name	Severity Level	Explanation
Emergency	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal, but Significant Condition
Informational	Level 6	Informational Message
Debugging	Level 7	Debugging Message

Each syslog level has its own meaning:

Warning Level 4 - Emergency Level 0: These messages are error messages about software or hardware malfunctions; these types of messages mean that the functionality of the device is affected. The severity of the issue determines the actual syslog level applied.

Notification Level 5: The notifications level is for normal, but significant events. For example, interface up or down transitions, and system restart messages are displayed at the notifications level.

Informational Level 6: A normal information message that does not affect device functionality. For example, when a Cisco device is booting, you might see the following informational message: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User License Agreement is accepted.

Debugging Level 7: This level indicates that the messages are output generated from issuing various debug commands.

In addition to specifying the severity, syslog messages also contain information on the facility. Syslog facilities are service identifiers that identify and categorize system state data for error and event message reporting. The logging facility options that are available are specific to the networking device. For example, Cisco 2960 Series switches running Cisco IOS Release 15.0(2) and Cisco 1941 routers

running Cisco IOS Release 15.2(4) support 24 facility options that are categorized into 12 facility types.

Field	Explanation
seq no	Stamps log messages with a sequence number only if the `service sequence-numbers` global configuration command is configured.
timestamp	Date and time of the message or event, which appears only if the `service timestamps` global configuration command is configured.
facility	The facility to which the message refers.
severity	Single-digit code from 0 to 7 that is the severity of the message.
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.

Some common syslog message facilities reported on Cisco IOS routers include:

- IP
- OSPF protocol
- SYS operating system
- IP security (IPsec)
- Interface IP (IF)

By default, the format of syslog messages on the Cisco IOS Software is as follows:

seq no: timestamp: %facility-severity-MNEMONIC: description

The fields contained in the Cisco IOS Software syslog message are explained in Figure 2.

For example, sample output on a Cisco switch for an EtherChannel link changing state to up is:

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up

Here the facility is LINK and the severity level is 3, with a MNEMONIC of UPDOWN.

The most common messages are link up and down messages, and messages that a device produces when it exits from configuration mode. If ACL logging is configured, the device generates syslog messages when packets match a parameter condition.

Service Timestamp

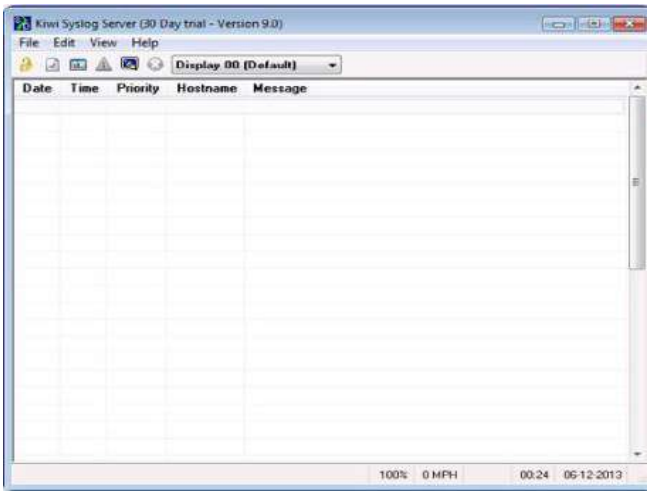
By default, log messages are not timestamped. For example, in the figure, the R1 GigabitEthernet 0/0 interface is shutdown. The message logged to the console does not identify when the interface state was changed. Log messages should be timestamped so that when they are sent to another destination, such as a Syslog server, there is record of when the message was generated. Use the command service timestamps log datetime to force logged events to display the date and time. As shown in the figure, when the R1 GigabitEthernet 0/0 interface is reactivated, the log messages now contain the date and time.

Note: When using the datetime keyword, the clock on the networking device must be set, either manually or through NTP, as previously discussed.

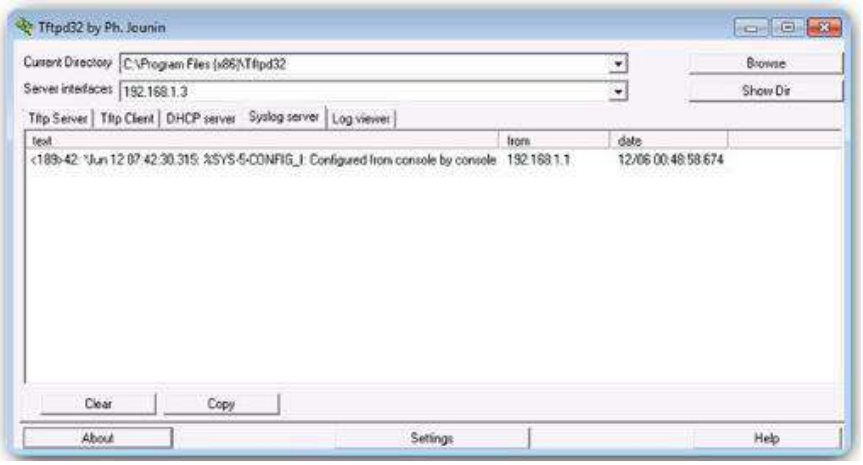
```
R1# conf t
R1(config)# interface g0/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to down
R1(config-if)# exit
R1(config)# service timestamps log datetime
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar  1 11:52:42: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to down
*Mar  1 11:52:45: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to up
*Mar  1 11:52:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)#
```

Syslog Server

To view syslog messages, a syslog server must be installed on a workstation in the network. There are several freeware and shareware versions of syslog, as well as enterprise versions for purchase. In Figure 1, an evaluation version of the Kiwi Syslog Daemon is displayed on a Windows 7 machine.



The syslog server provides a relatively user-friendly interface for viewing syslog output. The server parses the output and places the messages into pre-defined columns for easy interpretation. If timestamps are configured on the networking device sourcing the syslog messages, then the date and time of each message displays in the syslog server output, as shown in Figure 2.



Network administrators can easily navigate the large amount of data compiled on a syslog server. One

advantage of viewing syslog messages on a syslog server is the ability to perform granular searches through the data. Also, a network administrator can quickly delete unimportant syslog messages from the database.

Default Logging

By default, Cisco routers and switches send log messages for all severity levels to the console. On some IOS versions, the device also buffers log messages by default. To enable these two settings, use the logging console and logging buffered global configuration commands, respectively.

The show logging command displays the default logging service settings on a Cisco router, as shown in the figure. The first lines of output list information about the logging process, with the end of the output listing log messages.

The first highlighted line states that this router logs to the console and includes debug messages. This actually means that all debug level messages, as well as any lower level messages (such as notification level messages), are logged to the console. On most Cisco IOS routers, the default severity level is 7, debugging. The output also notes that 32 such messages have been logged.

The second highlighted line states that this router logs to an internal buffer. Because this router has enabled logging to an internal buffer, the show logging command also lists the messages in that buffer. You can view some of the system messages that have been logged at the end of the output.

Router and Switch Commands for Syslog Clients

There are three steps to configuring the router to send system messages to a syslog server where they can be stored, filtered, and analyzed:

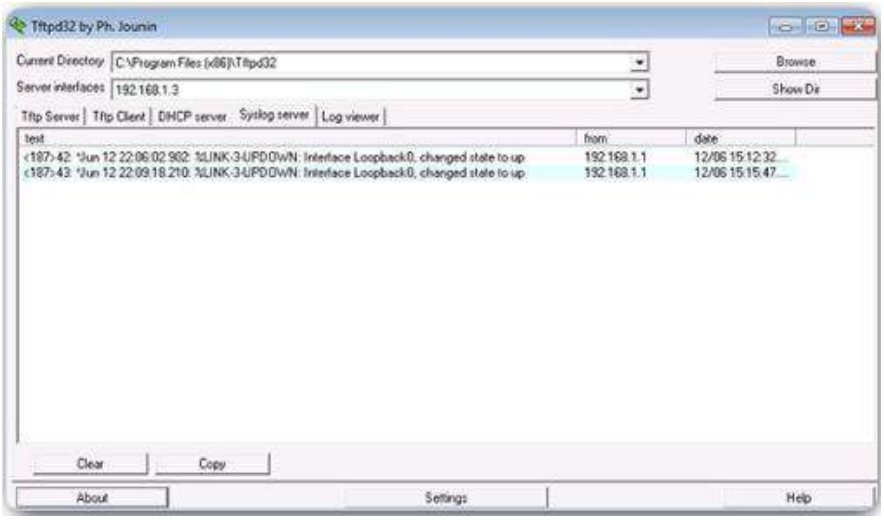
Step 1. In global configuration mode, use the logging command toconfigure the destination hostname or IPv4 address of the syslog.

Step 2. Control the messages that will be sent to the syslog server with the logging trap *level* global configuration mode command. For example, to limit the messages to levels 4 and lower (0 to 4), use one of the two equivalent commands.

Step 3. Optionally, configure the source interface with the logging source-interface *interface-type interface-number* global configuration mode command. This specifies that syslog packets contain the IPv4 or IPv6 address of a specific interface, regardless of which interface the packet uses to exit the router.

```
R1(config)# logging 192.168.1.3
R1(config)# logging trap 4
R1(config)# logging source-interface gigabitEthernet 0/0
R1(config)# interface loopback 0
R1(config-if)#
*Jun 12 22:06:02.902: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:06:03.902: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:06:03.902: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to
host 192.168.1.3 port 514 started - CLI initiated
R1(config-if)# shutdown
R1(config-if)#
*Jun 12 22:06:49.642: %LINK-5-CHANGED: Interface Loopback0,
changed state to administratively down
*Jun 12 22:06:50.642: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to down
R1(config-if)# no shutdown
R1(config-if)#
*Jun 12 22:09:18.210: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:09:19.210: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
R1(config-if)#
```

In Figure 1, R1 is configured to send log messages of levels 4 and lower to the syslog server at 192.168.1.3. The source interface is set as the G0/0 interface. A loopback interface is created, then shut down, and then brought back up. The console output reflects these actions.



Shown in Figure 2, the Tftpd32 syslog server has been set up on a Windows 7 machine with IPv4 address 192.168.1.3. As you can see, the only messages that appear on the syslog server are those with severity level of 4 or lower (more severe). The messages with severity level of 5 or higher (less severe) appear on the router console output, but do not appear on the syslog server output, because the logging traplimits the syslog messages sent to the syslog server based on severity.

Review questions

See the practical attachment

Router File Systems

The Cisco IOS File System (IFS) allows the administrator to navigate to different directories and list the files in a directory, and to create subdirectories in flash memory or on a disk. The directories available depend on the device.

```
Router# show file systems
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*    256487424     183234560      disk     rw   flash0: flash:#
             -             -      disk     rw   flash1:
        262136        254779     nvram     rw   nvram:
             -             -    opaque     wo   syslog:
             -             -    opaque     rw   xmodem:
             -             -    opaque     rw   ymodem:
             -             -   network     rw   rcp:
             -             -   network     rw   http:
             -             -   network     rw   ftp:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
```

Figure 1 displays the output of the show file systems command, which lists all of the available file systems on a Cisco 1941 router. This command provides useful information such as the amount of available and free memory, the type of file system, and its permissions. Permissions include read only (ro), write only (wo), and read and write (rw), shown in the Flags column of the command output.

Although there are several file systems listed, of interest to us will be the tftp, flash, and nvram file systems.

Notice that the flash file system also has an asterisk preceding it. This indicates that flash is the current default file system. The bootable IOS is located in flash; therefore, the pound symbol (#) is appended to the flash listing, indicating that it is a bootable disk.

The Flash File System

```
Router# dir
Directory of flash0:/

 1 -rw-     2903 Sep 7 2012 06:58:26 +00:00  cpconfig-
                                             19xx.cfg
 2 -rw-  3000320 Sep 7 2012 06:58:40 +00:00  cpexpress.tar
 3 -rw-     1038 Sep 7 2012 06:58:52 +00:00  home.shtml
 4 -rw-   122880 Sep 7 2012 06:59:02 +00:00  home.tar
 5 -rw-  1697952 Sep 7 2012 06:59:20 +00:00  securedesktop-
                                             ios-3.1.1.45-k9.pkg
 6 -rw-   415956 Sep 7 2012 06:59:34 +00:00  sslclient-win-
                                             1.1.4.176.pkg
 7 -rw- 67998028 Sep 26 2012 17:32:14 +00:00 c1900-
                                             universalk9-
                                             mz.SPA.152-4.M1.bin

256487424 bytes total (183234560 bytes free)
```

Figure 2 displays the output from the dir (directory) command. Because flash is the default file system, the dir command lists the contents of flash. Several files are located in flash, but of specific interest is the last listing. This is the name of the current Cisco IOS file image that is running in RAM.

The NVRAM File System

```
Router# cd nvram:
Router#pwd
nvram:/
Router#dir
Directory of nvram:/

  253  -rw-        1156      <no date>  startup-config
  254  ----           5      <no date>  private-config
  255  -rw-        1156      <no date>  underlying-config
    1  -rw-        2945      <no date>  cwmp_inventory
    4  ----          58      <no date>  persistent-data
    5  -rw-          17      <no date>  ecfm_ieee_mib
    6  -rw-         559      <no date>  IOS-Self-Sig#1.cer

262136 bytes total (254779 bytes free)
```

To view the contents of NVRAM, you must change the current default file system using the cd (change directory) command, as shown in Figure 3. The pwd (present working directory) command verifies that we are viewing the NVRAM directory. Finally, the dir command lists the contents of NVRAM. Although there are several configuration files listed, of specific interest is the startup-configuration file.

Switch File Systems

With the Cisco 2960 switch flash file system, you can copy configuration files, and archive (upload and download) software images.

```
Switch# show file systems
File Systems:

       Size(b)     Free(b)      Type  Flags  Prefixes
*    32514048    20887552     flash     rw    flash:
           -           -    opaque     rw       vb:
           -           -    opaque     ro       bs:
           -           -    opaque     rw   system:
           -           -    opaque     rw   tmpsys:
       65536       48897     nvram     rw    nvram:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
           -           -    opaque     rw     null:
           -           -    opaque     ro      tar:
           -           -   network     rw     tftp:
           -           -   network     rw      rcp:
           -           -   network     rw     http:
           -           -   network     rw      ftp:
           -           -   network     rw      scp:
           -           -   network     rw    https:
           -           -    opaque     ro      cns:
```

Backing Up and Restoring Using Text Files

Backup Configurations with Text Capture (Tera Term)

Configuration files can be saved/archived to a text file using Tera Term.

The steps are:

Step 1. On the File menu, click Log.

Step 2. Choose the location to save the file. Tera Term will begin capturing text.

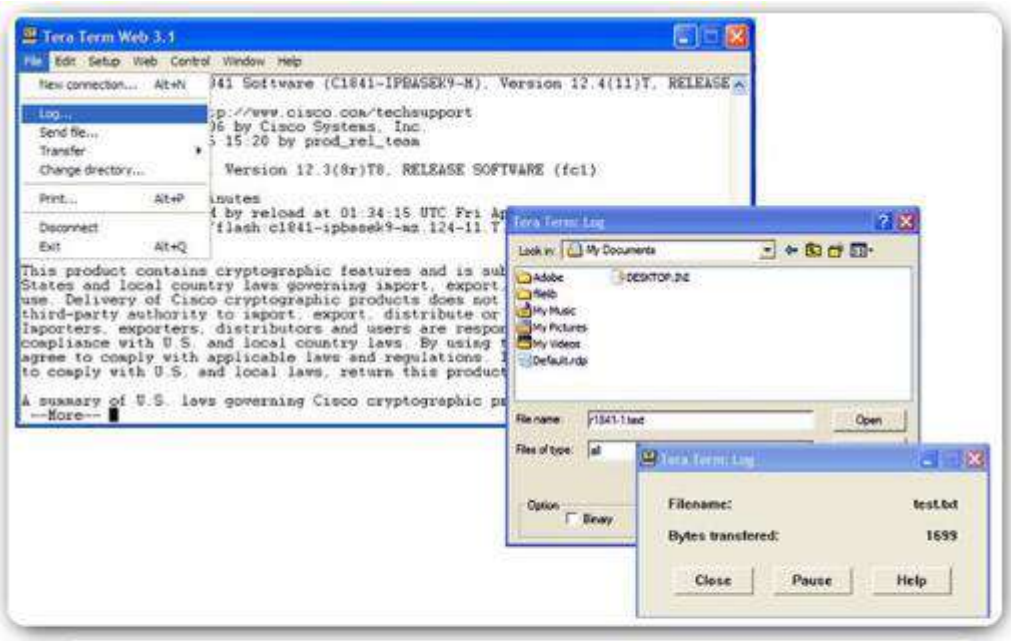
Step 3. After capture has been started, execute the show running-config or show startup-config command at the privileged EXEC prompt. Text displayed in the terminal window will be directed to the chosen file.

Step 4. When the capture is complete, select Close in the Tera Term: Log window.

Step 5. View the file to verify that it was not corrupted.

Restoring Text Configurations

A configuration can be copied from a file to a device. When copied from a text file and pasted into a terminal window, the IOS executes each line of the configuration text as a command. This means that the file will require editing to ensure that encrypted passwords are in plain text and that non-command text such as "--More--" and IOS messages are removed. This process is discussed in the lab.



1. Start the log process.
2. Issue a **show running-config** command.
3. Close the log.

Further, at the CLI, the device must be set at the global configuration mode to receive the commands from the text file being pasted into the terminal window.

When using Tera Term, the steps are:

Step 1. On the File menu, click Send file.

Step 2. Locate the file to be copied into the device and click Open.

Step 3. Tera Term will paste the file into the device.

The text in the file will be applied as commands in the CLI and become the running configuration on

the device. This is a convenient method for manually configuring a router.

Backing up and Restoring TFTP

Backup Configurations with TFTP

Copies of configuration files should be stored as backup files in the event of a problem. Configuration files can be stored on a Trivial File Transfer Protocol (TFTP) server or a USB drive. A configuration file should also be included in the network documentation.

To save the running configuration or the startup configuration to a TFTP server, use either the copy running-config tftp or copy startup-config tftp command as shown in the figure. Follow these steps to backup the running configuration to a TFTP server:

Step 1. Enter the copy running-config tftp command.

Step 2. Enter the IP address of the host where the configuration file will be stored.

Step 3. Enter the name to assign to the configuration file.

Step 4. Press Enter to confirm each choice.

Restoring Configurations with TFTP

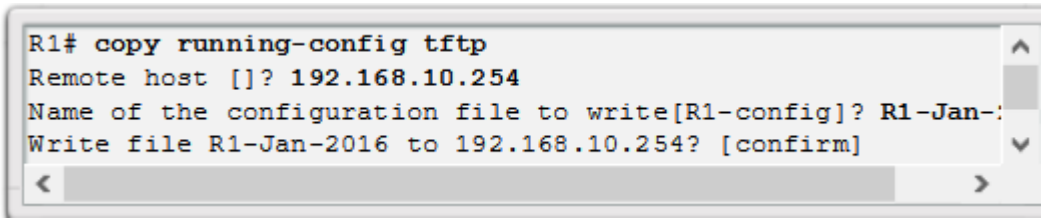
To restore the running configuration or the startup configuration from a TFTP server, use either the copy tftp running-config or copy tftp startup-config command. Use these steps to restore the running configuration from a TFTP server:

Step 1. Enter the copy tftp running-config command.

Step 2. Enter the IP address of the host where the configuration file is stored.

Step 3. Enter the name to assign to the configuration file.

Step 4. Press Enter to confirm each choice.



Using USB Ports on a Cisco Router

The Universal Serial Bus (USB) storage feature enables certain models of Cisco routers to support USB flash drives. The USB flash feature provides an optional secondary storage capability and an additional boot device. Images, configurations, and other files can be copied to or from the Cisco USB flash memory with the same reliability as storing and retrieving files using the Compact Flash card. In addition, modular integrated services routers can boot any Cisco IOS Software image saved on USB flash memory. Ideally, USB flash can hold multiple copies of the Cisco IOS and multiple router configurations.

Use the dir command to view the contents of the USB flash drive.


```
Router# dir usbflash0:
Directory of usbflash0:/
1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00
c3825-entservicesk9-mz.123-14.T
63158272 bytes total (33033216 bytes free)
```

Backing Up and Restoring Using a USB

Backup Configurations with a USB Flash Drive

When backing up to a USB port, it is a good idea to issue the show file systems command to verify that the USB drive is there and confirm the name, as shown in Figure 1.

```
R1# show file systems
File Systems:

         Size(b)       Free(b)      Type  Flags  Prefixes
               -             -    opaque     rw   archive:
               -             -    opaque     rw   system:
               -             -    opaque     rw   tmpsys:
               -             -    opaque     rw   null:
               -             -   network     rw   tftp:
*    256487424     184819712      disk     rw   flash0: flash:#
               -             -      disk     rw   flash1:
          262136        249270     nvram     rw   nvram:
               -             -    opaque     wo   syslog:
               -             -    opaque     rw   xmodem:
               -             -    opaque     rw   ymodem:
               -             -   network     rw   rcp:
               -             -   network     rw   http:
               -             -   network     rw   ftp:
               -             -   network     rw   scp:
               -             -    opaque     ro   tar:
               -             -   network     rw   https:
               -             -    opaque     ro   cns:
    4050042880    3774152704  usbflash     rw   usbflash0:
```

Shows the USB port and name: "usbflash0:"

Next, use the copy run usbflash0:/ command to copy the configuration file to the USB flash drive. Be sure to use the name of the flash drive, as indicated in the file system. The slash is optional but indicates the root directory of the USB flash drive.

The IOS will prompt for the filename. If the file already exists on the USB flash drive, the router will prompt to overwrite, as seen in Figure 2.

```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
5024 bytes copied in 0.736 secs (6826 bytes/sec)
```

Copying to USB flash drive, and no file pre-exists.

```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
5024 bytes copied in 1.796 secs (2797 bytes/sec)
```

Copying to USB flash drive, and the same configuration file already exists on the drive.

Use the dir command to see the file on the USB drive and use the more command to see the contents, as seen in Figure 3.

```
R1# dir usbflash0:/
Directory of usbflash0:/
    1  drw-     0  Oct 15 2010 16:28:30 +00:00  Cisco
   16  -rw-  5024   Jan 7 2013 20:26:50 +00:00  R1-Config

4050042880 bytes total (3774144512 bytes free)
R1# more usbflash0:/R1-Config
!
! Last configuration change at 20:19:54 UTC Mon Jan 7 2013 by
admin version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

Restore Configurations with a USB Flash Drive

In order to copy the file back, it will be necessary to edit the USB R1-Config file with a text editor. Assuming the file name is R1-Config, use the command copy usbflash0:/R1-Config *running-config* to restore a running configuration.

Password Recovery

Passwords on devices are used to prevent unauthorized access. For encrypted passwords, such as the enable secret passwords, the passwords must be replaced after recovery. Depending on the device, the detailed procedure for password recovery varies; however, all the password recovery procedures follow the same principle:

Step 1. Enter the ROMMON mode.

Step 2. Change the configuration register to 0x2142 to ignore the startup config file.

Step 3. Make necessary changes to the original startup config file.

Step 4. Save the new configuration.

Console access to the device through a terminal or terminal emulator software on a PC is required for password recovery. The terminal settings to access the device are:

9600 baud rate

No parity

8 data bits

1 stop bit

No flow control

With console access, a user can access the ROMMON mode by using a break sequence during the boot up process or removing the external flash memory when the device is powered off.

Note: The break sequence for PuTTY is Ctrl+Break. A list of standard break key sequences for other terminal emulators and operating systems can be found at: http://www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/12818-61.html

The ROMMON software supports some basic commands, such as confreg. The confreg 0x2142 command allows the user to set the configuration register to 0x2142. With the configuration register at 0x2142, the device will ignore the startup config file during startup. The startup config file is where the forgotten passwords are stored. After setting the configuration register to 0x2142, type reset at the prompt to restart the device. Enter the break sequence while the device is rebooting and decompressing the IOS. Figure 1 displays the terminal output of a 1941 router in the ROMMON mode after using a break sequence during the boot up process.

After the device has finished reloading, copy the startup config to the running config, as displayed in Figure 2.

```
Router# copy startup-config running-config
Destination filename [running-config]?

1450 bytes copied in 0.156 secs (9295 bytes/sec)
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# enable secret cisco
Router(config)# config-register 0x2102
Router(config)# end
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
```

CAUTION: Do *not* enter copy running-config startup-config. This command erases your original startup configuration.

Because you are in privileged EXEC mode, you can now configure all the necessary passwords. After

the new passwords are configured, change the configuration register back to 0x2102 using the config-register 0x2102 command in the global configuration mode. Save the running-config to startup-config and reload the device, as shown in Figure 2.

Note: The password cisco is not a strong password and is used here only as an example.

The device now uses the newly configured passwords for authentication. Be sure to use show commands to verify that all the configurations are still in place. For example, verify that the appropriate interfaces are not shut down after password recovery.

The following link provides detailed instructions for password recovery procedure for a specific device: http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/6130-index.html

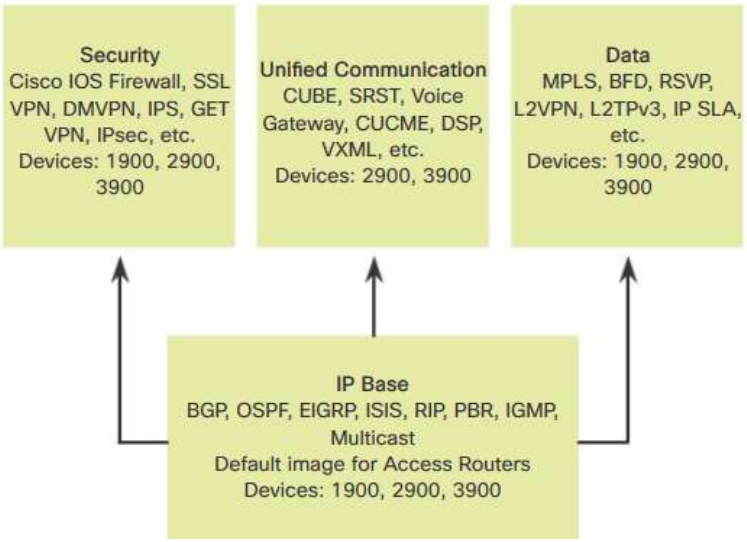
IOS 15 System Image Packaging

Cisco Integrated Services Routers Generation Two (ISR G2) 1900, 2900, and 3900 Series support services on demand through the use of software licensing. The Services on Demand process enables customers to realize operational savings through ease of software ordering and management. When an order is placed for a new ISR G2 platform, the router is shipped with a single universal Cisco IOS Software image and a license is used to enable the specific feature set packages, as shown in Figure 1.

There are two types of universal images supported in ISR G2:

Universal images with the “universalk9" designation in the image name - This universal image offers all of the Cisco IOS Software features, including strong payload cryptography features, such as IPsec VPN, SSL VPN, and Secure Unified Communications.

Universal images with the “universalk9_npe" designation in the image name - The strong enforcement of encryption capabilities provided by Cisco Software Activation satisfies requirements for the export of encryption capabilities. However, some countries have import requirements that require that the platform does not support any strong cryptography functionality, such as payload cryptography. To satisfy the import requirements of those countries, the npe universal image does not support any strong payload encryption.



With the ISR G2 devices, IOS image selection has been made easier because all features are included within the universal image. Features are activated through licensing. Each device ships with Universal image. The technology packages IP Base, Data, UC (Unified Communications), and SEC (Security), are enabled in the universal image using Cisco Software Activation licensing keys. Each licensing key is unique to a particular device and is obtained from Cisco by providing the product ID and serial number of the router and a Product Activation Key (PAK). The PAK is provided by Cisco at the time of software purchase. The IP Base is installed by default.

IOS Image Filenames

When selecting or upgrading a Cisco IOS router, it is important to choose the proper IOS image with the correct feature set and version. The Cisco IOS image file is based on a special naming convention. The name for the Cisco IOS image file contains multiple parts, each with a specific meaning. It is important to understand this naming convention when upgrading and selecting a Cisco IOS Software.

```
R1# show flash0:
-# - --length-- -----date/time------ path


8   68831808   Apr 2 2013 21:29:58 +00:00  c1900-
universalk9-mz.SPA.152-4.M3.bin

182394880 bytes available (74092544 bytes used)

R1#
```

As shown in Figure 1, the show flash command displays the files stored in flash memory, including the system image files.

Figure 2 illustrates the different parts of an IOS 15 system image file on an ISR G2 device:

Image Name (c1900) - Identifies the platform on which the image runs. In this example, the platform is a Cisco 1900 router.

universalk9 - Specifies the image designation. The two designations for an ISR G2 are universalk9 and

universalk9_npe. Universalk9_npe does not contain strong encryption and is meant for countries with encryption restrictions. Features are controlled by licensing and can be divided into four technology packages. These are IP Base, Security, Unified Communications, and Data.

mz - Indicates where the image runs and if the file is compressed. In this example, mz indicates that the file runs from RAM and is compressed.

SPA - Designates that file is digitally signed by Cisco.

152-4.M3 - Specifies the filename format for the image 15.2(4)M3. This is the version of IOS, which includes the major release, minor release, maintenance release, and maintenance rebuild numbers. The M indicates this is an extended maintenance release.

bin - The file extension. This extension indicates that this file is a binary executable file.

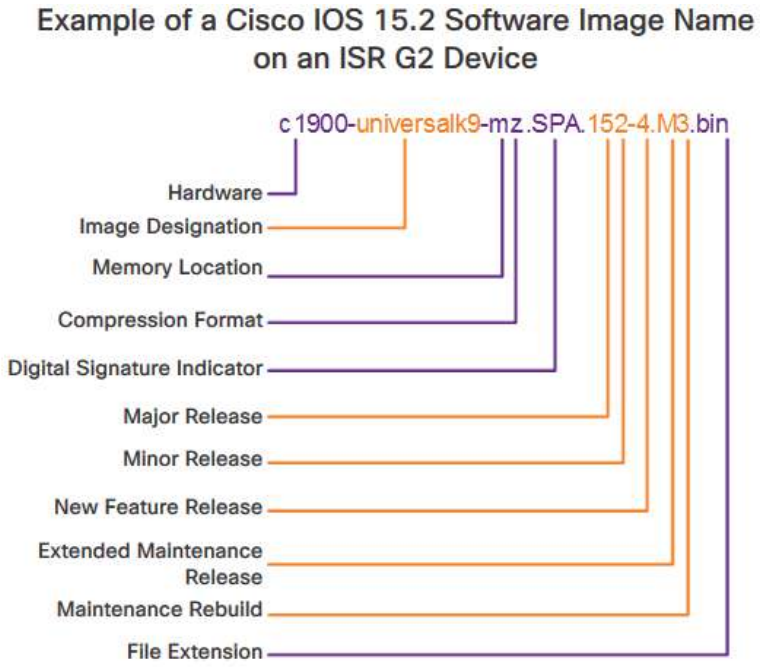
The most common designation for memory location and compression format is mz. The first letter indicates the location where the image is executed on the router. The locations can include:

f - flash

m - RAM

r - ROM

l - relocatable



The compression format can be either z for zip or x for mzip. Zipping is a method Cisco uses to compress some run-from-RAM images that is effective in reducing the size of the image. It is self-unzipping, so when the image is loaded into RAM for execution, the first action is to unzip.

Note: The Cisco IOS Software naming conventions, field meaning, image content, and other details are subject to change.

Memory Requirements

On most Cisco routers including the integrated services routers, the IOS is stored in compact flash as a

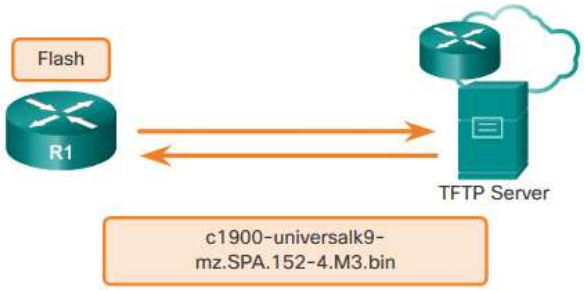
compressed image and loaded into DRAM during boot-up. The Cisco IOS Software Release 15.0 images available for the Cisco 1900 and 2900 ISR require 256MB of flash and 512MB of RAM. The 3900 ISR requires 256MB of flash and 1GB of RAM. This does not include additional management tools such as Cisco Configuration Professional (Cisco CP). For complete details, refer to the product data sheet for the specific router.

Review questions

See the practical attachment

TFTP Servers as a Backup Location

As a network grows, Cisco IOS Software images and configuration files can be stored on a central TFTP server. This helps to control the number of IOS images and the revisions to those IOS images, as well as the configuration files that must be maintained.



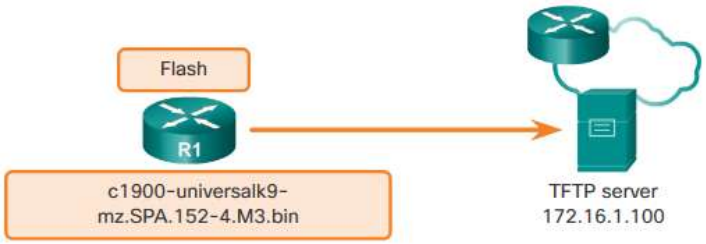
Production internetworks usually span wide areas and contain multiple routers. For any network, it is good practice to keep a backup copy of the Cisco IOS Software image in case the system image in the router becomes corrupted or accidentally erased.

Widely distributed routers need a source or backup location for Cisco IOS Software images. Using a network TFTP server allows image and configuration uploads and downloads over the network. The network TFTP server can be another router, a workstation, or a host system.

Steps to Backup IOS Image to TFTP Server

To maintain network operations with minimum down time, it is necessary to have procedures in place for backing up Cisco IOS images. This allows the network administrator to quickly copy an image back to a router in case of a corrupted or erased image.

In Figure 1, the network administrator wants to create a backup of the current image file on the router (c1900-universalk9-mz.SPA.152-4.M3.bin) to the TFTP server at 172.16.1.100.



To create a backup of the Cisco IOS image to a TFTP server, perform the following three steps:

Step 1. Ensure that there is access to the network TFTP server. Ping the TFTP server to test connectivity, as shown in Figure 2.

Verify connectivity to the server.

```
R1# ping 172.16.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 56/56/56 ms
```

Verify the image size.

```
R1# show flash0:
-# - --length-- -----date/time------ path
8   68831808   Apr 2 2013 21:29:58  +00:00
                        c1900-universalk9-mz.SPA.152-4.M3.bin
<output omitted>
```

Step 2. Verify that the TFTP server has sufficient disk space to accommodate the Cisco IOS Software image. Use the show flash0: command on the router to determine the size of the Cisco IOS image file. The file in the example is 68831808 bytes long.

Copy image to TFTP server.

```
R1# copy flash0: tftp:
Source filename []? c1900-universalk9-mz.SPA.152-4.M3.bin
Address or name of remote host []? 172.16.1.100
Destination filename [c1900-universalk9-mz.SPA.152-4.M3.bin]?
Writing c1900-universalk9-mz.SPA.152-4.M3.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
68831808 bytes copied in 363.468 secs (269058 bytes/sec)
```

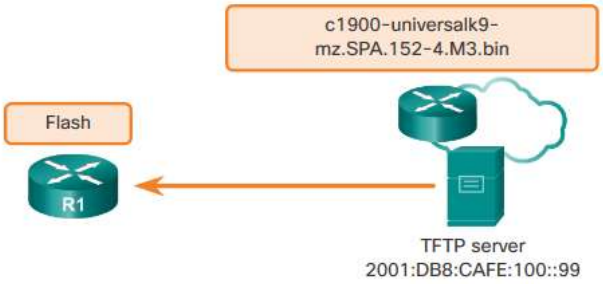
Step 3. Copy the image to the TFTP server using the copy *source-url destination-url* command, as shown in Figure 3.

After issuing the command using the specified source and destination URLs, the user is prompted for the source file name, IP address of the remote host, and destination file name. The transfer will then begin.

Steps to Copy an IOS Image to a Device

Cisco consistently releases new Cisco IOS software versions to resolve caveats and provide new features. This example uses IPv6 for the transfer to show that TFTP can also be used across IPv6 networks.

Figure 1 illustrates copying a Cisco IOS software image from a TFTP server. A new image file (c1900-universalk9-mz.SPA.152-4.M3.bin) will be copied from the TFTP server at 2001:DB8:CAFE:100::99 to the router.



Follow these steps to upgrade the software on the Cisco router:

Step 1. Select a Cisco IOS image file that meets the requirements in terms of platform, features, and software. Download the file from cisco.com and transfer it to the TFTP server.

Step 2. Verify connectivity to the TFTP server. Ping the TFTP server from the router. The output in Figure 2 shows the TFTP server is accessible from the router.

Verify connectivity to the server.

```
R1# ping 2001:DB8:CAFE:100::99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:CAFE:100::99,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 56/56/56 ms
```

Step 3. Ensure that there is sufficient flash space on the router that is being upgraded. The amount of free flash can be verified using the show flash0: command. Compare the free flash space with the new image file size. The show flash0: command in Figure 3 is used to verify free flash size. Free flash space in the example is 182,394,880 bytes.

Verify free flash size.

```
R1# show flash0:
-# - --length-- -----date/time------ path
 <output omitted>

 182394880 bytes available (74092544 bytes used)

R1#
```

Step 4. Copy the IOS image file from the TFTP server to the router using the copy command shown in Figure 4. After issuing this command with specified source and destination URLs, the user will be prompted for IP address of the remote host, source file name, and destination file name. The transfer of the file will begin.

Copy image from TFTP server.

```
R1# copy tftp: flash0:
Address or name of remote host []? 2001:DB8:CAFE:100::99
Source filename []? c1900-universalk9-mz.SPA.152-4.M3.bin
Destination filename []?
c1900-universalk9-mz.SPA.152-4.M3.bin
Accessing tftp://2001:DB8:CAFE:100::99/c1900-universalk9-
mz.SPA.152-4.M3.bin...
Loading c1900-universalk9-mz.SPA.152-4.M3.bin
from 2001:DB8:CAFE:100::99 (via
GigabitEthernet0/0): !!!!!!!!!!!!!!!!!!!
<output omitted>
[OK - 68831808 bytes]
68831808 bytes copied in 368.128 secs (265652 bytes/sec)
```

The boot system Command

Set the image to boot and reload the system.

```
R1# configure terminal
R1(config)# boot system
            flash0://c1900-universalk9-mz.SPA.152-4.M3.bin
R1(config)# exit
R1# copy running-config startup-config
R1# reload
```

To upgrade to the copied IOS image after that image is saved on the router's flash memory, configure the router to load the new image during bootup using the boot system command, as shown in Figure 1. Save the configuration. Reload the router to boot the router with new image. After the router has booted, to verify the new image has loaded, use the show version command, as shown in Figure 2.

```
R1# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M),
Version 15.2(4)M3, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Tue 26-Feb-13 02:11 by prod_rel_team

ROM:System Bootstrap, Version 15.0(1r)M15,RELEASE SOFTWARE
(fc1)

R1 uptime is 1 hour, 2 minutes
System returned to ROM by power-on
System image file is "flash0:
c1900-universalk9-mz.SPA.152-4.M3.bin"
```

During startup, the bootstrap code parses the startup configuration file in NVRAM for the boot system commands that specify the name and location of the Cisco IOS Software image to load. Several boot system commands can be entered in sequence to provide a fault-tolerant boot plan.

If there are no boot system commands in the configuration, the router defaults to loading the first valid Cisco IOS image in flash memory and running it.

Review questions

See the practical attachment

LEARNING UNIT 3 - IMPLEMENT VLAN

Learning Outcomes:	Configure a VLAN Configure a VTP Configure a switchport modes (access and trunk) Implement inter-VLAN routing Apply Spanning Tree Protocol Configure a switchport security Apply First Hop Redundancy Protocols and link Aggregationmodes
Learning hours:	20 Hours

Learning Outcome 3.1: Configure VLAN

VLANs

Network performance is an important factor in the productivity of an organization. One of the technologies used to improve network performance is the separation of large broadcast domains into smaller ones. By design, routers will block broadcast traffic at an interface. However, routers normally have a limited number of LAN interfaces. A router's primary role is to move information between networks, not to provide network access to end devices.

The role of providing access into a LAN is normally reserved for an access layer switch. A virtual local area network (VLAN) can be created on a Layer 2 switch to reduce the size of broadcast domains, similar to a Layer 3 device. VLANs are commonly incorporated into network design making it easier for a network to support the goals of an organization. While VLANs are primarily used within switched local area networks, modern implementations of VLANs allow them to span MANs and WANs.

Because VLANs segment the network, a Layer 3 process is required to allow traffic to move from one network segment to another.

This Layer 3 routing process can either be implemented using a router or a Layer 3 switch interface. The use of a Layer 3 device provides a method for controlling the flow of traffic between network segments, including network segments created by VLANs.

Benefits of VLANs

User productivity and network adaptability are important for business growth and success. VLANs make it easier to design a network to support the goals of an organization. The primary benefits of using VLANs are as follows:

Security - Groups that have sensitive data are separated from the rest of the network, decreasing the chances of confidential information breaches. As shown in the figure, faculty computers are on VLAN 10 and completely separated from student and guest data traffic.

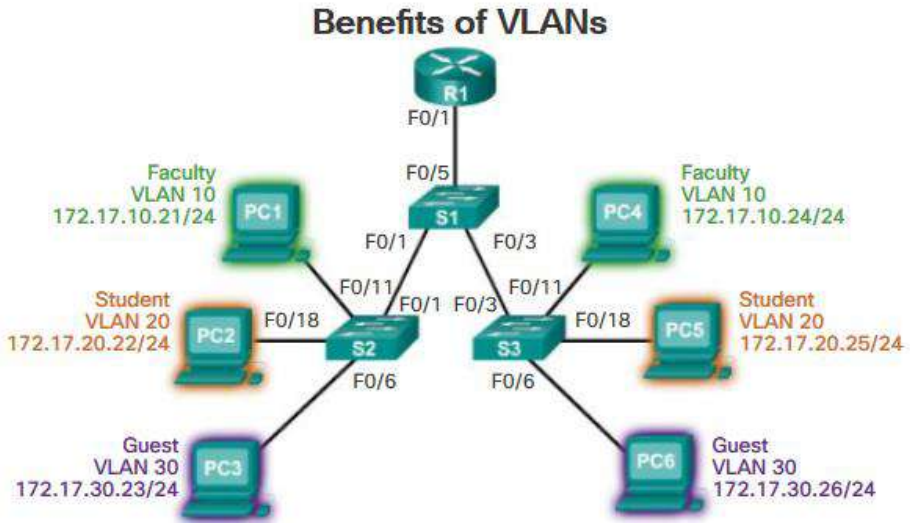
Cost reduction - Cost savings result from reduced need for expensive network upgrades and more efficient use of existing bandwidth and uplinks.

Better performance - Dividing flat Layer 2 networks into multiple logical workgroups (broadcast domains) reduces unnecessary traffic on the network and boosts performance.

Reduce the size of broadcast domains - Dividing a network into VLANs reduces the number of devices in the broadcast domain. As shown in the figure, there are six computers on this network but there are three broadcast domains: Faculty, Student, and Guest.

Improved IT staff efficiency - VLANs make it easier to manage the network because users with similar network requirements share the same VLAN. When a new switch is provisioned, all the policies and procedures already configured for the particular VLAN are implemented when the ports are assigned. It is also easy for the IT staff to identify the function of a VLAN by giving it an appropriate name. In the figure, for easy identification VLAN 10 has been named “Faculty”, VLAN 20 is named “Student”, and VLAN 30 “Guest.”

Simpler project and application management - VLANs aggregate users and network devices to support business or geographic requirements. Having separate functions makes managing a project or working with a specialized application easier; an example of such an application is an e-learning development platform for faculty.



Types of VLANs

There are a number of distinct types of VLANs used in modern networks. Some VLAN types are defined by traffic classes. Other types of VLANs are defined by the specific function that they serve.

Data VLAN

A data VLAN is a VLAN that is configured to carry user-generated traffic. A VLAN carrying voice or management traffic would not be a data VLAN. It is common practice to separate voice and

management traffic from data traffic. A data VLAN is sometimes referred to as a user VLAN. Data VLANs are used to separate the network into groups of users or devices.

Default VLAN

All switch ports become a part of the default VLAN after the initial boot up of a switch loading the default configuration. Switch ports that participate in the default VLAN are part of the same broadcast domain. This allows any device connected to any switch port to communicate with other devices on other switch ports. The default VLAN for Cisco switches is VLAN 1. In the figure, the show vlan brief command was issued on a switch running the default configuration. Notice that all ports are assigned to VLAN 1 by default.

VLAN 1 has all the features of any VLAN, except it cannot be renamed or deleted. By default, all Layer 2 control traffic is associated with VLAN 1.

Native VLAN

A native VLAN is assigned to an 802.1Q trunk port. Trunk ports are the links between switches that support the transmission of traffic associated with more than one VLAN. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic), as well as traffic that does not come from a VLAN (untagged traffic). Tagged traffic refers to traffic that has a 4-byte tag inserted within the original Ethernet frame header, specifying the VLAN to which the frame belongs. The 802.1Q trunk port places untagged traffic on the native VLAN, which by default is VLAN 1.

Native VLANs are defined in the IEEE 802.1Q specification to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. A native VLAN serves as a common identifier on opposite ends of a trunk link.

It is a best practice to configure the native VLAN as an unused VLAN, distinct from VLAN 1 and other VLANs. In fact, it is not unusual to dedicate a fixed VLAN to serve the role of the native VLAN for all trunk ports in the switched domain.

Management VLAN

A management VLAN is any VLAN configured to access the management capabilities of a switch. VLAN 1 is the management VLAN by default. To create the management VLAN, the switch virtual interface (SVI) of that VLAN is assigned an IP address and a subnet mask, allowing the switch to be managed via HTTP, Telnet, SSH, or SNMP. Because the out-of-the-box configuration of a Cisco switch has VLAN 1 as the default VLAN, VLAN 1 would be a bad choice for the management VLAN.

In the past, the management VLAN for a 2960 switch was the only active SVI. On 15.x versions of the Cisco IOS for Catalyst 2960 Series switches, it is possible to have more than one active SVI. Cisco IOS 15.x requires that the particular active SVI assigned for remote management be documented. While theoretically a switch can have more than one management VLAN, having more than one increases exposure to network attacks.

Voice VLANs

A separate VLAN is needed to support Voice over IP (VoIP). VoIP traffic requires:

Assured bandwidth to ensure voice quality

Transmission priority over other types of network traffic

Ability to be routed around congested areas on the network

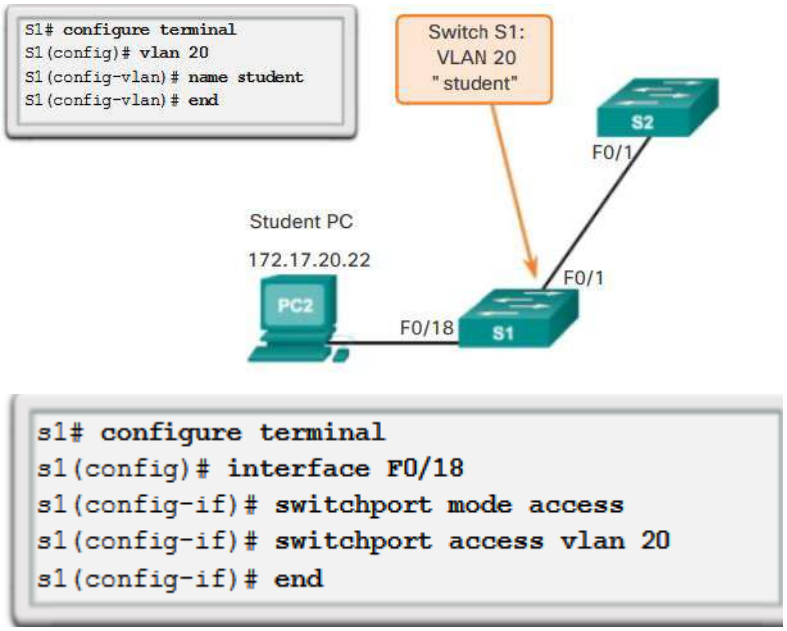
Delay of less than 150 ms across the network

VLAN Trunks

A trunk is a point-to-point link between two network devices that carries more than one VLAN. A VLAN trunk extends VLANs across an entire network. Cisco supports IEEE 802.1Q for coordinating trunks on Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces.

VLANs would not be very useful without VLAN trunks. VLAN trunks allow all VLAN traffic to propagate between switches, so that devices which are in the same VLAN, but connected to different switches, can communicate without the intervention of a router.

A VLAN trunk does not belong to a specific VLAN; rather, it is a conduit for multiple VLANs between switches and routers. A trunk could also be used between a network device and server or other device that is equipped with an appropriate 802.1Q-capable NIC. By default, on a Cisco Catalyst switch, all VLANs are supported on a trunk port.




```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```

VLAN Ranges on Catalyst Switches

Different Cisco Catalyst switches support various numbers of VLANs. The number of supported VLANs is large enough to accommodate the needs of most organizations. For example, the Catalyst 2960 and 3560 Series switches support over 4,000 VLANs. Normal range VLANs on these switches are numbered 1 to 1,005 and extended range VLANs are numbered 1,006 to 4,094. Figure 1 illustrates the available VLANs on a Catalyst 2960 switch running Cisco IOS Release 15.x. Figure 2 shows the features of normal range and extended range VLANs.

Normal Range VLANs

Used in small- and medium-sized business and enterprise networks.

Identified by a VLAN ID between 1 and 1005.

IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs.

IDs 1 and 1002 to 1005 are automatically created and cannot be removed.

Configurations are stored within a VLAN database file, called vlan.dat. The vlan.dat file is located in the flash memory of the switch.

The VLAN Trunking Protocol (VTP), which helps manage VLAN configurations between switches, can only learn and store normal range VLANs.

Extended Range VLANs

Enable service providers to extend their infrastructure to a greater number of customers. Some global enterprises could be large enough to need extended range VLAN IDs.

Are identified by a VLAN ID between 1006 and 4094. Configurations are not written to the vlan.dat file.

Support fewer VLAN features than normal range VLANs. Are, by default, saved in the running configuration file. VTP does not learn extended range VLANs.

Note: 4096 is the upper boundary for the number of VLANs available on Catalyst switches, because there are 12 bits in the VLAN ID field of the IEEE 802.1Q header.

Creating a VLAN

When configuring normal range VLANs, the configuration details are stored in flash memory on the switch in a file called vlan.dat. Flash memory is persistent and does not require the copy running-config startup-config command. However, because other details are often configured on a Cisco switch at the same time that VLANs are created, it is good practice to save running configuration changes to the startup configuration file.

Figure 1 displays the Cisco IOS command syntax used to add a VLAN to a switch and give it a name. Naming each VLAN is considered a best practice in switch configuration.

The student VLAN (VLAN 20) is configured on switch S1. In the topology example, notice that the student computer (PC2) has been an assigned an IP address that is appropriate for VLAN 20, but the port to which the PC attaches has not been associated with a VLAN yet.to create a VLAN and use the show vlan brief command to display the contents of the vlan.dat file.

In addition to entering a single VLAN ID, a series of VLAN IDs can be entered separated by commas, or a range of VLAN IDs separated by hyphens using the vlan *vlan-id* command. For example, use the following command to create VLANs 100, 102, 105, 106, and 107:

S1(config)# **vlan 100,102,105-107**

Note: For a Catalyst switch, the erase startup-config command must accompany the delete vlan.dat command prior to reload to restore the switch to its factory default condition.

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```

Review questions

See the practical attachment

Learning Outcome 3.2: configure VTP

VTP

As the number of switches increases on a small- or medium-sized business network, the overall administration required to manage VLANs and trunks in a network becomes a challenge. In larger networks, VLAN management can become daunting. Assume VLANs 10, 20, and 99 have already been implemented and you must now add VLAN 30 to all switches. Manually adding the VLAN in this network would consist of configuring 12 switches.

VLAN trunking protocol (VTP) allows a network administrator to manage VLANs on a switch configured as a VTP server. The VTP server distributes and synchronizes VLAN information over trunk links to VTP-enabled switches throughout the switched network. This minimizes the problems caused by incorrect configurations and configuration inconsistencies.

Note: VTP only learns about normal-range VLANs (VLAN IDs 1 to 1005). Extended-range VLANs (IDs greater than 1005) are not supported by VTP version 1 or version 2. VTP version 3 does support extended VLANs, but is beyond the scope of this course.

Note: VTP stores VLAN configurations in a database called vlan.dat.

VTP Components	Definition
VTP Domain	• Consists of one or more interconnected switches. • All switches in a domain share VLAN configuration details using VTP advertisements. • Switches that are in different VTP domains do not exchange VTP messages. • A router or Layer 3 switch defines the boundary of each domain.
VTP Advertisements	• Each switch in the VTP domain sends periodic global configuration advertisements from each trunk port to a reserved multicast address. • Neighboring switches receive these advertisements and update their VTP and VLAN configurations as necessary.
VTP Modes	A switch can be configured in one of three VTP modes: server, client, or transparent.
VTP Password	Switches in the VTP domain can be also be configured with a password.

VTP Advertisements

VTP includes three types of advertisements:

Summary advertisements - These inform adjacent switches of VTP domain name and configuration revision number.

Advertisement request - These are in response to a summary advertisement message when the summary advertisement contains a higher configuration revision number than the current value.

Subset advertisements - These contain VLAN information including any changes.

By default, Cisco switches issue summary advertisements every five minutes. Summary advertisements inform adjacent VTP switches of the current VTP domain name and the configuration revision number. The configuration revision number is a 32-bit number that indicates the level of revision for a VTP packet. Each VTP device tracks the VTP configuration revision number that is assigned to it.

This information is used to determine whether the received information is more recent than the current version. Each time that you make a VLAN change in a VTP device, the configuration revision is

incremented by one.

Note: To reset a configuration revision on a switch, change the VTP domain name, and then change the name back to the original name.

When the switch receives a summary advertisement packet, the switch compares the VTP domain name to its own VTP domain name. If the name is different, the switch simply ignores the packet. If the name is the same, the switch then compares the configuration revision to its own revision. If its own configuration revision number is higher or equal to the packet's configuration revision number, the packet is ignored. If its own configuration revision number is lower, an advertisement request is sent asking for the subset advertisement message.

The subset advertisement message contains the VLAN information with any changes. When you add, delete, or change a VLAN on the VTP server, the VTP server increments the configuration revision and issues a summary advertisement. One or several subset advertisements follow the summary advertisement containing the VLAN information including any changes. This process is shown in the figure.

VTP Versions

VTP Version 1 and Version 2 are described in the figure. Switches in the same VTP domain must use the same VTP version.

Note: VTPv2 is not much different than VTPv1 and is generally only configured if legacy Token Ring support is required. The newest version of VTP is Version 3. However, VTP Version 3 is beyond the scope of this course.

VTP Version	Definition
VTP Version 1	• Default VTP mode on all switches. • Supports normal range VLANs only.
VTP Version 2	• Supports normal range VLANs only. • Supports legacy Token Ring networks. • Supports advanced features including unrecognized Type-Length-Value (TLV), version-dependent transparent mode, and consistency checks.

Default VTP configuration

The show vtp status privileged EXEC command displays the VTP status. Executing the command on a Cisco 2960 Plus Series switch generates the output shown in the figure.

The following briefly describes the command output for the show vtp status parameters.

VTP Version capable and running

Displays the VTP version that the switch is capable of running and the version that it is currently running.

By default, switches implement version 1.

Most switches support version 2 while newer switches also support version 3.

VTP Domain Name

Name that identifies the administrative domain for the switch.By default, the VTP domain name is NULL.

VTP Pruning Mode

Displays whether pruning is enabled or disabled.By default, VTP pruning is disabled.

VTP Traps Generation

Displays whether VTP traps are sent to a network management station. By default, VTP traps are disabled.

Device ID

The switch MAC address.

Configuration Last Modified

Date and time of the last configuration modification.

Displays the IP address of the switch that caused the configuration change to the database.

VTP Operating Mode

Can be server, client, or transparent.

By default, a switch is in VTP server mode.

Maximum VLANs Supported Locally

The number of VLANs supported varies across switch platforms.

Number of Existing VLANs

Includes the number of default and configured VLANs.

The default number of existing VLANs varies across switch platforms.

Configuration Revision

Current configuration revision number on this switch.

The revision number is a 32-bit number that indicates the level of revision for a VTP frame.

The default configuration number for a switch is zero.

Each time a VLAN is added or removed, the configuration revision number is incremented.

Each VTP device tracks the VTP configuration revision number that is assigned to it.

MD5 Digest

A 16-byte checksum of the VTP configuration.

VTP Configuration Overview

Complete the following steps to configure VTP:

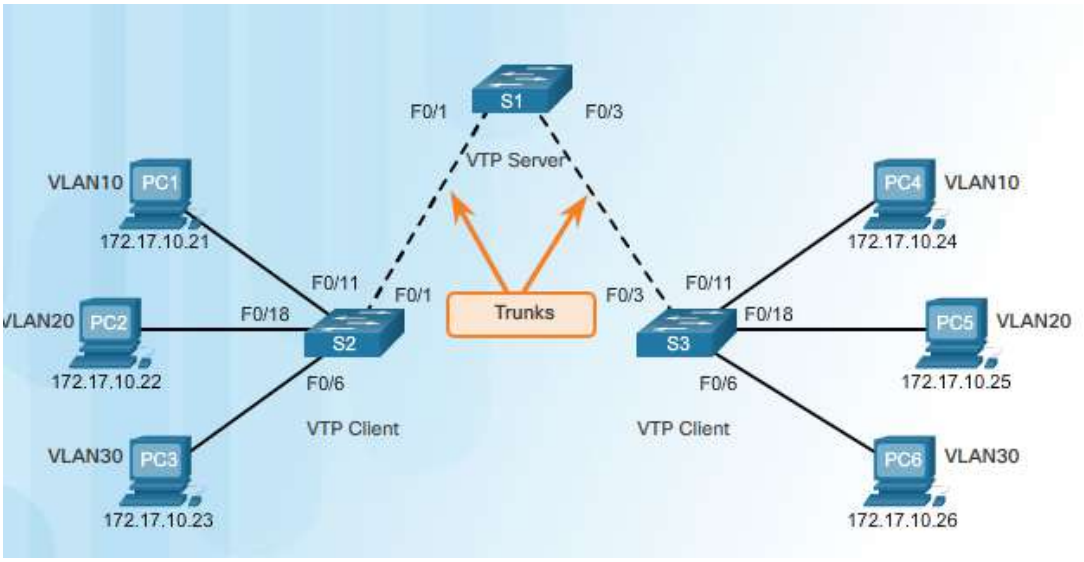
Step 1: Configure the VTP Server

Step 2: Configure the VTP Domain Name and Password

Step 3: Configure the VTP Clients

Step 4: Configure VLANs on the VTP Server

Step 5: Verify the VTP Clients Have Received the New VLAN Information



The figure shows the reference topology used in this section for configuring and verifying a VTP implementation. Switch S1 will be the VTP server while S2 and S3 will be clients.

The domain name is configured using the vtp domain *domain-name* global configuration command. In Figure 1, the domain name is configured as CCNA on S1. S1 will then send out a VTP advertisement to S2 and S3. If S2 and S3 have the default configuration with the NULL domain name, then both switches will accept CCNA as the new VTP domain name. A VTP client must have the same domain name as the VTP server before it will accept VTP advertisements.

For security reasons, a password should be configured using the vtp password *password* command. the VTP domain password is set to cisco12345. All switches in the VTP domain must use the same VTP domain password.Verify the VTP password using the show vtp password command.

Configure the VTP Clients

Configure S2 and S3 as VTP clients in the CCNA domain using the VTP password cisco12345. The configuration for S2.

```
S2(config)# vtp mode client
Setting device to VTP Client mode for VLANS.
S2(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
*Mar 1 00:12:22.484: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to CC
S2(config)# vtp password cisco12345
Setting device VTP password to cisco12345
S2(config)#
```

Assigning Ports to VLANs

After creating a VLAN, the next step is to assign ports to the VLAN. An access port can belong to only one VLAN at a time; one exception to this rule is that of a port connected to an IP phone, in which case, there are two VLANs associated with the port: one for voice and one for data. The switchport mode access command is optional, but strongly recommended as a security best practice. With this command, the interface changes to permanent access mode.

Note: Use the interface range command to simultaneously configure multiple interfaces.

The switchport access vlan command forces the creation of a VLAN if it does not already exist on the switch. For example, VLAN 30 is not present in the show vlan brief output of the switch. If the switchport access vlan 30 command is entered on any interface with no previous configuration, then the switch displays the following:% Access VLAN does not exist. Creating vlan 30

Cisco Switch IOS Commands

Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Set the port to access mode.	`S1(config-if)# switchport mode access`
Assign the port to a VLAN.	`S1(config-if)# switchport access vlan vlan_id`
Return to the privileged EXEC mode.	`S1(config-if)# end`

Review questions

See the practical attachment

Learning Outcome 3.3: Configure switchport modes (access and trunk)

VTP Mode	Definition
VTP Server	• VTP servers advertise the VTP domain VLAN information to other VTP-enabled switches in the same VTP domain. • VTP servers store the VLAN information for the entire domain in NVRAM. • Switches configured in VTP server mode are allowed to create, delete, or rename VLANs for the domain.
VTP Client	• VTP clients function the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client. • A VTP client only stores the VLAN information for the entire domain while the switch is on. • A switch reset deletes the VLAN information. • You must configure VTP client mode on a switch.
VTP Transparent	• Transparent switches do not participate in VTP except to forward VTP advertisements to VTP clients and VTP servers. • VLANs that are created, renamed, or deleted on transparent switches are local to that switch only. • To create an extended VLAN, a switch must be configured as a VTP transparent switch when using VTP versions 1 or 2.

VTP Question	VTP Server	VTP Client	VTP Transparent
What are the differences?	• Manages domain and VLAN configuration. • Multiple VTP servers can be configured.	• Updates local VTP configurations. • VTP client switches cannot change VLAN configurations.	• Manages local VLAN configurations. • VLAN configurations are not shared with VTP network.
Does it respond to VTP advertisements?	Participates fully	Participates fully	Only forwards VTP advertisements
Is the global VLAN configuration preserved on restart?	Yes, global configurations are stored in NVRAM	No, global configurations are stored in RAM only	No, local VLAN configuration is only stored in NVRAM
Does it update other VTP-enabled switches?	Yes	Yes	No

Learning Outcome 3.4: Implement inter-VLAN routing

What is Inter-VLAN Routing?

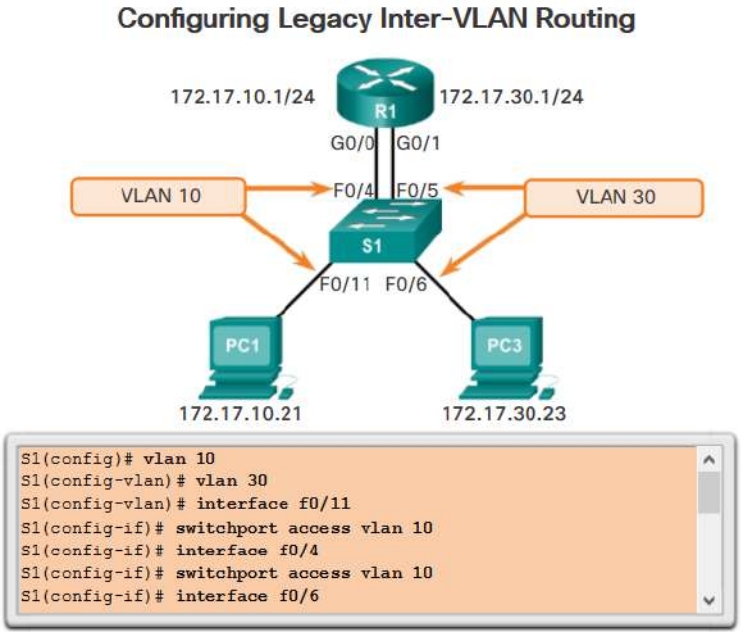
VLANs are used to segment switched networks. Layer 2 switches, such as the Catalyst 2960 Series, can be configured with over 4,000 VLANs. A VLAN is a broadcast domain, so computers on separate VLANs are unable to communicate without the intervention of a routing device. Layer 2 switches have very limited IPv4 and IPv6 functionality and cannot perform the dynamic routing function of routers. While Layer 2 switches are gaining more IP functionality, such as the ability to perform static routing, this is insufficient to handle these large number of VLANs.

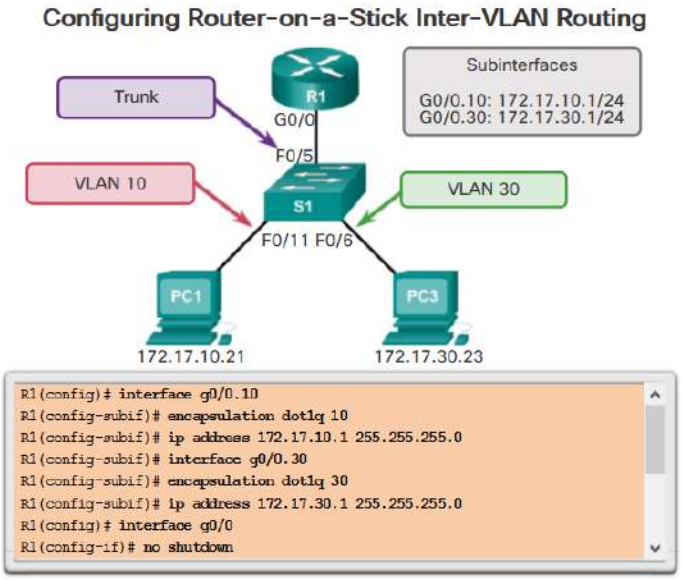
Any device that supports Layer 3 routing, such as a router or a multilayer switch, can be used to perform the necessary routing functionality. Regardless of the device used, the process of forwarding network traffic from one VLAN to another VLAN using routing is known as inter-VLAN routing.

There are three options for inter-VLAN routing :

- Legacy inter-VLAN routing
- Router-on-a-Stick
- Layer 3 switching using SVIs

Note: This chapter focuses on the first two options. Layer 3 switching using SVIs is beyond the scope of this course.





Learning Outcome 3.5: Apply Spanning Tree Protocol

Redundancy at OSI Layers 1 and 2

The three-tier hierarchical network design that uses core, distribution, and access layers with redundancy, attempts to eliminate a single point of failure on the network. Multiple cabled paths between switches provide physical redundancy in a switched network. This improves the reliability and availability of the network. Having alternate physical paths for data to traverse the network makes it possible for users to access network resources, despite path disruption.

PC1 is communicating with PC4 over a redundant network topology.

When the network link between S1 and S2 is disrupted, the path between PC1 and PC4 is automatically adjusted by the Spanning Tree Protocol (STP) to compensate for the disruption.

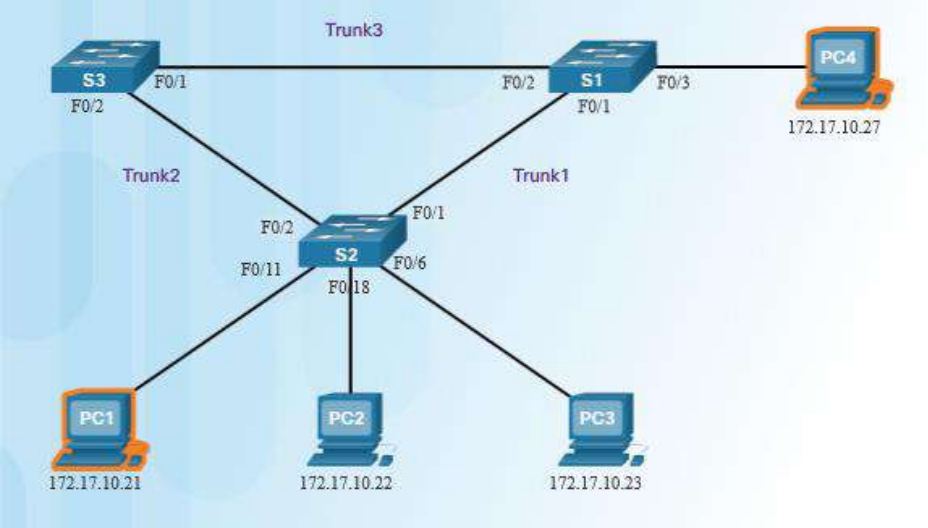
When the network connection between S1 and S2 is restored, the path is then readjusted by STP to route traffic directly from S2 to S1 to get to PC4.

For many organizations, the availability of the network is essential to supporting business needs; therefore, the network infrastructure design is a critical business element. Path redundancy provides the necessary availability of multiple network services by eliminating the possibility of a single point of failure.

Note: The OSI Layer 1 redundancy is illustrated using multiple links and devices, but more than just physical planning is required to complete the network setup. For the redundancy to work in a systematic way, the use of OSI Layer 2 protocols, such as STP, is also required.

Redundancy is an important part of the hierarchical design for preventing disruption of network services to users. Redundant networks require the addition of physical paths, but logical redundancy must also be part of the design. However, redundant paths in a switched Ethernet network may cause both physical and logical Layer 2 loops.

Logical Layer 2 loops may occur due to the natural operation of switches, specifically, the learning and forwarding process. When multiple paths exist between two devices on a network, and there is no spanning tree implementation on the switches, a Layer 2 loop occurs.



Issues with Layer 1 Redundancy: MAC Database Instability

Ethernet frames do not have a time to live (TTL) attribute. As a result, if there is no mechanism enabled to block continued propagation of these frames on a switched network, they continue to propagate between switches endlessly, or until a link is disrupted and breaks the loop. This continued propagation between switches can result in MAC database instability. This can occur due to broadcast frames forwarding.

Broadcast frames are forwarded out all switch ports, except the original ingress port. This ensures that all devices in a broadcast domain are able to receive the frame. If there is more than one path for the frame to be forwarded out of, an endless loop can result. When a loop occurs, it is possible for the MAC address table on a switch to constantly change with the updates from the broadcast frames, which results in MAC database instability.

PC1 sends a broadcast frame to S2. S2 receives the broadcast frame on F0/11. When S2 receives the broadcast frame, it updates its MAC address table to record that PC1 is available on port F0/11.

Because it is a broadcast frame, S2 forwards the frame out all ports, including Trunk1 and Trunk2. When the broadcast frame arrives at S3 and S1, the switches update their MAC address tables to indicate that PC1 is available out port F0/1 on S1 and out port F0/2 on S3.

Because it is a broadcast frame, S3 and S1 forward the frame out all ports, except the ingress port. S3 sends the broadcast frame from PC1 to S1. S1 sends the broadcast frame from PC1 to S3. Each switch updates its MAC address table with the incorrect port for PC1.

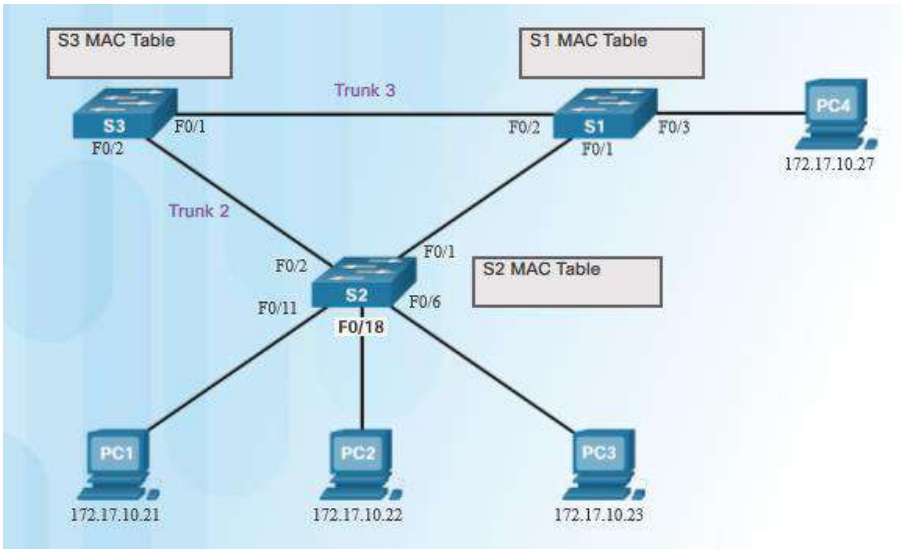
Each switch forwards the broadcast frame out all of its ports, except the ingress port, which results in both switches forwarding the frame to S2.

When S2 receives the broadcast frames from S3 and S1, the MAC address table is updated with the last entry received from the other two switches.

This process repeats over and over again until the loop is broken by physically disconnecting the connections that are causing the loop or powering down one of the switches in the loop. This creates a

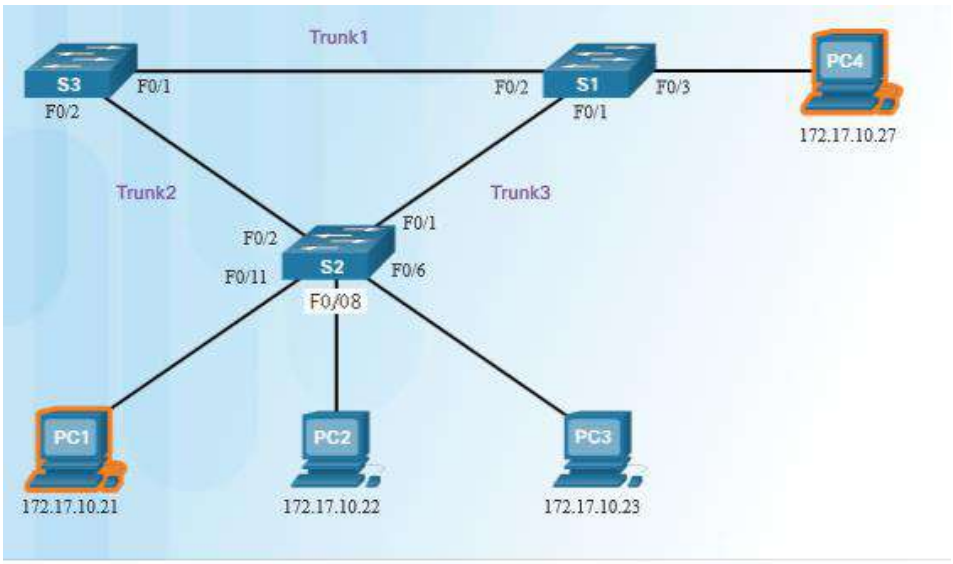
high CPU load on all switches caught in the loop. Because the same frames are constantly being forwarded back and forth between all switches in the loop, the CPU of the switch must process a lot of data. This slows down performance on the switch when legitimate traffic arrives.

A host caught in a network loop is not accessible to other hosts on the network. Additionally, due to the constant changes in the MAC address table, the switch does not know out of which port to forward unicast frames. In the example above, the switches will have the incorrect ports listed for PC1. Any unicast frame destined for PC1 loops around the network, just as the broadcast frames do. More and more frames looping around the network eventually creates a broadcast storm.



Issues with Layer 1 Redundancy: Duplicate Unicast Frames

Broadcast frames are not the only type of frames that are affected by loops. Unknown unicast frames sent onto a looped network can result in duplicate frames arriving at the destination device. An unknown unicast frame is when the switch does not have the destination MAC address in its MAC address table and must forward the frame out all ports, except the ingress port.



PC1 sends a unicast frame to PC4 via S2.

PC1 sends a unicast frame destined for PC4.

S2 does not have an entry for PC4 in its MAC table. In an attempt to find PC4, it floods the unknown unicast frame out all switch ports, except the port that received the traffic.

The frame arrives at switches S1 and S3.

S1 has a MAC address entry for PC4, so it forwards the frame out to PC4.

S3 has an entry in its MAC address table for PC4, so it forwards the unicast frame out Trunk3 to S1.

S1 receives the duplicate frame and forwards the frame out to PC4.

PC4 has now received the same frame twice.

Most upper-layer protocols are not designed to recognize duplicate transmissions. In general, protocols that make use of a sequence-numbering mechanism assume that the transmission has failed and that the sequence number has recycled for another communication session. Other protocols attempt to hand the duplicate transmission to the appropriate upper-layer protocol to be processed and possibly discarded.

Layer 2 LAN protocols, such as Ethernet, do not include a mechanism to recognize and eliminate endlessly looping frames. Some Layer 3 protocols implement a TTL mechanism that limits the number of times a Layer 3 networking device can retransmit a packet. Layer 2 devices do not have this mechanism, so they continue to retransmit looping traffic indefinitely. STP, a Layer 2 loop-avoidance mechanism, was developed to address these problems.

To prevent these issues from occurring in a redundant network, some type of spanning tree must be enabled on the switches. Spanning tree is enabled, by default, on Cisco switches to prevent Layer 2 loops from occurring.

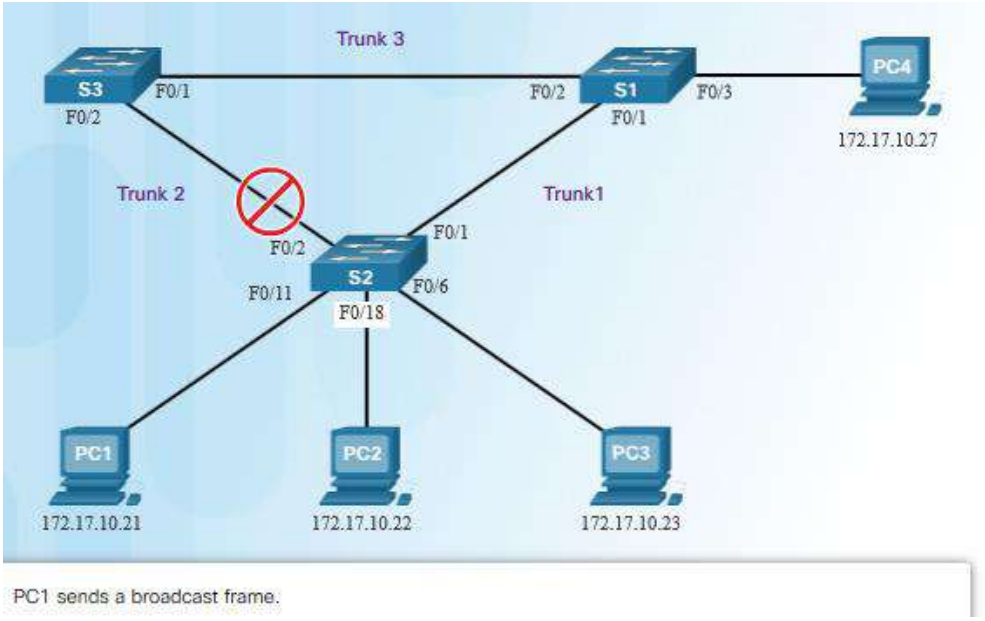
Spanning Tree Algorithm: Introduction

Redundancy increases the availability of the network topology by protecting the network from a single point of failure, such as a failed network cable or switch. When physical redundancy is introduced into a design, loops and duplicate frames occur. Loops and duplicate frames have severe consequences for a switched network. The Spanning Tree Protocol (STP) was developed to address these issues.

STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop. A port is considered blocked when user data is prevented from entering or leaving that port. This does not include bridge protocol data unit (BPDU) frames that are used by STP to prevent loops. Blocking the redundant paths is critical to preventing loops on the network. The physical paths still exist to provide redundancy, but these paths are disabled to prevent the loops from occurring. If the path is ever needed to compensate for a network cable or switch failure, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active.

S2 is configured with STP and has set the port for Trunk2 to a blocking state. The blocking state prevents ports from being used to forward user data, which prevents a loop from occurring. S2 forwards a broadcast frame out all switch ports, except the originating port from PC1 and the port for Trunk2.

S1 receives the broadcast frame and forwards it out all of its switch ports, where it reaches PC4 and S3. S3 forwards the frame out the port for Trunk2 and S2 drops the frame. The Layer 2 loop is prevented.



STP prevents loops from occurring by configuring a loop-free path through the network using strategically placed "blocking-state" ports. The switches running STP are able to compensate for failures by dynamically unblocking the previously blocked ports and permitting traffic to traverse the alternate paths.

Up to now, we have used the term Spanning Tree Protocol and the acronym STP. The usage of the Spanning Tree Protocol term and the STP acronym can be misleading. Many professionals generically use these to refer to various implementations of spanning tree, such as Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP). In order to communicate spanning tree concepts correctly, it is important to refer to the particular implementation or standard in context. The latest IEEE documentation on spanning tree (IEEE-802-1D-2004) says, "STP has now been superseded by the Rapid Spanning Tree Protocol (RSTP)."The IEEE uses "STP" to refer to the original implementation of spanning tree and "RSTP" to describe the version of spanning tree specified in IEEE-802.1D-2004. In this curriculum, when the original Spanning Tree Protocol is the context of a discussion, the phrase “original 802.1D spanning tree” is used to avoid confusion. Since the two protocols share much of the same terminology and methods for the loop-free path, the primary focus will be on the current standard and the Cisco proprietary implementations of STP and RSTP.

Note: STP is based on an algorithm invented by Radia Perlman while working for Digital Equipment Corporation, and published in the 1985 paper "An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN.”

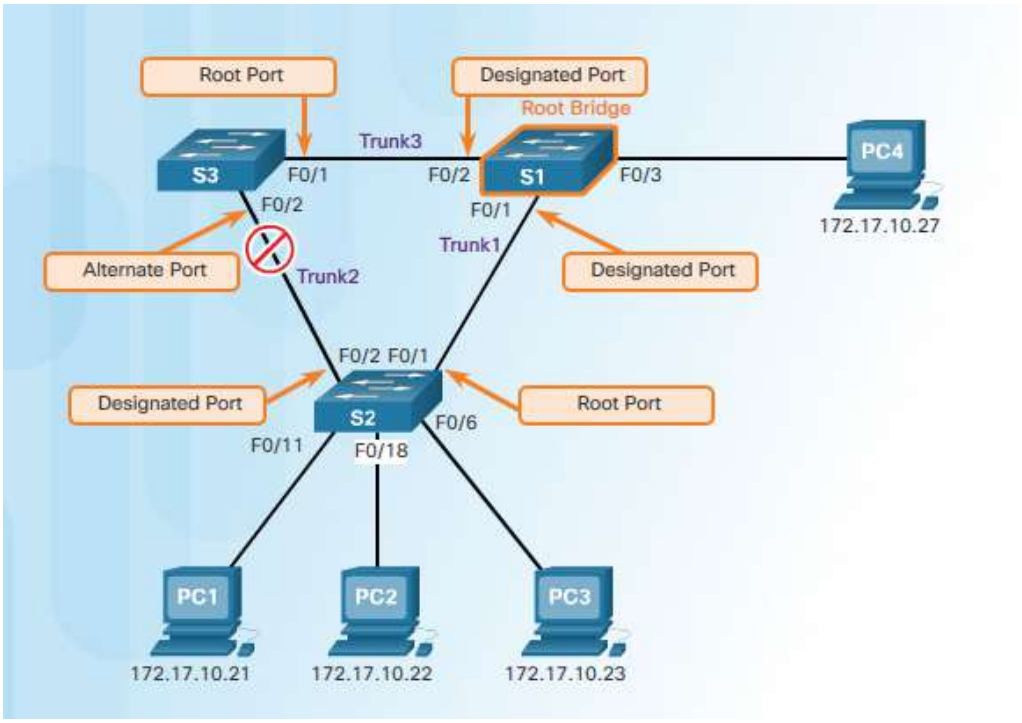
Spanning Tree Algorithm: Port Roles

IEEE 802.1D STP and RSTP use the Spanning Tree Algorithm (STA) to determine which switch ports on a network must be put in blocking state to prevent loops from occurring. The STA designates a single

switch as the root bridge and uses it as the reference point for all path calculations. In the figure, the root bridge (switch S1) is chosen through an election process. All switches that are participating in STP exchange BPDU frames to determine which switch has the lowest bridge ID (BID) on the network. The switch with the lowest BID automatically becomes the root bridge for the STA calculations.

Note: For simplicity, assume until otherwise indicated that all ports on all switches are assigned to VLAN 1. Each switch has a unique MAC address associated with VLAN 1.

A BPDU is a messaging frame exchanged by switches for STP. Each BPDU contains a BID that identifies the switch that sent the BPDU. The BID contains a priority value, the MAC address of the sending switch, and an optional extended system ID. The lowest BID value is determined by the combination of these three fields.



After the root bridge has been determined, the STA calculates the shortest path to the root bridge. Each switch uses the STA to determine which ports to block. While the STA determines the best paths to the root bridge for all switch ports in the broadcast domain, traffic is prevented from being forwarded through the network. The STA considers both path and port costs when determining which ports to block. The path costs are calculated using port cost values associated with port speeds for each switch port along a given path. The sum of the port cost values determines the overall path cost to the root bridge. If there is more than one path to choose from, STA chooses the path with the lowest path cost.

When the STA has determined which paths are most desirable relative to each switch, it assigns port roles to the participating switch ports. The port roles describe their relation in the network to the root bridge and whether they are allowed to forward traffic:

Root ports - Switch ports closest to the root bridge in terms of overall cost to the root bridge. In the figure, the root port selected by STP on S2 is F0/1, the link between S2 and S1. The root port selected

by STP on S3 is F0/1, the link between S3 and S1. Root ports are selected on a per-switch basis.

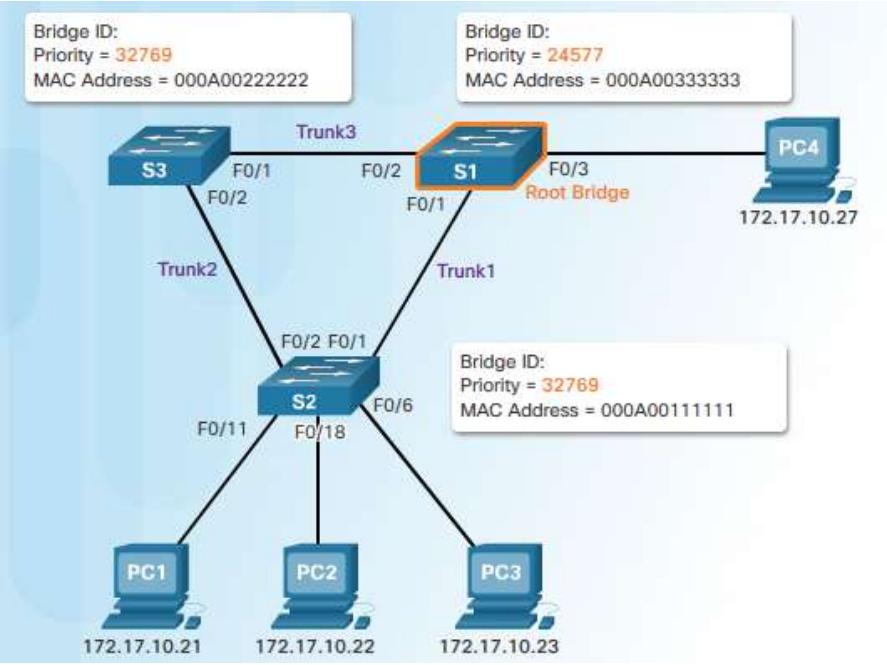
Designated ports - All non-root ports that are still permitted to forward traffic on the network. In the figure, switch ports (F0/1 and F0/2) on S1 are designated ports. S2 also has its port F0/2 configured as a designated port. Designated ports are selected on a per-segment basis based on the cost of each port on either side of the segment and the total cost calculated by STP for that port to get back to root bridge. If one end of a segment is a root port, then the other end is a designated port. All ports on the root bridge are designated ports.

Alternate and backup ports - Alternate ports and backup ports are in discarding or blocking state to prevent loops. In the figure, the STA configured port F0/2 on S3 in the alternate role. Port F0/2 on S3 is in the blocking state. Alternate ports are selected only on links where neither end is a root port. Notice in the figure that only one end of the segment is blocked. This allows for a faster transition to the forwarding state when necessary. (Blocking ports only come into play when two ports on the same switch provide redundant links through the network.)

Disabled ports - A disabled port is a switch port that is shut down.

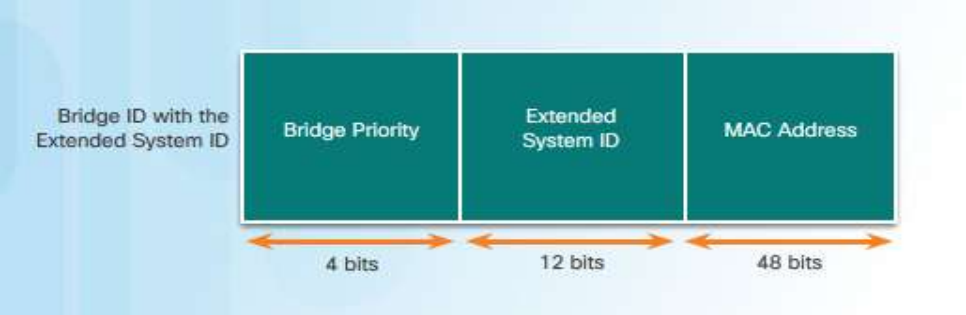
Note: The port roles displayed are those defined by RSTP. The role originally defined by the 802.1D STP for alternate and backup ports was non-designated.

Spanning Tree Algorithm: Root Bridge



Every spanning tree instance (switched LAN or broadcast domain) has a switch designated as the root bridge. The root bridge serves as a reference point for all spanning tree calculations to determine which redundant paths to block.

An election process determines which switch becomes the root bridge.



The BID is made up of a priority value, an extended system ID, and the MAC address of the switch. The bridge priority value is automatically assigned, but can be modified. The extended system ID is used to specify a VLAN ID or a multiple spanning tree protocol (MSTP) instance ID. The MAC address field initially contains the MAC address of the sending switch.

All switches in the broadcast domain participate in the election process. After a switch boots, it begins to send out BPDU frames every two seconds. These BPDUs contain the switch BID and the root ID.

The switch with the lowest BID will become the root bridge. At first, all switches declare themselves as the root bridge. Eventually, the switches exchange BPDUs, and agree on one root bridge.

As the switches forward their BPDU frames, adjacent switches in the broadcast domain read the root ID information from the BPDU frames. If the root ID from a BPDU received is lower than the root ID on the receiving switch, then the receiving switch updates its root ID, identifying the adjacent switch as the root bridge. However, it may not be an adjacent switch. It could be any other switch in the broadcast domain. The switch then forwards new BPDU frames with the lower root ID to the other adjacent switches. Eventually, the switch with the lowest BID ends up being identified as the root bridge for the spanning tree instance.

There is a root bridge elected for each spanning tree instance. It is possible to have multiple distinct root bridges for different sets of VLANs. If all ports on all switches are members of VLAN 1, then there is only one spanning tree instance. The extended system ID includes the VLAN ID, and plays a role in how spanning tree instances are determined.

The BID consists of a configurable bridge priority number and a MAC address. Bridge priority is a value between 0 and 65,535. The default is 32,768. If two or more switches have the same priority, the switch with the lowest MAC address will become the root bridge.

Note: The reason the bridge priority value in Figure 1 displays 32,769 instead of the default value of 32,768 is because STA algorithm also adds the default VLAN number (VLAN 1) to the priority v Port Role Decisions for RSTP

In the example, switch S1 is the root bridge. Switches S2 and S3 have root ports configured for the ports connecting back to S1.

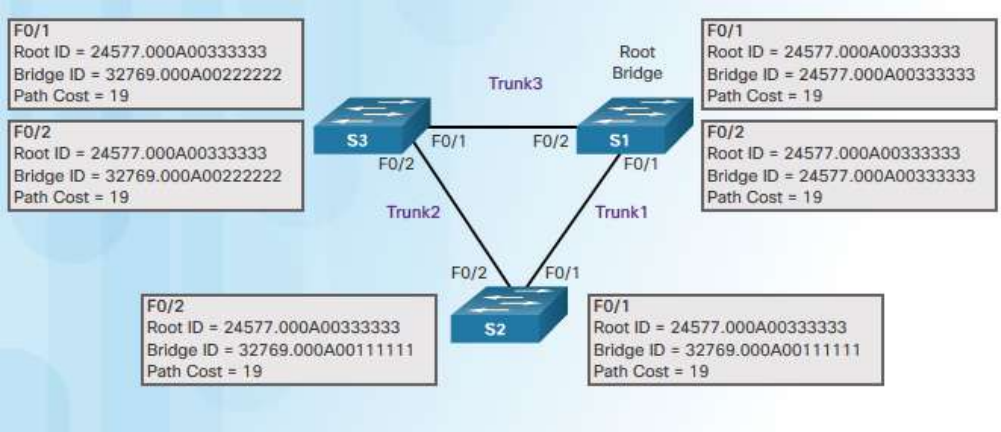
After STP has determined which switch port serves in the root port role on each switch, STP needs to decide which ports have the designated and alternate roles.

The root bridge automatically configures all of its switch ports in the designated role. Other switches in

the topology configure their non-root ports as designated or alternate ports.

Designated ports are configured for all LAN segments. When two switches are connected to the same LAN segment, and root ports have already been defined, the two switches have to decide which port to configure as a designated port and which port remains the alternate port.

The switches on the LAN segment exchange BPDU frames, which contain the switch BID. Generally, the switch with the lower BID has its port configured as a designated port while the switch with the higher BID has its port configured as an alternate port. However, keep in mind that the first priority is the lowest path cost to the root bridge and that the sender's BID is used only if the port costs are equal. Each switch determines which port roles are assigned to each of its ports to create the loop-free spanning tree.



Types of Spanning Tree Protocols

- **802.1D-1998**: The legacy standard for bridging and STP.
- **CST**: Assumes one spanning-tree instance for the entire bridged network, regardless of the number of VLANs.
- **PVST+**: A Cisco enhancement of STP that provides a separate 802.1D spanning-tree instance for each VLAN configured in the network.
- **802.1D-2004**: An updated bridging and STP standard.
- **802.1w (RSTP)**: Improves convergence over 1998 STP by adding roles to ports and enhancing BPDU exchanges.
- **Rapid PVST+**: A Cisco enhancement of RSTP using PVST+.
- **802.1s (MSTP)**: Maps multiple VLANs into the same spanning-tree instance.

Catalyst 2960 Default Configuration

The table shows the default spanning tree configuration for a Cisco Catalyst 2960 series switch. Notice that the default spanning tree mode is PVST+.

Configuring and Verifying the Bridge ID

When an administrator wants a specific switch to become a root bridge, the bridge priority value must be adjusted to ensure it is lower than the bridge priority values of all the other switches on the network. There are two different methods to configure the bridge priority value on a Cisco Catalyst switch.

Method 1

To ensure that the switch has the lowest bridge priority value, use the spanning-tree vlan *vlan-id* root

primary command in global configuration mode. The priority for the switch is set to the predefined value of 24,576 or to the highest multiple of 4,096, less than the lowest bridge priority detected on the network.

If an alternate root bridge is desired, use the spanning-tree vlan *vlan-id* root secondary global configuration mode command. This command sets the priority for the switch to the predefined value of 28,672. This ensures that the alternate switch becomes the root bridge if the primary root bridge fails. This assumes that the rest of the switches in the network have the default 32,768 priority value defined. S1 has been assigned as the primary root bridge using the spanning-tree vlan 1 root primary command, and S2 has been configured as the secondary root bridge using the spanning-tree vlan 1 root secondary command.

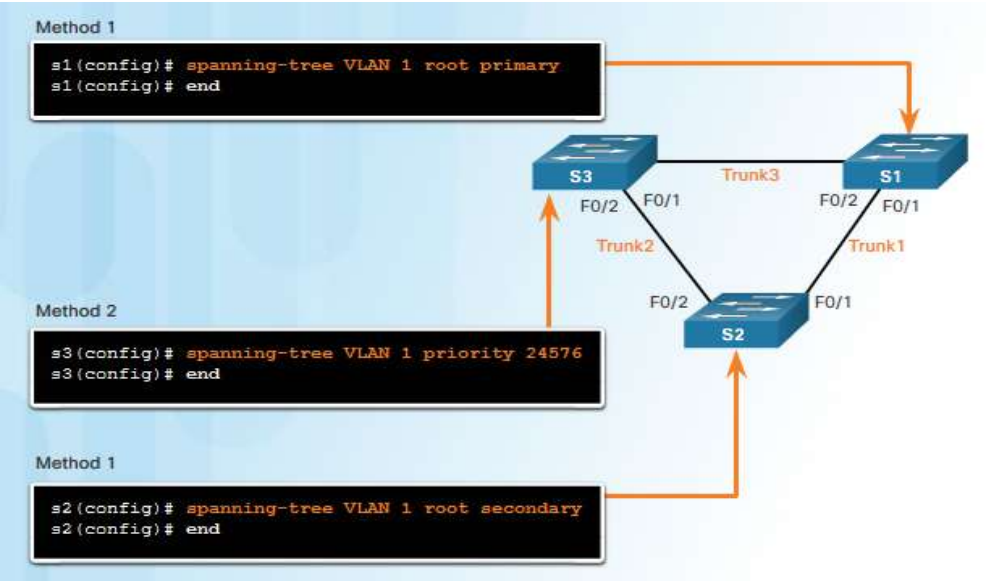
Method 2

Another method for configuring the bridge priority value is using the spanning-tree vlan *vlan-id* priority *value* global configuration mode command. This command gives more granular control over the bridge priority value. The priority value is configured in increments of 4,096 between 0 and 61,440.

In the example, S3 has been assigned a bridge priority value of 24,576 using the spanning-tree vlan 1 priority 24576 command.

To verify the bridge priority of a switch, use the show spanning-tree command. In Figure 2, the priority of the switch has been set to 24,576. Also notice that the switch is designated as the root bridge for the spanning tree instance.

To configure switches S1, S2, and S3. Using Method 2 described above, configure S3 manually, setting the priority to 24,576 for VLAN 1. Using Method 1, configure S2 as the secondary root VLAN 1 and configure S1 as the primary root for VLAN 1. Verify the configuration with the show spanning-tree command on S1.



Review questions

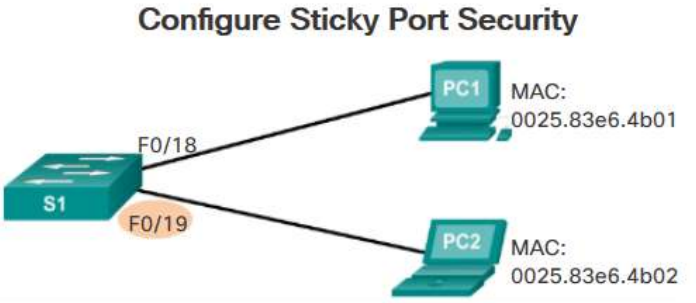
See the practical attachment

Learning Outcome 3.6: Configure switchport security

Port Security

All switch ports (interfaces) should be secured before the switch is deployed for production use. One way to secure ports is by implementing a feature called port security. Port security limits the number of valid MAC addresses allowed on a port. The MAC addresses of legitimate devices are allowed access, while other MAC addresses are denied.

Port security can be configured to allow one or more MAC addresses. If the number of MAC addresses allowed on the port is limited to one, then only the device with that specific MAC address can successfully connect to the port.



Cisco IOS CLI Commands	
Specify the interface to be configured for port security.	`S1(config)# interface fastethernet 0/19`
Set the interface mode to access.	`S1(config-if)# switchport mode access`
Enable port security on the interface.	`S1(config-if)# switchport port-security`
Set the maximum number of secure addresses allowed on the port.	`S1(config-if)# switchport port-security maximum 10`
Enable sticky learning.	`S1(config-if)# switchport port-security mac-address sticky`

Learning Outcome 3.7: Apply First Hop Redundancy Protocols and link Aggregationmodes

Introduction to Link Aggregation

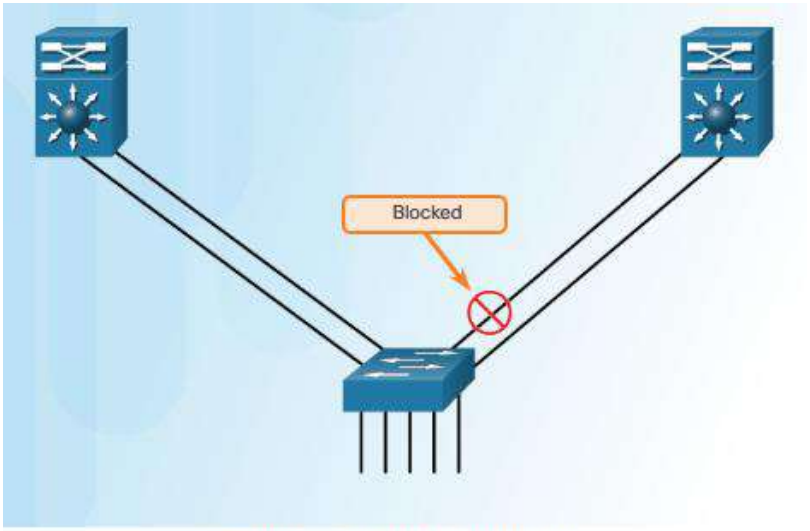
In the figure, traffic coming from several links (usually 100 or 1000 Mb/s) aggregates on the access switch and must be sent to distribution switches. Because of the traffic aggregation, links with higher

bandwidth must be available between the access and distribution switches.

It may be possible to use faster links, such as 10 Gb/s, on the aggregated link between the access and distribution layer switches. However, adding faster links is expensive. Additionally, as the speed increases on the access links, even the fastest possible port on the aggregated link is no longer fast enough to aggregate the traffic coming from all access links.

It is also possible to combine the number of physical links between the switches to increase the overall speed of switch-to-switch communication. However, by default, STP is enabled on Layer 2 devices such as switches. STP will block redundant links to prevent routing loops.

For these reasons, the best solution is to implement an EtherChannel configuration.



By default, STP will block redundant links.

Advantages of EtherChannel

EtherChannel technology was originally developed by Cisco as a LAN switch-to-switch technique of grouping several Fast Ethernet or Gigabit Ethernet ports into one logical channel. When an EtherChannel is configured, the resulting virtual interface is called a port channel. The physical interfaces are bundled together into a port channel interface.

EtherChannel technology has many advantages:

Most configuration tasks can be done on the EtherChannel interface instead of on each individual port, ensuring configuration consistency throughout the links.

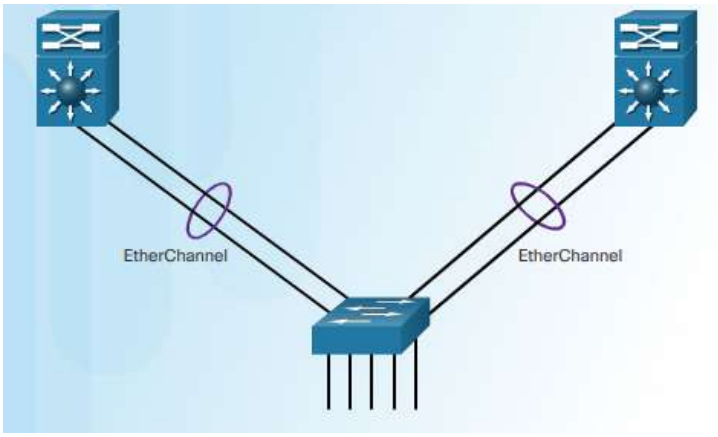
EtherChannel relies on existing switch ports. There is no need to upgrade the link to a faster and more expensive connection to have more bandwidth.

Load balancing takes place between links that are part of the same EtherChannel. Depending on the hardware platform, one or more load-balancing methods can be implemented. These methods include source MAC to destination MAC load balancing, or source IP to destination IP load balancing, across the physical links.

EtherChannel creates an aggregation that is seen as one logical link. When several EtherChannel bundles exist between two switches, STP may block one of the bundles to prevent switching loops.

When STP blocks one of the redundant links, it blocks the entire EtherChannel. This blocks all the ports belonging to that EtherChannel link. Where there is only one EtherChannel link, all physical links in the EtherChannel are active because STP sees only one (logical) link.

EtherChannel provides redundancy because the overall link is seen as one logical connection. Additionally, the loss of one physical link within the channel does not create a change in the topology; therefore a spanning tree recalculation is not required. Assuming at least one physical link is present; the EtherChannel remains functional, even if its overall throughput decreases because of a lost link within the EtherChannel.



Implementation Restrictions

EtherChannel can be implemented by grouping multiple physical ports into one or more logical EtherChannel links.

Note: Interface types cannot be mixed; for example, Fast Ethernet and Gigabit Ethernet cannot be mixed within a single EtherChannel.

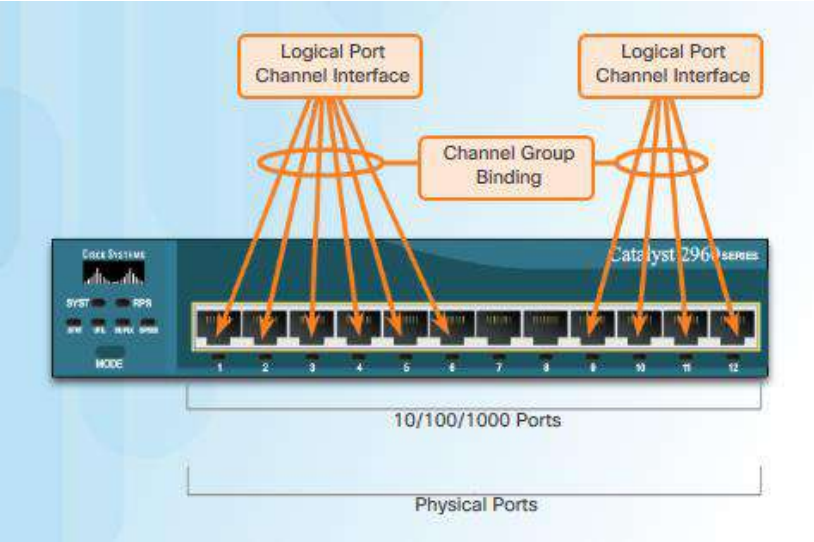
The EtherChannel provides full-duplex bandwidth up to 800 Mb/s (Fast EtherChannel) or 8 Gb/s (Gigabit EtherChannel) between one switch and another switch or host. Currently each EtherChannel can consist of up to eight compatibly-configured Ethernet ports. The Cisco IOS switch can currently support six EtherChannels. However, as new IOSs are developed and platforms change, some cards and platforms may support increased numbers of ports within an EtherChannel link, as well as support an increased number of Gigabit EtherChannels. The concept is the same no matter the speeds or number of links that are involved. When configuring EtherChannel on switches, be aware of the hardware platform boundaries and specifications.

The original purpose of EtherChannel was to increase speed capability on aggregated links between switches. However, this concept was extended as EtherChannel technology became more popular, and now many servers also support link aggregation with EtherChannel. EtherChannel creates a one-to-one relationship; that is, one EtherChannel link connects only two devices. An EtherChannel link can be created between two switches or an EtherChannel link can be created between an EtherChannel-enabled server and a switch.

The individual EtherChannel group member port configuration must be consistent on both devices. If the physical ports of one side are configured as trunks, the physical ports of the other side must also be configured as trunks within the same native VLAN. Additionally, all ports in each EtherChannel link must be configured as Layer 2 ports.

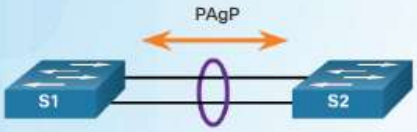
Each EtherChannel has a logical port channel interface, illustrated in the figure. A configuration applied to the port channel interface affects all physical interfaces that are assigned to that interface.

Note: Layer 3 EtherChannels can be configured on Cisco Catalyst multilayer switches, such as the Catalyst 3560, but these are not explored in this course. A Layer 3 EtherChannel has a single IP address associated with the logical aggregation of switch ports in the EtherChannel.



PAgP modes:

- On: Channel member without negotiation (no protocol).
- Desirable: Actively asking if the other side can or will participate.
- Auto: Passively waiting for the other side.



S1	S2	Channel Establishment
On	On	Yes
Auto/Desirable	Desirable	Yes
On/Auto/Desirable	Not Configured	No
On	Desirable	No
Auto/On	Auto	No

Link Aggregation Control Protocol

LACP

LACP is part of an IEEE specification (802.3ad) that allows several physical ports to be bundled to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP

packets to the peer. It performs a function similar to PAgP with Cisco EtherChannel. Because LACP is an IEEE standard, it can be used to facilitate EtherChannels in multivendor environments. On Cisco devices, both protocols are supported.

Note: LACP was originally defined as IEEE 802.3ad. However, LACP is now defined in the newer IEEE 802.1AX standard for local and metropolitan area networks.

LACP provides the same negotiation benefits as PAgP. LACP helps create the EtherChannel link by detecting the configuration of each side and making sure that they are compatible so that the EtherChannel link can be enabled when needed. The figure shows the modes for LACP.

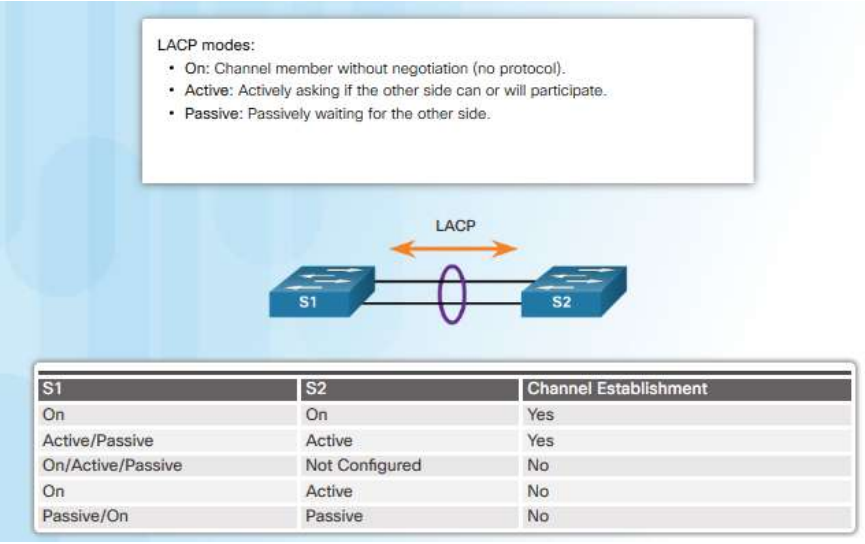
On - This mode forces the interface to channel without LACP. Interfaces configured in the on mode do not exchange LACP packets.

LACP active - This LACP mode places a port in an active negotiating state. In this state, the port initiates negotiations with other ports by sending LACP packets.

LACP passive - This LACP mode places a port in a passive negotiating state. In this state, the port responds to the LACP packets that it receives, but does not initiate LACP packet negotiation.

Just as with PAgP, modes must be compatible on both sides for the EtherChannel link to form. The on mode is repeated, because it creates the EtherChannel configuration unconditionally, without PAgP or LACP dynamic negotiation.

LACP allows for eight active links, and also eight standby links. A standby link will become active should one of the current active links fail.



S1	S2	Channel Establishment
On	On	Yes
Active/Passive	Active	Yes
On/Active/Passive	Not Configured	No
On	Active	No
Passive/On	Passive	No

Configuration Guidelines

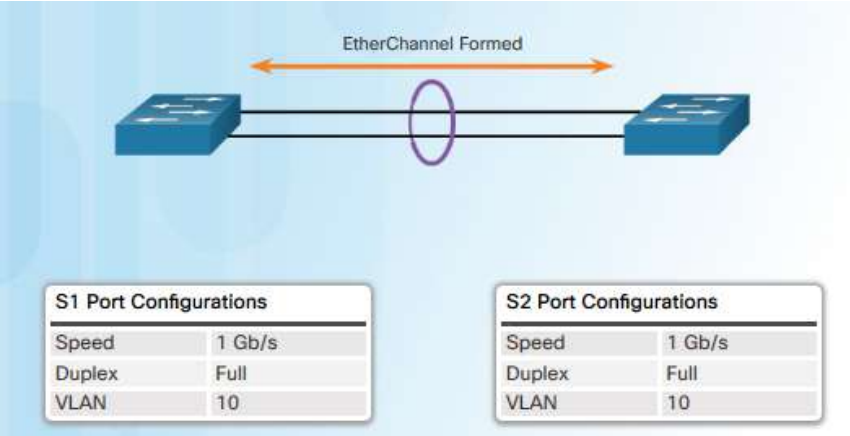
The following guidelines and restrictions are useful for configuring EtherChannel:

EtherChannel support - All Ethernet interfaces on all modules must support EtherChannel with no requirement that interfaces be physically contiguous, or on the same module.

Speed and duplex - Configure all interfaces in an EtherChannel to operate at the same speed and in the same duplex mode.

VLAN match - All interfaces in the EtherChannel bundle must be assigned to the same VLAN, or be configured as a trunk (also shown in the figure).

Range of VLANs - An EtherChannel supports the same allowed range of VLANs on all the interfaces in a trunking EtherChannel. If the allowed range of VLANs is not the same, the interfaces do not form an EtherChannel, even when set to auto or desirable mode.



If these settings must be changed, configure them in port channel interface configuration mode. Any configuration that is applied to the port channel interface also affects individual interfaces. However, configurations that are applied to the individual interfaces do not affect the port channel interface. Therefore, making configuration changes to an interface that is part of an EtherChannel link may cause interface compatibility issues.

The port channel can be configured in access mode, trunk mode (most common), or on a routed port.

Configuring Interfaces

Configuring EtherChannel with LACP requires two steps:

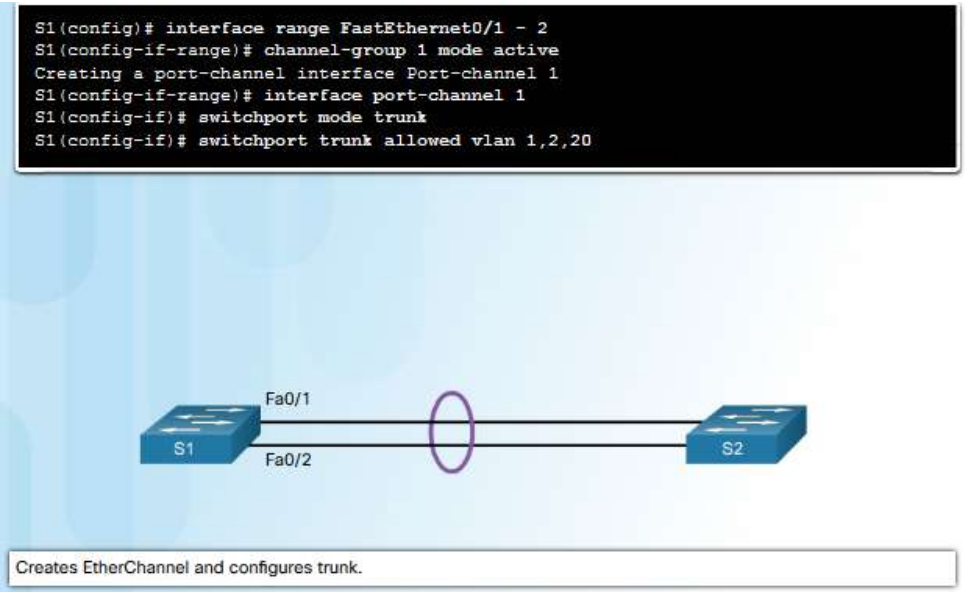
Step 1. Specify the interfaces that compose the EtherChannel group using the interface range *interface* global configuration mode command. The range keyword allows you to select several interfaces and configure them all together. A good practice is to start by shutting down those interfaces, so that any incomplete configuration does not create activity on the link.

Step 2. Create the port channel interface with the channel-group *identifier* mode active command in interface range configuration mode. The identifier specifies a channel group number. The mode active keywords identify this as an LACP EtherChannel configuration.

Note: EtherChannel is disabled by default.

In Figure 1, FastEthernet0/1 and FastEthernet0/2 are bundled into EtherChannel interface port channel 1.

To change Layer 2 settings on the port channel interface, enter port channel interface configuration mode using the interface port-channel command, followed by the interface identifier. In the example, the EtherChannel is configured as a trunk interface with allowed VLANs specified. Also shown in Figure 1, the port channel is configured as a trunk allowing traffic from VLANs 1, 2, and 20.



Verifying EtherChannel

There are a number of commands to verify an EtherChannel configuration. First, the show interfaces port-channel command displays the general status of the port channel interface The Port Channel 1 interface is up.

When several port channel interfaces are configured on the same device, use the show etherchannel summary command to simply display one line of information per port channel. The switch has one EtherChannel configured; group 1 uses LACP.

The interface bundle consists of the FastEthernet0/1 and FastEthernet0/2 interfaces. The group is a Layer 2 EtherChannel and it is in use, as indicated by the letters SU next to the port channel number.

Use the show etherchannel port-channel command to display information about a specific port channel interface. In the example, the Port Channel 1 interface consists of two physical interfaces, FastEthernet0/1 and FastEthernet0/2. It uses LACP in active mode. It is properly connected to another switch with a compatible configuration, which is why the port channel is said to be in use.

On any physical interface member of an EtherChannel bundle, the show interfaces etherchannel command can provide information about the role of the interface in the EtherChannel. The interface FastEthernet0/1 is part of the EtherChannel bundle 1. The protocol for this EtherChannel is LACP.

Review questions

See the practical attachment

Default Gateway Limitations

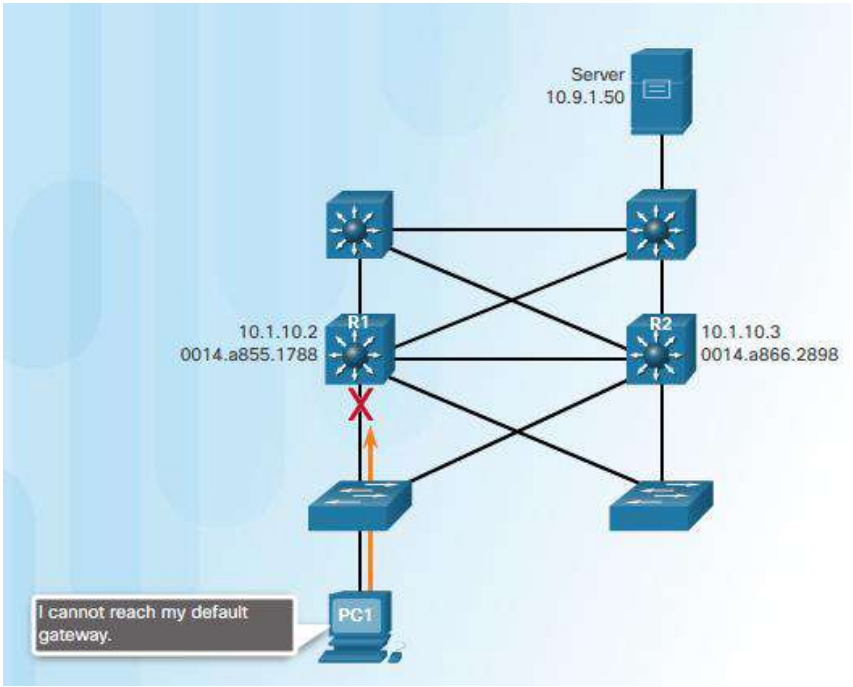
If a router or router interface (that serves as a default gateway) fails, the hosts configured with that default gateway are isolated from outside networks. A mechanism is needed to provide alternate default gateways in switched networks where two or more routers are connected to the same VLANs.

Note: For the purposes of the discussion on router redundancy, there is no functional difference between a multilayer switch and a router at the distribution layer. In practice, it is common for a multilayer switch to act as the default gateway for each VLAN in a switched network. This discussion focuses on the functionality of *routing*, regardless of the physical device used.

In a switched network, each client receives only one default gateway. There is no way to use a secondary gateway, even if a second path exists to carry packets off the local segment.

In the figure, R1 is responsible for routing packets from PC1. If R1 becomes unavailable, the routing protocols can dynamically converge. R2 now routes packets from outside networks that would have gone through R1. However, traffic from the inside network associated with R1, including traffic from workstations, servers, and printers configured with R1 as their default gateway, are still sent to R1 and dropped.

End devices are typically configured with a single IP address for a default gateway. This address does not change when the network topology changes. If that default gateway IP address cannot be reached, the local device is unable to send packets off the local network segment, effectively disconnecting it from other networks. Even if a redundant router exists that could serve as a default gateway for that segment, there is no dynamic method by which these devices can determine the address of a new default gateway.



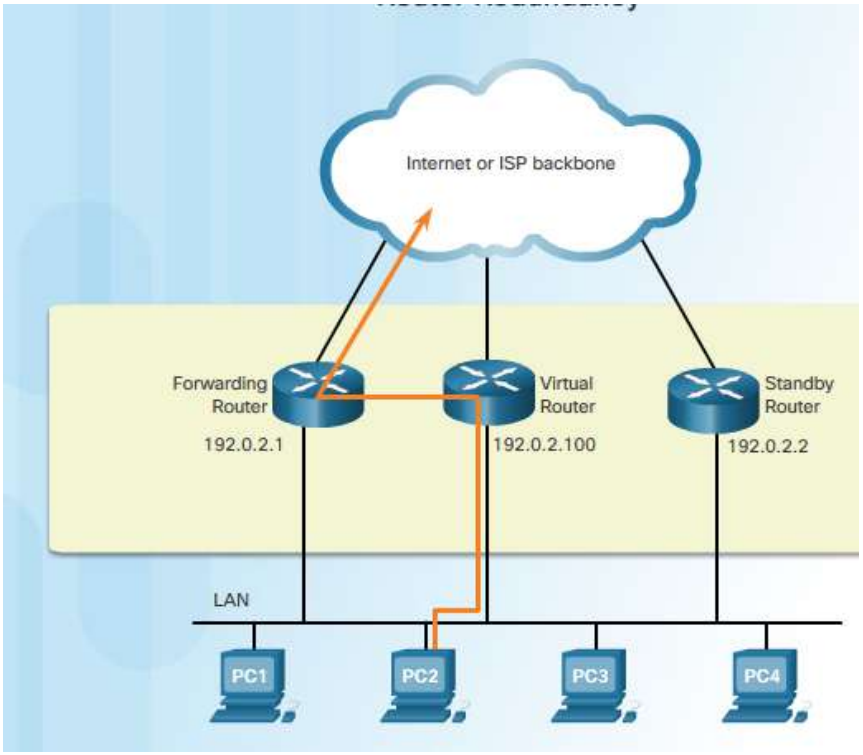
Router Redundancy

One way to prevent a single point of failure at the default gateway, is to implement a virtual router. To implement this type of router redundancy, multiple routers are configured to work together to present the illusion of a single router to the hosts on the LAN, as shown in the figure. By sharing an IP address and a MAC address, two or more routers can act as a single virtual router.

The IPv4 address of the virtual router is configured as the default gateway for the workstations on a specific IPv4 segment. When frames are sent from host devices to the default gateway, the hosts use ARP to resolve the MAC address that is associated with the IPv4 address of the default gateway. The ARP resolution returns the MAC address of the virtual router. Frames that are sent to the MAC address of the virtual router can then be physically processed by the currently active router within the virtual router group. A protocol is used to identify two or more routers as the devices that are responsible for processing frames that are sent to the MAC or IP address of a single virtual router. Host devices send traffic to the address of the virtual router. The physical router that forwards this traffic is transparent to the host devices.

A redundancy protocol provides the mechanism for determining which router should take the active role in forwarding traffic. It also determines when the forwarding role must be taken over by a standby router. The transition from one forwarding router to another is transparent to the end devices.

The ability of a network to dynamically recover from the failure of a device acting as a default gateway is known as first-hop redundancy.



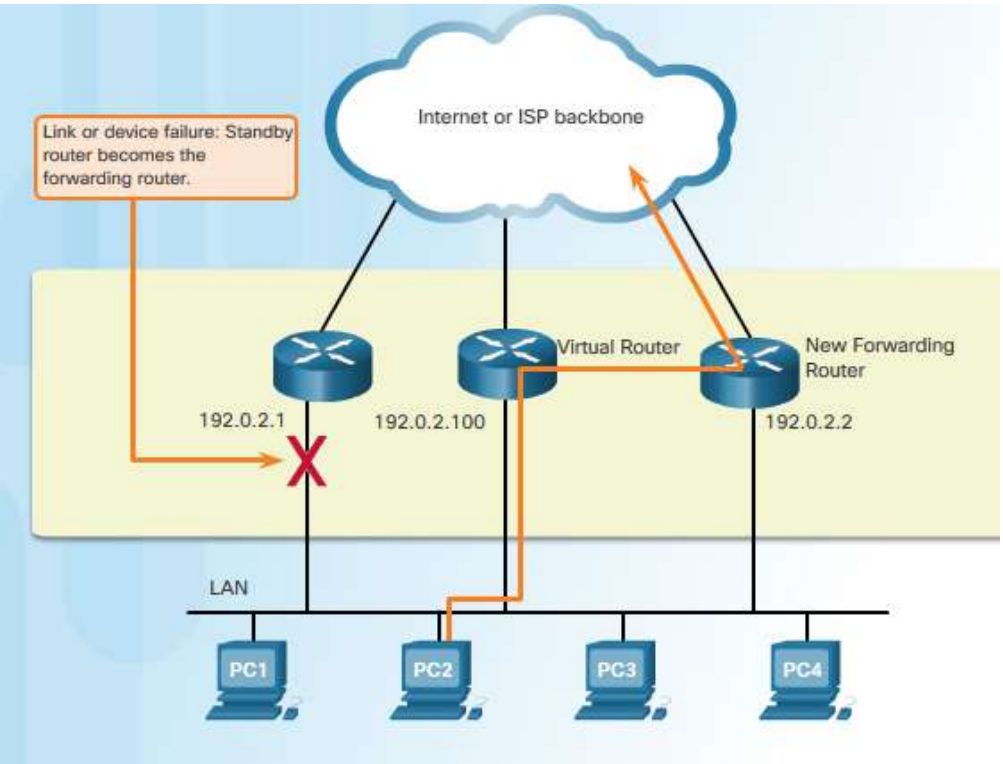
Steps for Router Failover

When the active router fails, the redundancy protocol transitions the standby router to the new active router role. These are the steps that take place when the active router fails:

1. The standby router stops seeing Hello messages from the forwarding router.

2. The standby router assumes the role of the forwarding router.

3. Because the new forwarding router assumes both the IPv4 and MAC addresses of the virtual router, the host devices see no disruption in service.



First Hop Redundancy Protocols

The following list defines the options available for First Hop Redundancy Protocols (FHRPs), as shown in the figure.

Hot Standby Router Protocol (HSRP) - A Cisco-proprietary FHRP designed to allow for transparent failover of a first-hop IPv4 device. HSRP provides high network availability by providing first-hop routing redundancy for IPv4 hosts on networks configured with an IPv4 default gateway address. HSRP is used in a group of routers for selecting an active device and a standby device. In a group of device interfaces, the active device is the device that is used for routing packets; the standby device is the device that takes over when the active device fails, or when pre-set conditions are met. The function of the HSRP standby router is to monitor the operational status of the HSRP group and to quickly assume packet-forwarding responsibility if the active router fails.

HSRP for IPv6 - Cisco-proprietary FHRP providing the same functionality of HSRP, but in an IPv6 environment. An HSRP IPv6 group has a virtual MAC address derived from the HSRP group number and a virtual IPv6 link-local address derived from the HSRP virtual MAC address. Periodic router advertisements (RAs) are sent for the HSRP virtual IPv6 link-local address when the HSRP group is active. When the group becomes inactive these RAs stop after a final RA is sent.

Virtual Router Redundancy Protocol version 2 (VRRPv2) - A non-proprietary election protocol that

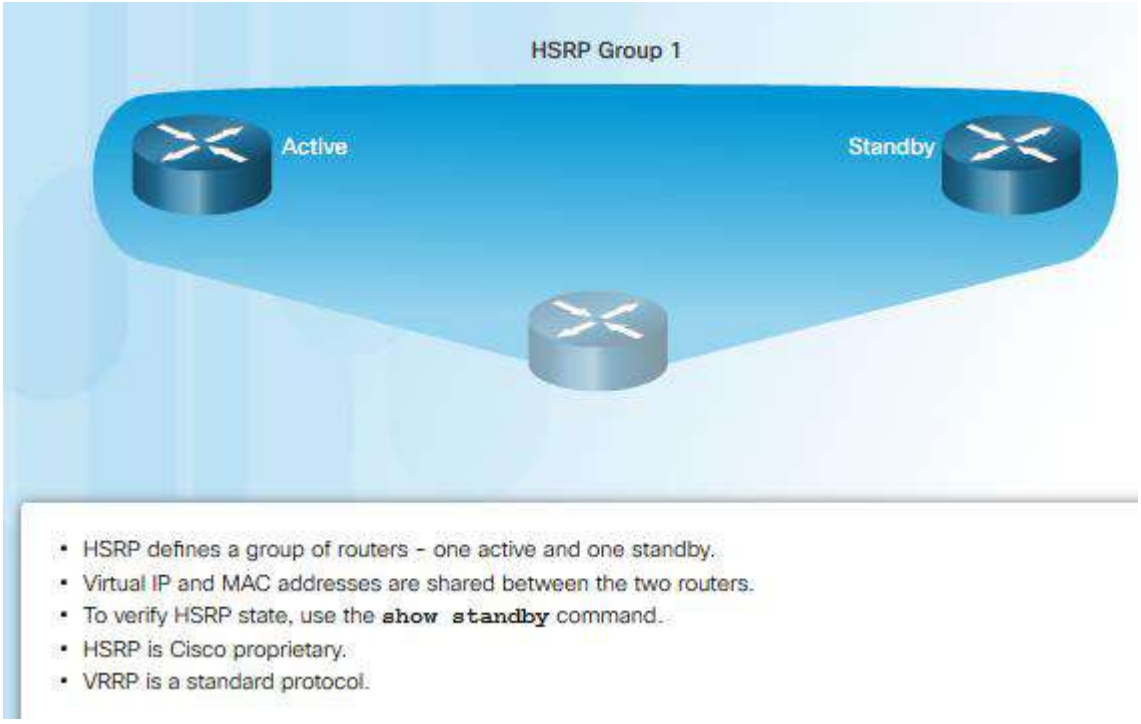
dynamically assigns responsibility for one or more virtual routers to the VRRP routers on an IPv4 LAN. This allows several routers on a multiaccess link to use the same virtual IPv4 address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, one router is elected as the virtual router master, with the other routers acting as backups, in case the virtual router master fails.

VRRPv3 - Provides the capability to support IPv4 and IPv6 addresses. VRRPv3 works in multi-vendor environments and is more scalable than VRRPv2.

Gateway Load Balancing Protocol (GLBP) - Cisco-proprietary FHRP that protects data traffic from a failed router or circuit, like HSRP and VRRP, while also allowing load balancing (also called load sharing) between a group of redundant routers.

GLBP for IPv6 - Cisco-proprietary FHRP providing the same functionality of GLBP, but in an IPv6 environment. GLBP for IPv6 provides automatic router backup for IPv6 hosts configured with a single default gateway on a LAN. Multiple first-hop routers on the LAN combine to offer a single virtual first-hop IPv6 router while sharing the IPv6 packet forwarding load.

ICMP Router Discovery Protocol (IRDP) - Specified in RFC 1256, is a legacy FHRP solution. IRDP allows IPv4 hosts to locate routers that provide IPv4 connectivity to other (nonlocal) IP networks.



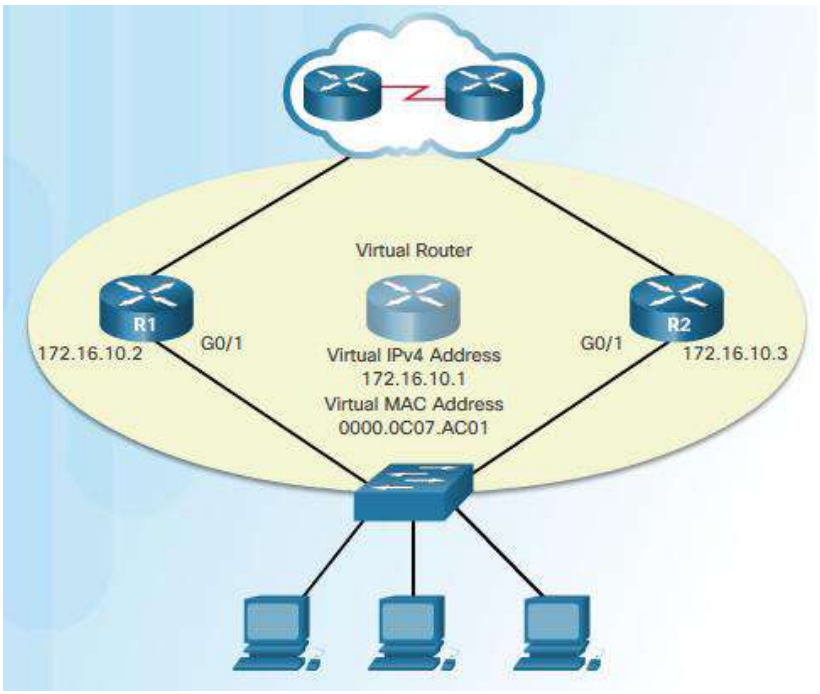
HSRP Overview

Hot Standby Router Protocol (HSRP) was designed by Cisco to allow for gateway redundancy without any additional configuration on end devices. Routers configured with HSRP work together to present themselves as a single virtual default gateway (router) to end devices, as shown in the figure. One of the routers is selected by HSRP to be the active router. The active router will act as the default gateway for end devices. The other router will become the standby router. If the active router fails, the standby

router will automatically assume the role of the active router. It will assume the role of default gateway for end devices. This does not require any configuration changes on the end devices.

Hosts are configured with a single default gateway address that is recognizable by both the active and standby routers. The default gateway address is a virtual IPv4 address along with a virtual MAC address that is shared amongst both HSRP routers. End devices use this virtual IPv4 address as their default gateway address. The HSRP virtual IPv4 address is configured by the network administrator. The virtual MAC address is created automatically. Regardless of which physical router is used, the virtual IPv4 and MAC addresses provide consistent default gateway addressing for the end devices.

Only the active router will receive and forward traffic sent to the default gateway. If the active router fails, or if communication to the active router fails, the standby router will assume the role of the active router.



HSRP Versions

The default HSRP version for Cisco IOS 15 is version 1. HSRP version 2 provides the following enhancements:

HSRPv2 expands the number of supported groups. HSRP version 1 supports group numbers from 0 to 255. HSRP version 2 supports group numbers from 0 to 4095.

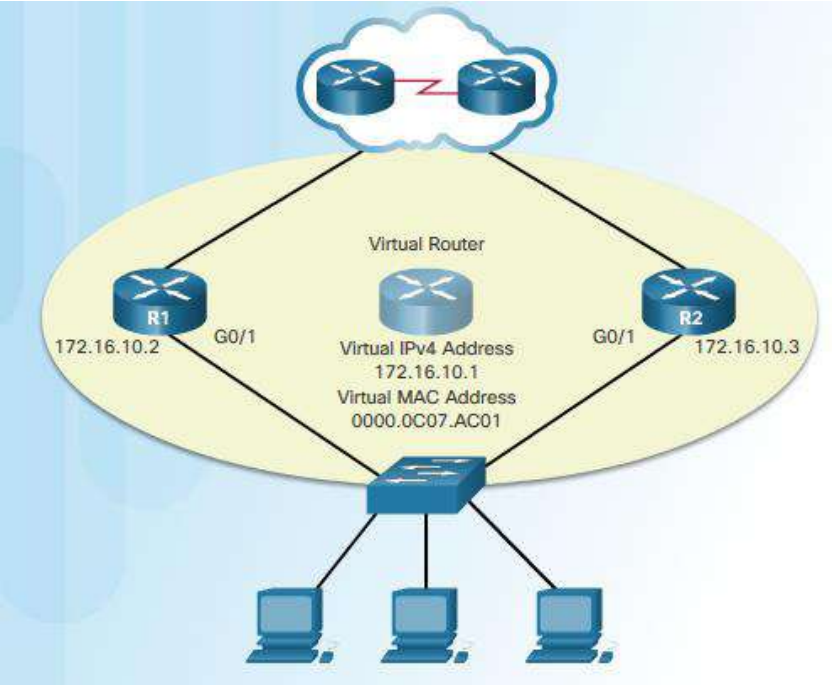
HSRPv1 uses the multicast address of 224.0.0.2. HSRP version 2 uses the IPv4 multicast address 224.0.0.102 or the IPv6 multicast address FF02::66 to send hello packets.

HSRPv1 uses the virtual MAC address range 0000.0C07.AC00 to 0000.0C07.ACFF, where the last two hexadecimal digits indicate the HSRP group number. HSRPv2 uses the MAC address range from 0000.0C9F.F000 to 0000.0C9F.FFFF for IPv4 and 0005.73A0.0000 through 0005.73A0.0FFF for IPv6 addresses. For both IPv4 and IPv6, the last three hexadecimal digits in the MAC address indicate the

HSRP group number.

HSRPv2 adds support for MD5 authentication, which is beyond the scope of this course.

Note: Group numbers are used for more advanced HSRP configurations that are beyond the scope of this course. For our purposes, we will use group number 1.



HSRP Priority and Preemption

The role of the active and standby routers is determined during the HSRP election process. By default, the router with the numerically highest IPv4 address is elected as the active router. However, it is always better to control how your network will operate under normal conditions rather than leaving it to chance.

HSRP Priority

HSRP priority can be used to determine the active router. The router with the highest HSRP priority will become the active router. By default, the HSRP priority is 100. If the priorities are equal, the router with the numerically highest IPv4 address is elected as the active router.

To configure a router to be the active router, use the standby priority interface command. The range of the HSRP priority is 0 to 255.

HSRP Preemption

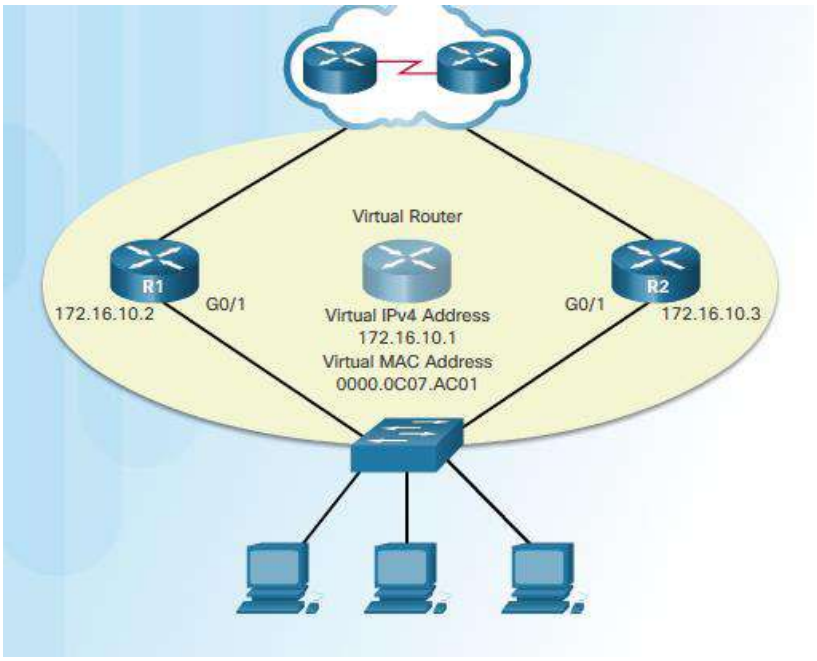
By default, after a router becomes the active router, it will remain the active router even if another router comes online with a higher HSRP priority.

To force a new HSRP election process, preemption must be enabled using the standby preempt interface command. Preemption is the ability of an HSRP router to trigger the re-election process. With preemption enabled, a router that comes online with a higher HSRP priority will assume the role of the active router.

Preemption only allows a router to become the active router if it has a higher priority. A router enabled for preemption, with equal priority but a higher IPv4 address will not preempt an active router. Refer to the topology in the figure.

R1 has been configured with the HSRP priority of 150 while R2 has the default HSRP priority of 100. Preemption has been enabled on R1. With a higher priority R1 is the active router and R2 is the standby router. Due to a power failure affecting only R1, the active router is no longer available and the standby router R2 assumes the role of the active router. After power is restored, R1 comes back online. Because R1 has a higher priority and preemption is enabled, it will force a new election process. R1 will re-assume the role of the active router and R2 will fall back to the role of the standby router.

Note: With preemption disabled, the router that boots up first will become the active router if there are no other routers online during the election process.



HSRP States and Timers

A router can either be the active HSRP router responsible for forwarding traffic for the segment, or it can be a passive HSRP router on standby, ready to assume the active role if the active router fails. When an interface is configured with HSRP or is first activated with an existing HSRP configuration, the router sends and receives HSRP hello packets to begin the process of determining which state it will assume in the HSRP group. The figure summarizes the HSRP states.

The active and standby HSRP routers send hello packets to the HSRP group multicast address every 3 seconds, by default. The standby router will become active if it does not receive a hello message from the active router after 10 seconds. You can lower these timer settings to speed up the failover or preemption. However, to avoid increased CPU usage and unnecessary standby state changes, do not set the hello timer below 1 second or the hold timer below 4 seconds.

State	Definition
Initial	This state is entered through a configuration change or when an interface first becomes available.
Learn	The router has not determined the virtual IP address and has not yet seen a hello message from the active router. In this state, the router waits to hear from the active router.
Listen	The router knows the virtual IP address, but the router is neither the active router nor the standby router. It listens for hello messages from those routers.
Speak	The router sends periodic hello messages and actively participates in the election of the active and/or standby router.
Standby	The router is a candidate to become the next active router and sends periodic hello messages.
Active	The router currently forwards packets that are sent to the group virtual MAC address. The router sends periodic hello messages.

HSRP Configuration Commands

Complete the following steps to configure HSRP:

Step 1. Configure HSRP version 2.

Step 2. Configure the virtual IP address for the group.

Step 3. Configure the priority for the desired active router to be greater than 100.

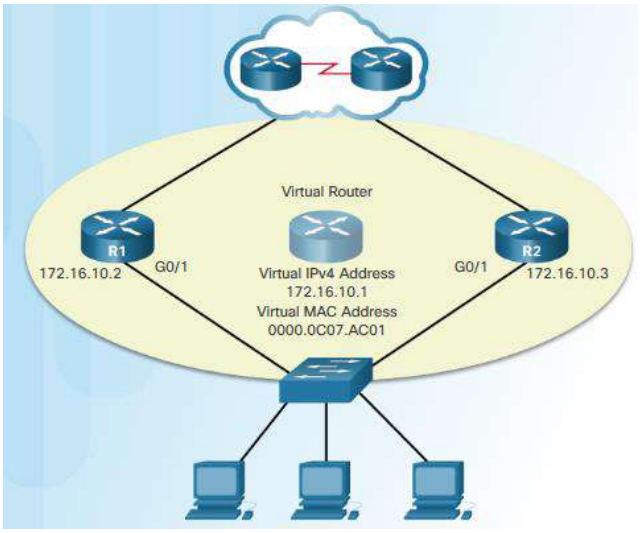
Step 4. Configure the active router to preempt the standby router in cases where the active router comes online after the standby router.

The figure lists the command syntax used to complete the configuration steps.

Command	Definition
`Router(config-if)# standby version 2`	Configures HSRP to use version 2. HSRP version 1 is the default.
`Router(config-if)# standby [group-number] ip-address`	Configures the HSRP virtual IP address that will be used by the specified group. If no group is configured, then the virtual IP address is assigned to group 0.
`Router(config-if)# standby [group-number] priority [priority-value]`	Configures the desired active router with a higher priority than default priority of 100. Range is 0 to 255. If no priority is configured or if priority is equal, than the router with the highest IP address has priority.
`Router(config-if)# standby [group-number] preempt`	Configures a router to preempt the currently active router.

HSRP Sample Configuration

Figure 1 shows the sample topology. Figure 2 shows the configurations for R1 and R2 in the sample topology.




```
R1(config)# interface g0/1
R1(config-if)# ip address 172.16.10.2 255.255.255.0
R1(config-if)# standby version 2
R1(config-if)# standby 1 ip 172.16.10.1
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt
R1(config-if)# no shutdown
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
R2(config)# interface g0/1
R2(config-if)# ip address 172.16.10.3 255.255.255.0
R2(config-if)# standby version 2
R2(config-if)# standby 1 ip 172.16.10.1
R2(config-if)# no shutdown
```

Review questions

See the practical attachment

LEARNING UNIT 4- IMPLEMENT SECURITY NETWORK POLICIE

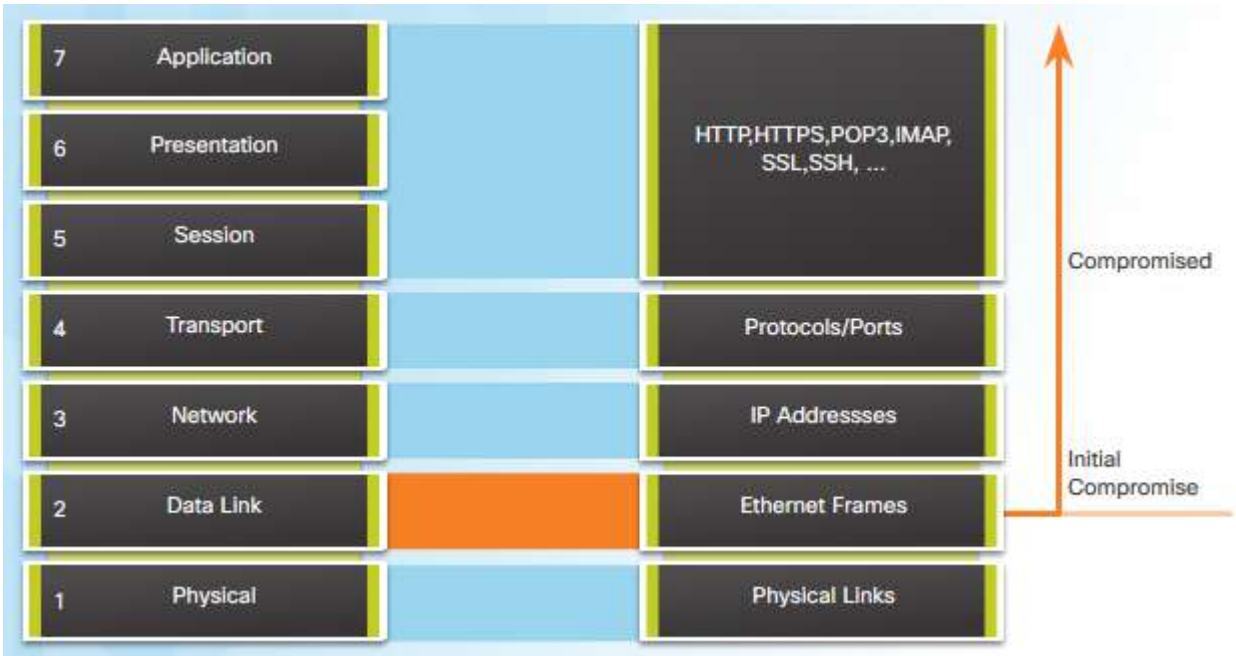
Learning Outcomes:	Identify Network security attacks and threats
	Identify and test vulnerabilities and threats
	Apply Network Attack Mitigation
	Implement secure network device access
	Apply Virtual Private Network

Learning hours:	20 Hours

Learning Outcome 4.1: Identify Network security attacks and threats

Common LAN Attacks

Organizations commonly implement security solutions using routers, firewalls, Intrusion Prevention System (IPSs), and VPN devices. These protect the elements in Layer 3 up through Layer 7.



Layer 2 LANs are often considered to be a safe and secure environment. However, as shown in the figure, if Layer 2 is compromised then all layers above it are also affected. Today, with BYOD and more sophisticated attacks, LANs have become more vulnerable.

For example, a disgruntled employee with internal network access could capture Layer 2 frames. This could render all of the security implemented in layers 3 and above useless. The attacker could also wreak havoc on the Layer 2 LAN networking infrastructure and create DoS situations. Therefore, in

addition to protecting Layer 3 to Layer 7, network security professionals must also mitigate threats against the Layer 2 LAN infrastructure.

The first step in mitigating attacks on the Layer 2 infrastructure is to understand the underlying operation of Layer 2 and the threats posed by the Layer 2 infrastructure.

Common attacks against the Layer 2 LAN infrastructure include:

CDP Reconnaissance Attack

Telnet Attacks

MAC Address Table Flooding Attack

VLAN Attacks

DHCP Attacks

The first two attacks are focused on gaining administrative access to the network device. The remaining attacks are focused on disrupting the network operation. Other more sophisticated attacks exist. However, the focus of this section is on common Layer 2 attacks.

Note: For more information on Layer 2 attacks, refer to the CCNA Security course.

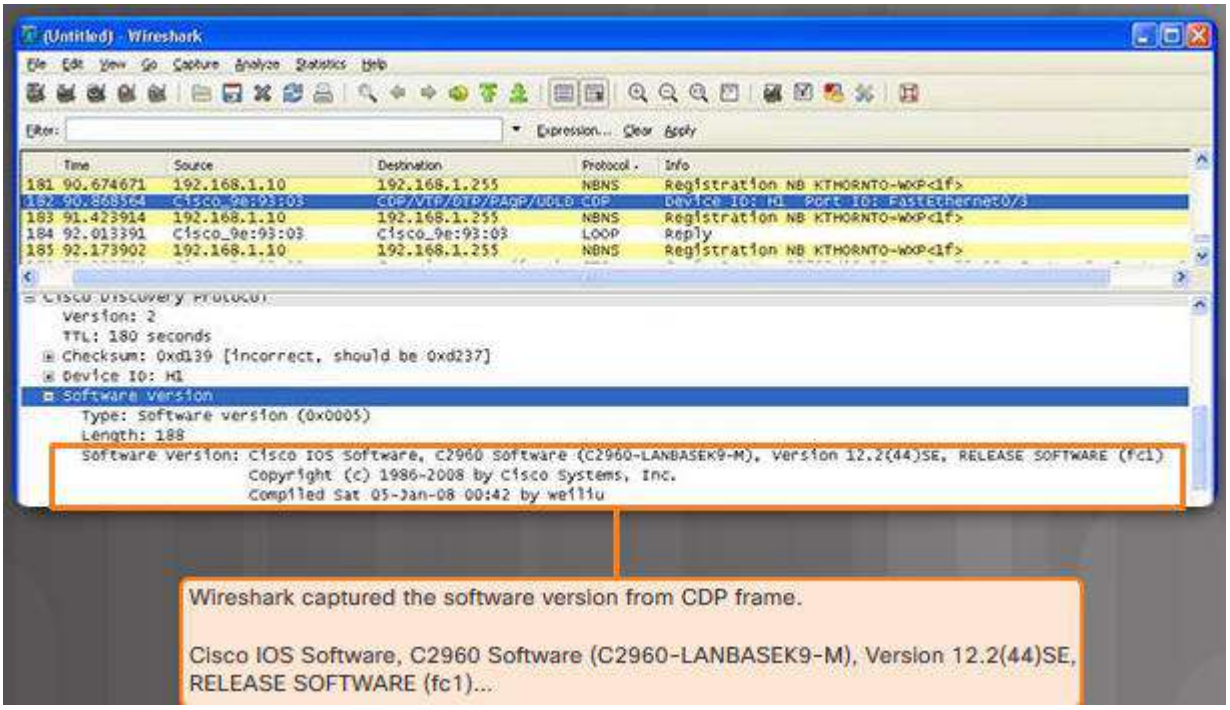
Review questions

What are Common LAN Attacks ?

Learning Outcome 4.2: Identify and test vulnerabilities and threats

CDP Reconnaissance Attack

The Cisco Discovery Protocol (CDP) is a proprietary Layer 2 link discovery protocol. It is enabled on all Cisco devices by default. CDP can automatically discover other CDP-enabled devices and help auto-configure their connection. Network administrators also use CDP to help configure and troubleshoot network devices.



CDP information is sent out CDP-enabled ports in periodic, unencrypted broadcasts. CDP information includes the IP address of the device, IOS software version, platform, capabilities, and the native VLAN. The device receiving the CDP message updates its CDP database.

CDP information is extremely useful in network troubleshooting. For example, CDP can be used to verify Layer 1 and 2 connectivity. If an administrator cannot ping a directly connected interface, but still receives CDP information, then the problem is most likely related to the Layer 3 configuration.

However, the information provided by CDP can also be used by an attacker to discover network infrastructure vulnerabilities.

In the figure, a sample Wireshark capture displays the contents of a CDP packet. The attacker is able to identify the Cisco IOS software version used by the device. This allows the attacker to determine whether there were any security vulnerabilities specific to that particular version of IOS.

CDP broadcasts are sent unencrypted and unauthenticated. Therefore, an attacker could interfere with the network infrastructure by sending crafted CDP frames containing bogus device information to directly-connected Cisco devices.

To mitigate the exploitation of CDP, limit the use of CDP on devices or ports. For example, disable

CDP on edge ports that connect to untrusted devices.

To disable CDP globally on a device, use the no cdp run global configuration mode command. To enable CDP globally, use the cdp run global configuration command.

To disable CDP on a port, use the no cdp enable interface configuration command. To enable CDP on a port, use the cdp enable interface configuration command.

Note: Link Layer Discovery Protocol (LLDP) in also vulnerable to reconnaissance attacks. Configure no lldp run to disable LLDP globally. To disable LLDP on the interface, configure no lldp transmit and no lldp receive.

Telnet Attacks

The ability to remotely manage a switched LAN infrastructure is an operational requirement; therefore, it must be supported.

However, the Telnet protocol is inherently insecure and can be leveraged by an attacker to gain remote access to a Cisco network device. There are tools available that allow an attacker to launch attacks against the vty lines on the switch.

There are two types of Telnet attacks:

Brute Force Password Attack - The attacker may use a list of common passwords, dictionary words, and variations of words to discover the administrative password. If the password is not discovered by the first phase, a second phase begins. The attacker uses specialized password auditing tools such as those shown in the figure. The software creates sequential character combinations in an attempt to guess the password. Given enough time and the right conditions, a brute force password attack can crack almost all passwords.

Telnet DoS Attack - The attacker continuously requests Telnet connections in an attempt to render the Telnet service unavailable and preventing an administrator from remotely accessing a switch. This can be combined with other direct attacks on the network as part of a coordinated attempt to prevent the network administrator from accessing core devices during the breach.

There are several way to mitigate against Telnet attacks:

Use SSH, rather than Telnet for remote management connections.

Use strong passwords that are changed frequently. A strong password should have a mix of upper and lowercase letters and should include numerals and symbols (special characters).

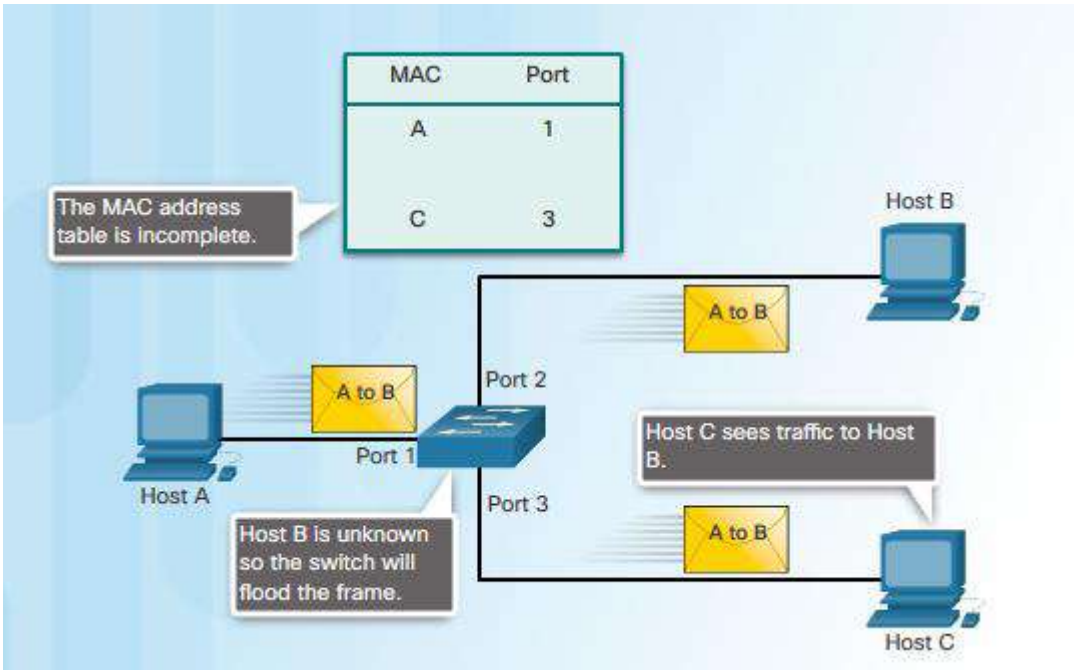
Limit access to the vty lines using an access control list (ACL) permitting only administrator devices and denying all other devices.

Authenticate and authorize administrative access to the device using AAA with either TACACS+ or RADIUS protocols

MAC Address Table Flooding Attack

One of the most basic and common LAN switch attacks is the MAC address flooding attack. This attack is also known as a MAC address table overflow attack, or a CAM table overflow attack.

Consider what happens when a switch receives incoming frames. The MAC address table in a switch contains the MAC addresses associated with each physical port, and the associated VLAN for each port. When a Layer 2 switch receives a frame, the switch looks in the MAC address table for the destination MAC address. All Catalyst switch models use a MAC address table for Layer 2 switching. As frames arrive on switch ports, the source MAC addresses are recorded in the MAC address table. If an entry exists for the MAC address, the switch forwards the frame to the correct port. If the MAC address does not exist in the MAC address table, the switch floods the frame out of every port on the switch, except the port where the frame was received.



In Figure , host A sends traffic to host B. The switch receives the frames and adds the source MAC address of host A to its MAC address table. The switch then looks up the destination MAC address in its MAC address table. If the switch does not find the destination MAC in the MAC address table, it copies the frame and floods (broadcasts) it out of every switch port, except the port where it was received.

A host receives and processes the frame. It then sends a reply to host A. The switch receives the incoming frame from host B. The switch then adds the source MAC address and port assignment for host B to its MAC address table. The switch then looks for the destination MAC address in its MAC address table and forwards the frames out of Port 1 towards host A.

The MAC address table of the switch eventually learns all MAC addresses connected to it and forwards frames between communicating ports only. Any frame sent by host A (or any other host) to host B is forwarded out port 2 of the switch. It is not broadcasted out every port because the switch knows the location of the destination MAC address.

An attacker can exploit this default switch behaviour to create a MAC address flooding attack. MAC address tables are limited in size. MAC flooding attacks exploit this limitation with fake source MAC

addresses until the switch MAC address table is full and the switch is overwhelmed.

An attacker uses a network attack tool and continuously sends frames with fake, randomly-generated source and destination MAC addresses to the switch. The switch keeps updating its MAC address table with the information in the fake frames.

Eventually, the MAC address table becomes full of fake MAC addresses and enters into what is known as fail-open mode. In this mode, the switch broadcasts all frames to all machines on the network. As a result, the attacker can capture all of the frames, even frames that are not addressed to its MAC address table.

The switch is in fail-open mode and broadcasts all received frames out of every port. Therefore, frames sent from host A to host B are also broadcast out of port 3 on the switch and seen by the attacker.

Configure port security on the switch to mitigate MAC address table overflow attacks.

VLAN Attacks

The VLAN architecture simplifies network maintenance and improves performance, but it also opens the door to abuse. There are a variety of VLAN related attacks that exist.

The figure illustrates one type of VLAN threat which is the switch spoofing attack. The attacker attempts to gain VLAN access by configuring a host to spoof a switch and use the 802.1Q trunking protocol and the Cisco-proprietary Dynamic Trunking Protocol (DTP) feature to trunk with the connecting switch. If successful and the switch establishes a trunk link with the host and the attacker can then access all the VLANS on the switch and hop (i.e., send and receive) traffic on all the VLANs.

There are several ways to mitigate VLAN attacks:

Explicitly configure access links

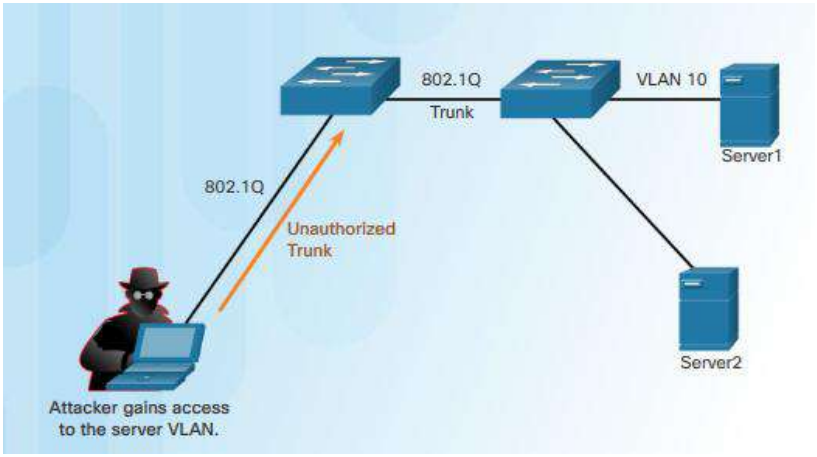
Explicitly disable auto trunking

Manually enable trunk links

Disable unused ports, make them access ports, and assign them to a black hole VLAN

Change the default native VLAN

Implement port security



DHCP Attacks

DHCP is the protocol that automatically assigns a host a valid IP address out of a DHCP pool.

There are two types of DHCP attacks which can be performed against a switched network:

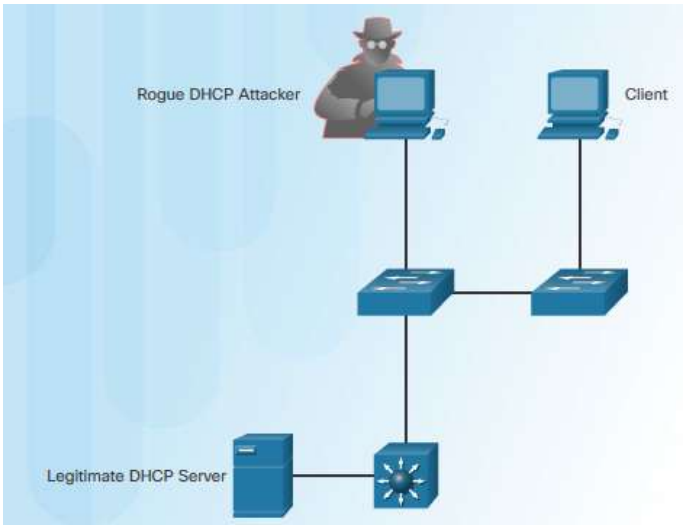
DHCP spoofing attack - An attacker configures a fake DHCP server on the network to issue IP addresses to clients. This type of attack forces the clients to use both a false Domain Name System (DNS) server and a computer which is under the control of the attacker as their default gateway.

DHCP starvation attack - An attacker floods the DHCP server with bogus DHCP requests and eventually leases all of the available IP addresses in the DHCP server pool. After these IP addresses are issued, the server cannot issue any more addresses, and this situation produces a denial-of-service (DoS) attack as new clients cannot obtain network access.

Note: A DoS attack is any attack that is used to overload specific devices and network services with illegitimate traffic, thereby preventing legitimate traffic from reaching those resources.

DHCP starvation is often used before a DHCP spoofing attack to deny service to the legitimate DHCP server. This makes it easier to introduce a fake DHCP server into the network.

Configure DHCP snooping and port security on the switch to mitigate DHCP attacks.



Review questions

Describe vulnerabilities and threats.

Learning Outcome 4.3: Apply Network Attack Mitigation

Secure the LAN

As noted at the beginning of this chapter, security is only as strong as the weakest link in the system, and Layer 2 is considered to be that weakest link. Therefore, Layer 2 security solutions must be implemented to help secure a network.

Many network management protocols including Telnet, Syslog, SNMP, TFTP, and FTP are insecure. There are several strategies to help secure Layer 2 of a network:

- Always use secure variants of these protocols such as SSH, SCP, SSL, SNMPv3, and SFTP.
- Always use strong passwords and change them often.
- Enable CDP on select ports only.
- Secure Telnet access.
- Use a dedicated management VLAN where nothing but management traffic resides.
- Use ACLs to filter unwanted access.

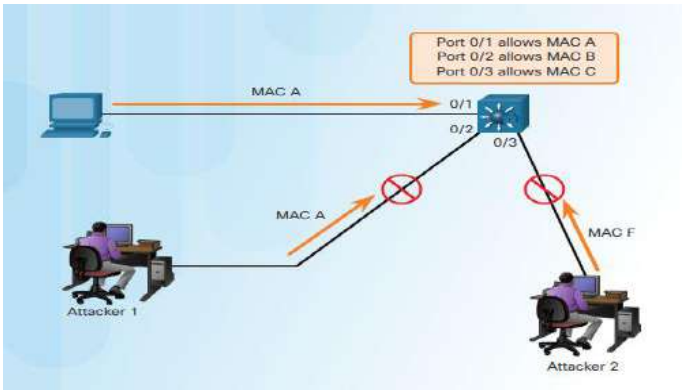
This topic covers several Layer 2 security solutions:

- Mitigating MAC address table flooding attacks using port security
- Mitigating VLAN attacks
- Mitigating DHCP attacks using DHCP snooping
- Securing administrative access using AAA
- Securing device access using 802.1X port authentication

Note: IP Source Guard (IPSG) and Dynamic ARP Inspection (DAI) are advanced switch security solutions discussed in the CCNA Security course.

Mitigate MAC Address Flooding Table Attacks

The simplest and most effective method to prevent MAC table flooding attacks is to enable port security.



Port security allows an administrator to statically specify MAC addresses for a port, or to permit the switch to dynamically learn a limited number of MAC addresses. By limiting the number of permitted MAC addresses on a port to one, port security can be used to control unauthorized expansion of the network, as shown in the figure.

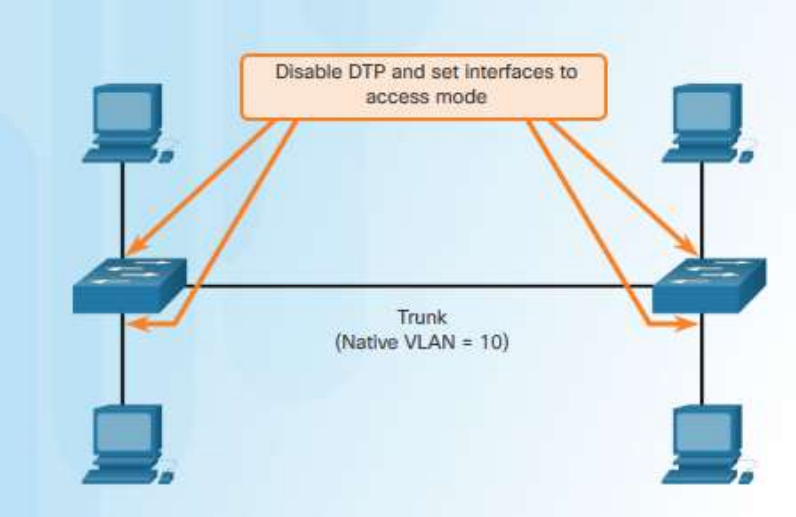
When MAC addresses are assigned to a secure port, the port does not forward frames with source MAC

addresses outside the group of defined addresses. When a port configured with port security receives a frame, the source MAC address of the frame is compared to the list of secure source addresses that were manually configured, or auto configured (learned), on the port.

If a port is configured as a secure port and the maximum number of MAC addresses is reached, any additional attempts to connect by unknown MAC addresses will generate a security violation. The figure summarizes these points.

Mitigate VLAN Attacks

The figure shows the best way to prevent basic VLAN attacks:



Disable DTP (auto trunking) negotiations on non-trunking ports by using the switchport mode access interface configuration command.

Manually enable the trunk link on a trunking port using the switchport mode trunk interface configuration command.

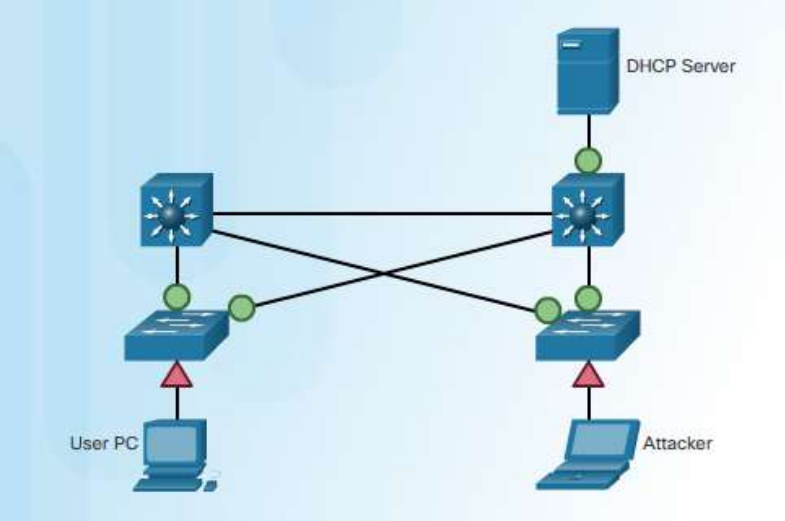
Disable DTP (auto trunking) negotiations on trunking ports using the switchport non-negotiate interface configuration command.

Set the native VLAN to be something other than VLAN 1. Set it on an unused VLAN using the switchport trunk native vlan *vlan_number* interface configuration mode command.

Disable unused ports and assign them to an unused VLAN.

Mitigate DHCP Attacks

A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. DHCP spoofing is dangerous because clients can be leased IP information for malicious DNS server addresses, malicious default gateways, and malicious IP assignments.



Security best practices recommend using DHCP snooping to mitigate DHCP spoofing attacks.

When DHCP snooping is enabled on an interface or VLAN and a switch receives a DHCP packet on an untrusted port, the switch compares the source packet information with that held in the DHCP Snooping Binding Database. The switch will deny packets containing any of the following information: Unauthorized DHCP server messages coming from an untrusted port, Unauthorized DHCP client messages not adhering to the DHCP Snooping Binding Database or rate limits.

In a large network, the DHCP Snooping Binding Database may take time to build after it is enabled. For example, it could take two days for DHCP snooping to complete the database if DHCP lease time is four days. DHCP snooping recognizes two types of ports: Trusted DHCP ports - Only ports connecting to upstream DHCP servers should be trusted. These ports should lead to legitimate DHCP servers replying with DHCP Offer and DHCP Ack messages. Trusted ports must be explicitly identified in the configuration.

Untrusted ports - These ports connect to hosts that should not be providing DHCP server messages. By default, all switch ports are untrusted.

The figure provides a visual example of how DHCP snooping ports should be assigned on a network. Notice how the trusted ports always lead to the legitimate DHCP server while all other ports (i.e., access ports connecting to endpoints) are untrusted by default.

Review questions

See the practical attachment.

Learning Outcome 4.4: Implement secure network device access

Secure Administrative Access using AAA

To keep malicious users from gaining access to sensitive network equipment and services, administrators must enable access control. Access control limits who or what can use specific resources. It also limits the services or options that are available after access is granted.

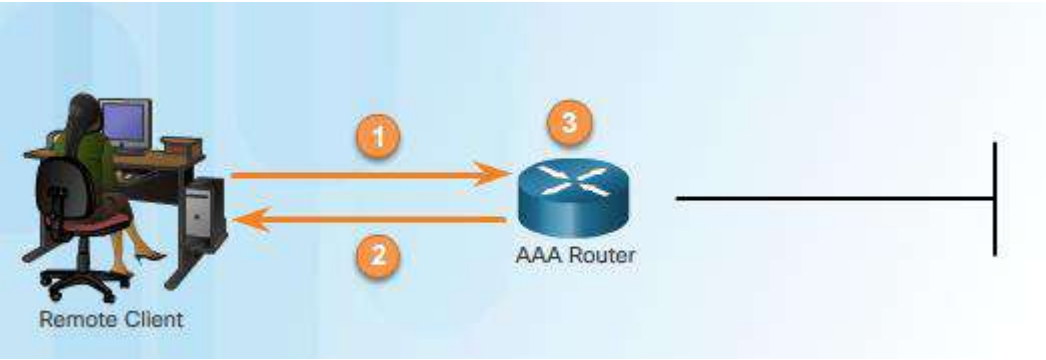
There are different methods of implementing authentication on a Cisco device, and each method offers varying levels of security. The Authentication, Authorization, and Accounting (AAA) framework is used to help secure device access. AAA Authentication can be used to authenticate users for administrative access or it can be used to authenticate users for remote network access.

Cisco provides two common methods of implementing AAA services:

Local AAA Authentication -Local AAA uses a local database for authentication. This method is sometimes known as self-contained authentication. This method stores usernames and passwords locally in the Cisco router, and users authenticate against the local database. Local AAA is ideal for small networks.

Server-Based AAA Authentication - Server-based AAA authentication is a much more scalable solution. With server-based method, the router accesses a central AAA server. The AAA server contains the usernames and password for all users and serves as a central authentication system for all infrastructure devices.

Figure 1 illustrates how local AAA authentication works:

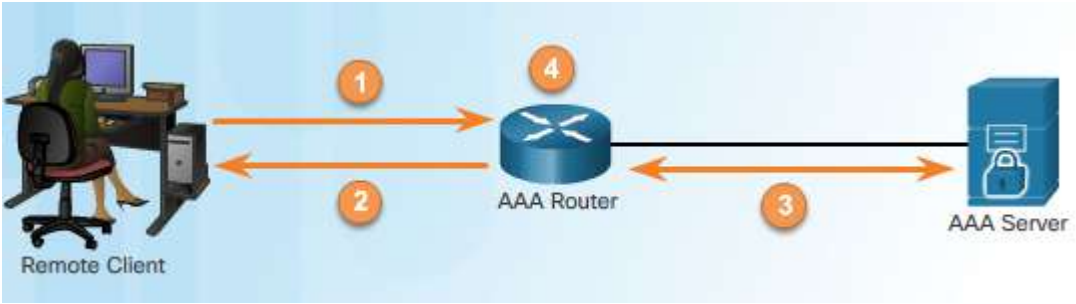


The client establishes a connection with the router.

The AAA router prompts the user for a username and password.

The router authenticates the username and password using the local database, and the user is provided access to the network based on the information in the local database.

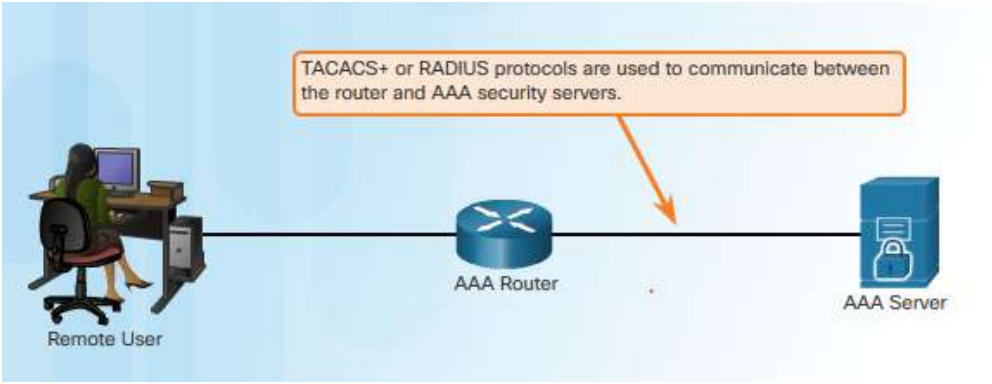
Figure 2 illustrates how server-based AAA authentication works:



The client establishes a connection with the router.

The AAA router prompts the user for a username and password.

The router authenticates the username and password using a remote AAA server.



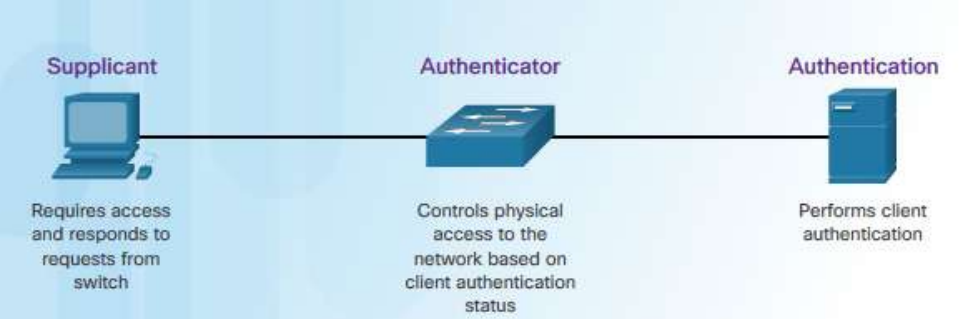
As shown in Figure 3, the AAA-enabled router uses either the Terminal Access Controller Access Control System (TACACS+) protocol or the Remote Authentication Dial-In User Service (RADIUS) protocol to communicate with the AAA server. While both protocols can be used to communicate between a router and AAA servers, TACACS+ is considered the more secure protocol. This is because all TACACS+ protocol exchanges are encrypted, while RADIUS only encrypts the user's password. RADIUS does not encrypt user names, accounting information, or any other information carried in the RADIUS message.

Note: For more information on AAA, refer to the CCNA Security course.

Secure Device Access using 802.1X

Network user authentication can be provided with AAA server-based authentication. The 802.1X protocol/standard can be used to authenticate network devices on the corporate network. There is another protocol used to secure computers connecting to a LAN.

The IEEE 802.1X standard defines a port-based access control and authentication protocol. IEEE 802.1X restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports. The authentication server authenticates each workstation that is connected to a switch port before making available any services offered by the switch or the LAN.



With 802.1X port-based authentication, the devices in the network have specific roles, as shown in the figure:

Client (Supplicant) - This is usually the 802.1X-enabled port on the device. The device requests access to LAN and switch services and then responds to requests from the switch. In the figure, the device is a PC running 802.1X-compliant client software. Another client supplicant is the 802.1X-compliant wireless device such as a laptop or tablet.

Switch (Authenticator) – This controls physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server. It requests identifying information from the client, verifies that information with the authentication server, and relays a response to the client. The switch uses a RADIUS software agent, which is responsible for encapsulating and de-encapsulating the EAP (Extensible Authentication Protocol) frames and interacting with the authentication server. Another device that could act as authenticator is a wireless access point acting as the intermediary between the wireless client and the authentication server.

Authentication server – This performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch or other authenticator such as a wireless access point whether the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. The RADIUS security system with EAP extensions is the only supported authentication server.

Note: For more information on 802.1X, refer to the CCNA Security course.

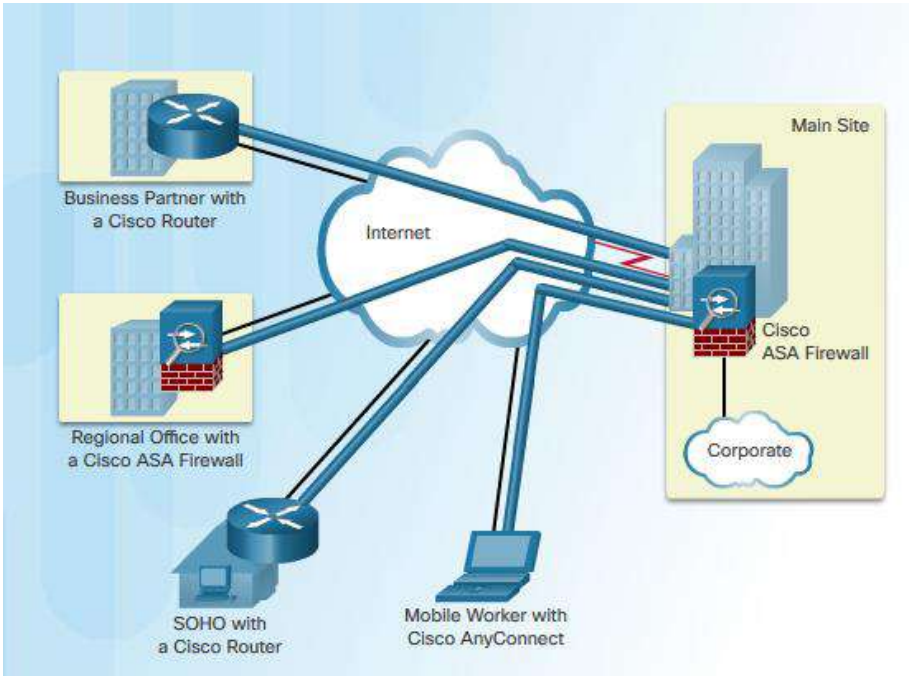
Review questions

How is the AAA implemented in network?

Learning Outcome 4.5: Apply Virtual Private Networks

Introducing VPNs

Organizations need secure, reliable, and cost-effective ways to interconnect multiple networks, such as allowing branch offices and suppliers to connect to a corporation's headquarter network. Additionally, with the growing number of teleworkers, enterprises have an increasing need for secure, reliable, and cost-effective ways to connect employees working in small office/home office (SOHO) and other remote locations, with resources on corporate sites.



As shown in the figure, organizations use VPNs to create an end-to-end private network connection over third-party networks, such as the Internet. The tunnel eliminates the distance barrier and enables remote users to access central site network resources. A VPN is a private network created via tunneling over a public network, usually the Internet. A VPN is a communications environment in which access is strictly controlled to permit peer connections within a defined community of interest.

The first VPNs were strictly IP tunnels that did not include authentication or encryption of the data. For example, Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco that can encapsulate a wide variety of network layer protocol packet types inside IP tunnels but it doesn't support encryption. This creates a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

Today, a secure implementation of VPN with encryption, such as IPsec VPNs, is what is usually meant by virtual private networking.

To implement VPNs, a VPN gateway is necessary. The VPN gateway could be a router, a firewall, or a Cisco Adaptive Security Appliance (ASA). An ASA is a standalone firewall device that combines firewall, VPN concentrator, and intrusion prevention functionality into one software image.

Benefits of VPNs

VPN uses virtual connections that are routed through the Internet from the private network of an organization to the remote site or employee host. The information from a private network is securely transported over the public network, to form a virtual network.

The benefits of a VPN include the following:

Cost savings - VPNs enable organizations to use cost-effective, third-party Internet transport to connect remote offices and remote users to the main site; therefore, eliminating expensive, dedicated WAN links and modem banks. Furthermore, with the advent of cost-effective, high-bandwidth technologies, such as DSL, organizations can use VPNs to reduce their connectivity costs while simultaneously increasing remote connection bandwidth.

Scalability - VPNs enable organizations to use the Internet infrastructure within ISPs and devices, which makes it easy to add new users. Therefore, organizations are able to add large amounts of capacity without adding significant infrastructure.

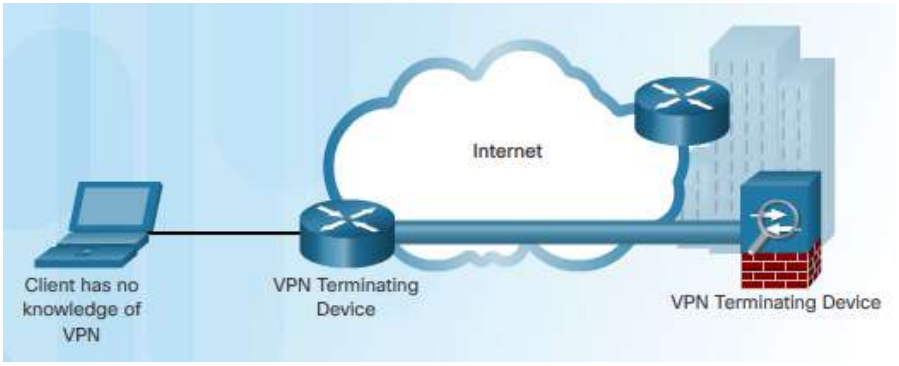
Compatibility with broadband technology - VPNs allow mobile workers and telecommuters to take advantage of high-speed, broadband connectivity, such as DSL and cable, to access to their organizations' networks. Broadband connectivity provides flexibility and efficiency. High-speed, broadband connections also provide a cost-effective solution for connecting remote offices.

Security - VPNs can include security mechanisms that provide the highest level of security by using advanced encryption and authentication protocols that protect data from unauthorized access.

Types of VPN

Site-to-Site VPNs

A site-to-site VPN is created when devices on both sides of the VPN connection are aware of the VPN configuration in advance, as shown in the figure. The VPN remains static, and internal hosts have no knowledge that a VPN exists. In a site-to-site VPN, end hosts send and receive normal TCP/IP traffic through a VPN "gateway". The VPN gateway is responsible for encapsulating and encrypting outbound traffic for all traffic from a particular site. The VPN gateway then sends it through a VPN tunnel over the Internet to a peer VPN gateway at the target site. Upon receipt, the peer VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network.



A site-to-site VPN is an extension of a classic WAN network. Site-to-site VPNs connect entire networks

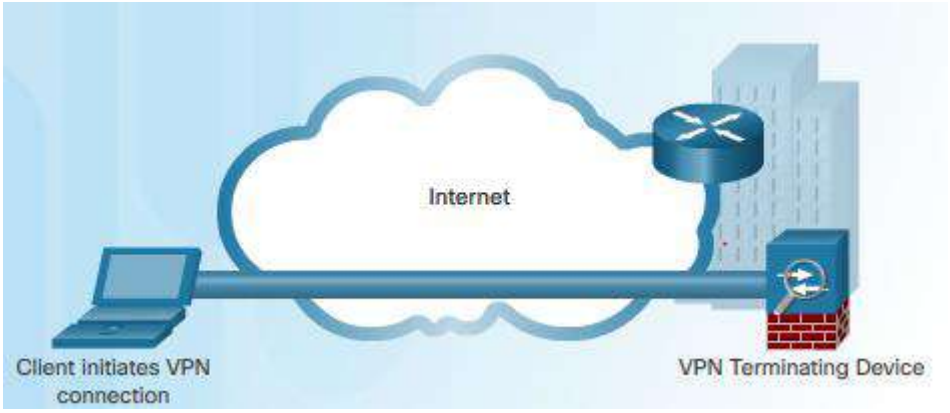
to each other, for example, they can connect a branch office network to a company headquarters network. In the past, a leased line or Frame Relay connection was required to connect sites, but because most corporations now have Internet access, these connections can be replaced with site-to-site VPNs.

Remote Access VPNs

Where a site-to-site VPN is used to connect entire networks, a remote-access VPN supports the needs of telecommuters, mobile users, and extranet, consumer-to-business traffic. A remote-access VPN is created when VPN information is not statically set up, but instead allows for dynamically changing information, and can be enabled and disabled. Remote-access VPNs support a client/server architecture, where the VPN client (remote host) gains secure access to the enterprise network via a VPN server device at the network edge, as shown in the figure.

Remote-access VPNs are used to connect individual hosts that must access their company network securely over the Internet. Internet connectivity used by telecommuters is typically a broadband connection.

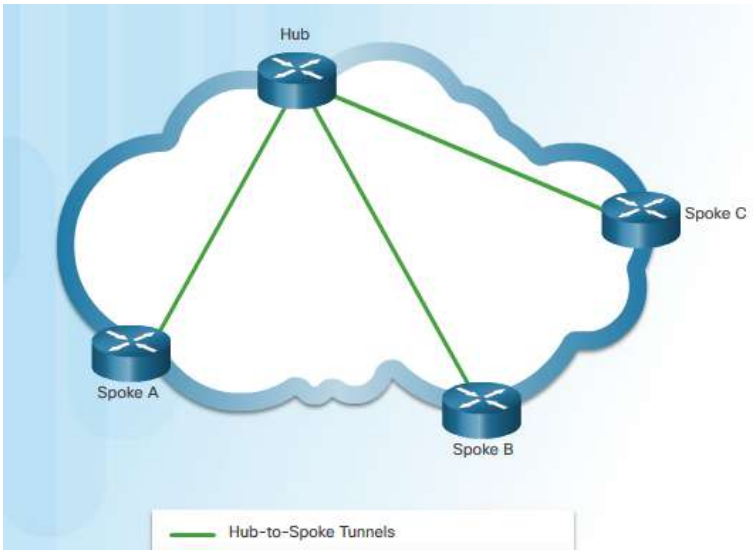
VPN client software may need to be installed on the mobile user's end device; for example, each host may have Cisco AnyConnect Secure Mobility Client software installed. When the host tries to send any traffic, the Cisco AnyConnect VPN Client software encapsulates and encrypts this traffic. The encrypted data is then sent over the Internet to the VPN gateway at the edge of the target network. Upon receipt, the VPN gateway behaves as it does for site-to-site VPNs.



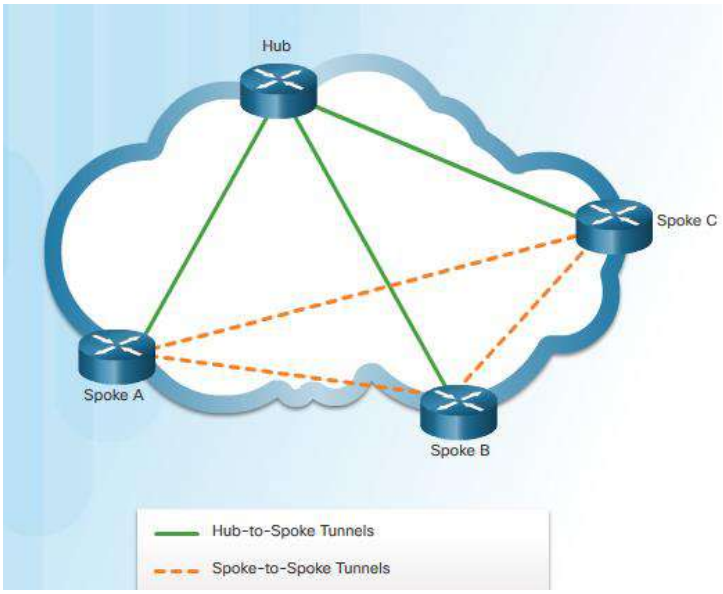
Note: The Cisco AnyConnect Secure Mobility Client software builds on prior Cisco AnyConnect VPN Client and Cisco VPN Client offerings to improve the always-on VPN experience across more laptop and smart phone-based mobile devices. This client supports IPv6.

DMVPN

Dynamic Multipoint VPN (DMVPN) is a Cisco software solution for building multiple VPNs in an easy, dynamic, and scalable manner. The goal is to simplify the configuration while easily and flexibly connecting central office sites with branch sites. This is called hub-to-spoke, as shown in Figure 1.



With DMVPNs, branch sites can also communicate directly with other branch sites, as shown in Figure 2.



DMVPN is built using the following technologies:

Next Hop Resolution Protocol (NHRP)

Multipoint Generic Routing Encapsulation (mGRE) tunnels

IP Security (IPsec) encryption

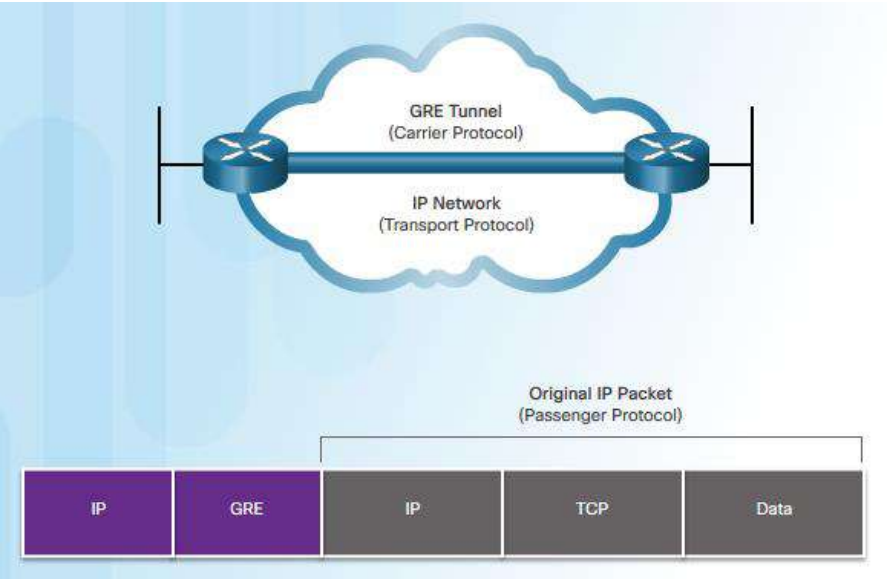
NHRP is a Layer 2 resolution and caching protocol similar to Address Resolution Protocol (ARP). NHRP creates a distributed mapping database of public IP addresses for all tunnel spokes. NHRP is a client server protocol consisting of the NHRP hub known as the Next Hop Server (NHS), and the NHRP spokes known as the Next Hop Clients (NHCs).

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels. An mGRE tunnel interface allows a single GRE interface to support multiple IPsec tunnels. With mGRE, dynamically allocated tunnels are created

through a permanent tunnel source at the hub and dynamically allocated tunnel destinations, created as necessary, at the spokes. This reduces the size and simplifies the complexity of the configuration.
Like other VPN types, DMVPN relies on IPsec to provide secure transport of private information over public networks, such as the Internet.

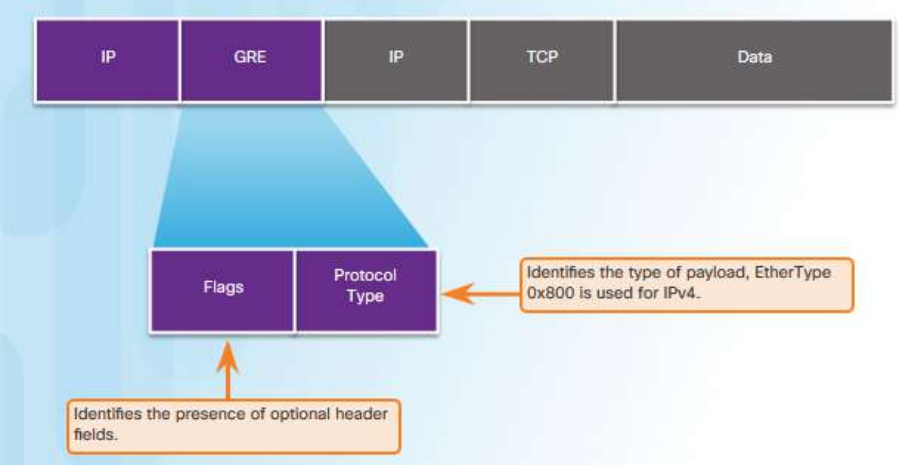
GRE Introduction

Generic Routing Encapsulation (GRE) is one example of a basic, non-secure, site-to-site VPN tunneling protocol. GRE is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels. GRE creates a virtual point-to-point link to Cisco routers at remote points, over an IP internetwork.
GRE is designed to manage the transportation of multiprotocol and IP multicast traffic between two or more sites, that may only have IP connectivity. It can encapsulate multiple protocol packet types inside an IP tunnel.
A tunnel interface supports a header for each of the following:
An encapsulated protocol (or passenger protocol), such as IPv4, IPv6, AppleTalk, DECnet, or IPX
An encapsulation protocol (or carrier), such as GRE
A transport delivery protocol, such as IP, which is the protocol that carries the encapsulated protocol



GRE Characteristics

GRE is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. IP tunneling using GRE enables network expansion across a single-protocol backbone environment. It does this by connecting multiprotocol subnetworks in a single-protocol backbone environment.



GRE has these characteristics:

GRE is defined as an IETF standard (RFC 2784).

In the outer IP header, 47 is used in the protocol field to indicate that a GRE header will follow.

GRE encapsulation uses a protocol type field in the GRE header to support the encapsulation of any OSI Layer 3 protocol. Protocol Types are defined in RFC 1700 as "EtherTypes".

GRE itself is stateless; by default, it does not include any flow-control mechanisms.

GRE does not include any strong security mechanisms to protect its payload.

The GRE header, together with the tunneling IP header indicated in the figure, creates at least 24 bytes of additional overhead for tunneled packets.

1. what is VPN?
2. what are the types of VPN?
3. Describe the benefits of VPN

Configure GRE

GRE is used to create a VPN tunnel between two sites, as shown in Figure 1. To implement a GRE tunnel, the network administrator must first learn the IP addresses of the endpoints. After that, there are five steps to configuring a GRE tunnel:

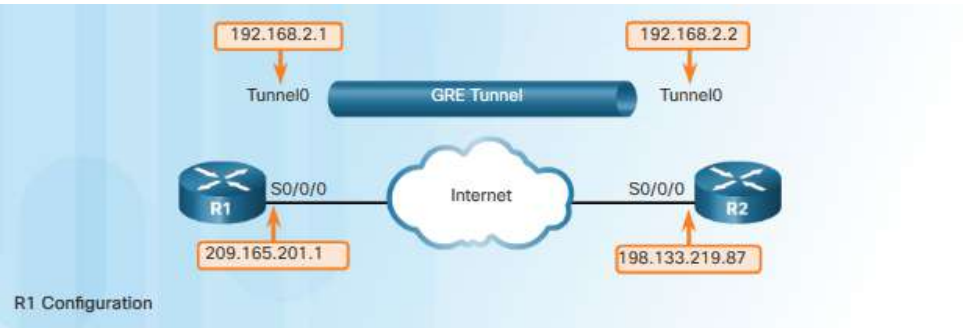
Step 1. Create a tunnel interface using the interface tunnel *number*command.

Step 2. Configure an IP address for the tunnel interface. This is normally a private IP address.

Step 3. Specify the tunnel source IP address.

Step 4. Specify the tunnel destination IP address.

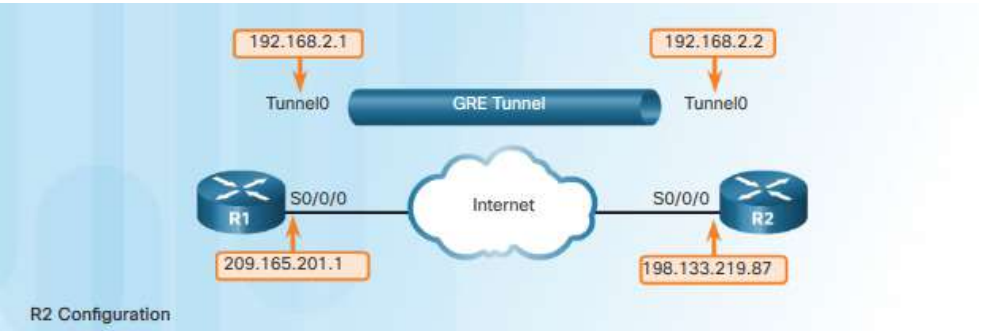
Step 5. (Optional) Specify GRE tunnel mode as the tunnel interface mode. GRE tunnel mode is the default tunnel interface mode for Cisco IOS software.



R1 Configuration

```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 198.133.219.87
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

The sample configuration in Figure 2 illustrates a basic GRE tunnel configuration for router R1.



R2 Configuration

```
R2(config)# interface Tunnel0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 198.133.219.87
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

The configuration of R2 in Figure 3 mirrors the configuration of R1.

The minimum configuration requires specification of the tunnel source and destination addresses. The IP subnet must also be configured to provide IP connectivity across the tunnel link. Both tunnel

interfaces have the tunnel source set as the local serial S0/0/0 interface and the tunnel destination set as the peer router serial S0/0/0 interface. A private IP address is commonly assigned to the tunnel interface on both routers. OSPF has also been configured to exchange routes over the GRE tunnel.
The individual GRE tunnel command descriptions are displayed in Figure 4.

Command	Description
tunnel mode gre ip	Specifies that the mode of the tunnel interface is GRE over IP.
tunnel source *ip_address*	Specifies the tunnel source address.
tunnel destination *ip_address*	Specifies the tunnel destination address.
ip address *ip_address mask*	Specifies the IP address of the tunnel interface.

Note: When configuring GRE tunnels, it can be difficult to remember which IP networks are associated with the physical interfaces and which IP networks are associated with the tunnel interfaces. Remember that before a GRE tunnel is created, the physical interfaces have already been configured. The tunnel source and tunnel destination commands reference the IP addresses of the preconfigured physical interfaces. The ip address command on the tunnel interfaces refers to an IP network (usually a private IP network) specifically selected for the purposes of the GRE tunnel.

LEARNING UNIT 5- APPLY QUALITY OF SERVICE

Learning Outcomes:	Identify traffic characteristics Select Quality of service (QoS) model Implement of QoS
Learning hours:	15Hours

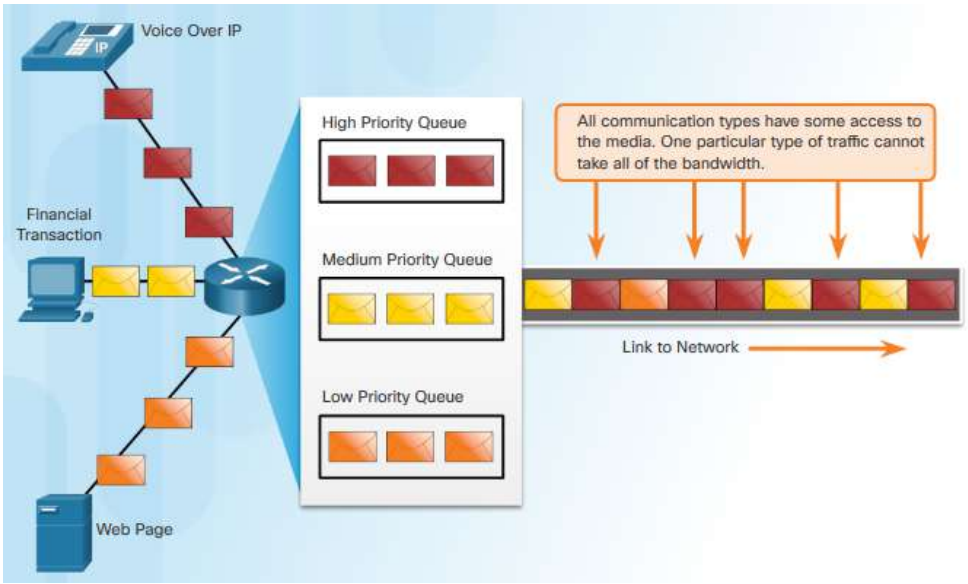
In today's networks, users expect content to be immediately available. But if the traffic exceeds the bandwidth of the links between the source of the content and the user, how do network administrators ensure a quality experience? Quality of Service (QoS) tools can be designed into the network to guarantee that certain traffic types, such as voice and video, are prioritized over traffic that is not as time-sensitive, such as email and web browsing.

Learning Outcome 5.1: Identify traffic characteristics

Prioritizing Traffic

Quality of Service (QoS) is an ever-increasing requirement of networks today. New applications available to users, such as voice and live video transmissions, create higher expectations for quality delivery.

Congestion occurs when multiple communication lines aggregate onto a single device such as a router, and then much of that data is placed on fewer outbound interfaces, or onto a slower interface. Congestion can also occur when large data packets prevent smaller packets from being transmitted in a timely manner.



When the volume of traffic is greater than what can be transported across the network, devices queue, or hold, the packets in memory until resources become available to transmit them. Queuing packets

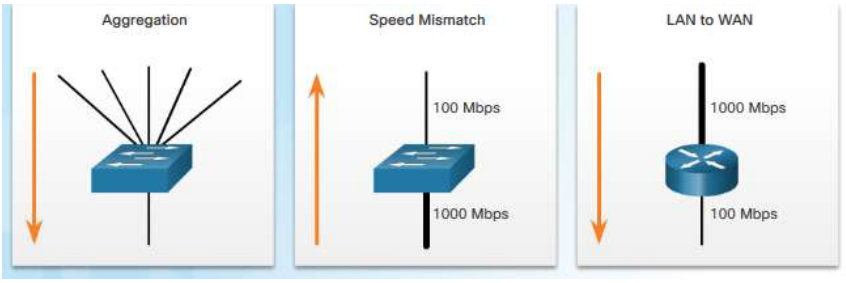
causes delay because new packets cannot be transmitted until previous packets have been processed. If the number of packets to be queued continues to increase, the memory within the device fills up and packets are dropped. One QoS technique that can help with this problem is to classify data into multiple queues, as shown in the figure.

Note: A device implements QoS only when it is experiencing some type of congestion.

Bandwidth, Congestion, Delay, and Jitter

Network bandwidth is measured in the number of bits that can be transmitted in a single second, or bits per second (bps). For example, a network device may be described as having the capability to perform at 10 gigabits per second (Gbps).

Network congestion causes delay. An interface experiences congestion when it is presented with more traffic than it can handle. Network congestion points are strong candidates for QoS mechanisms. Figure 1 shows three examples of typical congestion points.



Delay or latency refers to the time it takes for a packet to travel from the source to the destination. Two types of delays are fixed and variable. A fixed delay is a specific amount of time a specific process takes, such as how long it takes to place a bit on the transmission media. A variable delay take an unspecified amount of time and is affected by factors such as how much traffic is being processed.

The sources of delay are summarized in table in Figure 2.

Delay	Description
Code delay	The fixed amount of time it takes to compress data at the source before transmitting to the first internetworking device, usually a switch.
Packetization delay	The fixed time it takes to encapsulate a packet with all the necessary header information.
Queuing delay	The variable amount of time a frame or packet waits to be transmitted on the link.
Serialization delay	The fixed amount of time it takes to transmit a frame onto the wire.
Propagation delay	The variable amount of time it takes for the frame to travel between the source and destination.
De-jitter delay	The fixed amount of time it takes to buffer a flow of packets and then send them out in evenly spaced intervals.

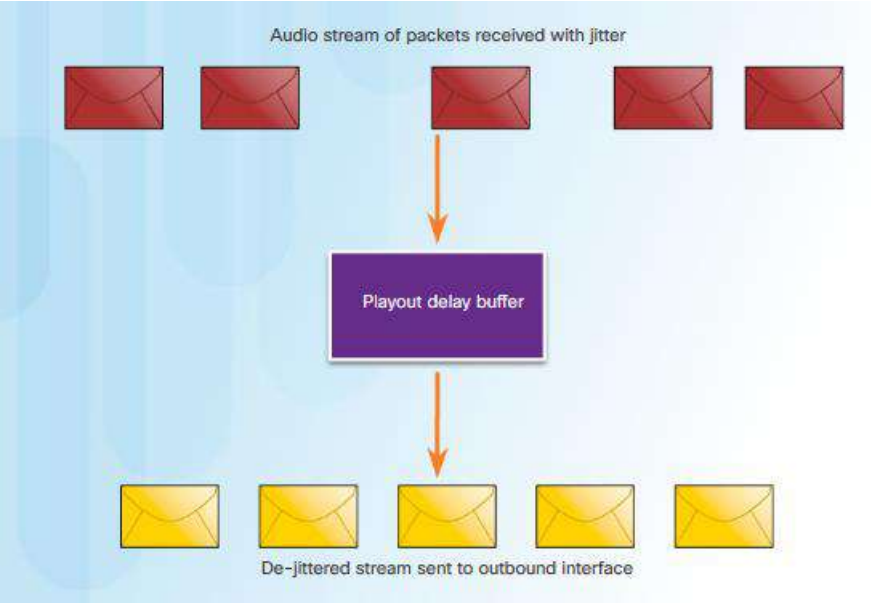
Jitter is the variation in the delay of received packets. At the sending side, packets are sent in a continuous stream with the packets spaced evenly apart. Due to network congestion, improper queuing, or configuration errors, the delay between each packet can vary instead of remaining constant. Both delay and jitter need to be controlled and minimized to support real-time and interactive traffic.

Packet Loss

Without any QoS mechanisms in place, packets are processed in the order in which they are received.

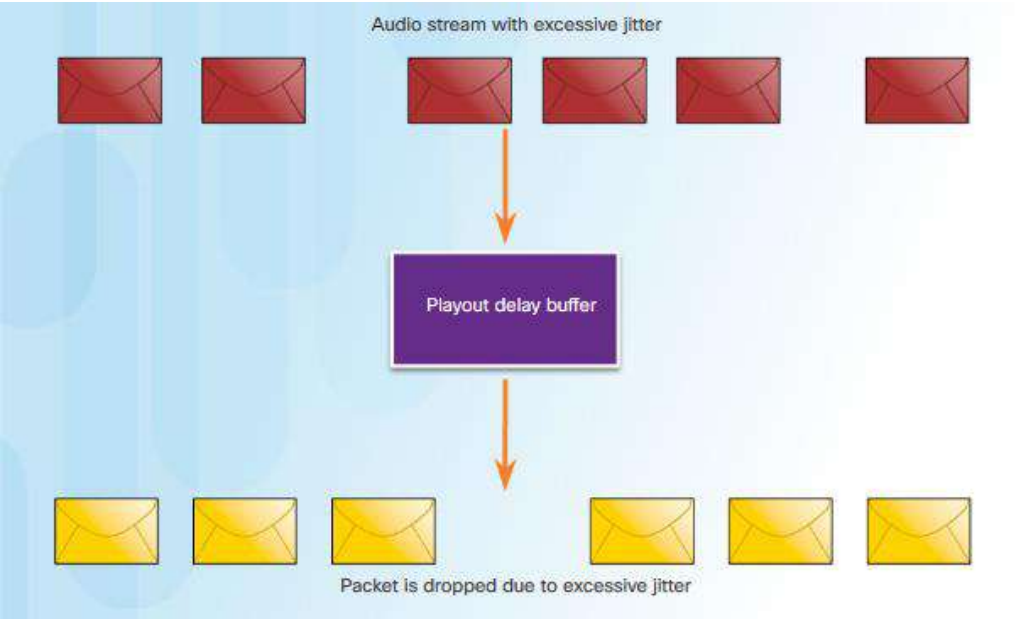
When congestion occurs, network devices such as routers and switches can drop packets. This means that time-sensitive packets, such as real-time video and voice, will be dropped with the same frequency as data that is not time-sensitive, such as email and web browsing.

For example, when a router receives a Real-Time Protocol (RTP) digital audio stream for Voice over IP (VoIP), it must compensate for the jitter that is encountered. The mechanism that handles this function is the playout delay buffer. The playout delay buffer must buffer these packets and then play them out in a steady stream as shown in Figure 1. The digital packets are later converted back to an analog audio stream.



If the jitter is so large that it causes packets to be received out of the range of this buffer, the out-of-range packets are discarded and dropouts are heard in the audio, as shown in Figure 2.

For losses as small as one packet, the digital signal processor (DSP) interpolates what it thinks the audio should be and no problem is audible to the user. However, when jitter exceeds what the DSP can do to make up for the missing packets, audio problems are heard.



Packet loss is a very common cause of voice quality problems on an IP network. In a properly designed network, packet loss should be near zero. The voice codecs used by the DSP can tolerate some degree of packet loss without a dramatic effect on voice quality. Network engineers use QoS mechanisms to classify voice packets for zero packet loss. Bandwidth is guaranteed for the voice calls by giving priority to voice traffic over traffic that is not time-sensitive.

Voice

Voice traffic is predictable and smooth, as shown in the figure. However, voice is very sensitive to delays and dropped packets; there is no reason to re-transmit voice if packets are lost. Therefore, voice packets must receive a higher priority than other types of traffic. Therefore, it must receive a higher priority. For example, Cisco products use the RTP port range 16384 to 32767 to prioritize voice traffic. Voice can tolerate a certain amount of latency, jitter, and loss without any noticeable effects. Latency should be no more than 150 milliseconds (ms). Jitter should be no more than 30 ms, and voice packet loss should be no more than 1%. Voice traffic requires at least 30 Kbps of bandwidth.

Video

Without QoS and a significant amount of extra bandwidth capacity, video quality typically degrades. The picture appears blurry, jagged, or in slow motion. The audio portion of the feed may become unsynchronized with the video.

Video traffic tends to be unpredictable, inconsistent, and bursty compared to voice traffic. Compared to voice, video is less resilient to loss and has a higher volume of data per packet. Notice how voice packets arrive every 20 ms and are a predictable 200 bytes each. In contrast, the number and size of video packets varies every 33 ms based on the content of the video. For example, if the video stream consists of content that is not changing much from frame to frame, then the video packets will be small and fewer are required to maintain acceptable user experience. However, if the video steam consists of content that is rapidly changing, such as in an action sequence in a movie, then the video packets will

be larger and more are required per 33 ms time slot to maintain an acceptable user experience.

UDP ports, such as 554 used for the Real-Time Streaming Protocol (RSTP), should be given priority over other, less time-sensitive, network traffic. Similar to voice, video can tolerate a certain amount of latency, jitter, and loss without any noticeable affects. Latency should be no more than 400 milliseconds (ms). Jitter should be no more than 50 ms, and video packet loss should be no more than 1%. Video traffic requires at least 384 Kbps of bandwidth.

Data

Most applications use either TCP or UDP. Unlike UDP, TCP performs error recovery. Data applications that have no tolerance for data loss, such as email and web pages, use TCP to ensure that, if packets are lost in transit, they will be resent. Data traffic can be smooth or bursty. Network control traffic is usually smooth and predictable. When there is a topology change, the network control traffic may burst for a few seconds. But the capacity of today's networks can easily handle the increase in network control traffic as the network converges.

However, some TCP applications can be very greedy, consuming a large portion of network capacity. FTP will consume as much bandwidth as it can get when you download a large file, such as a movie or game.

Although data traffic is relatively insensitive to drops and delays compared to voice and video, a network administrator still needs to consider the quality of the user experience, sometimes referred to as Quality of Experience or QoE. The two main factors a network administrator needs to ask about the flow of data traffic are the following:

Does the data come from an interactive application?

Is the data mission critical?

Review questions

1. Identify the traffic characteristics in converged network.

Learning Outcome 5.2: Select Quality of service (QoS) model

Queuing Overview

The QoS policy implemented by the network administrator becomes active when congestion occurs on the link. Queuing is a congestion management tool that can buffer, prioritize, and, if required, reorder packets before being transmitted to the destination. A number of queuing algorithms are available. For the purposes of this course, we will focus on the following:

- First-In, First-Out (FIFO)
- Weighted Fair Queuing (WFQ)
- Class-Based Weighted Fair Queuing (CBWFQ)
- Low Latency Queuing (LLQ)
- First In First Out (FIFO)

In its simplest form, FIFO queuing, also known as first-come, first-served (FCFS) queuing, involves buffering and forwarding of packets in the order of arrival.

FIFO has no concept of priority or classes of traffic and consequently, makes no decision about packet priority. There is only one queue, and all packets are treated equally. Packets are sent out an interface in the order in which they arrive, as shown in the figure. Although some traffic is more important or time-sensitive based on the priority classification, notice that the traffic is sent out in the order it is received.

When FIFO is used, important or time-sensitive traffic can be dropped when congestion occurs on the router or switch interface. When no other queuing strategies are configured, all interfaces except serial interfaces at E1 (2.048 Mbps) and below use FIFO by default. (Serial interfaces at E1 and below use WFQ by default.)

FIFO, which is the fastest method of queuing, is effective for large links that have little delay and minimal congestion. If your link has very little congestion, FIFO queuing may be the only queuing you need to use.

Weighted Fair Queuing (WFQ)

WFQ is an automated scheduling method that provides fair bandwidth allocation to all network traffic. WFQ applies priority, or weights, to identified traffic and classifies it into conversations or flows, as shown in the figure.

WFQ then determines how much bandwidth each flow is allowed relative to other flows. The flow-based algorithm used by WFQ simultaneously schedules interactive traffic to the front of a queue to reduce response time. It then fairly shares the remaining bandwidth among high-bandwidth flows. WFQ allows you to give low-volume, interactive traffic, such as Telnet sessions and voice, priority over high-volume traffic, such as FTP sessions. When multiple file transfers flows are occurring simultaneously, the transfers are given comparable bandwidth.

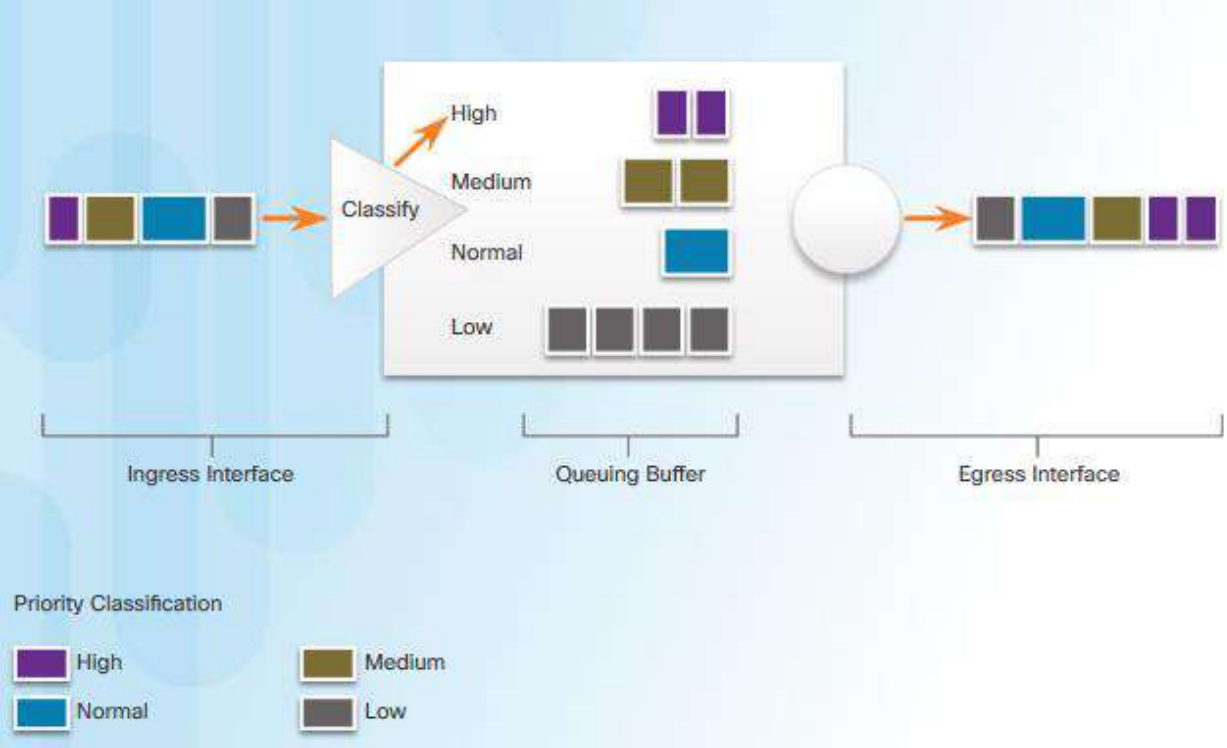
WFQ classifies traffic into different flows based on packet header addressing, including such characteristics as source and destination IP addresses, MAC addresses, port numbers, protocol, and Type of Service (ToS) value. The ToS value in the IP header can be used to classify traffic. ToS will be discussed later in the chapter.

Low-bandwidth traffic streams, which comprise the majority of traffic, receive preferential service, allowing their entire offered loads to be sent in a timely fashion. High-volume traffic streams share the remaining capacity proportionally among themselves.

Limitations

WFQ is not supported with tunneling and encryption because these features modify the packet content information required by WFQ for classification.

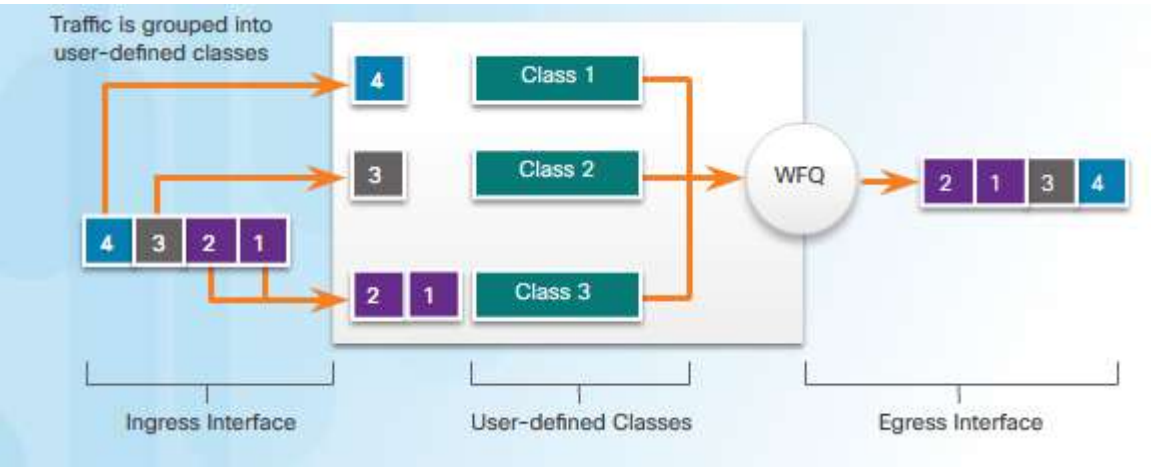
Although WFQ automatically adapts to changing network traffic conditions, it does not offer the degree of precision control over bandwidth allocation that CBWFQ offers.



Class-Based Weighted Fair Queuing (CBWFQ)

CBWFQ extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces. Packets satisfying the match criteria for a class constitute the traffic for that class. A FIFO queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class, as shown in the figure.

When a class has been defined according to its match criteria, you can assign it characteristics. To characterize a class, you assign it bandwidth, weight, and maximum packet limit. The bandwidth assigned to a class is the guaranteed bandwidth delivered to the class during congestion.

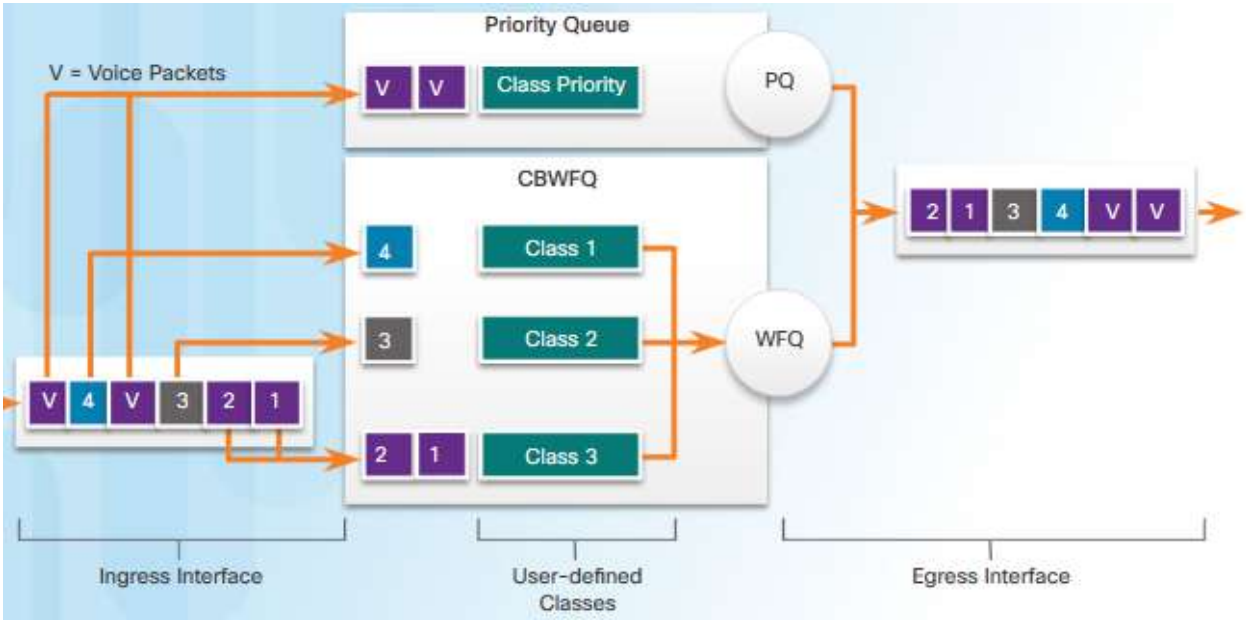


To characterize a class, you also specify the queue limit for that class, which is the maximum number of packets allowed to accumulate in the queue for the class. Packets belonging to a class are subject to the bandwidth and queue limits that characterize the class.

After a queue has reached its configured queue limit, adding more packets to the class causes tail drop or packet drop to take effect, depending on how class policy is configured. Tail drop means a router simply discards any packet that arrives at the tail end of a queue that has completely used up its packet-holding resources. This is the default queuing response to congestion. Tail drop treats all traffic equally and does not differentiate between classes of service.

Low Latency Queuing (LLQ)

The LLQ feature brings strict priority queuing (PQ) to CBWFQ. Strict PQ allows delay-sensitive data such as voice to be sent before packets in other queues. LLQ provides strict priority queuing for CBWFQ, reducing jitter in voice conversations, as shown in the figure.



Without LLQ, CBWFQ provides WFQ based on defined classes with no strict priority queue available for real-time traffic. The weight for a packet belonging to a specific class is derived from the bandwidth you assigned to the class when you configured it. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced fairly based on weight; no class of packets may be granted strict priority. This scheme poses problems for voice traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission manifesting as jitter in the heard conversation.

With LLQ, delay-sensitive data is sent first, before packets in other queues are treated. LLQ allows delay-sensitive data such as voice to be sent first (before packets in other queues), giving delay-sensitive data preferential treatment over other traffic. Although it is possible to enqueue various types of real-time traffic to the strict priority queue, Cisco recommends that only voice traffic be directed to the priority queue.

Review questions

1. Explain the QoS models.

Learning Outcome 5.3: Implement of QoS

Selecting an Appropriate QoS Policy Model

How can QoS be implemented in a network? The three models for implementing QoS are:

- Best-effort model
- Integrated services (IntServ)
- Differentiated services (DiffServ)

Model	Description
Best-effort model	• Not really an implementation as QoS is not explicitly configured. • Use when QoS is not required.
Integrated services (IntServ)	• Provides very high QoS to IP packets with guaranteed delivery. • It defines a signaling process for applications to signal to the network that they require special QoS for a period and that bandwidth should be reserved. • However, IntServ can severely limit the scalability of a network.
Differentiated services (DiffServ)	• Provides high scalability and flexibility in implementing QoS. • Network devices recognize traffic classes and provide different levels of QoS to different traffic classes.

The table in the figure summarizes these three models. QoS is really implemented in a network using either IntServ or DiffServ. While IntServ provides the highest guarantee of QoS, it is very resource-intensive and therefore, limited in scalability. In contrast, DiffServ is less resource-intensive and more scalable. The two are sometimes co-deployed in network QoS implementations.

Best-Effort

The basic design of the Internet provides for best-effort packet delivery and provides no guarantees. This approach is still predominant on the Internet today and remains appropriate for most purposes. The best-effort model treats all network packets in the same way, so an emergency voice message is treated the same way a digital photograph attached to an email is treated. Without QoS, the network cannot tell the difference between packets and, as a result, cannot treat packets preferentially.

The best-effort model is similar in concept to sending a letter using standard postal mail. Your letter is treated exactly the same as every other letter. With the best-effort model, the letter may never arrive, and, unless you have a separate notification arrangement with the letter recipient, you may never know that the letter did not arrive.

Benefits	Drawbacks
The model is the most scalable.	There are no guarantees of delivery.
Scalability is only limited by bandwidth limits, in which case all traffic is equally affected.	Packets will arrive whenever they can and in any order possible, if they arrive at all.
No special QoS mechanisms are required.	No packets have preferential treatment.
It is the easiest and quickest model to deploy.	Critical data is treated the same as casual email is treated.

The table in the figure lists the benefits and drawbacks of the best effort model.

Integrated Services

The needs of real-time applications, such as remote video, multimedia conferencing, visualization, and virtual reality, motivated the development of the IntServ architecture model in 1994 (RFC 1633, 2211, and 2212). IntServ is a multiple-service model that can accommodate multiple QoS requirements.

IntServ provides a way to deliver the end-to-end QoS that real-time applications require by explicitly managing network resources to provide QoS to specific user packet streams, sometimes called microflows. It uses resource reservation and admission-control mechanisms as building blocks to establish and maintain QoS. This practice is similar to a concept known as "hard QoS." Hard QoS guarantees traffic characteristics, such as bandwidth, delay, and packet-loss rates, from end to end. Hard QoS ensures both predictable and guaranteed service levels for mission-critical applications.

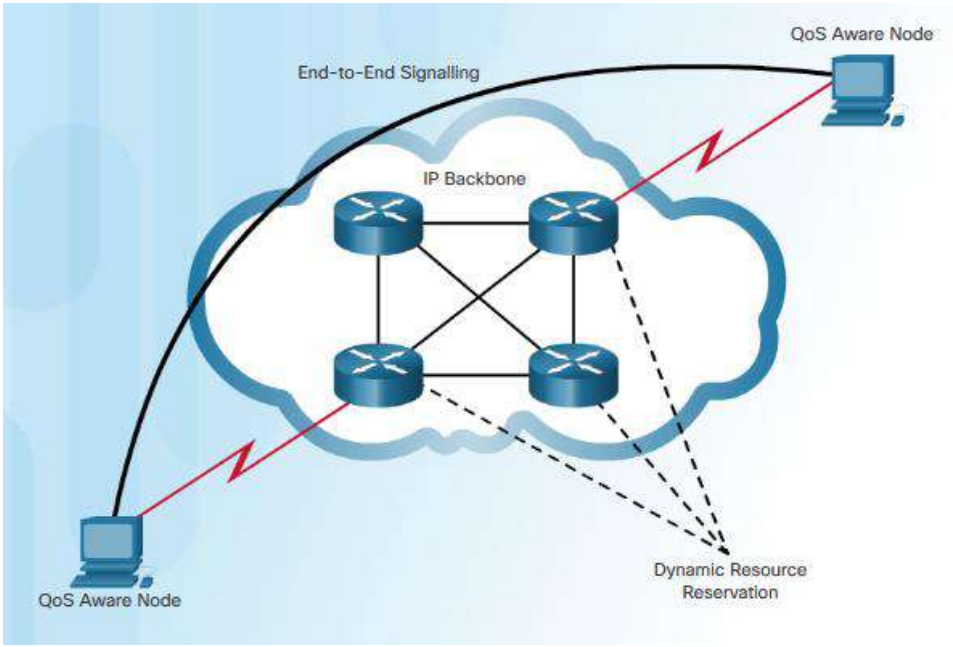


Figure 1 is a simple illustration of the IntServ model.

IntServ uses a connection-oriented approach inherited from telephony network design. Each individual communication must explicitly specify its traffic descriptor and requested resources to the network. The edge router performs admission control to ensure that available resources are sufficient in the network. The IntServ standard assumes that routers along a path set and maintain the state for each individual communication.

In the IntServ model, the application requests a specific kind of service from the network before sending data. The application informs the network of its traffic profile and requests a particular kind of service that can encompass its bandwidth and delay requirements. IntServ uses the Resource Reservation Protocol (RSVP) to signal the QoS needs of an application's traffic along devices in the end-to-end path through the network. If network devices along the path can reserve the necessary bandwidth, the originating application can begin transmitting. If the requested reservation fails along the path, the originating application does not send any data.

The edge router performs admission control based on information from the application and available

network resources. The network commits to meeting the QoS requirements of the application as long as the traffic remains within the profile specifications. The network fulfills its commitment by maintaining the per-flow state and then performing packet classification, policing, and intelligent queuing based on that state.

The table in Figure 2 lists the benefits and drawbacks of the IntServ model.

Benefits	Drawbacks
• Explicit end-to-end resource admission control • Per-request policy admission control • Signaling of dynamic port numbers	• Resource intensive due to the stateful architecture requirement for continuous signaling. • Flow-based approach not scalable to large implementations such as the Internet.

Differentiated Services

The differentiated services (DiffServ) QoS model specifies a simple and scalable mechanism for classifying and managing network traffic and providing QoS guarantees on modern IP networks. For example, DiffServ can provide low-latency guaranteed service to critical network traffic such as voice or video while providing simple best-effort traffic guarantees to non-critical services such as web traffic or file transfers.

The DiffServ design overcomes the limitations of both the best-effort and IntServ models. The DiffServ model is described in RFCs 2474, 2597, 2598, 3246, 4594. DiffServ can provide an "almost guaranteed" QoS while still being cost-effective and scalable.

The DiffServ model is similar in concept to sending a package using a delivery service. You request (and pay for) a level of service when you send a package. Throughout the package network, the level of service you paid for is recognized and your package is given either preferential or normal service, depending on what you requested.

DiffServ is not an end-to-end QoS strategy because it cannot enforce end-to-end guarantees. However, DiffServ QoS is a more scalable approach to implementing QoS. Unlike IntServ and hard QoS in which the end-hosts signal their QoS needs to the network, DiffServ does not use signaling. Instead, DiffServ uses a "soft QoS" approach. It works on the provisioned-QoS model, where network elements are set up to service multiple classes of traffic each with varying QoS requirements.

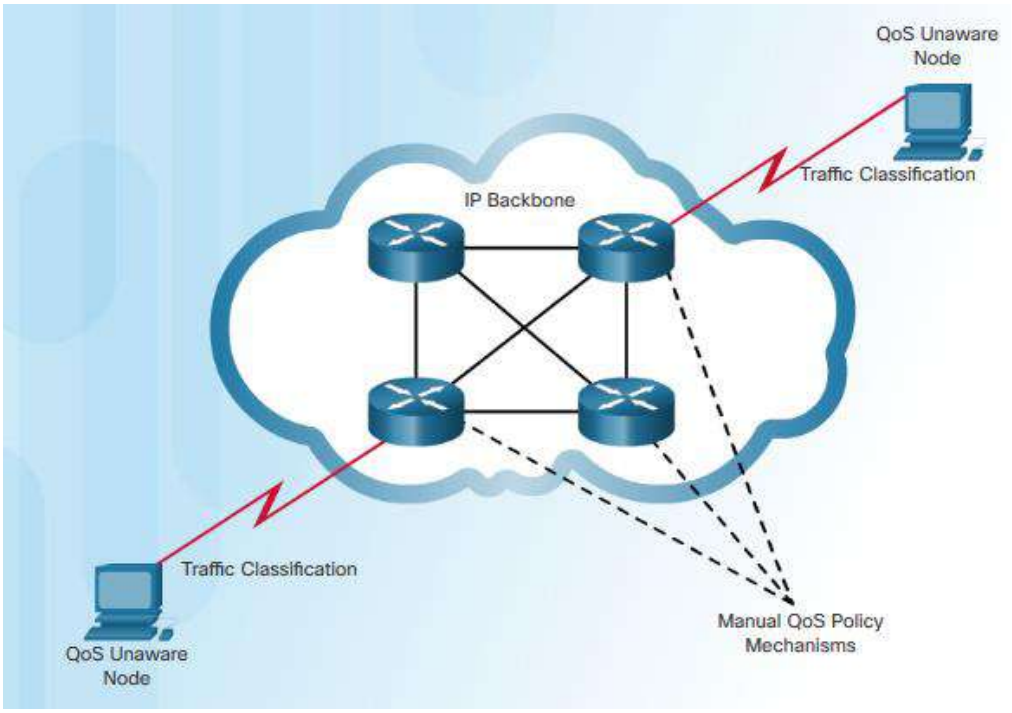


Figure 1 is a simple illustration of the DiffServ model.

As a host forwards traffic to a router, the router classifies the flows into aggregates (classes) and provides the appropriate QoS policy for the classes. DiffServ enforces and applies QoS mechanisms on a hop-by-hop basis, uniformly applying global meaning to each traffic class to provide both flexibility and scalability. For example, DiffServ could be configured to group all TCP flows as a single class, and allocate bandwidth for that class, rather than for the individual flows as IntServ would do. In addition to classifying traffic, DiffServ minimizes signaling and state maintenance requirements on each network node.

Specifically, DiffServ divides network traffic into classes based on business requirements. Each of the classes can then be assigned a different level of service. As the packets traverse a network, each of the network devices identifies the packet class and services the packet according to that class. It is possible to choose many levels of service with DiffServ. For example, voice traffic from IP phones is usually given preferential treatment over all other application traffic, email is generally given best-effort service, and nonbusiness traffic can either be given very poor service or blocked entirely.

Figure 2 lists the benefits and drawbacks of the DiffServ model.

Note: Modern networks primarily use the DiffServ model. However, due to the increasing volumes of delay- and jitter-sensitive traffic, IntServ and RSVP are sometimes co-deployed.

Avoiding Packet Loss

Packet loss is usually the result of congestion on an interface. Most applications that use TCP experience slowdown because TCP automatically adjusts to network congestion. Dropped TCP segments cause TCP sessions to reduce their window sizes. Some applications do not use TCP and cannot handle drops (fragile flows).

The following approaches can prevent drops in sensitive applications:

Increase link capacity to ease or prevent congestion.

Guarantee enough bandwidth and increase buffer space to accommodate bursts of traffic from fragile flows. There are several mechanisms available in Cisco IOS QoS software that can guarantee bandwidth and provide prioritized forwarding to drop-sensitive applications. Examples being WFQ, CBWFQ, and LLQ.

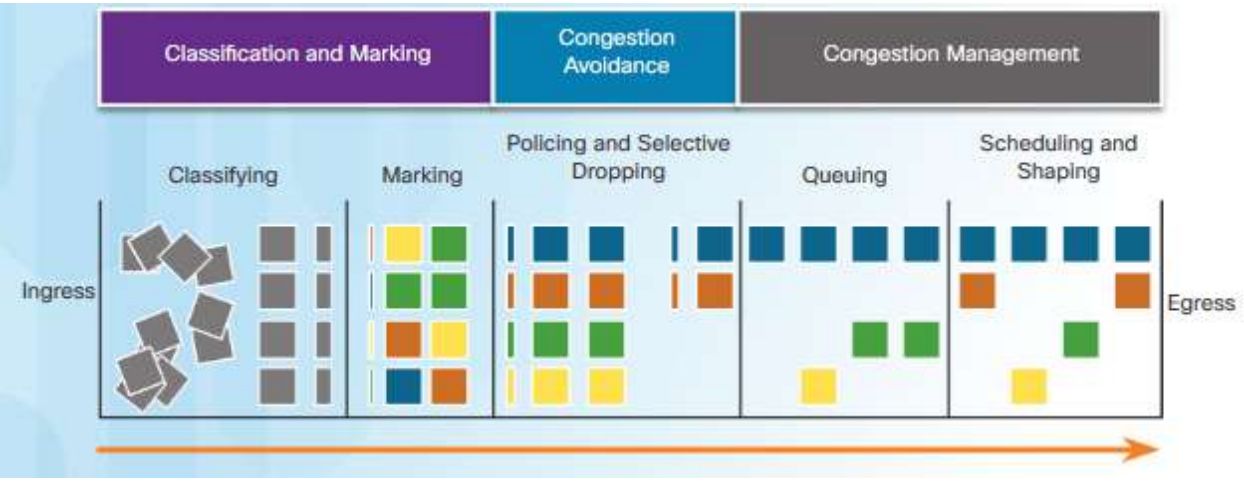
Prevent congestion by dropping lower-priority packets before congestion occurs. Cisco IOS QoS provides queuing mechanisms that start dropping lower-priority packets before congestion occurs. An example being weighted random early detection (WRED).

QoS Tools

There are three categories of QoS tools, as described in the table in Figure 1:

- Classification and marking tools
- Congestion avoidance tools
- Congestion management tools

QoS Tools	Description
Classification and marking tools	• Sessions, or flows, are analyzed to determine what traffic class they belong to. • Once determined, the packets are marked.
Congestion avoidance tools	• Traffic classes are allotted portions of network resources as defined by the QoS policy. • The QoS policy also identifies how some traffic may be selectively dropped, delayed, or re-marked to avoid congestion. • The primary congestion avoidance tool is WRED and is used to regulate TCP data traffic in a bandwidth-efficient manner before tail drops caused by queue overflows occur.
Congestion management tools	• When traffic exceeds available network resources, traffic is queued to await availability of resources. • Common Cisco IOS-based congestion management tools include CBWFQ and LLQ algorithms.



Refer to Figure 2 to help understand the sequence of how these tools are used when QoS is applied to packet flows.

As shown in the figure, ingress packets (gray squares) are classified and their respective IP header is marked (colored squares). To avoid congestion, packets are then allocated resources based on defined policies. Packets are then queued and forwarded out the egress interface based on their defined QoS shaping and policing policy.

Note: Classification and marking can be done on ingress or egress, whereas other QoS actions such queuing and shaping are usually done on egress.

Classification and Marking

Before a packet can have a QoS policy applied to it, the packet has to be classified. Classification and marking allows us to identify or "mark" types of packets. Classification determines the class of traffic to which packets or frames belong. Only after traffic is marked can policies be applied to it.

How a packet is classified depends on the QoS implementation. Methods of classifying traffic flows at Layer 2 and 3 include using interfaces, ACLs, and class maps. Traffic can also be classified at Layers 4 to 7 using Network Based Application Recognition (NBAR).

Note: NBAR is a classification and protocol discovery feature of Cisco IOS software that works with QoS features. NBAR is out of scope for this course.

QoS Tools	Layer	Marking Field	Width in Bits
Ethernet (802.1Q, 802.1p)	2	Class of Service (CoS)	3
802.11 (Wi-Fi)	2	Wi-Fi Traffic Identifier (TID)	3
MPLS	2	Experimental (EXP)	3
IPv4 and IPv6	3	IP Precedence (IPP)	3
IPv4 and IPv6	3	Differentiated Services Code Point (DSCP)	6

Marking means that we are adding a value to the packet header. Devices receiving the packet look at this field to see if it matches a defined policy. Marking should be done as close to the source device as possible. This establishes the trust boundary.

How traffic is marked usually depends on the technology. The table in the figure describes some the marking fields used in various technologies. The decision of whether to mark traffic at Layers 2 or 3 (or both) is not trivial and should be made after consideration of the following points:

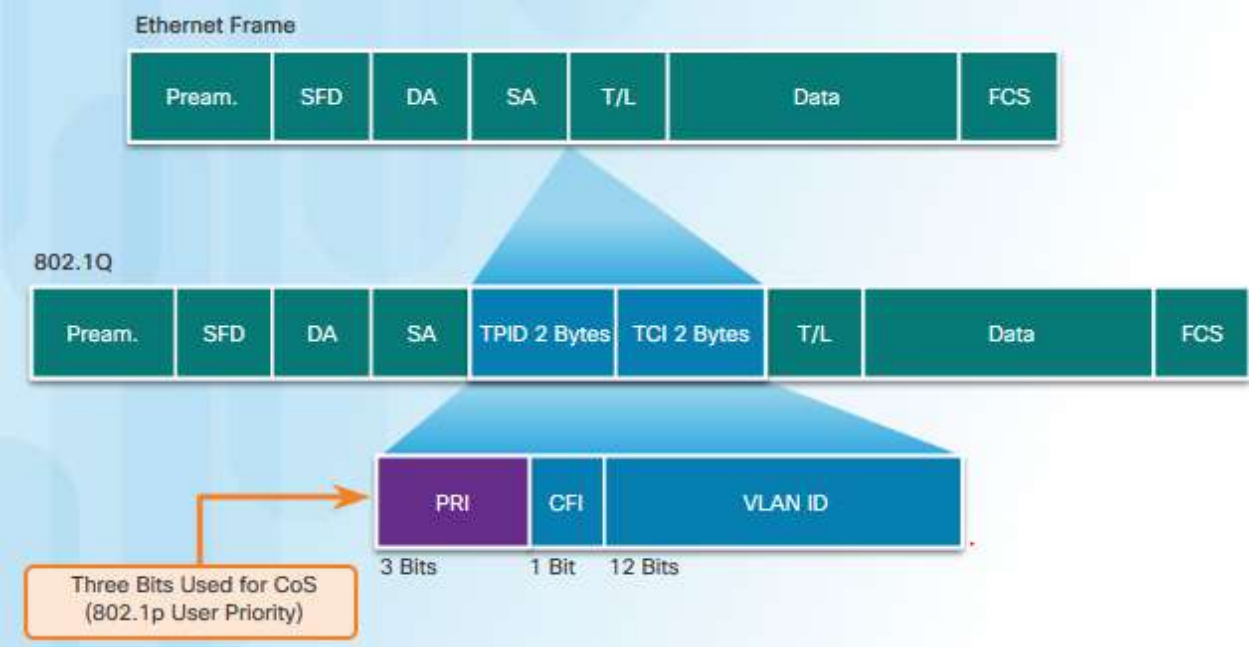
Layer 2 marking of frames can be performed for non-IP traffic.

Layer 2 marking of frames is the only QoS option available for switches that are not "IP aware".

Layer 3 marking will carry the QoS information end-to-end.

Marking at Layer 2

802.1Q is the IEEE standard that supports VLAN tagging at layer 2 on Ethernet networks. When 802.1Q is implemented, two fields are added to the Ethernet Frame. As shown in Figure 1, these two fields are inserted into the Ethernet frame following the source MAC address field.



The 802.1Q standard also includes the QoS prioritization scheme known as IEEE 802.1p. The 802.1p standard uses the first three bits in the Tag Control Information (TCI) field. Known as the Priority (PRI) field, this 3-bit field identifies the Class of Service (CoS) markings. Three bits means that a Layer 2 Ethernet frame can be marked with one of eight levels of priority (values 0–7)

Trust Boundaries

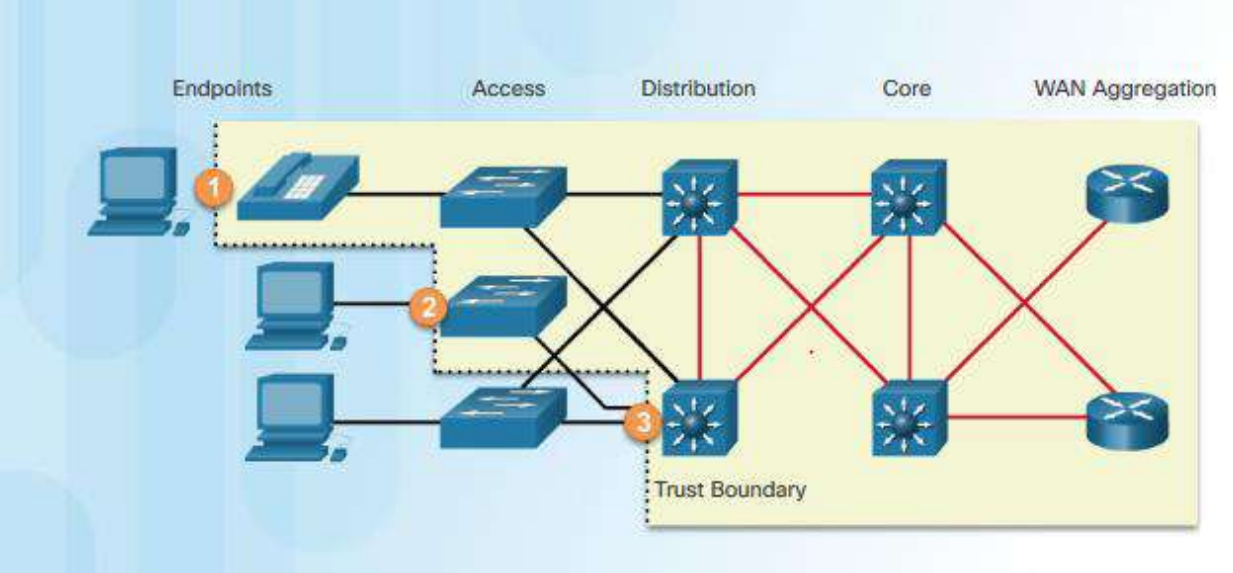
Where should markings occur? Traffic should be classified and marked as close to its source as technically and administratively feasible. This defines the trust boundary as shown in the figure.

Trusted endpoints have the capabilities and intelligence to mark application traffic to the appropriate Layer 2 CoS and/or Layer 3 DSCP values. Examples of trusted endpoints include IP phones, wireless access points, videoconferencing gateways and systems, IP conferencing stations, and more.

Secure endpoints can have traffic marked at the Layer 2 switch.

Traffic can also be marked at Layer 3 switches / routers.

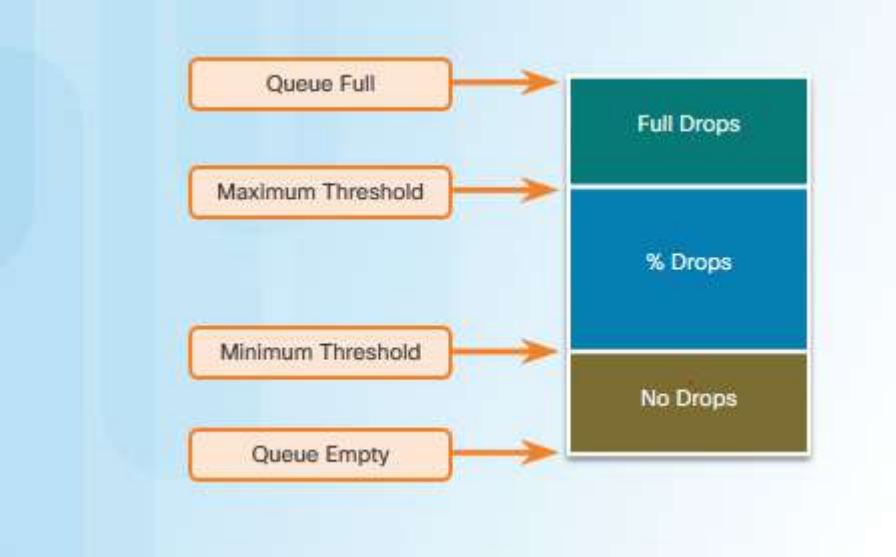
Re-marking of traffic is typically necessary.



Congestion Avoidance

Congestion management includes queuing and scheduling methods where excess traffic is buffered or queued (and sometimes dropped) while it waits to be sent on an egress interface. Congestion avoidance tools are simpler. They monitor network traffic loads in an effort to anticipate and avoid congestion at common network and internetwork bottlenecks before congestion becomes a problem. These tools can monitor the average depth of the queue, as represented in the figure. When the queue is below the minimum threshold, there are no drops. As the queue fills up to the maximum threshold, a small percentage of packets are dropped. When the maximum threshold is passed, all packets are dropped.

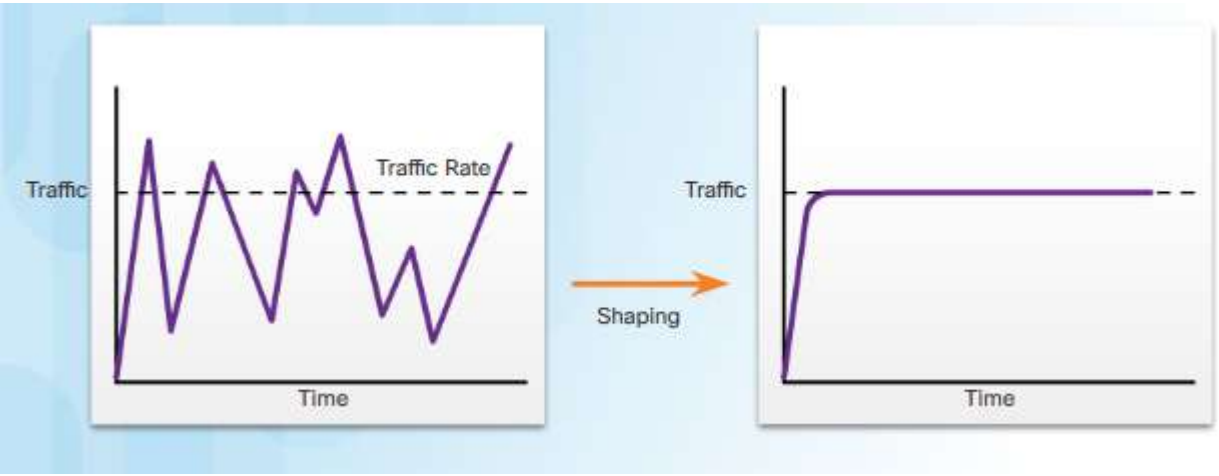
Some congestion avoidance techniques provide preferential treatment for which packets will get dropped. For example, Cisco IOS QoS includes weighted random early detection (WRED) as a possible congestion avoidance solution. The WRED algorithm allows for congestion avoidance on network interfaces by providing buffer management and allowing TCP traffic to decrease, or throttle back, before buffers are exhausted. Using WRED helps avoid tail drops and maximizes network use and TCP-based application performance. There is no congestion avoidance for User Datagram Protocol (UDP)-based traffic, such as voice traffic. In case of UDP-based traffic, methods such as queuing and compression techniques help to reduce and even prevent UDP packet loss.



Shaping and Policing

Traffic shaping and traffic policing are two mechanisms provided by Cisco IOS QoS software to prevent congestion.

Traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time. The result of traffic shaping is a smoothed packet output rate, as shown in Figure 1.



Shaping implies the existence of a queue and of sufficient memory to buffer delayed packets, while policing does not.

Ensure that you have sufficient memory when enabling shaping. In addition, shaping requires a scheduling function for later transmission of any delayed packets. This scheduling function allows you to organize the shaping queue into different queues. Examples of scheduling functions are CBWFQ and LLQ.

Shaping is an outbound concept; packets going out an interface get queued and can be shaped. In contrast, policing is applied to inbound traffic on an interface. When the traffic rate reaches the configured maximum rate, excess traffic is dropped (or remarked).

Policing is commonly implemented by service providers to enforce a contracted customer information rate (CIR). However, the service provider may also allow bursting over the CIR if the service provider's network is not currently experiencing congestion.

Review questions

1. Identify the traffic characteristics in converged network.
2. Explain the QoS models.
3.How to implement Th QoS?

References:

[1] Groth, David and Skandler, Toby *(2005). Network+ Study Guide, Fourth Edition. Sybex,Inc. ISBN 0-7821-4406-3.*

[2] Forouzan, Behrouz (2012-02-17*). Data Communications and Networking. McGraw- Hill. p. 14. ISBN 9780073376226.*

[3] David, Hemmendinger. (2000). *Wide area network. Schenectady, New York. Cisco - Introduction to WAN Technologies*

[4] « WAN Technologies », *CISCO, netacad, searchcontent, retrieved 2020-08-11*

[5]"What is WAN (wide area network). Definition from WhatIs.com", SearchEnterpriseWAN, retrieved 2020-08-11

APPANDICES

A. PRACTICE EXERCISES

See Attached files (Contact Trainer)

B. Summative Assessment

Integrated situation	Resources
Rwanda Polytechinc has decided to extend its activitities and opened a new TVETcolleges.The new college devices are connected to it main router. It has also decided to create VLAN in the existing LANs connected to its main switch at its offices in Kigali. Main router A interface Serial 0/0/0 is connected to serial 0/0/1 of ISP.Main router A is connected to main switch E in the LAN via gigabit interface .Main router A is connected to one routers B via a serial interfaces 0/0/2. Router B is connected to two routers: C and D and those routers are connected each others (all via gigabit interfaces). Router C and D are connected to Remote switch and via the switch to branch -A and Branch-B routers.Main switch E is connected to following 6 switches:	- Computers - Internet - Routers - Switches - Ethernet cables - Packet tracer - Console - Terminal emulation

	Name	Number of hosts	VLAN Number
1	Students Lab1 switch VLAN	48 hosts	Vlan 1
2	Students Lab2 switch VLAN	62 hosts	Vlan 2
3	e-learning room switch VLAN	200 hosts	Vlan 3
4	Innovation center switch VLAN	120 hosts	Vlan 4
5	Managerial block offices switch VLAN	20 hosts	Vlan 5
6	NOC office switch VLAN	10 hosts	Vlan 6
7	Local Server room switch VLAN	12 hosts	

Tasks: **Duration 10 hours**

1. Build the topology in packet tracer.
2. Subnet the given IP addressing for addressing all devices interfaces in the LAN andhosts
3. Configure all routers and all switches basic configurations and assign them IP address (switches should be managed trough IP address on their interfaces (hostnames, password, VTY and console lines, and IP addresses on interfaces).
4. Configure switch ports to be either access ports or trunking ports according to the topology. (Port 1 is advisable to be trunk port).
5. Configure VLAN for hosts so that each switch can isolate packets broadcasting.
6. Configure main switch to be a VTP server.
7. Configure InterVlan routing in the Main Switch.
8. Configure static route from Main router A to ISP.
9. Build a VPN between Main router A and Branch-A so that traffic packets are encrypted.
10. Configure dynamic routing with EIGRP between router A and B.
11. Configure dynamic routing with OSPF with area 0 between router B, C and D.
12. Configure the multiaccess OSPF area 10 between Router C, D and Branch-A. They are connected via Remote-switch.
13. Apply the Hot Standby Router Protocol(HSRP) so that the Branch_A could have the two routers (C,D) as default gateways.
14. Configure Access Control Lists (ACLs) to:

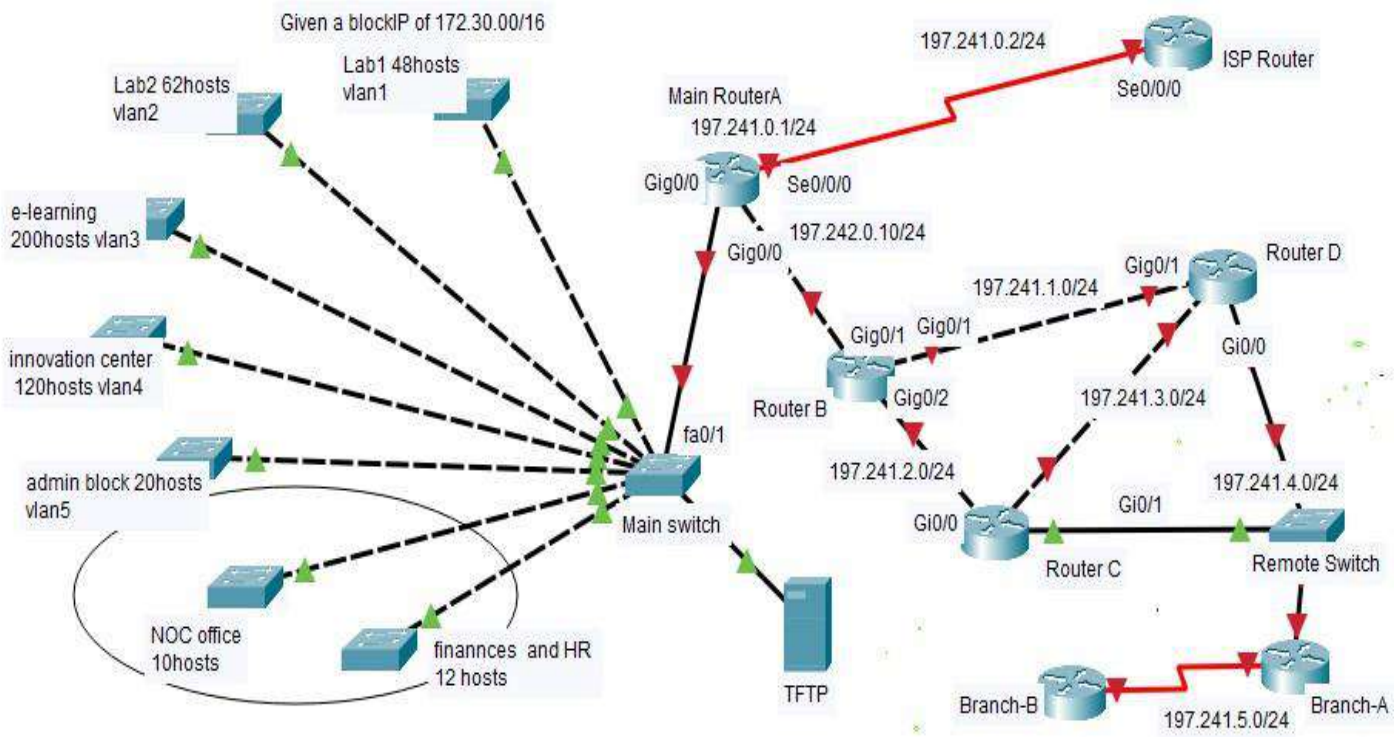
i. Bloc http for students during teaching hours
ii. To block accessing internal LAN from internet side only IP address197.241.0.227
iii. Block telnet protocol from outside LAN
iv. Allow ssh protocol outside LAN

15. Enable following services :

i. CDP , syslog and NTP on routers by NTP server /TFTP
ii. STP on switches

16. Upload the configuration for all routers and switches to TFTP server.

Duration 10 hours


Given a blockIP of 172.30.00/16
Lab2 62hosts
vlan2
Lab1 48hosts
vlan1
e-learning
200hosts vlan3
innovation center
120hosts vlan4
admin block 20hosts
vlan5
NOC office
10hosts
finannces and HR
12 hosts
Main switch
fa0/1
TFTP
Main RouterA
197.241.0.1/24
Gig0/0
Se0/0/0
197.241.0.2/24
ISP Router
Se0/0/0
Gig0/0
197.242.0.10/24
Router B
Gig0/1
Gig0/2
197.241.1.0/24
Gig0/1
Router D
Gi0/0
197.241.3.0/24
197.241.2.0/24
Gi0/0
Router C
Gi0/1
197.241.4.0/24
Remote Switch
Branch-B
197.241.5.0/24
Branch-A