CCNA 2

SWITCHING, ROUTING, AND WIRELESS ESSENTIALS

* + 1. Switch Boot Sequence

After a Cisco switch is powered on, it goes through the following five-step boot sequence:

* Step 1: First, the switch loads a power-on self-test (POST) program stored in ROM. POST checks the CPU subsystem. It tests the CPU, DRAM, and the portion of the flash device that makes up the flash file system.
* Step 2: Next, the switch loads the boot loader software. The boot loader is a small program stored in ROM that is run immediately after POST successfully completes.
* Step 3: The boot loader performs low-level CPU initialization. It initializes the CPU registers, which control where physical memory is mapped, the quantity of memory, and its speed.
* Step 4: The boot loader initializes the flash file system on the system board.
* Step 5: Finally, the boot loader locates and loads a default IOS operating system software image into memory and gives control of the switch over to the IOS.

1.1.2 The Boot System Command

* The switch automatically tries to boot by using the info in the BOOT environment variable.
* If no information available, the switch attempts to load and execute the first executable file it can find.
* The IOS OS then initializes the interfaces using the Cisco IOS commands found in the startup-config file. (config.text and is located in flash)
  + 1. Switch LED Indicators
* The mode button is used to toggle through port status, port duplex, port speed, and if supported, the Power over Ethernet (PoE) status of the port LEDs

1. SYST – System LED – Shows whether the system is receiving power and is functioning properly. If off, the system is not powered on. If LED is green, the system is operating normally. If LED is amber, the system is receiving power but not functioning properly.
2. RPS – Redundant Power System LED – Shows the RPS status. If the LED is off, the RPS is off, or not properly connected. If the LED is green, the RPS is connected and is ready to provide backup power. If the LED is blinking green, the RPS is connected but is unavailable because it is providing power to another device. If the LED is amber, the RPS is in standby mode, or in a fault condition. If the LED is blinking amber, the internal power supply in the switch has failed, and the RPS is providing power.
3. STAT – Port Status LED – Indicates that the port status mode is selected when the LED is green (the default mode). When selected, the port LEDs will display colours with different meanings. If the LED is off, there is no link, or the port was administratively shutdown. If the LED is green, a link is present. If the LED is blinking green, there is an activity and the port is sending or receiving data. If the LED is alternating green-amber, there is a link fault. If the LED is amber, the port is blocked to ensure that a loop does not exist in the forwarding domain and is not forwarding data. If the LED is blinking amber, the port is blocked to prevent possible loop in the forwarding domain.
4. DUPLX – Port Duplex LED – Indicates that the port duplex mode is selected when the LED is green. When selected, port LEDs that are off are on half-duplex mode. If the LED is green, the port is in full-duplex mode.
5. SPEED – Indicates the port speed mode is selected. When selected, the port LEDs will display colours with different meanings. If the LED is off, the port is operating at 10 Mbps. If the LED is green, the port is operating at 100 Mbps. If the LED is blinking green, the port is operating at 1000 Mbps.
6. PoE – Power over Ethernet Mode LED – If PoE is supported, a PoE LED will be present. Off means PoE is not selected and none of the ports have been denied power or placed in a fault condition. Blinking amber means the PoE mode is not selected but at least one of the ports has been denied power or has PoE fault. Green indicates that PoE mode is selected, and the port LEDs will display colours with different meanings. Off means PoE is off. Port LED green means PoE is on. Port LED alternating green-amber means PoE is denied because providing power to the powered device will exceed the switch power capacity. Blinking amber means that PoE is off because of a fault. Amber means PoE for the port has been disabled.
   * 1. Switch Management Access

* To prepare a witch for remote management access, the switch must have a switch virtual interface (SVI) configured with an IPv4 address and a subnet mask, or an IPv6 address and a prefix length.
* Configure the default gateway for the SVI

Step 1. Configure Management Interface

* Enter global config mode – configure terminal
* Enter interface config mode for the SVI – interface vlan 99
* Configure the management interface IPv4 address – ip address 192.168.1.19 255.255.255.0
* Configure the management interface IPv6 address – ipv6 address 2001:db8:acad:99::11/64
* Enable the management interface – no shutdown
* Return to privileged EXEC mode – end
* Save the running-config to the startup-config – copy running-config startup-config

Step 2. Configure the Default Gateway

* Note: Because the switch will receive its default gateway information from a router advert (RA) message, the switch does not require an IPv6 default gateway
* Enter global config mode – configure terminal
* Configure the gateway for the switch – ip default-gateway 192.168.1.254
* Return to privileged EXEC - end
* Save the running-config to startup-config – write
* Verify configurations – show ip interface brief.
  1. Configure Switch Ports

1.2.1 Duplex Communication

Full-duplex communication increases bandwidth efficiency by allowing both ends of a connection to transmit and receive data simultaneously. This is also known as bidirectional communication and it requires microsegmentation. A microsegmented LAN is created when a switch port has only one device connected and is operating in full-duplex mode. There is no collision domain associated with a switch port operating in full-duplex mode.

Unlike full-duplex communication, half-duplex communication is unidirectional. Half-duplex communication creates performance issues because data can flow in only one direction at a time, often resulting in collisions.

Configurations

* configure terminal
* interface [interface name]
* duplex full
* speed 100
* end
* write

The default setting for both duplex and speed for switch ports on Cisco Catalyst 2960 and 3560 switches is auto. The 10/100/1000 ports operate in either half- or full-duplex mode when they are set to 10 or 100 Mbps and operate only in full-duplex mode when it is set to 1000 Mbps (1 Gbps)

Autonegotiation is useful when the speed and duplex settings of the device connecting to the port are unknown or may change. When connecting to known devices such as servers, dedicated workstations, or network devices, a best practice is to manually set the speed and duplex settings.

Auto-MDIX (automatic medium-dependent interface crossover)

When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately.

When connecting to switches without the auto-MDIX feature, straight-through cables must be used to connect to devices such as servers, workstations, or routers. Crossover cables must be used to connect to other switches or repeaters.

With auto-MDIX enabled, either type of cable can be used to connect to other devices, and the interface automatically adjusts to communicate successfully. On newer Cisco switches, the mdix auto interface configuration mode command enables the feature. When using auto-MDIX on an interface, the interface speed and duplex must be set to auto so that the feature operates correctly.

* The command to enable auto-MDIX – mdix auto
* The auto-MDIX feature is enabled by default on Catalyst 2960 and Catalyst 3560 switches but is not available on the older Catalyst 2950 and Catalyst 3550 switches.
* show controllers ethernet-controller fa0/1 phy | include MDIX

Switch Verification Commands

* Display interface status and config – show interfaces [interface id]
* Display current startup-config – show startup-config
* Display current running config – show running-config
* Display info about flash system – show flash
* Display hardware and software status – show version
* Display history of commands entered – show history
* Display IP info about an interface – show ip interface [interface id], OR show ipv6 interface [interface id]
* Display MAC address table – show mac-address-table, OR show mac address-table

Network Access Layer Issues

* Input errors – total number of errors
* Runts – frames that are discarded because they are smaller than the minimum frame size for the medium. E.g. less than 64 bytes
* Giants – frames that are discarded because they exceed the maximum frame size for the medium. i.e greater than 1518 bytes
* CRC – errors generated when the calculated checksum is not the same as the checksum received.
* Output errors – sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined.
* Collisions – sum of messages transmitted because of an Ethernet collision
* Late collisions – collisions that occur after 512 bits of the frames have been submitted.

1.2.6 Interface Input and Output Errors

“Input errors” is the sum of all errors in datagrams that were received on the interface being examined. This includes runts, giants, CRC, no buffer, frame, overrun, and ignored counts. The reported input errors from the show interfaces command include the following:

Runt Frames - Ethernet frames that are shorter than the 64-byte minimum allowed length are called runts. Malfunctioning NICs are the usual cause of excessive runt frames, but they can also be caused by collisions.

Giants - Ethernet frames that are larger than the maximum allowed size are called giants.

CRC errors - On Ethernet and serial interfaces, CRC errors usually indicate a media or cable error. Common causes include electrical interference, loose or damaged connections, or incorrect cabling. If you see many CRC errors, there is too much noise on the link and you should inspect the cable. You should also search for and eliminate noise sources.

“Output errors” is the sum of all errors that prevented the final transmission of datagrams out the interface that is being examined. The reported output errors from the show interfaces command include the following:

Collisions - Collisions in half-duplex operations are normal. However, you should never see collisions on an interface configured for full-duplex communication.

Late collisions - A late collision refers to a collision that occurs after 512 bits of the frame have been transmitted. Excessive cable lengths are the most common cause of late collisions. Another common cause is duplex misconfiguration. For example, you could have one end of a connection configured for full-duplex and the other for half-duplex. You would see late collisions on the interface that is configured for half-duplex. In that case, you must configure the same duplex setting on both ends. A properly designed and configured network should never have late collisions.

Secure Remote Access

Telnet operation - Telnet uses TCP port 23. It is an older protocol that uses unsecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices.

SSH operation - Secure Shell (SSH) is a secure protocol that uses TCP port 22. It provides a secure (encrypted) management connection to a remote device.

1.3.1 Verify the Switch Supports SSH

To enable SSH on a Catalyst 2960 switch, the switch must be using a version of the IOS software including cryptographic (encrypted) features and capabilities. Use the show version command on the switch to see which IOS the switch is currently running. An IOS filename that includes the combination “k9” supports cryptographic (encrypted) features and capabilities. – show version

1.3.2 Configure SSH

Step 1 - Verify SSH support.

Use the show ip ssh command to verify that the switch supports SSH. If the switch is not running an IOS that supports cryptographic features, this command is unrecognized.

S1# show ip ssh

Step 2 - Configure the IP domain.

Configure the IP domain name of the network using the ip domain-name domain-name global configuration mode command.

S1(config)# ip domain-name cisco.com

Step 3 - Generate RSA key pairs.

Not all versions of the IOS default to SSH version 2, and SSH version 1 has known security flaws. To configure SSH version 2, issue the ip ssh version 2 global configuration mode command. Generating an RSA key pair automatically enables SSH. Use the crypto key generate rsa global configuration mode command to enable the SSH server on the switch and generate an RSA key pair. When generating RSA keys, the administrator is prompted to enter a modulus length.

Note: To delete the RSA key pair, use the crypto key zeroize rsa global configuration mode command. After the RSA key pair is deleted, the SSH server is automatically disabled.

S1(config)# crypto key generate rsa

How many bits in the modulus [512]: 1024

Step 4 - Configure user authentication.

The SSH server can authenticate users locally or using an authentication server. To use the local authentication method, create a username and password pair using the username username secret password global configuration mode command. In the example, the user admin is assigned the password ccna.

S1(config)# username admin secret ccna

Step 5 - Configure the vty lines.

Enable the SSH protocol on the vty lines by using the transport input ssh line configuration mode command. The Catalyst 2960 has vty lines ranging from 0 to 15. This configuration prevents non-SSH (such as Telnet) connections and limits the switch to accept only SSH connections. Use the line vty global configuration mode command and then the login local line configuration mode command to require local authentication for SSH connections from the local username database.

S1(config)# line vty 0 15

S1(config-line)# transport input ssh

S1(config-line)# login local

S1(config-line)# exit

Step 6 - Enable SSH version 2.

By default, SSH supports both versions 1 and 2. When supporting both versions, this is shown in the show ip ssh output as supporting version 2. Enable SSH version using the ip ssh version 2 global configuration command.

S1(config)# ip ssh version 2

Basic Router Configuration

Enter global configuration mode and name the router R2.

Router#configure terminal

Router(config)#hostname R2

Configure class as the secret password.

R1(config)#enable secret class

Configure cisco as the console line password and require users to login. Then exit line configuration mode.

R1(config)#line console 0

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#exit

Configure cisco as the vty password for lines 0 through 4 and require users to login.

R1(config)#line vty 0 4

R1(config-line)#password cisco

R1(config-line)#login

Exit line configuration mode and encrypt all plaintext passwords.

R1(config-line)#exit

R1(config)#service password-encryption

Enter the banner Authorized Access Only! and use # as the delimiting character.

R1(config)#banner motd #Authorized Access Only!#

Exit global configuration mode and save the configuration.

R1(config)#exit

R1#copy running-config startup-config

Configure GigabitEthernet 0/0/0.

Use g0/0/0 to enter interface configuration mode.

Configure the IPv4 address 10.1.1.1 and subnet mask 255.255.255.0.

Configure the IPv6 address 2001:db8:acad:4::1/64.

Describe the link as Link to LAN 3.

Activate the interface.

Router(config)#interface g0/0/0

Router(config-if)#ip address 10.1.1.1 255.255.255.0

Router(config-if)#ipv6 address 2001:db8:acad:4::1/64

Router(config-if)#description Link to LAN 3

Router(config-if)#no shutdown

1.4.6 IPv4 Loopback Interfaces

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

The loopback interface is a logical interface that is internal to the router. It is not assigned to a physical port and can 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.

Loopback interfaces are also commonly used in lab environments to create additional interfaces. For example, you can create multiple loopback interfaces on a router to simulate more networks for configuration practice and testing purposes.

Enabling and assigning a loopback address is simple:

Router(config)# interface loopback number

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

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.

R1(config)# interface loopback 0

R1(config-if)# ip address 10.0.0.1 255.255.255.0

R1(config-if)# exit

1.6.4 Module Quiz - Basic Device Configuration

Question 1

Which tasks can be accomplished by using the command history feature? (Choose two.)

Set the command history buffer size.

Recall previously entered commands.

Topic 1.5.0 - The history command allows you to view and reuse previously entered commands stored in the buffer. It is also used to manage the size of the buffer.

Question 2

Which statement describes the system LED operation on Cisco Catalyst switches?

If the LED is blinking green, the system is operating normally.

If the LED is amber, the system is receiving power but it is not functioning properly.

Topic 1.1.0 - The system LED shows whether the system is receiving power and is functioning properly. If the LED is off, the system is not powered on. If the LED is green, the system is operating normally. If the LED is amber, the system is receiving power but is not functioning properly.

Question 3

What type of Ethernet cable would be used to connect one switch to another switch when neither switch supports the auto-MDIX feature?

Crossover

Topic 1.2.0 - A straight-through cable can be used to connect a computer or a router to a switch. A rollover cable can be used to access a router or switch console line. A coaxial cable is not used any longer in Ethernet networks, but can be found in video connections. A crossover cable can be used to connect a switch to a switch, a computer to a computer, and a router to a router.

Question 4

What advantage does SSH offer over Telnet?

Encryption

Topic 1.3.0 - Both Telnet and SSH are used to remotely connect to a network device for management tasks. However, Telnet uses plaintext communications, whereas SSH provides security for remote connections by providing encryption of all transmitted data between devices.

Question 5

A network administrator has configured ​VLAN 99 as the management VLAN and has configured it with an IP address and subnet mask. The administrator issues the show interface vlan 99 command and notices that the line protocol is down. Which action can change the state of the line protocol to up?

Connect a host to an interface associated with VLAN 99.

Topic 1.1.0 - Once an SVI is configured with an IP address and subnet mask, it can be used for remote management. An SVI interface will be active when the SVI VLAN has an active port associated with it.

Question 6

Which statement describes SVIs?

A default SVI is created for VLAN 1 for switch administration.

Topic 1.1.0 - To allow for remote switch administration, an SVI is created by default for VLAN 1.

Question 7

Which prompt is displayed when a network administrator successfully accesses the boot loader on a switch to recover from a system crash?

Switch:

Topic 1.1.0 - The boot loader provides access into the switch if the operating system cannot be used because of missing or damaged system files. After some steps have been completed, the boot loader can be accessed through a console connection, through the switch: prompt.

Question 8

Which router bootup sequence is correct?​

1 - perform the POST and load the bootstrap program

2 - locate and load the Cisco IOS software

3 - locate and load the startup configuration file or enter setup mode

Topic 1.1.0 - When a router is powered on, it undergoes a POST to verify that the hardware is functional, after which it proceeds by locating and loading the Cisco IOS software and then loading the startup configuration file if one is present.

Question 9

What is the first action in the boot sequence when a switch is powered on?

Load a power-on self-test program

Topic 1.1.0 - The first action to take place when a switch is powered on is the POST or power-on self-test. POST performs tests on the CPU, memory, and flash in preparation for loading the boot loader.

Question 10

What must an administrator have in order to reset a lost password on a router?

Physical access to the router

Topic 1.4.0 - Console access to the device through a terminal or terminal emulator software on a PC is required for password recovery.

Question 11

When configuring a switch for SSH access, what other command that is associated with the login local command is required to be entered on the switch?

username username secret secret

Topic 1.3.0 - The login local command designates that the local username database is used to authenticate interfaces such as console or vty.

Question 12

Which command will provide information about the status of all interfaces including the number of giants, runts, and collisions on the interface?

show interfaces

Topic 1.2.0 - The show interfaces command is the most comprehensive in providing information about interfaces. The show ip interface brief command does not provide information on giants, runts, or collisions. The show history command provides a history of the commands that are used. The show running-config command will show configuration information, but not status information.

**2.1 Frame Forwarding**

Ingress – the port where a frame enters the device.

Egress – the port that frames will use when leaving the device.

A LAN Switch forwards traffic based on the ingress port and the destination MAC address of the Ethernet frame.

The MAC address table is stored in content addressable memory (CAM).

The Switch Learn and Forward Method

Step 1. Learn – Examining the source MAC address

Every frame that enters a switch is checked for new information to learn. It does this by examining the source MAC address of the frame and port number where the frame entered the switch:

* If the source MAC address does not exist in the MAC address table, the MAC address and incoming port number are added to the table.
* If the source MAC address does exist, the switch updates the refresh timer for that entry. By default, most switches keep an entry in the table for five minutes. If the source MAC does exist in the table but on a different port, the switch treats this as a new entry. The entry is replaced using the same MAC address, but with the more current port number,

Step 2. Forward – Examining the Destination MAC Address

If the destination is a unicast address, the switch will look for a match between the destination MAC address of the frame and an entry in its MAC address table:

* If the destination MAC address is in the table, it will forward the frame out of the specified port.
* If the destination MAC address is not in the table, the switch will forward the frame out of all ports except the incoming port. This is called unknown unicast.
* If the destination address is a broadcast or a multicast, the frame is also flooded out of all ports except the incoming port.

Switch Forwarding Methods

Switches makes Layer 2 forwarding decisions very quickly because of ASICs (application-specific-integrated-circuits) which reduce frame-handling time within the device and allow the device to manage an increased number of frames without degrading performance.

* Store-and-forwarding switching – This method makes a forwarding decision on a frame after it has received the entire frame and checked the frame for errors using CRC checksum. This is the primary switching method.
* Cut-through switching – This method begins the forwarding process after the destination address of the incoming frame and the egress port have been determined.

Collision and Broadcast Domains

The network segments that share the same bandwidth between devices are known as collision domains. When two or more devices within the same collision domain try to communicate at the same time, a collision will occur.

A collection of interconnected switches forms a single broadcast domain.

Routers are used to segment broadcast and collision domains

How Switches Alleviate Network Congestion

* Fast port speeds
* Fast internal switching – switches use a fast internal bus or shared memory to provide high performance.
* Large frame buffers – switches use large memory buffers to temporarily store more received frames before having to start dropping them. This enables ingress traffic forms a faster port (e.g. 1 Gbps) to be forwarded to a slower (e.g. 100 Mbps) egress port without losing frames.
* High port density – helps keep traffic local.

2.3.2 Module Quiz - Switching Concepts

Question 1

Which statement is true about broadcast and collision domains?

Adding a switch to a network will increase the size of the broadcast domain.

Topic 2.2.0 - A switch that receives a broadcast frame will forward the frame out all other interfaces, including interfaces that connect to other switches. These switches will also perform the same forwarding action. By adding more switches to the network, the size of the broadcast domain increases.

Question 2

What is one function of a Layer 2 switch?

Determines which interface is used to forward a frame based on the destination MAC address

Topic 2.1.0 - A switch builds a MAC address table of MAC addresses and associated port numbers by examining the source MAC address found in inbound frames. To forward a frame onward, the switch examines the destination MAC address, looks in the MAC address for a port number associated with that destination MAC address, and sends it to the specific port. If the destination MAC address is not in the table, the switch forwards the frame out all ports except the inbound port that originated the frame.

Question 3

What is the significant difference between a hub and a Layer 2 LAN switch?

A switch creates many smaller collision domains, and a hub increases the size of a single collision domain.

Topic 2.2.0 - Hubs operate only at the physical layer, forwarding bits as wire signals out all ports, and extend the collision domain of a network. Switches forward frames at the data link layer and each switch port is a separate collision domain, and thus more, but smaller, collision domains are created. Switches do not manage broadcast domains because broadcast frames are always forwarded out all active ports.

Question 4

What will a Cisco LAN switch do if it receives an incoming frame and the destination MAC address is not listed in the MAC address table?

Forward the frame out all ports except the port where the frame is received.

Topic 2.1.0 - A LAN switch populates the MAC address table based on source MAC addresses. When a switch receives an incoming frame with a destination MAC address that is not listed in the MAC address table, the switch forwards the frame out all ports except for the ingress port of the frame. When the destination device responds, the switch adds the source MAC address and the port on which it was received to the MAC address table.

Question 5

Which switch characteristic helps alleviate network congestion when a 10 Gbps port is forwarding data to a 1 Gbps port?

Frame buffering

Topic 2.2.0 - The large frame buffers on a switch hold the ingress traffic until such time that the slower egress port can transmit the data. This reduces the number of dropped frames and alleviates network congestion.

Question 6

Which switching method makes use of the FCS value?

Store-and-forward

Topic 2.1.0 - The store-and-forward method performs error checking on the frame using the frame-check sequence (FCS) value before sending the frame. The FCS value is the last field in the frame.

Question 7

What does the term "port density" represent for an Ethernet switch?

The number of available ports

Topic 2.2.0 - The term port density represents the number of ports available in a switch. A one rack unit access switch can have up to 48 ports. Larger switches may support hundreds of ports.

Question 8

Which information does a switch use to keep the MAC address table information current?

The source MAC address and the incoming port

Topic 2.1.0 - To maintain the MAC address table, the switch uses the source MAC address of the incoming packets and the port that the packets enter. The destination address is used to select the outgoing port.

Question 9

Which two statements are true about half-duplex and full-duplex communications? (Choose two.)

Full duplex allows both ends to transmit and receive simultaneously.

Full duplex increases the effective bandwidth.

Topic 2.2.0 - Full-duplex communication allows both ends to transmit and receive simultaneously, offering 100 percent efficiency in both directions for a 200 percent potential use of stated bandwidth. Half-duplex communication is unidirectional, or one direction at a time. Gigabit Ethernet and 10 Gb/s NICs require full duplex to operate, and do not support half-duplex operation.

Question 10

Which type of address does a switch use to build the MAC address table?

Source MAC address

Topic 2.1.0 - When a switch receives a frame with a source MAC address that is not in the MAC address table, the switch will add that MAC address to the table and map that address to a specific port. Switches do not use IP addressing in the MAC address table.

Question 11

Which option correctly describes a switching method?

Store-and-forward: ensures that the frame is free of physical and data-link errors

Topic 2.1.0 - Store-and-forward switching performs an error check on an incoming frame after receiving the entire frame on the ingress port. Switches which use this method have the flexibility to support any mix of Ethernet speeds. The cut-through method begins the forwarding process after the destination MAC address of an incoming frame is looked up and the egress port has been determined.

Question 12

Which network device can serve as a boundary to divide a Layer 2 broadcast domain?

Router

Topic 2.2.0 - Layer 1 and 2 devices (LAN switch and Ethernet hub) and access point devices do not filter MAC broadcast frames. Only a Layer 3 device, such as a router, can divide a Layer 2 broadcast domain.

Question 13

What is the purpose of frame buffers on a switch?

They hold traffic, thus alleviating network congestion.

Topic 2.2.0 - Switches have large frame buffers that allow data waiting to be transmitted to be stored so the data will not be dropped. This feature is beneficial especially if the incoming traffic is from a faster port than the egress port used for transmitting.

Question 14

Which network device can be used to eliminate collisions on an Ethernet network?

Switch

Topic 2.2.0 - A switch provides microsegmentation so that no other device competes for the same Ethernet network bandwidth.

**3.1 VLANs**

VLANs allows admins to segment networks based on factors such as function, team, or application, without regard for the physical location of the users or devices.

Each VLAN act as separate logical network.

A VLAN creates a logical broadcast domain that can span multiple physical LAN segments.

VLANs can improve network performance by separating large broadcast domains into smaller ones.

Benefits of VLANs

* Smaller Broadcast Domains
* Improved security
* Improved IT Efficiency
* Reduced Cost
* Better performance
* Simpler project and application management

Types of VLANs

>> show vlan brief

1. Default VLANs –

* VLAN 1 is the default
* All ports are assigned to VLAN 1 by default
* The native VLAN is VLAN 1 by default
* The management VLAN is VLAN 1 by default
* The VLAN 1 cannot be renamed or deleted.

1. Data VLAN –

* VLANs configured to separate user-generated traffic. They separate the network into groups of users or devices
* Voice and network management traffic should not be permitted on data VLANs.

1. Native VLANs –

* All untagged traffic is forwarded here.

1. Management VLAN –

* A data VLAN configured specifically for network management traffic including SSH, Telnet, HTTPS, HTTP, and SNMP

1. Voice VLAN –

* A VLAN that support Voice over IP (VoIP)
* It 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

3.6.4 Module Quiz - VLANs

Question 1

What happens to a port that is associated with VLAN 10 when the administrator deletes VLAN 10 from the switch?

The port becomes inactive.

Topic 3.3.0 - If the VLAN that is associated with a port is deleted, the port becomes inactive and cannot communicate with the network any more. To verify that a port is in an inactive state, use the show interfaces switchport command.

Question 2

In which memory location are the VLAN configurations of normal range VLANs stored on a Catalyst switch?

Flash

Topic 3.3.0 - When a normal range VLAN is created the configuration information of the VLAN is stored in flash in the vlan.dat file.

Question 3

An administrator is investigating a failure on a trunk link between a Cisco switch and a switch from another vendor. After a few show commands, the administrator notices that the switches are not negotiating a trunk. What is a probable cause for this issue?

Switches from other vendors do not support DTP.

Topic 3.5.0 - DTP is a Cisco proprietary protocol. Non-Cisco switches do not support DTP.

Question 4

What is the purpose of the vlan.dat file on a switch?

It holds the VLAN database.

Topic 3.3.0 - The VLAN database (vlan.dat) contains information about normal range VLANs such as the VLAN number, name, and VTP mode.

Question 5

What is the purpose of setting the native VLAN separate from data VLANs?

A separate VLAN should be used to carry uncommon untagged frames to avoid bandwidth contention on data VLANs.

Topic 3.1.0 - When a Cisco switch trunk port receives untagged frames (unusual in well-designed networks), it forwards these frames to the native VLAN. When the native VLAN is moved away from data VLANs, those untagged frames will not compete for bandwidth in the data VLANs. The native VLAN is not designed for carrying management traffic, but rather it is for backward compatibility with legacy LAN scenarios.

Question 6

When a Cisco switch receives untagged frames on a 802.1Q trunk port, which VLAN ID is the traffic switched to by default?

Native VLAN ID

Topic 3.2.0 - A native VLAN is used to forward untagged frames that are received on a Cisco switch 802.1Q trunk port. Untagged frames that are received on a trunk port are not forwarded to any other VLAN except the native VLAN.

Question 7

A network administrator is determining the best placement of VLAN trunk links. Which two types of point-to-point connections utilize VLAN trunking?​ (Choose two.)

Between two switches that utilize multiple VLANs

Between a switch and a server that has an 802.1Q NIC

Topic 3.2.0 - VLAN trunk links are used to allow all VLAN traffic to propagate between devices such as the link between a switch and a server that has an 802.1Q-capable NIC. Switches can also utilize trunk links to routers, servers, and to other switches.

Question 8

What are three primary benefits of using VLANs? (Choose three.)

Security

Cost reduction

Improved IT Staff efficiency

Topic 3.1.0 - Security, cost reduction, and improved IT staff efficiency are all benefits of using VLANs, along with higher performance, broadcast storm mitigation, and simpler project and application management. End users are not usually aware of VLANs, and VLANs do require configuration. Because VLANs are assigned to access ports, they do not reduce the number of trunk links.

Question 9

On a Cisco switch, where is extended range VLAN information stored?

Running configuration file

Topic 3.3.0 - Extended range VLANs, 1006 through 4094, are not written to the vlan.dat file but are saved in the running configuration file.

Question 10

In which location are the normal range VLANs stored on a Cisco switch by default?

Flash memory

Topic 3.1.0 - Normal range VLANs are stored in a file called vlan.dat and located in the flash memory.

Question 11

Which distinct type of VLAN is used by an administrator to access and configure a switch?

Management VLAN

Topic 3.1.0 - A management VLAN is used to remotely access and configure a switch. Data VLANs are used to separate a network into groups of users or devices. The default VLAN is the initial VLAN all switch ports are placed in when loading the default configuration on a switch. The 802.1Q trunk port places untagged traffic on the native VLAN.

Question 12

For what reason would a network administrator use the show interfaces trunk command on a switch?

To view the native VLAN

Topic 3.3.0 - The show interfaces trunk command displays the ports that are trunk ports, the trunking mode, the encapsulation type, the trunk status, the native VLAN, and the allowed VLANs on the link.

Question 13

Where is the vlan.dat file stored on a switch?

In flash memory

Topic 3.3.0 - Normal range VLAN configurations are stored within a VLAN database file, called vlan.dat, which is located in the flash memory of the switch.

Question 14

If an organization is changing to include Cisco IP phones in its network, what design feature must be considered to ensure voice quality?

A separate VLAN is needed for voice traffic.

Topic 3.1.0 - A PC commonly connects to an IP phone and the IP phone, in turn, connects to a switch. The phone does not require a separate port. Because voice traffic cannot tolerate much packet delay, it needs to be in a separate VLAN. The voice VLAN can be configured to provide quality of service (QoS), which will ensure that the voice traffic has a higher priority than data traffic.

Question 15

A Cisco switch currently allows traffic tagged with VLANs 10 and 20 across trunk port Fa0/5. What is the effect of issuing a switchport trunk allowed vlan 30 command on Fa0/5?

It allows only VLAN 30 on Fa0/5.

Topic 3.4.0 - The switchport trunk allowed vlan 30 command allows traffic that is tagged with VLAN 30 across the trunk port. Any VLAN that is not specified in this command will not be allowed on this trunk port.

**4.1 Inter-VLAN Routing Operation**

Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN.

There are three inter-VLAN routing options:

* Legacy Inter-VLAN routing - This is a legacy solution. It does not scale well. Relied on using a router with multiple Ethernet interfaces. Each router interface was connected to a switch port in different VLANs. The router interfaces served as the default gateways to the local hosts on the VLAN subnet.
* Router-on-a-Stick - This is an acceptable solution for a small to medium-sized network. The ‘router-on-a-stick’ inter-VLAN routing method overcomes the limitation of the legacy inter-VLAN routing method. It only requires one physical Ethernet interface to route traffic between multiple VLANs on a network.

A Cisco IOS router Ethernet interface is configured as an 802.1Q trunk and connected to a trunk port on a Layer 2 switch. Specifically, the router interface is configured using subinterfaces to identify routable VLANs.

The configured subinterfaces are software-based virtual interfaces. Each is associated with a single physical Ethernet interface. Subinterfaces are configured in software on a router. Each subinterface is independently configured with an IP address and VLAN assignment. Subinterfaces are configured for different subnets that correspond to their VLAN assignment. This facilitates logical routing.

When VLAN-tagged traffic enters the router interface, it is forwarded to the VLAN subinterface. After a routing decision is made based on the destination IP network address, the router determines the exit interface for the traffic. If the exit interface is configured as an 802.Q subinterface, the data frames are VLAN-tagged with the new VLAN and sent back out the physical interface.

Note: The router-on-a-stick method of inter-VLAN routing does not scale beyond 50 VLANs.

* Layer 3 switch using switched virtual interfaces (SVIs) - This is the most scalable solution for medium to large organizations.

The modern method of performing inter-VLAN routing is to use Layer 3 switches and switched virtual interfaces (SVI). An SVI is a virtual interface that is configured on a Layer 3 switch.

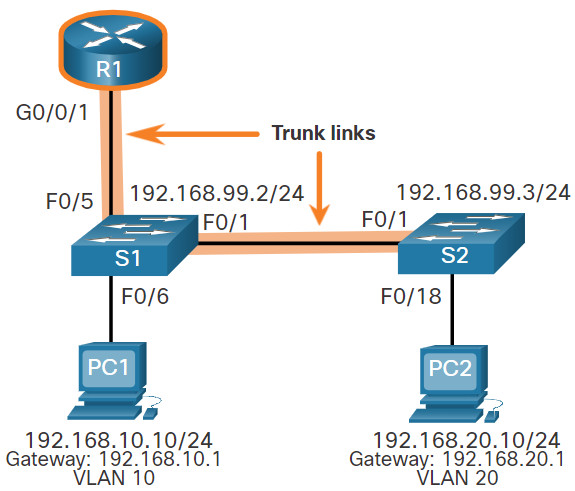
Note: A Layer 3 switch is also called a multilayer switch as it operates at Layer 2 and Layer 3.

Inter-VLAN SVIs are created the same way that the management VLAN interface is configured. The SVI is created for a VLAN that exists on the switch. Although virtual, the SVI performs the same functions for the VLAN as a router interface would. Specifically, it provides Layer 3 processing for packets that are sent to or from all switch ports associated with that VLAN.

The following are advantages of using Layer 3 switches for inter-VLAN routing:

* They are much faster than router-on-a-stick because everything is hardware switched and routed.
* There is no need for external links from the switch to the router for routing.
* They are not limited to one link because Layer 2 EtherChannels can be used as trunk links between the switches to increase bandwidth.
* Latency is much lower because data does not need to leave the switch in order to be routed to a different network.
* They more commonly deployed in a campus LAN than routers.

**4.2 Router-on-a-Stick Inter-VLAN Routing Configuration**



4.2.2 S1 VLAN and Trunking Configuration

Complete the following steps to configure S1 with VLANs and trunking:

Step 1. Create and name the VLANs.

Step 2. Create the management interface.

Step 3. Configure access ports.

Step 4. Configure trunking ports.

1. Create and name the VLANs.

First, the VLANs are created and named. VLANs are only created after you exit out of VLAN subconfiguration mode.

S1(config)# vlan 10

S1(config-vlan)# name LAN10

S1(config-vlan)# exit

S1(config)# vlan 20

S1(config-vlan)# name LAN20

S1(config-vlan)# exit

S1(config)# vlan 99

S1(config-vlan)# name Management

S1(config-vlan)# exit

S1(config)#

2. Create the management interface.

Next, the management interface is created on VLAN 99 along with the default gateway of R1.

S1(config)# interface vlan 99

S1(config-if)# ip add 192.168.99.2 255.255.255.0

S1(config-if)# no shut

S1(config-if)# exit

S1(config)# ip default-gateway 192.168.99.1

S1(config)#

3. Configure access ports.

Next, port Fa0/6 connecting to PC1 is configured as an access port in VLAN 10. Assume PC1 has been configured with the correct IP address and default gateway.

S1(config)# interface fa0/6

S1(config-if)# switchport mode access

S1(config-if)# switchport access vlan 10

S1(config-if)# no shut

S1(config-if)# exit

S1(config)#

4. Configure trunking ports.

Finally, ports Fa0/1 connecting to S2 and Fa05 connecting to R1 are configured as trunk ports.

S1(config)# interface fa0/1

S1(config-if)# switchport mode trunk

S1(config-if)# no shut

S1(config-if)# exit

S1(config)# interface fa0/5

S1(config-if)# switchport mode trunk

S1(config-if)# no shut

S1(config-if)# end

4.2.3 S2 VLAN and Trunking Configuration

S2(config)# vlan 10

S2(config-vlan)# name LAN10

S2(config-vlan)# exit

S2(config)# vlan 20

S2(config-vlan)# name LAN20

S2(config-vlan)# exit

S2(config)# vlan 99

S2(config-vlan)# name Management

S2(config-vlan)# exit

S2(config)#

S2(config)# interface vlan 99

S2(config-if)# ip add 192.168.99.3 255.255.255.0

S2(config-if)# no shut

S2(config-if)# exit

S2(config)# ip default-gateway 192.168.99.1

S2(config)# interface fa0/18

S2(config-if)# switchport mode access

S2(config-if)# switchport access vlan 20

S2(config-if)# no shut

S2(config-if)# exit

S2(config)# interface fa0/1

S2(config-if)# switchport mode trunk

S2(config-if)# no shut

S2(config-if)# exit

S2(config-if)# end

4.2.4 R1 Subinterface Configuration

The router-on-a-stick method requires you to create a subinterface for each VLAN to be routed.

A subinterface is created using the interface interface\_id.subinterface\_id global configuration mode command. The subinterface syntax is the physical interface followed by a period and a subinterface number. Although not required, it is customary to match the subinterface number with the VLAN number.

Each subinterface is then configured with the following two commands:

encapsulation dot1q vlan\_id [native] - This command configures the subinterface to respond to 802.1Q encapsulated traffic from the specified vlan-id. The native keyword option is only appended to set the native VLAN to something other than VLAN 1.

ip address ip-address subnet-mask - This command configures the IPv4 address of the subinterface. This address typically serves as the default gateway for the identified VLAN.

Repeat the process for each VLAN to be routed. Each router subinterface must be assigned an IP address on a unique subnet for routing to occur.

When all subinterfaces have been created, enable the physical interface using the no shutdown interface configuration command. If the physical interface is disabled, all subinterfaces are disabled.

R1(config)# interface G0/0/1.10

R1(config-subif)# description Default Gateway for VLAN 10

R1(config-subif)# encapsulation dot1Q 10

R1(config-subif)# ip add 192.168.10.1 255.255.255.0

R1(config-subif)# exit

R1(config)#

R1(config)# interface G0/0/1.20

R1(config-subif)# description Default Gateway for VLAN 20

R1(config-subif)# encapsulation dot1Q 20

R1(config-subif)# ip add 192.168.20.1 255.255.255.0

R1(config-subif)# exit

R1(config)#

R1(config)# interface G0/0/1.99

R1(config-subif)# description Default Gateway for VLAN 99

R1(config-subif)# encapsulation dot1Q 99

R1(config-subif)# ip add 192.168.99.1 255.255.255.0

R1(config-subif)# exit

R1(config)#

R1(config)# interface G0/0/1

R1(config-if)# description Trunk link to S1

R1(config-if)# no shut

R1(config-if)# end

4.2.6 Router-on-a-Stick Inter-VLAN Routing Verification

In addition to using ping between devices, the following show commands can be used to verify and troubleshoot the router-on-a-stick configuration.

* show ip route - Verify that the subinterfaces are appearing in the routing table of R1 by using the show ip route command.
* show ip interface brief - The output confirms that the subinterfaces have the correct IPv4 address configured, and that they are operational.
* show interfaces -
* show interfaces trunk - The misconfiguration could also be on the trunking port of the switch. Therefore, it is also useful to verify the active trunk links on a Layer 2 switch by using the show interfaces trunk command.

**4.3.1 Layer 3 Switch Inter-VLAN Routing**

Modern, enterprise networks rarely use router-on-a-stick because it does not scale easily to meet requirements. In these very large networks, network administrators use Layer 3 switches to configure inter-VLAN routing.

*Inter-VLAN routing using the router-on-a-stick method is simple to implement for a small to medium-sized organization*. However, a large enterprise requires a faster, much more scalable method to provide inter-VLAN routing.

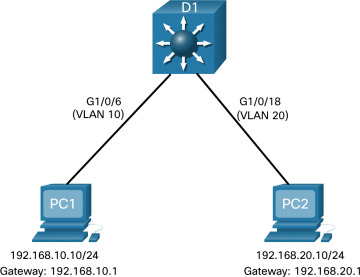
Enterprise campus LANs use Layer 3 switches to provide inter-VLAN routing. Layer 3 switches use hardware-based switching to achieve higher-packet processing rates than routers. Layer 3 switches are also commonly implemented in enterprise distribution layer wiring closets.

Capabilities of a Layer 3 switch include the ability to do the following:

Route from one VLAN to another using multiple switched virtual interfaces (SVIs).

Convert a Layer 2 switchport to a Layer 3 interface (i.e., a routed port). A routed port is similar to a physical interface on a Cisco IOS router.

To provide inter-VLAN routing, Layer 3 switches use SVIs. SVIs are configured using the same interface vlan vlan-id command used to create the management SVI on a Layer 2 switch. A Layer 3 SVI must be created for each of the routable VLANs.



4.3.3 Layer 3 Switch Configuration

Complete the following steps to configure S1 with VLANs and trunking:

Step 1. Create the VLANs.

Step 2. Create the SVI VLAN interfaces.

Step 3. Configure access ports.

Step 4. Enable IP routing.

1. Create the VLANs.

First, create the two VLANs as shown in the output.

*D1(config)# vlan 10*

*D1(config-vlan)# name LAN10*

*D1(config-vlan)# vlan 20*

*D1(config-vlan)# name LAN20*

*D1(config-vlan)# exit*

*D1(config)#*

2. Create the SVI VLAN interfaces.

Configure the SVI for VLANs 10 and 20. The IP addresses that are configured will serve as the default gateways to the hosts in the respective VLANs. Notice the informational messages showing the line protocol on both SVIs changed to up.

*D1(config)# interface vlan 10*

*D1(config-if)# description Default Gateway SVI for 192.168.10.0/24*

*D1(config-if)# ip add 192.168.10.1 255.255.255.0*

*D1(config-if)# no shut*

*D1(config-if)# exit*

*D1(config)#*

*D1(config)# int vlan 20*

*D1(config-if)# description Default Gateway SVI for 192.168.20.0/24*

*D1(config-if)# ip add 192.168.20.1 255.255.255.0*

*D1(config-if)# no shut*

*D1(config-if)# exit*

3. Configure access ports.

Next, configure the access ports connecting to the hosts and assign them to their respective VLANs.

*D1(config)# interface GigabitEthernet1/0/6*

*D1(config-if)# description Access port to PC1*

*D1(config-if)# switchport mode access*

*D1(config-if)# switchport access vlan 10*

*D1(config-if)# exit*

*D1(config)#*

*D1(config)# interface GigabitEthernet1/0/18*

*D1(config-if)# description Access port to PC2*

*D1(config-if)# switchport mode access*

*D1(config-if)# switchport access vlan 20*

*D1(config-if)# exit*

4. Enable IP routing.

Finally, enable IPv4 routing with the ip routing global configuration command to allow traffic to be exchanged between VLANs 10 and 20. This command must be configured to enable inter-VAN routing on a Layer 3 switch for IPv4.

*D1(config)# ip routing*

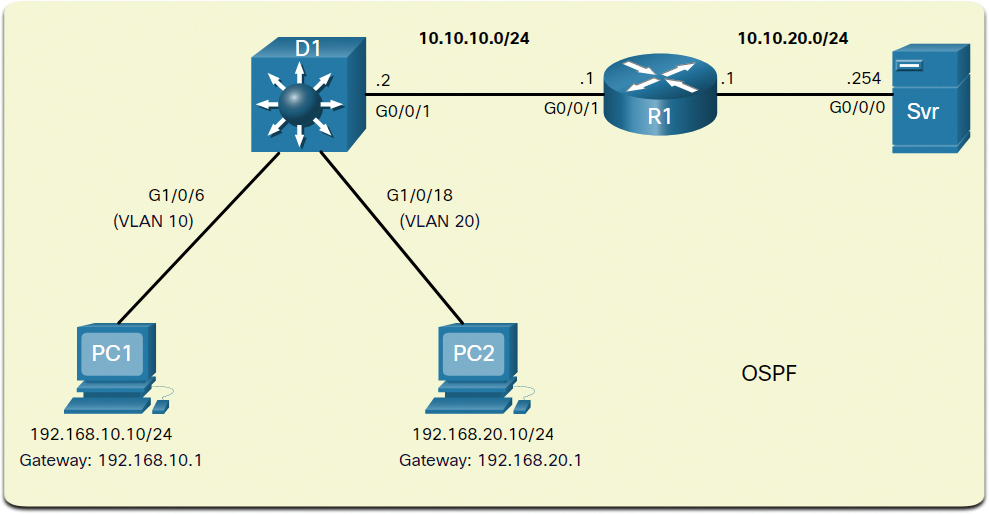
4.3.5 Routing on a Layer 3 Switch

If VLANs are to be reachable by other Layer 3 devices, then they must be advertised using static or dynamic routing. To enable routing on a Layer 3 switch, a routed port must be configured.

A routed port is created on a Layer 3 switch by disabling the switchport feature on a Layer 2 port that is connected to another Layer 3 device. Specifically, configuring the no switchport interface configuration command on a Layer 2 port converts it into a Layer 3 interface. Then the interface can be configured with an IPv4 configuration to connect to a router or another Layer 3 switch.

**4.3.6 Routing Scenario on a Layer 3 Switch**

In the figure, the previously configured D1 Layer 3 switch is now connected to R1. R1 and D1 are both in an Open Shortest Path First (OSPF) routing protocol domain. Assume inter-VLAN has been successfully implemented on D1. The G0/0/1 interface of R1 has also been configured and enabled. Additionally, R1 is using OSPF to advertise its two networks, 10.10.10.0/24 and 10.20.20.0/24.



4.3.7 Routing Configuration on a Layer 3 Switch

Complete the following steps to configure D1 to route with R1:

Step 1. Configure the routed port.

Step 2. Enable routing.

Step 3. Configure routing.

Step 4. Verify routing.

Step 5. Verify connectivity.

1. Configure the routed port.

Configure G0/0/1 to be a routed port, assign it an IPv4 address, and enable it.

D1(config)# interface GigabitEthernet0/0/1

D1(config-if)# description routed Port Link to R1

D1(config-if)# no switchport

D1(config-if)# ip address 10.10.10.2 255.255.255.0

D1(config-if)# no shut

D1(config-if)# exit

2. Enable routing.

Ensure IPv4 routing is enabled with the ip routing global configuration command.

D1(config)# ip routing

3. Configure routing.

Configure the OSPF routing protocol to advertise the VLAN 10 and VLAN 20 networks, along with the network that is connected to R1. Notice the message informing you that an adjacency has been established with R1.

D1(config)# router ospf 10

D1(config-router)# network 192.168.10.0 0.0.0.255 area 0

D1(config-router)# network 192.168.20.0 0.0.0.255 area 0

D1(config-router)# network 10.10.10.0 0.0.0.3 area 0

D1(config-router)# ^Z

4. Verify routing.

Verify the routing table on D1. Notice that D1 now has a route to the 10.20.20.0/24 network.

D1# show ip route | begin Gateway

5. Verify connectivity.

At this time, PC1 and PC2 are able to ping the server connected to R1.

**4.4 Troubleshoot Inter-VLAN Routing**

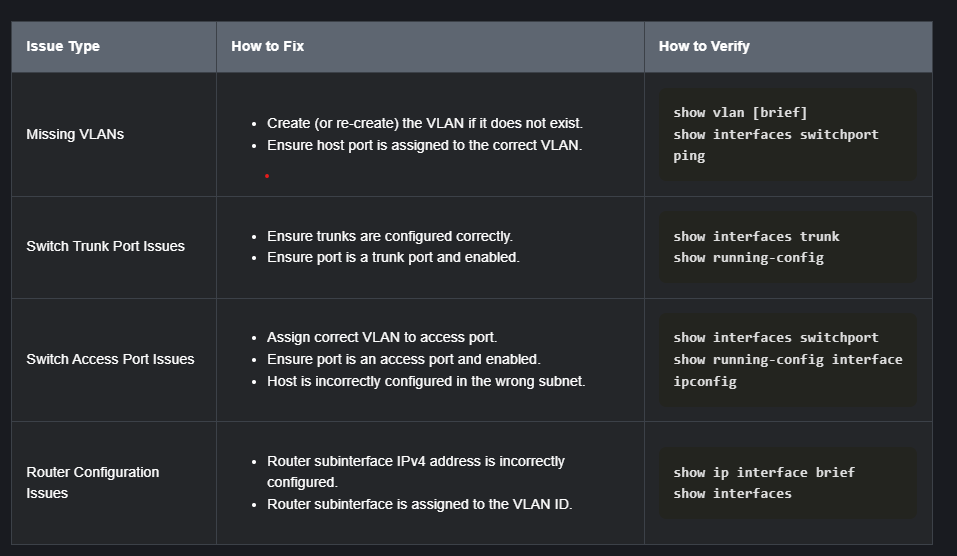
There are a number of reasons why an inter-VAN configuration may not work. All are related to connectivity issues. First, check the physical layer to resolve any issues where a cable might be connected to the wrong port. If the connections are correct, then use the list in the table for other common reasons why inter-VLAN connectivity may fail.

**4.4.4 Switch Trunk Port Issues**

Another issue for inter-VLAN routing includes misconfigured switch ports. In a legacy inter-VLAN solution, this could be caused when the connecting router port is not assigned to the correct VLAN.

However, with a router-on-a-stick solution, the most common cause is a misconfigured trunk port.

show interfaces trunk



**4.4.5 Switch Access Port Issues**

When a problem is suspected with a switch access port configuration, use verification commands to examine the configuration and identify the problem.

show interface fa0/6 switchport

show running-config interface fa0/6

**4.4.6 Router Configuration Issues**

Router-on-a-stick configuration problems are usually related to subinterface misconfigurations. For example, an incorrect IP address was configured or the wrong VLAN ID was assigned to the subinterface.

show ip interface brief

show interfaces | include Gig|802.1Q

show running-config interface g0/0/1.10

Quiz

Question 1

You are troubleshooting an inter-VLAN issue on a switch and need to verify that the subinterfaces are in the routing table. Which inter-VLAN routing troubleshooting command would you use to do this?

show ip route

Question 2

You are troubleshooting an inter-VLAN issue on a switch and need to check the list of VLANs and their assigned ports. Which inter-VLAN routing troubleshooting command would you use to do this?

show vlan

Question 3

You are troubleshooting an inter-VLAN issue on a switch and need to verify the status of an access port and its access mode VLAN. Which troubleshooting command would you use to do this?

show interfaces interface-id switchport

Question 4

You are troubleshooting an inter-VLAN issue on a switch and need to verify the status and IP address of all interfaces in a condensed format. Which inter-VLAN routing troubleshooting command would you use to do this?

show ip interface brief

**4.5.4 Module Quiz - Inter-VLAN Routing**

Question 1

A PC is to access a web server on another network. Which inter-VLAN method will provide the highest bandwidth at Layer 3 and also provide a default gateway for the PC?

Multilayer switch with routing enabled

Topic 4.3.0 - A router-on-a-stick design is the same as having a trunked interface between the router and the switch. This design works, but does not scale well because all VLANs must traverse the one connection between the router and the switch. Multiple physical interfaces on the router would be faster than the router-on-a-stick design, but a router has a limited number of physical interfaces. Layer 3 switches with routing enabled have more Ethernet ports as well as the ability to route.

Question 2

Which scalable method must be implemented in order to provide inter-VLAN routing on a switched network with more than 1000 VLANs?

Routing traffic internally to a Layer 3 switch device

Topic 4.1.0 - Layer 2 switches are able to perform static routing, but this method is inefficient with a large number of VLANs. Multilayer switching is more scalable than any other inter-VLAN routing implementation, with traffic being routed internally to the switch device. In router-on-a-stick inter-VLAN routing, where a single physical interface routes traffic among multiple VLANs on a network, there is no practical scalability. The legacy inter-VLAN routing is very inefficient and is no longer used in switched networks, because each VLAN requires a physical router interface that is connected to a different physical switch port.

Question 3

When configuring a router as part of a router-on-a-stick inter-VLAN routing topology, where should the IP address be assigned?

To the subinterface

Topic 4.2.0 - The IP address and the encapsulation type should be assigned to each router subinterface in a router-on-a-stick inter-VLAN topology.

Question 4

A small college uses VLAN 10 for the classroom network and VLAN 20 for the office network. What is needed to enable communication between these two VLANs while using legacy inter-VLAN routing?

A router with at least two LAN interfaces should be used.

Topic 4.1.0 - With legacy inter-VLAN routing, different physical router interfaces are connected to different physical switch ports. The switch ports that connect to the router are in access mode, each belonging to a different VLAN. Switches can have ports that are assigned to different VLANs, but communication between VLANs requires routing function from the router.

Question 5

What is a disadvantage of using multilayer switches for inter-VLAN routing?

Multilayer switches are more expensive than router-on-a-stick implementations.

Topic 4.1.0 - The main disadvantage of the multilayer switches is their higher cost. Because both routing and switching are done in hardware, multilayer switches are faster than router-on-a-stick.

Question 6

Which type of inter-VLAN communication design requires the configuration of multiple subinterfaces?

Router on a stick

Topic 4.1.0 - The router-on-a-stick design always includes subinterfaces on a router. When a multilayer switch is used, multiple SVIs are created. When the number of VLANs equals the number of ports on a router, or when the management VLAN needs to be routed, any of the inter-VLAN design methods can be used.

Question 7

What is a disadvantage of using router-on-a-stick inter-VLAN routing?

Does not scale well beyond 50 VLANs

Topic 4.1.0 - Router-on-a-stick inter-VLAN routing does not scale beyond 50 VLANs. The router can receive VLAN-tagged packets and send VLAN-tagged packets to a destination. Router-on-a-stick inter-VLAN routing can utilize a single router interface as a trunk link to receive and forward VLAN traffic and does not require multiple interfaces.

Question 8

What is the meaning of the number 10 in the encapsulation dot1Q 10 native router subinterface command?​

The VLAN ID

Topic 4.2.0 - The administrator can use the encapsulation command to specify the encapsulation type (IEEE 802.1Q or ISL), the VLAN ID, and optionally the native VLAN.

Question 9

While configuring inter-VLAN routing on a multilayer switch, a network administrator issues the no switchport command on an interface that is connected to another switch. What is the purpose of this command?

To create a routed port for a single network

Topic 4.3.0 - When a Layer 2 interface on a multilayer switch is configured with the no switchport command, it becomes a routed port. A routed port is configured with an IP address for a specific subnet.

Question 10

A network administrator enters the following command sequence on a Cisco 3560 switch. What is the purpose of these commands?

Switch(config)# interface gigabitethernet 0/1

Switch(config-if)# no switchport

To make the Gi0/1 port a routed port

Topic 4.3.0 - By default, the physical ports on a 3560 switch are Layer 2 interfaces. To make them routed ports, the interface command no switchport should be used. The other options do not describe the purpose of this command.

Question 11

What operational mode should be used on a switch port to connect it to a router for router-on-a-stick inter-VLAN routing?

Trunk

Topic 4.2.0 - Routers do not support Dynamic Trunking Protocol, and access mode is used to connect hosts.

Question 12

Which sentence correctly describes the SVI inter-VLAN routing method?

An SVI is needed for each VLAN.

Topic 4.1.0 - In order to create SVI inter-VLAN routing on a Layer 3 switch, the VLAN must exist in the database and the SVI must be explicitly created. The only exception is VLAN1, which is created by default.

Question 13

How is traffic routed between multiple VLANs on a multilayer switch?

Traffic is routed via internal VLAN interfaces.

Topic 4.1.0 - Multilayer switches can perform inter-VLAN routing by the use of internal VLAN interfaces. External physical interfaces can receive traffic but are not necessary for routing functions. When routing between VLANs, any broadcast traffic that is received on a VLAN would remain on ports that are members of that VLAN. Subinterfaces are not usable for inter-VLAN routing on multilayer switches.

Question 14

What is required to perform router-on-a-stick inter-VLAN routing?

A router that is configured with multiple subinterfaces

Topic 4.2.0 - With router-on-a-stick inter-VLAN routing, a single physical router interface is used to route packets between multiple VLANs if the interface is configured with multiple subinterfaces. A separate subinterface is needed for each VLAN that will be routed. Because the router is performing all routing functions, a multilayer switch is not required.

Question 15

An administrator was troubleshooting a router-on-a-stick topology and concluded that the problem was related to the configuration of VLANs on the router subinterfaces. Which two commands can the administrator use in the router to identify the problem? (Choose two.)

show ip interface

show running-config

Topic 4.4.0 - The show ip interface and show running-config commands can be useful in troubleshooting routing issues like wrong VLAN IDs that are assigned to subinterfaces. The show controllers and show ip protocols commands do not display any information about VLANs. The show vlan command is not useful to show information about the router subinterfaces.

**5. SPANNING TREE PROTOCOL**

This topic covers the causes of loops in a Layer 2 network and briefly explains how spanning tree protocol works. Redundancy is an important part of the hierarchical design for eliminating single points of failure and 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. Having alternate physical paths for data to traverse the network makes it possible for users to access network resources, despite path disruption. However, redundant paths in a switched Ethernet network may cause both physical and logical Layer 2 loops.

When multiple paths exist between two devices on an Ethernet network, and there is no spanning tree implementation on the switches, a Layer 2 loop occurs. A Layer 2 loop can result in MAC address table instability, link saturation, and high CPU utilization on switches and end-devices, resulting in the network becoming unusable.

Ethernet LANs require a loop-free topology with a single path between any two devices. A loop in an Ethernet LAN can cause continued propagation of Ethernet frames until a link is disrupted and breaks the loop.

Spanning Tree Protocol (STP) is a loop-prevention network protocol that allows for redundancy while creating a loop-free Layer 2 topology. IEEE 802.1D is the original IEEE MAC Bridging standard for STP.

**5.1.6 Broadcast Storm**

A broadcast storm is an abnormally high number of broadcasts overwhelming the network during a specific amount of time. Broadcast storms can disable a network within seconds by overwhelming switches and end devices. Broadcast storms can be caused by a hardware problem such as a faulty NIC or from a Layer 2 loop in the network.

Layer 2 broadcasts in a network, such as ARP Requests are very common. A Layer 2 loop is likely to have immediate and disabling consequences on the network. Layer 2 multicasts are typically forwarded the same way as a broadcast by the switch. So, although IPv6 packets are never forwarded as a Layer 2 broadcast, ICMPv6 Neighbor Discovery uses Layer 2 multicasts.

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.

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.

**5.2 STP Operations**

Now you know how loops are created and the basics of using spanning tree protocol to prevent them. This topic will take you, step by step, through the operation of STP. Using the STA, STP builds a loop-free topology in a four-step process:

1. Elect the root bridge.
2. Elect the root ports.
3. Elect designated ports.
4. Elect alternate (blocked) ports.

During STA and STP functions, switches use Bridge Protocol Data Units (BPDUs) to share information about themselves and their connections. BPDUs are used to elect the root bridge, root ports, designated ports, and alternate ports. Each BPDU contains a bridge ID (BID) that identifies which switch sent the BPDU. The BID is involved in making many of the STA decisions including root bridge and port roles. As shown in the figure, the BID contains a priority value, an extended system ID, and the MAC address of the switch. The lowest BID value is determined by the combination of these three fields.

Bridge Priority

The default priority value for all Cisco switches is the decimal value 32768. The range is 0 to 61440 in increments of 4096. A lower bridge priority is preferable. A bridge priority of 0 takes precedence over all other bridge priorities.

Extended System ID

The extended system ID value is a decimal value added to the bridge priority value in the BID to identify the VLAN for this BPDU.

MAC address

When two switches are configured with the same priority and have the same extended system ID, the switch having the MAC address with the lowest value, expressed in hexadecimal, will have the lower BID.

5.2.2 1. Elect the Root Bridge

The STA designates a single switch as the root bridge and uses it as the reference point for all path calculations. Switches exchange BPDUs to build the loop-free topology beginning with selecting the root bridge.

An election process determines which switch becomes the root bridge. 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 BPDU frames contain the BID of the sending switch and the BID of the root bridge, known as the Root ID.

The switch with the lowest BID will become the root bridge. At first, all switches declare themselves as the root bridge with their own BID set as the Root ID. Eventually, the switches learn through the exchange of BPDUs which switch has the lowest BID and will agree on one root bridge.

5.2.3 Impact of Default BIDs

Because the default priority is 32768, it is possible for two or more switches to have the same priority. In this scenario, where the priorities are the same, the switch with the lowest MAC address will become the root bridge. To ensure that the root bridge decision best meets network requirements, it is recommended that the administrator configure the desired root bridge switch with a lower priority.

5.2.4 Determine the Root Path Cost

When the root bridge has been elected for a given spanning tree instance, the STA starts the process of determining the best paths to the root bridge from all destinations in the broadcast domain. The path information, known as the internal root path cost, is determined by the sum of all the individual port costs along the path from the switch to the root bridge.

Note: The BPDU includes the root path cost. This is the cost of the path from the sending switch to the root bridge.

When a switch receives the BPDU, it adds the ingress port cost of the segment to determine its internal root path cost.

The default port costs are defined by the speed at which the port operates.

|  |  |  |
| --- | --- | --- |
| Speed | STP Cost | RSTP Cost |
| 10 Mbps | 100 | 2000000 |
| 100 Mbps | 19 | 200000 |
| 1 Gbps | 4 | 20000 |
| 10 Gbps | 2 | 2000 |
| 100 Gbps | X | 200 |
| 1 Tbps | X | 20 |

Although switch ports have a default port cost associated with them, the port cost is configurable. The ability to configure individual port costs gives the administrator the flexibility to manually control the spanning tree paths to the root bridge.

5.2.5 2. Elect the Root Ports

After the root bridge has been determined, the STA algorithm is used to select the root port. Every non-root switch will select one root port. The root port is the port closest to the root bridge in terms of overall cost (best path) to the root bridge. This overall cost is known as the internal root path cost.

The internal root path cost is equal to the sum of all the port costs along the path to the root bridge. Paths with the lowest cost become preferred, and all other redundant paths are blocked.

5.2.6 3. Elect Designated Ports

The loop prevention part of spanning tree becomes evident during these next two steps. After each switch selects a root port, the switches will then select designated ports.

Every segment between two switches will have one designated port. The designated port on the segment (with two switches) that has the LOWEST internal root path cost to the root bridge. In other words, the designated port has the best path to receive traffic leading to the root bridge.

What is not a root port or a designated port becomes an alternate or blocked port. The end result is a single path from every switch to the root bridge.

Designated Ports on Root Bridge

All ports on the root bridge are designated ports, as shown in the figure. This is because the root bridge has the lowest cost to itself.

Designated Port When There is a Root Port

If one end of a segment is a root port, then the other end is a designated port.

Designated Port When There is No Root Port

This leaves only segments between two switches where neither of the switches is the root bridge. In this case, the port on the switch with the least-cost path to the root bridge is the designated port for the segment.

5.2.7 4. Elect Alternate (Blocked) Ports

If a port is not a root port or a designated port, then it becomes an alternate (or backup) port. Alternate ports and backup ports are in discarding or blocking state to prevent loop.

5.2.8 Elect a Root Port from Multiple Equal-Cost Paths

Root port and designated ports are based on the lowest path cost to the root bridge. But what happens if the switch has multiple equal-cost paths to the root bridge? How does a switch designate a root port?

When a switch has multiple equal-cost paths to the root bridge, the switch will determine a port using the following criteria:

1. Lowest sender BID
2. Lowest sender port priority
3. Lowest sender port ID

5.2.9 STP Timers and Port States

STP convergence requires three timers, as follows:

Hello Timer -The hello time is the interval between BPDUs. The default is 2 seconds but can be modified to between 1 and 10 seconds.

Forward Delay Timer -The forward delay is the time that is spent in the listening and learning state. The default is 15 seconds but can be modified to between 4 and 30 seconds.

Max Age Timer -The max age is the maximum length of time that a switch waits before attempting to change the STP topology. The default is 20 seconds but be modified to between 6 and 40 seconds.

Note: The default times can be changed on the root bridge, which dictates the value of these timers for the STP domain.

5.2.11 Per-VLAN Spanning Tree

Up until now, we have discussed STP in an environment where there is only one VLAN. However, STP can be configured to operate in an environment with multiple VLANs.

In Per-VLAN Spanning Tree (PVST) versions of STP, there is a root bridge elected for each spanning tree instance. This makes it possible to have different root bridges for different sets of VLANs. STP operates a separate instance of STP for each individual VLAN. If all ports on all switches are members of VLAN 1, then there is only one spanning tree instance.

QUIZ

Question 1

By default (without any configuration on a switch), what will determine which switch is the root bridge?

The MAC address of the switch

Question 2

The root bridge will be the switch with the:

Lowest bridge ID

Question 3

The port closest to the root bridge in terms of least overall cost (best path) to the root bridge is the:

Root port

Question 4

The port on the segment (with two switches) that has the lowest path cost to the root bridge is the:

Designated port

Question 5

Which of the following ports will forward Ethernet frames? (Choose two.)

Designated port

Root port

Question 6

The sum of individual port costs along the path from the switch to the root bridge is known as the:

Root path cost

Question 7

How often does a switch send a BPDU?

Every 2 seconds

5.3.2 RSTP Concepts

RSTP (IEEE 802.1w) supersedes the original 802.1D while retaining backward compatibility. The 802.1w STP terminology remains primarily the same as the original IEEE 802.1D STP terminology. Most parameters have been left unchanged. Users that are familiar with the original STP standard can easily configure RSTP. The same spanning tree algorithm is used for both STP and RSTP to determine port roles and topology.

RSTP increases the speed of the recalculation of the spanning tree when the Layer 2 network topology changes. RSTP can achieve much faster convergence in a properly configured network, sometimes in as little as a few hundred milliseconds. If a port is configured to be an alternate port it can immediately change to a forwarding state without waiting for the network to converge.

Note: Rapid PVST+ is the Cisco implementation of RSTP on a per-VLAN basis. With Rapid PVST+ an independent instance of RSTP runs for each VLAN.

5.4.2 Module Quiz - STP

Question 1

Which port state will switch ports immediately transition to when configured for PortFast?

Forwarding

Topic 5.3.0 - PortFast allows a switch port to bypass the listening and learning states and transition immediately to the forwarding state.

Question 2

After the election of the root bridge has been completed, how will switches find the best paths to the root bridge?

Each switch will analyze the sum of all port costs to reach the root and use the path with the lowest cost.

Topic 5.2.0 - After the election of a root bridge has occurred, each switch will have to determine the best path to the root bridge from its location. The path is determined by summing the individual port costs along the path from each switch port to the root bridge.

Question 3

Which is the default STP operation mode on Cisco Catalyst switches?

PVST+

Question 4

What value determines the root bridge when all switches connected by trunk links have default STP configurations?

MAC address

Topic 5.2.0 - When all switches are configured with the same default bridge priority, the MAC address becomes the deciding factor for the election of the root bridge. All links on the same VLAN will also have the same extended system ID so this will not contribute to determine which switch is the root for that VLAN.

Question 5

During the implementation of Spanning Tree Protocol, all switches are rebooted by the network administrator. What is the first step of the spanning-tree election process?

All the switches send out BPDUs advertising themselves as the root bridge.

Topic 5.2.0 - After a Cisco switch boots, it will send out BPDUs containing its individual BID and the root ID for the network. By default, the initial root ID at bootup will be the ID of that individual switch. After a root bridge is elected, port states and paths are chosen.

Question 6

Which two concepts relate to a switch port that is intended to have only end devices attached and intended never to be used to connect to another switch? (Choose two.)

Edge port

PortFast

Topic 5.3.0 - The RSTP edge port concept corresponds to the PVST+ PortFast feature. An edge port connects to an end station and assumes that the switch port does not connect to another switch. RSTP edge ports should immediately transition to the forwarding state, thereby skipping the time-consuming 802.1D listening and learning port states. PVST+ is the default spanning-tree configuration for a Cisco Catalyst switch. The bridge ID (BID) is used to determine the root bridge on a network and includes the bridge priority, the extended system ID, and the MAC address.

Question 7

Which three port states are used by Rapid PVST+? (Choose three.)

Discarding

Learning

Forwarding

Topic 5.3.0 - The Rapid PVST+ port states are discarding, learning, and forwarding.

Question 8

When PVST is running over a switched network, which port state can participate in BPDU frame forwarding based on BPDUs received, but does not forward data frames?

Listening

Topic 5.2.0 - Ports in the blocking state are nondesignated ports and do not participate in frame forwarding. Ports in the listening state can participate in BPDU frame forwarding according to received BPDU frames, but do not forward data frames. Ports in the forwarding state forward data frames and send and receive BPDU frames. Ports in the disabled state are administratively disabled.

Question 9

Which STP port role is adopted by a switch port if there is no other port with a lower cost to the root bridge?

Root port

Topic 5.2.0 - The root port is the port with the lowest cost to reach the root bridge.

Question 10

Which two statements describe a switch port that is configured with PortFast? (Choose two.)

The switch port immediately transitions from blocking to the forwarding state.

The switch port should never receive BPDUs.

Topic 5.3.0 - A port that is configured with PortFast will immediately transition from blocking to the forwarding state. PortFast should only be configured on switch ports that support end devices, so no BPDUs should ever be received through a port that is configured with PortFast. Configuring a port with PortFast supports DHCP because PortFast will speed up the transition from blocking to forwarding. Without PortFast, an end device may begin to issue DHCP requests before the port has transitioned to the forwarding state.

Question 11

What is one way to correct a spanning tree failure?

Manually remove redundant links in the switched network.

Topic 5.3.0 - An action that can be taken when there is a spanning tree failure in a Layer 2 network is to remove all redundant links in the failed segment of the network. This will eliminate the loops in the topology allowing for a normalization of the traffic and CPU loads. The next step would be to investigate the failure of STP on the redundant links and fix these issues prior to restoring these links.

Question 12

What additional information is contained in the 12-bit extended system ID of a BPDU?

VLAN ID

Topic 5.2.0 - The BPDU has three fields; the bridge priority, the extended system ID, and the MAC address. The extended system ID contains 12 bits that identify the VLAN ID.

Question 13

An administrator is troubleshooting a switch and wants to verify if it is a root bridge. What command can be used to do this?

show spanning-tree

Topic 5.1.0 - Of all the commands that are listed, only the correct option, show spanning-tree, displays STP root bridge information.

Question 14

What is an accurate description of redundancy?

Designing a network to use multiple paths between switches to ensure there is no single point of failure

Topic 5.1.0 - Redundancy attempts to remove any single point of failure in a network by using multiple physically cabled paths between switches in the network.

**6.1 EtherChannel Operation**

6.1.1 Link Aggregation

There are scenarios in which more bandwidth or redundancy between devices is needed than what can be provided by a single link. Multiple links could be connected between devices to increase bandwidth. However, Spanning Tree Protocol (STP), which is enabled on Layer 2 devices like Cisco switches by default, will block redundant links to prevent switching loops.

A link aggregation technology is needed that allows redundant links between devices that will not be blocked by STP. That technology is known as EtherChannel.

EtherChannel is a link aggregation technology that groups multiple physical Ethernet links together into one single logical link. It is used to provide fault-tolerance, load sharing, increased bandwidth, and redundancy between switches, routers, and servers.

EtherChannel technology makes it possible to combine the number of physical links between the switches to increase the overall speed of switch-to-switch communication.

6.1.2 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.

6.1.3 Advantages of EtherChannel

EtherChannel technology has many advantages, including the following:

* 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 and destination MAC load balancing, or source IP and 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.

6.1.4 Implementation Restrictions

EtherChannel implementation on the catalyst 2960 switch has certain implementation restrictions, including the following:

* Interface types cannot be mixed. For example, Fast Ethernet and Gigabit Ethernet cannot be mixed within a single EtherChannel.

Currently each EtherChannel can consist of up to eight compatibly-configured Ethernet ports. EtherChannel provides full-duplex bandwidth up to 800 Mbps (Fast EtherChannel) or 8 Gbps (Gigabit EtherChannel) between one switch and another switch or host.

The Cisco Catalyst 2960 Layer 2 switch currently supports up to 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 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.

6.1.5 AutoNegotiation Protocols

EtherChannels can be formed through negotiation using one of two protocols, Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP). These protocols allow ports with similar characteristics to form a channel through dynamic negotiation with adjoining switches.

Note: It is also possible to configure a static or unconditional EtherChannel without PAgP or LACP.

6.1.6 PAgP Operation

PAgP (pronounced “Pag - P”) is a Cisco-proprietary protocol that aids in the automatic creation of EtherChannel links. When an EtherChannel link is configured using PAgP, PAgP packets are sent between EtherChannel-capable ports to negotiate the forming of a channel. When PAgP identifies matched Ethernet links, it groups the links into an EtherChannel. The EtherChannel is then added to the spanning tree as a single port.

When enabled, PAgP also manages the EtherChannel. PAgP packets are sent every 30 seconds. PAgP checks for configuration consistency and manages link additions and failures between two switches. It ensures that when an EtherChannel is created, all ports have the same type of configuration.

Note: In EtherChannel, it is mandatory that all ports have the same speed, duplex setting, and VLAN information. Any port-channel modification after the creation of the channel also changes the aggregated channel ports.

PAgP helps create the EtherChannel link by detecting the configuration of each side and ensuring that links are compatible so that the EtherChannel link can be enabled when needed. The modes for PAgP as follows:

On - This mode forces the interface to channel without PAgP. Interfaces configured in the on mode do not exchange PAgP packets.

PAgP desirable - This PAgP mode places an interface in an active negotiating state in which the interface initiates negotiations with other interfaces by sending PAgP packets.

PAgP auto - This PAgP mode places an interface in a passive negotiating state in which the interface responds to the PAgP packets that it receives but does not initiate PAgP negotiation.

The modes must be compatible on each side. If one side is configured to be in auto mode, it is placed in a passive state, waiting for the other side to initiate the EtherChannel negotiation. If the other side is also set to auto, the negotiation never starts and the EtherChannel does not form. If all modes are disabled by using the no command, or if no mode is configured, then the EtherChannel is disabled.

The on mode manually places the interface in an EtherChannel, without any negotiation. It works only if the other side is also set to on. If the other side is set to negotiate parameters through PAgP, no EtherChannel forms, because the side that is set to on mode does not negotiate.

No negotiation between the two switches means there is no checking to make sure that all the links in the EtherChannel are terminating on the other side, or that there is PAgP compatibility on the other switch.

6.1.8 LACP Operation

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 other switch. 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 modes for LACP are as follows:

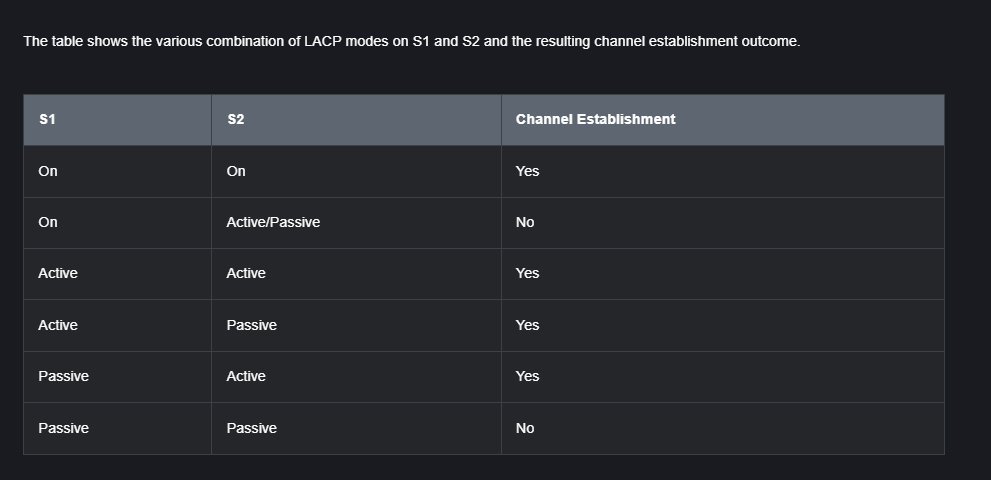
On - This mode forces the interface to channel without LACP. Interfaces configured in the on mode do not exchange LACP packets.

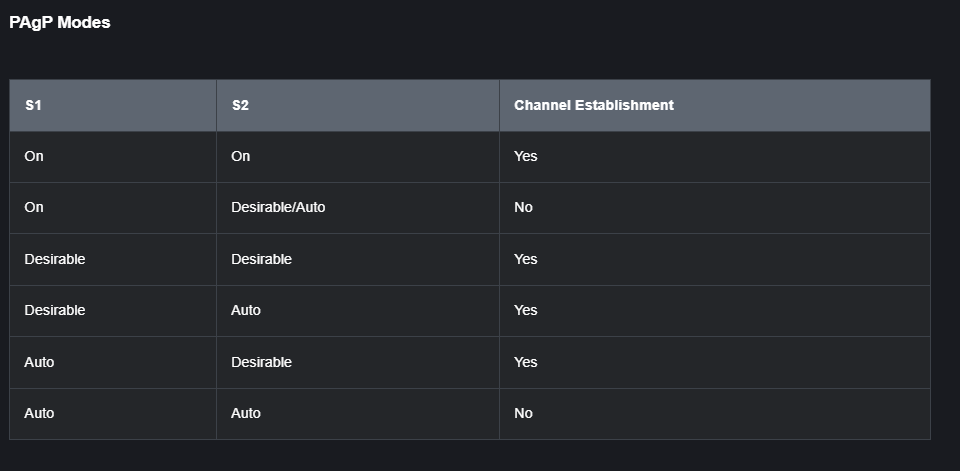
LACP active - This LACP mode places a port in an active negotiating state. In this state, the port initiates negotiations with other ports by sending LACP packets.

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.





QUIZ  
Question 1

Which are benefits of EtherChannel technology? (Choose all that apply.)

Fault-tolerance

Load sharing

Increased bandwidth

Link redundancy

Question 2

True or False? FastEthernet and GigabitEthernet links can be combined into a single EtherChannel.

False

Question 3

True or False? PAgP and LACP are both Cisco-proprietary link aggregation protocols.

False

Question 4

Which three are PAgP interface modes? (Choose three.)

On

Auto

Desirable

Question 5

Which PAgP interface mode will initiate negotiation with other interfaces?

Desirable

Question 6

Which combinations of PAgP modes will form an EtherChannel? (Choose all that apply.)

Auto > desirable

On > on

6.2 Configure EtherChannel

6.2.1 Configuration Guidelines

* EtherChannel support - All Ethernet interfaces must support EtherChannel with no requirement that interfaces be physically contiguous.
* 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 (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 they are set to auto or desirable 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.

6.2.2 LACP Configuration Example

Configuring EtherChannel with LACP requires the following three 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.

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.

Step 3. 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, S1 is configured with an LACP EtherChannel. The port channel is configured as a trunk interface with the allowed VLANs specified.

*S1(config)# interface range FastEthernet 0/1 - 2*

*S1(config-if-range)# channel-group 1 mode active*

*Creating a port-channel interface Port-channel 1*

*S1(config-if-range)# exit*

*S1(config)# interface port-channel 1*

*S1(config-if)# switchport mode trunk*

*S1(config-if)# switchport trunk allowed vlan 1,2,20*

6.3 Verify and Troubleshoot EtherChannel

* The show interfaces port-channel command displays the general status of the port channel interface.
* When several port channel interfaces are configured on the same device, use the show etherchannel summary command to display one line of information per port channel.
* Use the show etherchannel port-channel command to display information about a specific port channel interface.
* 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.

6.4.4 Module Quiz - Etherchannel

Question 1

An EtherChannel link using LACP was formed between two switches, S1 and S2. While verifying the configuration, which mode combination could be utilized on both switches?​

S1-passive and S2-active

Topic 6.1.0 - An EtherChannel link will be formed using LACP when both switches are in on mode or in active mode, or when one of them is in passive mode and the other is in active mode.

Question 2

When a range of ports is being configured for EtherChannel, which mode will configure PAgP so that it initiates the EtherChannel negotiation?

Desirable

Topic 6.1.0 - The command channel-group mode active enables LACP unconditionally, and the command channel-group mode passive enables LACP only if the port receives an LACP packet from another device. The command channel-group mode desirable enables PAgP unconditionally, and the command channel-group mode auto enables PAgP only if the port receives a PAgP packet from another device.

Question 3

Which three interface parameters must match for an EtherChannel to form? (Choose three.)

Allowed VLANs

Native VLAN

Trunking mode

Topic 6.1.0 - There are some EtherChannel modes that can be different and an EtherChannel will form, such as auto/desirable and active/passive. A port that is currently in the spanning tree blocking mode or has been configured for PortFast can still be used to form an EtherChannel.

Question 4

What are three advantages of using EtherChannel technology? (Choose three.)

Configuration tasks can be done on the EtherChannel interface.

There is no need to upgrade links to faster connections to increase bandwidth.

A spanning tree recalculation is not required when a single link within the channel goes down.

Topic 6.1.0 - Most configuration tasks can be done on the EtherChannel interface, rather than on individual ports. Existing ports can be used, eliminating the need to upgrade ports to faster speeds. Spanning Tree Protocol runs on EtherChannel links in the same manner as it does on regular links, but it does not recalculate when an individual link within the channel goes down. EtherChannel also supports load balancing.

Question 5

A network administrator is configuring an EtherChannel link between two physical ports on a switch. Which statement describes the result when one of the physical ports fails?

The EtherChannel continues transmitting data with reduced bandwidth.

Topic 6.1.0 - An EtherChannel is seen as one logical connection. The loss of one physical link within the channel does not create a change in the topology and therefore a spanning tree recalculation is not required. When one of the member ports in the EtherChannel fails, the EtherChannel link remains functional, although its overall throughput decreases because of a lost link within the EtherChannel.

Question 6

When EtherChannel is implemented, multiple physical interfaces are bundled into which type of logical connection?

Port channel

Topic 6.1.0 - When EtherChannel is being configured, the first step is to specify what physical ports will be used in an EtherChannel group. The second step is to create the logical EtherChannel port channel interface which contains the group of physical interfaces.

Question 7

When a range of ports is being configured for EtherChannel by the use of PAgP, which mode will form the bundled channel only if the port receives PAgP packets from another device?

Auto

Topic 6.1.0 - The command channel-group mode active enables LACP unconditionally, and the command channel-group mode passive enables LACP only if the port receives an LACP packet from another device. The command channel-group mode desirable enables PAgP unconditionally, and the command channel-group mode auto enables PAgP only if the port receives a PAgP packet from another device.

Question 8

Which two load balancing methods can be implemented with EtherChannel technology? (Choose two.)

Source MAC to destination MAC

Source IP to destination IP

Topic 6.1.0 - Source MAC to destination MAC load balancing and source IP to destination IP load balancing are two implementation methods used in EtherChannel technology.

Question 9

Which function is provided by EtherChannel?

Creating one logical link by using multiple physical links between two LAN switches

Topic 6.1.0 - EtherChannel technology allows the grouping, or aggregating, of several Fast Ethernet or Gigabit switch ports into one logical channel.

Question 10

Which statement is true about EtherChannel technology?

EtherChannel uses existing switch ports.

Topic 6.1.0 - EtherChannel relies on existing switch ports, so there is no need to upgrade the links. Some configuration tasks are done on individual ports and some configuration tasks are done on the EtherChannel group. STP operates on EtherChannel in the same manner as it does on other redundant links.

Question 11

Which two mode combinations would result in the successful negotiation of an EtherChannel? (Choose two.)

Active; passive

Desirable; desirable

Topic 6.1.0 - The combinations of modes that will form an EtherChannel are as follows: on/on, active/passive, active/active, desirable/auto, and desirable/desirable.

Question 12

Which two protocols are link aggregation protocols? (Choose two.)

802.3ad

PAgP

Topic 6.1.0 - The two protocols that can be used to form an EtherChannel are PAgP (Cisco proprietary) and LACP, also know as IEEE 802.3ad. STP (Spanning Tree Protocol) or RSTP (Rapid Spanning Tree Protocol) is used to avoid loops in a Layer 2 network. EtherChannel is the term that describes the bundling of two or more links that are treated as a single link for spanning tree and configuration.

Question 13

When a range of ports is being configured for EtherChannel, which mode will configure LACP so that it initiates the EtherChannel negotiation?

Active

Topic 6.1.0 - The command channel-group mode active enables LACP unconditionally, and the command channel-group mode passive enables LACP only if the port receives an LACP packet from another device. The command channel-group mode desirable enables PAgP unconditionally, and the command channel-group mode auto enables PAgP only if the port receives a PAgP packet from another device.

Question 14

What will happen if a network administrator puts a port that is part of an EtherChannel bundle into a different VLAN than the other ports in that bundle?

The EtherChannel will fail.

Topic 6.2.0 - All ports in an EtherChannel bundle must either be trunk ports or be access ports in the same VLAN. If VLAN pruning is enabled on the trunk, the allowed VLANs must be the same on both sides of the EtherChannel.

Question 15

When a range of ports is being configured for EtherChannel, which mode will configure LACP on a port only if the port receives LACP packets from another device?

Passive

Topic 6.1.0 - The command channel-group mode active enables LACP unconditionally, and the command channel-group mode passive enables LACP only if the port receives an LACP packet from another device. The command channel-group mode desirable enables PAgP unconditionally, and the command channel-group mode auto enables PAgP only if the port receives a PAgP packet from another device.

Checkpoint Exam: Redundant Networks Exam

Question 1

Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.

Which set of configuration commands issued on SW1 will successfully complete the EtherChannel link between SW1 and SW2?

interface GigabitEthernet0/1,channel-group 1 mode desirable

Issuing the show running-configuration command on SW1 shows that interface GigabitEthernet0/1 is missing the channel-group 1 mode desirable command which will compete the EtherChannel configuration for interface GigabitEthernet0/1 and interface GigabitEthernet0/2.

Question 2

The graphic shows a Layer 3 switch at the top. The Layer 3 switch connects to three Layer 2 switches with two links between the Layer 3 switch and each of the Layer 2 switches.

Refer to the exhibit. Which switching technology would allow each access layer switch link to be aggregated to provide more bandwidth between each Layer 2 switch and the Layer 3 switch?

EtherChannel

PortFast is used to reduce the amount of time that a port spends going through the spanning-tree algorithm, so that devices can start sending data sooner. Trunking can be implemented in conjunction with EtherChannel, but trunking alone does not aggregate switch links. HSRP is used to load-balance traffic across two different connections to Layer 3 devices for default gateway redundancy. HSRP does not aggregate links at either Layer 2 or Layer 3 as EtherChannel does.

Question 3

The graphic contains two switches, S1 and S2, that are connected through two links that use the Fa0/0 and Fa0/1 interfaces.

Refer to the exhibit. An administrator wants to form an EtherChannel between the two switches by using the Port Aggregation Protocol. If switch S1 is configured to be in auto mode, which mode should be configured on S2 to form the EtherChannel?

desirable

An EtherChannel will be formed via PAgP when both switches are in on mode or when one of them is in auto or desirable mode and the other is in desirable mode.

Question 4

The graphic shows the following information: Switch S1 (the root bridge) uses a port that is labeled B to connect to switch S3 on a port labeled D. S3 is connected to switch S2 on a port labeled A. S2 uses a port labeled C to connect to S1. S2 is connected also to three PC workstations labeled A, B, and C.

Refer to the exhibit. What are the possible port roles for ports A, B, C, and D in this RSTP-enabled network?

alternate, designated, root, root

Because S1 is the root bridge, B is a designated port, and C and D root ports. RSTP supports a new port type, alternate port in discarding state, that can be port A in this scenario.

Question 5

Which spanning tree standard supports only one root bridge so that traffic from all VLANs flows over the same path?

802.1D

MST is the Cisco implementation of MSTP, an IEEE standard protocol that provides up to 16 instances of RSTP. PVST+ provides a separate 802.1D spanning-tree instance for each VLAN that is configured in the network. 802.1D is the original STP standard defined by the IEEE and allows for only one root bridge for all VLANs. 802.1w, or RSTP, provides faster convergence but still uses only one STP instance for all VLANs.

Question 6

If no bridge priority is configured in PVST, which criteria is considered when electing the root bridge?

lowest MAC address

Only one switch can be the root bridge for a VLAN. The root bridge is the switch with the lowest BID. The BID is determined by priority and the MAC address. If no priority is configured then all switches use the default priority and the election of the root bridge will be based on the lowest MAC address.

Question 7

What is the outcome of a Layer 2 broadcast storm?

New traffic is discarded by the switch because it is unable to be processed.

When the network is saturated with broadcast traffic that is looping between switches, new traffic is discarded by each switch because it is unable to be processed.

Question 8

Four switches labeled S1, S2, S3, and S4, are connected. S1 connects to S2 and S3. S4 also connects to S2 and S3. There is a text box attached to each switch: S1 text box shows: Bridge ID: Priority: 32769 MAC: 000A00032222 S2 text box shows: Bridge ID: Priority: 32769 MAC: 000A00031111 S3 text box shows: Bridge ID: Priority: 32769 MAC: 000A00033333 S4 text box shows: Bridge ID: Priority: 32769 MAC: 000A00031212

Refer to the exhibit. Which switch will be the root bridge after the election process is complete?

S2

The root bridge is determined by the lowest bridge ID, which consists of the priority value and the MAC address. Because the priority values of all of the switches are identical, the MAC address is used to determine the root bridge. Because S2 has the lowest MAC address, S2 becomes the root bridge.

Question 9

What are two drawbacks to turning spanning tree off and having multiple paths through the Layer 2 switch network? (Choose two.)

The MAC address table becomes unstable.

Broadcast frames are transmitted indefinitely.

Spanning tree should never be disabled. Without it, the MAC address table becomes unstable, broadcast storms can render network clients and the switches unusable, and multiple copies of unicast frames can be delivered to the end devices.

Question 10

What is the value used to determine which port on a non-root bridge will become a root port in a STP network?

the path cost

STP establishes one root port on each non-root bridge. The root port is the lowest-cost path from the non-root bridge to the root bridge, indicating the direction of the best path to the root bridge. This is primarily based on the path cost to the root bridge.

Question 11

Which protocol provides up to 16 instances of RSTP, combines many VLANs with the same physical and logical topology into a common RSTP instance, and provides support for PortFast, BPDU guard, BPDU filter, root guard, and loop guard?

MST

MST is the Cisco implementation of MSTP, an IEEE standard protocol that provides up to 16 instances of RSTP and combines many VLANs with the same physical and logical topology into a common RSTP instance. Each instance supports PortFast, BPDU guard, BPDU filter, root guard, and loop guard. STP and RSTP assume only one spanning-tree instance for the entire bridged network, regardless of the number of VLANs. PVST+ provides a separate 802.1D spanning-tree instance for each VLAN that is configured in the network.

Question 12

Which three components are combined to form a bridge ID?

Bridge priority

MAC address

Extended system ID

The three components that are combined to form a bridge ID are bridge priority, extended system ID, and MAC address.

Question 13

A set of switches is being connected in a LAN topology. Which STP bridge priority value will make it least likely for the switch to be selected as the root?

32768

4096

61440

65535

The STP bridge priority is a two byte number, but it can only be customized in increments of 4096. The smaller number is preferred, but the largest usable priority value is 61440.

Question 14

What is the function of STP in a scalable network?

It disables redundant paths to eliminate Layer 2 loops.

STP is an important component in a scalable network because it allows redundant physical connections between Layer 2 devices to be implemented without creating Layer 2 loops. STP prevents Layer 2 loops from forming by disabling interfaces on Layer 2 devices when they would create a loop.

Question 15

Which port role is assigned to the switch port that has the lowest cost to reach the root bridge?

root port

The root port on a switch is the port with the lowest cost to reach the root bridge.

Question 16

Which two network design features require Spanning Tree Protocol (STP) to ensure correct network operation? (Choose two.)

redundant links between Layer 2 switches

removing single points of failure with multiple Layer 2 switches

Spanning Tree Protocol (STP) is required to ensure correct network operation when designing a network with multiple interconnected Layer 2 switches or using redundant links to eliminate single points of failure between Layer 2 switches. Routing is a Layer 3 function and does not relate to STP. VLANs do reduce the number of broadcast domains but relate to Layer 3 subnets, not STP.

Question 17

When the show spanning-tree vlan 33 command is issued on a switch, three ports are shown in the forwarding state. In which two port roles could these interfaces function while in the forwarding state? (Choose two.)

designated

root

The role of each of the three ports will be either designated port or root port. Ports in the disabled state are administratively disabled. Ports in the blocking state are alternate ports.

Question 18

What is the purpose of the Spanning Tree Protocol (STP)?

prevents Layer 2 loops

The Spanning-Tree Protocol (STP) creates one path through a switch network in order to prevent Layer 2 loops.

Question 19

A network administrator has configured an EtherChannel between two switches that are connected via four trunk links. If the physical interface for one of the trunk links changes to a down state, what happens to the EtherChannel?

The EtherChannel will remain functional.

EtherChannel offers redundancy by bundling multiple trunk links into one logical connection. Failure of one physical link within the EtherChannel will not create a change in the topology and therefore a recalculation by Spanning Tree is unnecessary. Just one physical link must remain operational for the EtherChannel to continue to function.

Question 20

The graphic contains two switches, S1 and S2, that are connected through two links that use the Fa0/0 and Fa0/1 interfaces. It also contains the following commands: S1(config)# interface range FastEthernet0/0 - 1 S1(config-if-range)# channel-group 1 mode active S1(config-if-range)# interface port-channel 1 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk allowed vlan 1-5,10 S2(config)# interface range FastEthernet0/0 - 1 S2(config-if-range)# channel-group 1 mode active S2(config-if-range)# interface port-channel 1 S2(config-if)# switchport mode trunk S2(config-if)# switchport trunk allowed vlan 1,5,10

Refer to the exhibit. An EtherChannel was configured between switches S1 and S2, but the interfaces do not form an EtherChannel. What is the problem?

The EtherChannel was not configured with the same allowed range of VLANs on each interface.

The switch ports were not configured with speed and duplex mode.

The switch ports have to be configured as access ports with each port having a VLAN assigned.​

The interface port-channel number has to be different on each switch.

The guidelines for configuring an EtherChannel link are:

Interfaces which form an EtherChannel can be physically discontiguous, and on different modules.

Interfaces in an EtherChannel have to operate at the same speed and in the same duplex mode.

Interfaces in the EtherChannel must be assigned to the same VLAN, or be configured as a trunk.

Interfaces in the EtherChannel have to support the same allowed range of VLANs.

Question 21

Which technology is an open protocol standard that allows switches to automatically bundle physical ports into a single logical link?

LACP

LACP, or Link Aggregation Control Protocol, is defined by IEEE 802.3ad and is an open standard protocol. LACP allows switches to automatically bundle switch ports into a single logical link to increase bandwidth. PAgP, or Port Aggregation Protocol, performs a similar function, but it is a Cisco proprietary protocol. DTP is Dynamic Trunking Protocol and is used to automatically and dynamically build trunks between switches. Multilink PPP is used to load-balance PPP traffic across multiple serial interfaces.

Question 22

Two switches, SW1 and SW2, are interconnected with two cables. SW1 Gi0/1 connects to SW2 Gi0/1 and SW1 Gi0/2 connects to SW2 Gi0/2. There are two boxes showing the configuration commands. Box 1 shows the following information: SW1(config)# interface gigabitEthernet 0/1 SW1(config-if)# switchport mode trunk SW1(config-if)# channel-group 1 mode on SW1(config-if)# exit SW1(config)# interface gigabitEthernet 0/2 SW1(config-if)# switchport mode trunk SW1(config-if)# channel-group 1 mode on SW1(config-if)# exit SW2(config)# interface port-channel 1 SW1(config-if)# switchport mode trunk SW1(config-if)# end Box 2 shows the following information: SW2(config)# interface gigabitEthernet 0/1 SW2(config-if)# switchport mode trunk SW2(config-if)# channel-group 1 mode desirable SW2(config-if)# exit SW2(config)# interface gigabitEthernet 0/2 SW2(config-if)# switchport mode trunk SW2(config-if)# channel-group 1 mode desirable SW2(config-if)# exit SW2(config)# interface port-channel 1 SW2(config-if)# switchport mode trunk SW2(config-if)# end

Refer to the exhibit. A network administrator is configuring an EtherChannel link between two switches, SW1 and SW2. Which statement describes the effect after the commands are issued on SW1 and SW2?

The EtherChannel fails to establish.

The interfaces GigabitEthernet 0/1 and GigabitEthernet 0/2 are configured "on" for the EtherChannel link. This mode forces the interface to channel without PAgP or LACP. The EtherChannel will be established only if the other side is also set to "on". However, the mode on SW2 side is set to PAgP desirable. Thus the EtherChannel link will not be established.

Question 23

The following words appear in the graphic: S\_ATC\_1.1# show etherchannel summary Flags: D - down P - in port-channel I - stand-alone s - suspended H - Hot-standby (LACP only) R - Layer3 S - Layer2 U - in use f - failed to allocate aggregator u - unsuitable for bundling w - waiting to be aggregated d - default port Number of channel-groups in use: 1 Number of aggregators: 1 Group Port-channel Protocol Ports ------+-------------+-----------+--------------------- 1 Po1(SU) PAgP Fa0/1(P) Fa0/2(P)

Refer to the exhibit. On the basis of the output that is shown, what can be determined about the EtherChannel bundle?

A Cisco proprietary protocol was used to negotiate the EtherChannel link.

Two protocols can be used to send negotiation frames that are used to try to establish an EtherChannel link: PAgP and LACP. PAgP is Cisco proprietary, and LACP adheres to the industry standard.

Question 24

Which two channel group modes would place an interface in a negotiating state using PAgP? (Choose two.)

auto

desirable

There are three modes available when configuring an interface for PAgP: on, desirable, and auto. Only desirable and auto place the interface in a negotiating state. The active and passive states are used to configure LACP and not PAgP.

Question 25

The exhibit displays the following command and some output from the command: S1# show etherchannel summary Flags: D - down P - in port-channel I - stand-alone s - suspended H - Hot-standby (LACP only) R - Layer3 S - Layer2 U - in use f - failed to allocate aggregator u - unsuitable for bundling w - waiting to be aggregated d - default port Number of channel-groups in use: 1 Number of aggregators: 1 Group Port-channel Protocol Ports ------+-------------+-----------+---------------------------------------------- 1 Po1(SD) PAgP Fa0/1(I) Fa0/2(I) Fa0/3(I)

Refer to the exhibit. A network administrator issued the show etherchannel summary command on the switch S1. What conclusion can be drawn?

The EtherChannel is not functional.

The EtherChannel status shows as (SD), which means it is a Layer 2 EtherChannel with a status of D or down. Because the EtherChannel is down, the status of the interfaces in the channel group is stand-alone. PAgP is configured on S1, but there is no indication whether it is configured correctly on S1. The problem might also be the adjacent switch EtherChannel configuration.

Question 26

Two switches, SW1 and SW2, are interconnected with two cables. SW1 Gi0/1 connects to SW2 Gi0/1 and SW1 Gi0/2 connects to SW2 Gi0/2. There are two boxes showing the configuration commands. Box 1 shows the following information: SW1# show running-config <output omitted> interface GigabitEthernet0/1 channel-group 1 mode auto switchport mode trunk ! interface GigabitEthernet0/2 channel-group 1 mode auto switchport mode trunk ! interface Port-channel 1 switchport mode trunk Box 2 shows the following information: SW2# show running-config <output omitted> interface GigabitEthernet0/1 channel-group 1 mode active switchport mode trunk ! interface GigabitEthernet0/2 channel-group 1 mode active switchport mode trunk ! interface Port-channel 1 switchport mode trunk

Refer to the exhibit. A network administrator is configuring an EtherChannel link between two switches, SW1 and SW2. However, the EtherChannel link fails to establish. What change in configuration would correct the problem?

Configure SW2 EtherChannel mode to desirable.

The EtherChannel mode must be compatible on each side for the link to work. The three modes from PAgP protocol are on, desirable, and auto. The three modes from LACP protocol are on, active, and passive. The compatible modes include on-on, auto-desirable, desirable-desirable, active-passive, and active-active. Any other combinations will not form an EtherChannel link.

Question 27

Which statement describes a characteristic of EtherChannel?

It is made by combining multiple physical links that are seen as one link between two switches.

An EtherChannel is formed by combining multiple (same type) Ethernet physical links so they are seen and configured as one logical link. It provides an aggregated link between two switches. Currently each EtherChannel can consist of up to eight compatibly configured Ethernet ports.

Question 28

When EtherChannel is configured, which mode will force an interface into a port channel without exchanging aggregation protocol packets?

on

For both LACP and PAgP, the "on" mode will force an interface into an EtherChannel without exchanging protocol packets.

Question 29

A network administrator is configuring an EtherChannel link between switches SW1 and SW2 by using the command SW1(config-if-range)# channel-group 1 mode auto. Which command must be used on SW2 to enable this EtherChannel?

SW2(config-if-range)# channel-group 1 mode desirable

The possible combinations to establish an EtherChannel between SW1 and SW2 using LACP or PAgP are as follows:

PAgP

on on

auto desirable

desirable desirable

LACP

on on

active active

passive active

The EtherChannel mode chosen on each side of the EtherChannel must be compatible in order to enable it.

Question 30

What is a requirement to configure a trunking EtherChannel between two switches?

The allowed range of VLANs must be the same on both switches.

To enable a trunking EtherChannel successfully, the range of VLANs allowed on all the interfaces must match; otherwise, the EtherChannel cannot be formed. The interfaces involved in an EtherChannel do not have to be physically contiguous, or on the same module. Because the EtherChannel is a trunking one, participating interfaces are configured as trunk mode, not access mode.

Question 31

Which mode configuration setting would allow formation of an EtherChannel link between switches SW1 and SW2 without sending negotiation traffic?

SW1: on

SW2: on

Trunking enabled on both switches

The auto channel-group keyword enables PAgP only if a PAgP device is detected on the opposite side of the link. If the auto keyword is used, the only way to form an EtherChannel link is if the opposite connected device is configured with the desirable keyword. PortFast and trunking technologies are irrelevant to forming an EtherChannel link. Even though an EtherChannel can be formed if both sides are configured in desirable mode, PAgP is active and PAgP messages are being sent constantly across the link, decreasing the amount of bandwidth available for user traffic.

Question 32

A switch is configured to run STP. What term describes the switch port closest, in terms of overall cost, to the root bridge?

root port

**7.0 DHCPv4**

7.1.1 DHCPv4 Server and Client

Dynamic Host Configuration Protocol v4 (DHCPv4) assigns IPv4 addresses and other network configuration information dynamically.

A dedicated DHCPv4 server is scalable and relatively easy to manage. However, in a small branch or SOHO location, a Cisco router can be configured to provide DHCPv4 services without the need for a dedicated server. Cisco IOS software supports an optional, full-featured DHCPv4 server.

The DHCPv4 server dynamically assigns, or leases, an IPv4 address from a pool of addresses for a limited period of time chosen by the server, or until the client no longer needs the address.

Clients lease the information from the server for an administratively defined period. Administrators configure DHCPv4 servers to set the leases to time out at different intervals. The lease is typically anywhere from 24 hours to a week or more. When the lease expires, the client must ask for another address, although the client is typically reassigned the same address.

7.1.2 DHCPv4 Operation

DHCPv4 works in a client/server mode. When a client communicates with a DHCPv4 server, the server assigns or leases an IPv4 address to that client. The client connects to the network with that leased IPv4 address until the lease expires. The client must contact the DHCP server periodically to extend the lease. This lease mechanism ensures that clients that move or power off do not keep addresses that they no longer need. When a lease expires, the DHCP server returns the address to the pool where it can be reallocated as necessary.

7.1.3 Steps to Obtain a Lease

When the client boots (or otherwise wants to join a network), it begins a four-step process to obtain a lease:

1. DHCP Discover (DHCPDISCOVER) - The client starts the process using a broadcast DHCPDISCOVER message with its own MAC address to discover available DHCPv4 servers. Because the client has no valid IPv4 information at bootup, it uses Layer 2 and Layer 3 broadcast addresses to communicate with the server. The purpose of the DHCPDISCOVER message is to find DHCPv4 servers on the network.
2. DHCP Offer (DHCPOFFER) - When the DHCPv4 server receives a DHCPDISCOVER message, it reserves an available IPv4 address to lease to the client. The server also creates an ARP entry consisting of the MAC address of the requesting client and the leased IPv4 address of the client. The DHCPv4 server sends the binding DHCPOFFER message to the requesting client.
3. DHCP Request (DHCPREQUEST) - When the client receives the DHCPOFFER from the server, it sends back a DHCPREQUEST message. This message is used for both lease origination and lease renewal. When used for lease origination, the DHCPREQUEST serves as a binding acceptance notice to the selected server for the parameters it has offered and an implicit decline to any other servers that may have provided the client a binding offer.

Many enterprise networks use multiple DHCPv4 servers. The DHCPREQUEST message is sent in the form of a broadcast to inform this DHCPv4 server and any other DHCPv4 servers about the accepted offer.

1. DHCP Acknowledgment (DHCPACK) - On receiving the DHCPREQUEST message, the server may verify the lease information with an ICMP ping to that address to ensure it is not being used already, it will create a new ARP entry for the client lease, and reply with a DHCPACK message. The DHCPACK message is a duplicate of the DHCPOFFER, except for a change in the message type field. When the client receives the DHCPACK message, it logs the configuration information and may perform an ARP lookup for the assigned address. If there is no reply to the ARP, the client knows that the IPv4 address is valid and starts using it as its own.

7.1.4 Steps to Renew a Lease

Prior to lease expiration, the client begins a two-step process to renew the lease with the DHCPv4 server, as shown in the figure:

1. DHCP Request (DHCPREQUEST)

Before the lease expires, the client sends a DHCPREQUEST message directly to the DHCPv4 server that originally offered the IPv4 address. If a DHCPACK is not received within a specified amount of time, the client broadcasts another DHCPREQUEST so that one of the other DHCPv4 servers can extend the lease.

2. DHCP Acknowledgment (DHCPACK)

On receiving the DHCPREQUEST message, the server verifies the lease information by returning a DHCPACK.

Note: These messages (primarily the DHCPOFFER and DHCPACK) can be sent as unicast or broadcast according to IETF RFC 2131.

7.2 Configure a Cisco IOS DHCPv4 Server

7.2.1 Cisco IOS DHCPv4 Server

A Cisco router running Cisco IOS software can be configured to act as a DHCPv4 server. The Cisco IOS DHCPv4 server assigns and manages IPv4 addresses from specified address pools within the router to DHCPv4 clients.

7.2.2 Steps to Configure a Cisco IOS DHCPv4 Server

Use the following steps to configure a Cisco IOS DHCPv4 server:

* Step 1. Exclude IPv4 addresses.

The router functioning as the DHCPv4 server assigns all IPv4 addresses in a DHCPv4 address pool unless it is configured to exclude specific addresses. Typically, some IPv4 addresses in a pool are assigned to network devices that require static address assignments. Therefore, these IPv4 addresses should not be assigned to other devices. The command syntax to exclude IPv4 addresses is the following:

Router(config)# ip dhcp excluded-address low-address [high-address]

A single address or a range of addresses can be excluded by specifying the low-address and high-address of the range. Excluded addresses should be those addresses that are assigned to routers, servers, printers, and other devices that have been, or will be, manually configured. You can also enter the command multiple times.

* Step 2. Define a DHCPv4 pool name.

Configuring a DHCPv4 server involves defining a pool of addresses to assign.

Router(config)# ip dhcp pool pool-name

* Step 3. Configure the DHCPv4 pool.

The table lists the tasks to complete the DHCPv4 pool configuration.

The address pool and default gateway router must be configured. Use the network statement to define the range of available addresses. Use the default-router command to define the default gateway router. Typically, the gateway is the LAN interface of the router closest to the client devices. One gateway is required, but you can list up to eight addresses if there are multiple gateways.



The example shows the configuration to make R1 a DHCPv4 server for the 192.168.10.0/24 LAN.

R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9

R1(config)# ip dhcp excluded-address 192.168.10.254

R1(config)# ip dhcp pool LAN-POOL-1

R1(dhcp-config)# network 192.168.10.0 255.255.255.0

R1(dhcp-config)# default-router 192.168.10.1

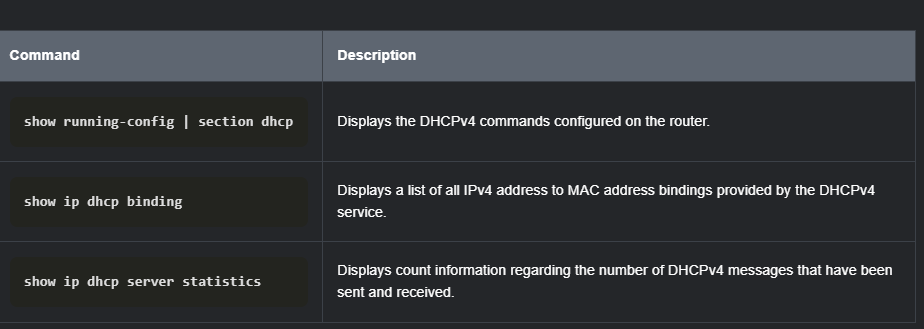
R1(dhcp-config)# dns-server 192.168.11.5

R1(dhcp-config)# domain-name example.com

R1(dhcp-config)# end

7.2.4 DHCPv4 Verification Commands

Use the commands in the table to verify that the Cisco IOS DHCPv4 server is operational.



7.2.7 Disable the Cisco IOS DHCPv4 Server

The DHCPv4 service is enabled by default. To disable the service, use the no service dhcp global configuration mode command. Use the service dhcp global configuration mode command to re-enable the DHCPv4 server process.

7.2.5 Verify DHCPv4 is Operational

Verify the DHCPv4 Configuration

As shown in the example, the show running-config | section dhcp command output displays the DHCPv4 commands configured on R1. The | section parameter displays only the commands associated with DHCPv4 configuration.

R1# show running-config | section dhcp

ip dhcp excluded-address 192.168.10.1 192.168.10.9

ip dhcp excluded-address 192.168.10.254

ip dhcp pool LAN-POOL-1

network 192.168.10.0 255.255.255.0

default-router 192.168.10.1

dns-server 192.168.11.5

domain-name example.com

Verify DHCPv4 Bindings

As shown in the example, the operation of DHCPv4 can be verified using the show ip dhcp binding command. This command displays a list of all IPv4 address to MAC address bindings that have been provided by the DHCPv4 service.

R1# show ip dhcp binding

Bindings from all pools not associated with VRF:

IP address Client-ID/ Lease expiration Type State Interface

Hardware address/

User name

192.168.10.10 0100.5056.b3ed.d8 Sep 15 2019 8:42 AM Automatic Active GigabitEthernet0/0/0

Verify DHCPv4 Statistics

The output of the show ip dhcp server statistics is used to verify that messages are being received or sent by the router. This command displays count information regarding the number of DHCPv4 messages that have been sent and received.

R1# show ip dhcp server statistics

Verify DHCPv4 Client Received IPv4 Addressing

The ipconfig /all command, when issued on PC1, displays the TCP/IP parameters, as shown in the example. Because PC1 was connected to the network segment 192.168.10.0/24, it automatically received a DNS suffix, IPv4 address, subnet mask, default gateway, and DNS server address from that pool. No DHCP-specific router interface configuration is required. If a PC is connected to a network segment that has a DHCPv4 pool available, the PC can obtain an IPv4 address from the appropriate pool automatically.

C:\Users\Student> ipconfig /all

Windows IP Configuration

Host Name . . . . . . . . . . . . : ciscolab

Primary Dns Suffix . . . . . . . :

Node Type . . . . . . . . . . . . : Hybrid

IP Routing Enabled. . . . . . . . : No

WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : example.com

Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller

Physical Address. . . . . . . . . : 00-05-9A-3C-7A-00

DHCP Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

IPv4 Address. . . . . . . . . . . : 192.168.10.10

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Lease Obtained . . . . . . . . . : Saturday, September 14, 2019 8:42:22AM

Lease Expires . . . . . . . . . : Sunday, September 15, 2019 8:42:22AM

Default Gateway . . . . . . . . . : 192.168.10.1

DHCP Server . . . . . . . .. . . : 192.168.10.1

DNS Servers . . . . . . . .. . . : 192.168.11.5

7.2.8 DHCPv4 Relay

In a complex hierarchical network, enterprise servers are usually located centrally. These servers may provide DHCP, DNS, TFTP, and FTP services for the network. Network clients are not typically on the same subnet as those servers. In order to locate the servers and receive services, clients often use broadcast messages.

In the figure, PC1 is attempting to acquire an IPv4 address from a DHCPv4 server using a broadcast message. In this scenario, R1 is not configured as a DHCPv4 server and does not forward the broadcast. Because the DHCPv4 server is located on a different network, PC1 cannot receive an IP address using DHCP. R1 must be configured to relay DHCPv4 messages to the DHCPv4 server.

ip helper-address

A better solution is to configure R1 with the ip helper-address address interface configuration command. This will cause R1 to relay DHCPv4 broadcasts to the DHCPv4 server. As shown in the example, the interface on R1 receiving the broadcast from PC1 is configured to relay DHCPv4 address to the DHCPv4 server at 192.168.11.6.

R1(config)# interface g0/0/0

R1(config-if)# ip helper-address 192.168.11.6

R1(config-if)# end

R1#

show ip interface

When R1 has been configured as a DHCPv4 relay agent, it accepts broadcast requests for the DHCPv4 service and then forwards those requests as a unicast to the IPv4 address 192.168.11.6. The network administrator can use the show ip interface command to verify the configuration.

R1# show ip interface g0/0/0

GigabitEthernet0/0/0 is up, line protocol is up

Internet address is 192.168.10.1/24

Broadcast address is 255.255.255.255

Address determined by setup command

MTU is 1500 bytes

Helper address is 192.168.11.6

(output omitted)

7.2.9 Other Service Broadcasts Relayed

DHCPv4 is not the only service that the router can be configured to relay. By default, the ip helper-address command forwards the following eight UDP services:

* Port 37: Time
* Port 49: TACACS
* Port 53: DNS
* Port 67: DHCP/BOOTP server
* Port 68: DHCP/BOOTP client
* Port 69: TFTP
* Port 137: NetBIOS name service
* Port 138: NetBIOS datagram service

7.3.1 Cisco Router as a DHCPv4 Client

There are scenarios where you might have access to a DHCP server through your ISP. In these instances, you can configure a Cisco IOS router as a DHCPv4 client.

Sometimes, Cisco routers in a small office or home office (SOHO) and branch sites have to be configured as DHCPv4 clients in a similar manner to client computers. The method used depends on the ISP. However, in its simplest configuration, the Ethernet interface is used to connect to a cable or DSL modem.

To configure an Ethernet interface as a DHCP client, use the ip address dhcp interface configuration mode command.

7.3.2 Configuration Example

To configure an Ethernet interface as a DHCP client, use the ip address dhcp interface configuration mode command. This configuration assumes that the ISP has been configured to provide select customers with IPv4 addressing information.

SOHO(config)# interface G0/0/1

SOHO(config-if)# ip address dhcp

SOHO(config-if)# no shutdown

Sep 12 10:01:25.773: %DHCP-6-ADDRESS\_ASSIGN: Interface GigabitEthernet0/0/1 assigned DHCP address 209.165.201.12, mask 255.255.255.224, hostname SOHO

The show ip interface g0/0/1 command confirms that the interface is up and that the address was allocated by a DHCPv4 server.

SOHO# show ip interface g0/0/1

GigabitEthernet0/0/1 is up, line protocol is up

Internet address is 209.165.201.12/27

Broadcast address is 255.255.255.255

Address determined by DHCP

7.4.4 Module Quiz - DHCPv4

Question 1

A DHCP-enabled client PC has just booted. During which two steps will the client PC use broadcast messages when communicating with a DHCP server? (Choose two.)

DHCPDISCOVER

DHCPREQUEST

Topic 7.1.0 - All DHCP messages between a DHCP-enabled client and a DHCP server are using broadcast messages until after the DHCPACK message. The DHCPDISCOVER and DHCPREQUEST messages are the only messages that are sent by a DHCP-enabled client. All DHCP messages between a DHCP-enabled client and a DHCP server use broadcast messages when the client is obtaining a lease for the first time.

Question 2

An administrator issues the commands:

Router(config)# interface g0/1

Router(config-if)# ip address dhcp

What is the administrator trying to achieve?

Configuring the router to obtain IP parameters from a DHCPv4 server

Topic 7.3.0 - The ip address dhcp command activates the DHCPv4 client on a given interface. By doing this, the router will obtain the IP parameters from a DHCPv4 server.

Question 3

When a client is requesting an initial address lease from a DHCP server, why is the DHCPREQUEST message sent as a broadcast?

The client may have received offers from multiple servers, and the broadcast serves to implicitly decline those other offers.

Topic 7.1.0 - During the initial DHCP exchange between a client and server, the client broadcasts a DHCPDISCOVER message looking for DHCP servers. Multiple servers may be configured to respond to this request with DHCPOFFER messages. The client will choose the lease from one of the servers by sending a DHCPREQUEST message. It sends this message as a broadcast so that the other DHCP servers that sent offers will know that their offers were declined and the corresponding address can go back into the pool.

Question 4

Which DHCP IPv4 message contains the following information?

Destination address: 255.255.255.255

Client IPv4 address: 0.0.0.0

Default gateway address: 0.0.0.0

Subnet mask: 0.0.0.0

DHCPDISCOVER

Topic 7.1.0 - A client will first send the DHCPDISCOVER broadcast message to find DHCPv4 servers on the network. This message will have the limited broadcast address, 255.255.255.255, as the destination address. The client IPv4 address, the default gateway address, and subnet fields will all be 0.0.0.0 because these have not yet been configured on the client. When the DHCPv4 server receives a DHCPDISCOVER message, it reserves an available IPv4 address to lease to the client and sends the unicast DHCPOFFER message to the requesting client. When the client receives the DHCPOFFER from the server, it sends back a DHCPREQUEST broadcast message. On receiving the DHCPREQUEST message, the server replies with a unicast DHCPACK message.

Question 5

What kind of message is sent by a DHCPv4 client requesting an IP address?

DHCPDISCOVER broadcast message

Topic 7.1.0 - When the DHCPv4 client requests an IP address, it sends a DHCPDISCOVER broadcast message seeking a DHCPv4 server on the network.

Question 6

As a DHCPv4 client lease is about to expire, what is the message that the client sends the DHCP server?

DHCPREQUEST

Topic 7.1.0 - When a DHCP client lease is about to expire, the client sends a DHCPREQUEST message to the DHCPv4 server that originally provided the IPv4 address.​ This allows the client to request that the lease be extended.​

Question 7

What is the destination IP address when an IPv4 host sends a DHCPDISCOVER message?

255.255.255.255

Topic 7.1.0 - Because a DHCP client does not have a valid IPv4 address, it must use a broadcast IP address of 255.255.255.255 as the destination address to communicate with the DHCP server. The DHCPDISCOVER message sent by the client is the first message sent in order to make initial contact with a DHCP server.

Question 8

If more than one DHCP server is available on the local network, in which order will DHCP messages be sent between a host and a DHCP server?

Discover, offer, request, acknowledgment

Topic 7.1.0 - A DHCP host broadcasts a DHCP discover message to locate available servers. If more than one DHCP server is available, each server will respond to the host with a unicast DHCP offer message, which offers a lease to the client. The client then broadcasts a DHCP request message that identifies the specific server and offer that the client will accept. The identified server will unicast a DHCP acknowledgment message to finalize the offer.

Question 9

What is the most likely scenario in which the WAN interface of a router would be configured as a DHCP client to be assigned a dynamic IP address from an ISP?

It is a SOHO or home broadband router.

Topic 7.3.0 - SOHO and home broadband routers are typically set to acquire an IPv4 address automatically from the ISP. The IP address that is assigned is typically a dynamic address to reduce the cost, but a static IP address is possible with more cost. However, if the router is assigned a dynamic IP address, DNS issues will result in the web server behind the router not being easily accessible to the public. Routers are typically also gateways for LANs, but this has no bearing on whether the router is configured as a DHCP client on its WAN link or not. Likewise, a router can be configured to be a DHCP client in order to obtain an IP address from the ISP, but at the same time, it can be configured as a DHCP server to serve the IP addressing for the devices on its LAN.

Question 10

Which is a DHCPv4 address allocation method that assigns IPv4 addresses for a limited lease period?

Dynamic allocation

Topic 7.1.0 - Dynamic allocation is the most commonly implemented allocation mechanism. It leases the IP parameters for a predefined period of time.

Question 11

What is the reason why the DHCPREQUEST message is sent as a broadcast during the DHCPv4 process?

To notify other DHCP servers on the subnet that the IP address was leased

Topic 7.1.0 - The DHCPREQUEST message is broadcast to inform other DHCP servers that an IP address has been leased.

Question 12

How is a DHCPDISCOVER transmitted on a network to reach a DHCP server?

A DHCPDISCOVER message is sent with the broadcast IP address as the destination address.

Topic 7.1.0 - The DHCPDISCOVER message is sent by a DHCPv4 client and targets a broadcast IP along with the destination port 67. The DHCPv4 server or servers respond to the DHCPv4 clients by targeting port 68.

Question 13

Which destination IPv4 address does a DHCPv4 client use to send the initial DHCP Discover packet when the client is looking for a DHCP server?

255.255.255.255

Topic 7.1.0 - Broadcast communications on a network may be directed or limited. A directed broadcast is sent to all hosts on a specific network. A limited broadcast is sent to 255.255.255.255. When a DHCP client needs to send a DHCP Discover packet in order to seek DHCP servers, the client will use this IP address of 255.255.255.255 as the destination in the IP header because it has no knowledge of the IP addresses of DHCP servers.

Question 14

Under which two circumstances would a router usually be configured as a DHCPv4 client? (Choose two.)

The router is intended to be used as a SOHO gateway.

This is an ISP requirement.

Topic 7.3.0 - SOHO routers are frequently required by the ISP to be configured as DHCPv4 clients in order to be connected to the provider.

Question 15

Which address does a DHCPv4 server target when sending a DHCPOFFER message to a client that makes an address request?

Client hardware address

Topic 7.1.0 - When a DHCPv4 client does not have an IPv4 address, a DHCPv4 server will send a DHCPOFFER message back to the client hardware address of the requesting DHCPv4 client.

**8.0 SLAAC AND DHCPv6**

8.1 IPv6 GUA Assignment

8.1.1 IPv6 Host Configuration

On a router, an IPv6 global unicast address (GUA) is manually configured using the ipv6 address ipv6-address/prefix-length interface configuration command.

Manually entering an IPv6 GUA can be time consuming and somewhat error prone. Therefore, most Windows host are enabled to dynamically acquire an IPv6 GUA configuration

8.1.2 IPv6 Host Link-Local Address

When automatic IPv6 addressing is selected, the host will attempt to automatically obtain and configure IPv6 address information on the interface. The host will use one of three methods defined by the Internet Control Message Protocol version 6 (ICMPv6) Router Advertisement (RA) message received on the interface.

An IPv6 router that is on the same link as the host sends out RA messages that suggest to the hosts how to obtain their IPv6 addressing information. The IPv6 link-local address is automatically created by the host when it boots and the Ethernet interface is active.

**Dynamic GUA Assignment**

**Stateless** - No device is tracking the assignment of IPv6 addresses.

**Stateful** - A DHCPv6 server is managing the assignment of IPv6 addresses.

**SLAAC Only**

* Router sends Router Advertisement (RA) messages providing all IPv6 addressing information (i.e., network prefix, prefix-length, and default gateway information).
* Hosts use the RA information exclusively for all their addressing including creating their own GUA.

**SLAAC with DHCP server**  
**(Stateless DHCPv6)**

* Router RA messages provide IPv6 configuration information to hosts and inform them to contact a stateless DHCPv6 server for additional configuration information.
* Hosts use the RA information to create their own unique GUA and get additional information from a DHCPv6 server.

**DHCPv6 Server**  
**(Stateful DHCPv6)**

* Router RA messages inform hosts to contact a stateful DHCPv6 server or DHCPv6-enabled router for all IPv6 configuration information, except the default gateway address.
* Hosts contact a DHCPv6 server to acquire all of their IPv6 addressing information.
* Host obtains default gateway information from router RA messages.

8.1.4 Three RA Message Flags

The decision of how a client will obtain an IPv6 GUA depends on the settings within the RA message.

An ICMPv6 RA message includes three flags to identify the dynamic options available to a host, as follows:

* A flag - This is the Address Autoconfiguration flag. Use Stateless Address Autoconfiguration (SLAAC) to create an IPv6 GUA.
* O flag - This is the Other Configuration flag. Other information is available from a stateless DHCPv6 server.
* M flag - This is the Managed Address Configuration flag. Use a stateful DHCPv6 server to obtain an IPv6 GUA.

Using different combinations of the A, O and M flags, RA messages inform the host about the dynamic options available.

8.2 SLAAC

Not every network has or needs access to a DHCPv6 server. But every device in an IPv6 network needs a GUA. The SLAAC method enables hosts to create their own unique IPv6 global unicast address without the services of a DHCPv6 server.

SLAAC is a stateless service. This means there is no server that maintains network address information to know which IPv6 addresses are being used and which ones are available.

SLAAC uses ICMPv6 RA messages to provide addressing and other configuration information that would normally be provided by a DHCP server. A host configures its IPv6 address based on the information that is sent in the RA. RA messages are sent by an IPv6 router every 200 seconds.

8.2.2 Enabling SLAAC

The output of the show ipv6 interface command displays the current settings on the G0/0/1 interface. – To verify IPv6 address

To enable the sending of RA messages, a router must join the IPv6 all-routers group using the ipv6 unicast-routing global config command, as show in the output.

R1(config)# ipv6 unicast-routing

The IPv6 all-routers group responds to the IPv6 multicast address ff02::2. You can use the show ipv6 interface command to verify if a router is enabled as shown, in the output.

An IPv6-enabled Cisco router sends RA messages to the IPv6 all-nodes multicast address ff02::1 every 200 seconds.

R1# show ipv6 interface G0/0/1 | section Joined

Joined group address(es):

FF02::1

FF02::2

FF02::1:FF00:1

8.2.3 SLAAC Only Method

The SLAAC only method is enabled by default when the ipv6 unicast-routing command is configured. All enabled Ethernet interfaces with an IPv6 GUA configured will start sending RA messages with the A flag set to 1, and the O and M flags set to 0,

The A = 1 flag suggests to the client that it create its own IPv6 GUA using the prefix advertised in the RA. The client can create its own Interface ID using either Extended Unique Identifier method (EUI-64) or have it randomly generated.

The O =0 and M=0 flags instruct the client to use the information in the RA message exclusively. The RA includes the prefix, prefix-length, DNS server, MTU, and default gateway information. There is no further information available from a DHCPv6 server.

8.2.4 ICMPv6 RS Messages

A router sends RA messages every 200 seconds. However, it will also send an RA message if it receives an RS message from a host.

When a client is configured to obtain its addressing information automatically, it sends an RS message to the IPv6 all-routers multicast address of **ff02::2**.

8.2.5 Host Process to Generate Interface ID

Using SLAAC, a host typically acquires its 64-bit IPv6 subnet information from the router RA. However, it must generate the remainder 64-bit interface identifier (ID) using one of two methods:

* Randomly generated - The 64-bit interface ID is randomly generated by the client operating system. This is the method now used by Windows 10 hosts.
* EUI-64 - The host creates an interface ID using its 48-bit MAC address. The host inserts the hex value of fffe in the middle of the address, and flips the seventh bit of the interface ID. This changes the value of the second hexadecimal digit of the interface ID. Some operating systems default to the randomly generated interface ID instead of the EUI-64 method, due to privacy concerns. This is because the Ethernet MAC address of the host is used by EUI-64 to create the interface ID.

**Note**: Windows, Linux, and Mac OS allow for the user to modify the generation of the interface ID to be either randomly generated or to use EUI-64.

8.2.6 Duplicate Address Detection

The process enables the host to create an IPv6 address. However, there is no guarantee that the address is unique on the network.

SLAAC is a stateless process; therefore, a host has the option to verify that a newly created IPv6 address is unique before it can be used. The Duplicate Address Detection (DAD) process is used by a host to ensure that the IPv6 GUA is unique.

DAD is implemented using ICMPv6. To perform DAD, the host sends an ICMPv6 Neighbor Solicitation (NS) message with a specially constructed multicast address, called a solicited-node multicast address. This address duplicates the last 24 bits of IPv6 address of the host.

If no other devices respond with a NA message, then the address is virtually guaranteed to be unique and can be used by the host. If an NA is received by the host, then the address is not unique, and the operating system has to determine a new interface ID to use.

The Internet Engineering Task Force (IETF) recommends that DAD is used on all IPv6 unicast addresses regardless of whether it is created using SLAAC only, obtained using stateful DHCPv6, or manually configured. DAD is not mandatory because a 64-bit interface ID provides 18 quintillion possibilities and the chance that there is a duplication is remote. However, most operating systems perform DAD on all IPv6 unicast addresses, regardless of how the address is configured.

8.3 DHCPv6

The steps for DHCPv6 operations are as follows:

* The host sends an RS message.
* The router responds with an RA message.
* The host sends a DHCPv6 SOLICIT message.
* The DHCPv6 server responds with an ADVERTISE message.
* The host responds to the DHCPv6 server.
* The DHCPv6 server sends a REPLY message.

8.3.2 Stateless DHCPv6 Operation

The stateless DHCPv6 server is only providing information that is identical for all devices on the network such as the IPv6 address of a DNS server.

This process is known as stateless DHCPv6 because the server is not maintaining any client state information (i.e., a list of available and allocated IPv6 addresses). The stateless DHCPv6 server is only providing configuration parameters for clients, not IPv6 addresses.

8.3.3 Enable Stateless DHCPv6 on an Interface

Stateless DHCPv6 is enabled on a router interface using the ipv6 nd other-config-flag interface configuration command. This sets the O flag to 1.

Note: You can use the no ipv6 nd other-config-flag to reset the interface to the default SLAAC only option (O flag = 0).

8.3.4 Stateful DHCPv6 Operation

This option is most similar to DHCPv4. In this case, the RA message tells the client to obtain all addressing information from a stateful DHCPv6 server, except the default gateway address which is the source IPv6 link-local address of the RA.

This is known as stateful DHCPv6 because the DHCPv6 server maintains IPv6 state information. This is similar to a DHCPv4 server allocating addresses for IPv4.

Note: If A=1 and M=1, some operating systems such as Windows will create an IPv6 address using SLAAC and obtain a different address from the stateful DHCPv6 server. In most cases it is recommended to manually set the A flag to 0.

8.3.5 Enable Stateful DHCPv6 on an Interface

Stateful DHCPv6 is enabled on a router interface using the ipv6 nd managed-config-flag interface configuration command. This sets the M flag to 1. The ipv6 nd prefix default no-autoconfig interface command disables SLAAC by setting the A flag to 0.

R1(config)# int g0/0/1

R1(config-if)# ipv6 nd managed-config-flag

R1(config-if)# ipv6 nd prefix default no-autoconfig

R1(config-if)# end

R1#

R1# show ipv6 interface g0/0/1 | begin ND

QUIZ

Question 1

What destination UDP port do DHCPv6 clients use to send DHCPv6 messages?

67

68

**547**

546

Question 2

What DHCPv6 message does a host send to look for a DHCPv6 server?

ADVERTISE

**SOLICIT**

INFORMATION-REQUEST

REQUEST

Question 3

What DHCPv6 message does a host send to the DHCPv6 server if it is using stateful DHCPv6?

ADVERTISE

SOLICIT

INFORMATION-REQUEST

**REQUEST**

Question 4

What flag settings combination is used for stateless DHCP?

A=1, M=0, O=0

A=0, M=1, O=0

**A=1, M=0, O=1**

A=0, M=1, O=1

Question 5

What M flag setting indicates that stateful DHCPv6 is used?

M=0

**M=1**

8.4 Configure DHCPv6 Server

8.4.1 DHCPv6 Router Roles

Cisco IOS routers are powerful devices. In smaller networks, you do not have to have separate devices to have a DHCPv6 server, client, or relay agent. A Cisco IOS router can be configured to provide DHCPv6 server services.

Specifically, it can be configured to be one of the following:

DHCPv6 Server - Router provides stateless or stateful DHCPv6 services.

DHCPv6 Client - Router interface acquires an IPv6 IP configuration from a DHCPv6 server.

DHCPv6 Relay Agent - Router provides DHCPv6 forwarding services when the client and the server are located on different networks.

8.4.2 Configure a Stateless DHCPv6 Server

The stateless DHCPv6 server option requires that the router advertise the IPv6 network addressing information in RA messages. However, the client must contact a DHCPv6 server for more information.

There are five steps to configure and verify a router as a stateless DHCPv6 server:

Step 1. Enable IPv6 routing.

R1(config)# ipv6 unicast-routing

R1(config)#

Step 2. Define a DHCPv6 pool name.

R1(config)# ipv6 dhcp pool IPV6-STATELESS

R1(config-dhcpv6)#

Step 3. Configure the DHCPv6 pool.

R1(config-dhcpv6)# dns-server 2001:db8:acad:1::254

R1(config-dhcpv6)# domain-name example.com

R1(config-dhcpv6)# exit

R1(config)#

Step 4. Bind the DHCPv6 pool to an interface.

R1(config)# interface GigabitEthernet0/0/1

R1(config-if)# description Link to LAN

R1(config-if)# ipv6 address fe80::1 link-local

R1(config-if)# ipv6 address 2001:db8:acad:1::1/64

R1(config-if)# ipv6 nd other-config-flag

R1(config-if)# ipv6 dhcp server IPV6-STATELESS

R1(config-if)# no shut

R1(config-if)# end

R1#

Step 5. Verify that the hosts have received IPv6 addressing information.

To verify stateless DHCP on a Windows host, use the ipconfig /all command. The example output displays the settings on PC1.

Notice in the output that PC1 created its IPv6 GUA using the 2001:db8:acad:1::/64 prefix. Also notice that the default gateway is the IPv6 link-local address of R1. This confirms that PC1 derived its IPv6 configuration from the RA of R1.

The highlighted output confirms that PC1 has learned the domain name and DNS server address information from the stateless DHCPv6 server.

8.4.3 Configure a Stateless DHCPv6 Client

A router can also be a DHCPv6 client and get an IPv6 configuration from a DHCPv6 server, such as a router functioning as a DHCPv6 server

There are five steps to configure and verify a router as a stateless DHCPv6 client.

Step 1. Enable IPv6 routing.

R3(config)# ipv6 unicast-routing

R3(config)#

Step 2. Configure the client router to create an LLA.

The client router needs to have a link-local address. An IPv6 link-local address is created on a router interface when a global unicast address is configured. It can also be created without a GUA using the ipv6 enable interface configuration command. Cisco IOS uses EUI-64 to create a randomized Interface ID.

In the output, the ipv6 enable command is configured on the Gigabit Ethernet 0/0/1 interface of the R3 client router.

R3(config)# interface g0/0/1

R3(config-if)# ipv6 enable

R3(config-if)#

Step 3. Configure the client router to use SLAAC.

The client router needs to be configured to use SLAAC to create an IPv6 configuration. The ipv6 address autoconfig command enables the automatic configuration of IPv6 addressing using SLAAC.

R3(config-if)# ipv6 address autoconfig

R3(config-if)# end

R3#

Step 4. Verify that the client router is assigned a GUA.

Use the show ipv6 interface brief command to verify the host configuration as shown. The output confirms that the G0/0/1 interface on R3 was assigned a valid GUA.

Step 5. Verify that the client router received other necessary DHCPv6 information.

The show ipv6 dhcp interface g0/0/1 command confirms that the DNS and domain names were also learned by R3.

8.4.4 Configure a Stateful DHCPv6 Server

The stateful DHCP server option requires that the IPv6 enabled router tells the host to contact a DHCPv6 server to obtain all necessary IPv6 network addressing information.

There are five steps to configure and verify a router as a stateful DHCPv6 server:

Step 1. Enable IPv6 routing.

The ipv6 unicast-routing command is required to enable IPv6 routing.

R1(config)# ipv6 unicast-routing

R1(config)#

Step 2. Define a DHCPv6 pool name.

Create the DHCPv6 pool using the ipv6 dhcp pool POOL-NAME global config command.

R1(config)# ipv6 dhcp pool IPV6-STATEFUL

R1(config-dhcpv6)#

Step 3. Configure the DHCPv6 pool.

R1 will be configured to provide IPv6 addressing, DNS server address, and domain name, as shown in the command output. With stateful DHCPv6, all addressing and other configuration parameters must be assigned by the DHCPv6 server. The address prefix command is used to indicate the pool of addresses to be allocated by the server. Other information provided by the stateful DHCPv6 server typically includes DNS server address and the domain name, as shown in the output.

Note: This example is setting the DNS server to Google's public DNS server.

R1(config-dhcpv6)# address prefix 2001:db8:acad:1::/64

R1(config-dhcpv6)# dns-server 2001:4860:4860::8888

R1(config-dhcpv6)# domain-name example.com

R1(config-dhcpv6)#

Step 4. Bind the DHCPv6 pool to an interface.

The example shows the full configuration of the GigabitEthernet 0/0/1 interface on R1.

The DHCPv6 pool has to be bound to the interface using the ipv6 dhcp server POOL-NAME interface config command.

The M flag is manually changed from 0 to 1 using the interface command ipv6 nd managed-config-flag.

The A flag is manually changed from 1 to 0 using the interface command ipv6 nd prefix default no-autoconfig. The A flag can be left at 1, but some client operating systems such as Windows will create a GUA using SLAAC and get a GUA from the stateful DHCPv6 server. Setting the A flag to 0 tells the client not to use SLAAC to create a GUA.

The ipv6 dhcp server command binds the DHCPv6 pool to the interface. R1 will now respond with the information contained in the pool when it receives stateful DHCPv6 requests on this interface.

Note: You can use the no ipv6 nd managed-config-flag command to set the M flag back to its default of 0. The no ipv6 nd prefix default no-autoconfig command sets the A flag back to its default of 1.

R1(config)# interface GigabitEthernet0/0/1

R1(config-if)# description Link to LAN

R1(config-if)# ipv6 address fe80::1 link-local

R1(config-if)# ipv6 address 2001:db8:acad:1::1/64

R1(config-if)# ipv6 nd managed-config-flag

R1(config-if)# ipv6 nd prefix default no-autoconfig

R1(config-if)# ipv6 dhcp server IPV6-STATEFUL

R1(config-if)# no shut

R1(config-if)# end

R1#

Step 5. Verify that the hosts have received IPv6 addressing information.

To verify on a Windows host, use the ipconfig /all command to verify the stateless DHCP configuration method. The output displays the settings on PC1

8.4.5 Configure a Stateful DHCPv6 Client

A router can also be a DHCPv6 client. The client router needs to have ipv6 unicast-routing enabled and an IPv6 link-local address to send and receive IPv6 messages.

There are five steps to configure and verify a router as a stateful DHCPv6 client.

Step 1. Enable IPv6 routing.

The DHCPv6 client router needs to have ipv6 unicast-routing enabled.

R3(config)# ipv6 unicast-routing

R3(config)#

Step 2. Configure the client router to create an LLA.

In the output, the ipv6 enable command is configured on the R3 Gigabit Ethernet 0/0/1 interface. This enables the router to create an IPv6 LLA without needing a GUA.

R3(config)# interface g0/0/1

R3(config-if)# ipv6 enable

R3(config-if)#

Step 3. Configure the client router to use DHCPv6.

The ipv6 address dhcp command configures R3 to solicit its IPv6 addressing information from a DHCPv6 server.

R3(config-if)# ipv6 address dhcp

R3(config-if)# end

R3#

Step 4. Verify that the client router is assigned a GUA.

Use the show ipv6 interface brief command to verify the host configuration as shown.

R3# show ipv6 interface brief

GigabitEthernet0/0/0 [up/up]

unassigned

GigabitEthernet0/0/1 [up/up]

FE80::2FC:BAFF:FE94:29B1

2001:DB8:ACAD:1:B4CB:25FA:3C9:747C

Serial0/1/0 [up/up]

unassigned

Serial0/1/1 [up/up]

unassigned

R3#

Step 5. Verify that the client router received other necessary DHCPv6 information.

The show ipv6 dhcp interface g0/0/1 command confirms that the DNS and domain names were learned by R3.

R3# show ipv6 dhcp interface g0/0/1

GigabitEthernet0/0/1 is in client mode

Prefix State is IDLE

Address State is OPEN

Renew for address will be sent in 11:56:33

List of known servers:

Reachable via address: FE80::1

DUID: 000300017079B3923640

Preference: 0

Configuration parameters:

IA NA: IA ID 0x00060001, T1 43200, T2 69120

Address: 2001:DB8:ACAD:1:B4CB:25FA:3C9:747C/128

preferred lifetime 86400, valid lifetime 172800

expires at Sep 29 2019 11:52 AM (172593 seconds)

DNS server: 2001:4860:4860::8888

Domain name: example.com

Information refresh time: 0

Prefix Rapid-Commit: disabled

Address Rapid-Commit: disabled

R3#

8.4.6 DHCPv6 Server Verification Commands

The show ipv6 dhcp pool command verifies the name of the DHCPv6 pool and its parameters. The command also identifies the number of active clients. In this example, the IPV6-STATEFUL pool currently has 2 clients, which reflects PC1 and R3 receiving their IPv6 global unicast address from this server.

When a router is providing stateful DHCPv6 services, it also maintains a database of assigned IPv6 addresses.

R1# show ipv6 dhcp pool

DHCPv6 pool: IPV6-STATEFUL

Address allocation prefix: 2001:DB8:ACAD:1::/64 valid 172800 preferred 86400 (2 in use, 0 conflicts)

DNS server: 2001:4860:4860::8888

Domain name: example.com

Active clients: 2

R1#

Use the show ipv6 dhcp binding command output to display the IPv6 link-local address of the client and the global unicast address assigned by the server.

The output displays the current stateful binding on R1. The first client in the output is PC1 and the second client is R3.

This information is maintained by a stateful DHCPv6 server. A stateless DHCPv6 server would not maintain this information.

R1# show ipv6 dhcp binding

Client: FE80::192F:6FBC:9DB:B749

DUID: 0001000125148183005056B327D6

Username : unassigned

VRF : default

IA NA: IA ID 0x03000C29, T1 43200, T2 69120

Address: 2001:DB8:ACAD:1:A43C:FD28:9D79:9E42

preferred lifetime 86400, valid lifetime 172800

expires at Sep 27 2019 09:10 AM (171192 seconds)

Client: FE80::2FC:BAFF:FE94:29B1

DUID: 0003000100FCBA9429B0

Username : unassigned

VRF : default

IA NA: IA ID 0x00060001, T1 43200, T2 69120

Address: 2001:DB8:ACAD:1:B4CB:25FA:3C9:747C

preferred lifetime 86400, valid lifetime 172800

expires at Sep 27 2019 09:29 AM (172339 seconds)

8.4.7 Configure a DHCPv6 Relay Agent

If the DHCPv6 server is located on a different network than the client, then the IPv6 router can be configured as a DHCPv6 relay agent. The configuration of a DHCPv6 relay agent is similar to the configuration of an IPv4 router as a DHCPv4 relay.

The command syntax to configure a router as a DHCPv6 relay agent is as follows:

Router(config-if)# ipv6 dhcp relay destination ipv6-address [interface-type interface-number]

8.4.8 Verify the DHCPv6 Relay Agent

Verify that the DHCPv6 relay agent is operational with the show ipv6 dhcp interface and show ipv6 dhcp binding commands. Verify Windows hosts received IPv6 addressing information with the ipconfig /all command.

QUIZ

Question 1

Which three DHCPv6 roles can a router perform? (Choose all that apply.)

**DHCPv6 client**

**DHCPv6 relay agent**

**DHCPv6 server**

Question 2

Which command is not configured in stateless DHCPv6?

**address prefix ipv6-address/prefix**

Question 3

An IPv6-enabled router is to acquire its IPv6 GUA from another IPv6 router using SLAAC. Which interface configuration command should be configured on the client router?

**ipv6 address autoconfig**

Question 4

A router is to provide DHCPv6 server services. Which command should be configured on the client facing interface?

**ipv6 dhcp server POOL-NAME**

Question 5

An IPv6-enabled router is to acquire its IPv6 GUA from a DHCPv6 server. Which interface configuration command should be configured on client router?

**ipv6 address dhcp**

Question 6

Which DHCPv6 verification command would display the link-local and GUA assigned address for each active client?

**show ipv6 dhcp binding**

Question 7

Which command is configured on the client LAN interface of the DHCPv6 relay agent?

**ipv6 dhcp relay destination**

8.5.3 Module Quiz - SLAAC and DHCPv6

Question 1

How does an IPv6 client ensure that it has a unique address after it configures its IPv6 address using the SLAAC allocation method?

It sends an ICMPv6 Neighbor Solicitation message with the IPv6 address as the target IPv6 address.

Topic 8.2.0 - SLAAC is a stateless allocation method and does not use a DHCP server to manage the IPv6 addresses. When a host generates an IPv6 address, it must verify that it is unique. The host will send an ICMPv6 Neighbor Solicitation message with its own IPv6 address as the target. As long as no other device responds with a Neighbor Advertisement message, then the address is unique.

Question 2

Which method would an IPv6-enabled host using SLAAC employ to learn the address of the default gateway?

Router advertisements that are received from the link router

Topic 8.2.0 - When using SLAAC, a host will learn from the router advertisement that is sent by the link router the address to use as a default gateway.

Question 3

What two methods can be used to generate an interface ID by an IPv6 host that is using SLAAC? (Choose two.)

EUI-64

Random generation

Topic 8.2.0 - A host that is using SLAAC has two means to configure an interface ID: EUI-64 and random generation by the host operating system.

Question 4

A client is using SLAAC to obtain an IPv6 address for its interface. After an address has been generated and applied to the interface, what must the client do before it can begin to use this IPv6 address?

It must send an ICMPv6 Neighbor Solicitation message to ensure that the address is not already in use on the network.

Topic 8.3.0 - Stateless DHCPv6 or stateful DHCPv6 uses a DHCP server, but Stateless Address Autoconfiguration (SLAAC) does not. A SLAAC client can automatically generate an address that is based on information from local routers via Router Advertisement (RA) messages. Once an address has been assigned to an interface via SLAAC, the client must ensure via Duplicate Address Detection (DAD) that the address is not already in use. It does this by sending out an ICMPv6 Neighbor Solicitation message and listening for a response. If a response is received, then it means that another device is already using this address.

Question 5

Which command should be configured on a router interface to set the router as a stateful DHCPv6 client?

ipv6 address dhcp

Topic 8.4.0 - When the ipv6 address dhcp command is configured on a router interface, it enables the router as a DHCPv6 client on this interface. The ipv6 enable command enables IPv6 on an interface and allows the router to configure its link-local address. The ipv6 address autoconfigure command tells the router to use either SLAAC or stateless DHCPv6 to configure its global unicast address. The ipv6 dhcp server command is used on a router that is running a DHCPv6 server to indicate what address information should be served to clients.

Question 6

What message informs IPv6 enabled interfaces to use stateful DHCPv6 for obtaining an IPv6 address?

The ICMPv6 Router Advertisement

Topic 8.2.0 - Before an IPv6 enabled interface will use stateful DHCPv6 to obtain an IPv6 address, the interface must receive an ICMPv6 Router Advertisement with the managed configuration flag (M flag) set to 1

Question 7

Which destination IP address is used when an IPv6 host sends a DHCPv6 SOLICIT message to locate a DHCPv6 server?

FF02::2

Topic 8.3.0 - DHCPv6 hosts will send a DHCP SOLICIT message to the all DHCP routers multicast address of FF02::2.

Question 8

In which alternative to DHCPv6 does a router dynamically provide IPv6 configuration information to hosts?

SLAAC

Topic 8.2.0 - Stateless Address Autoconfiguration (SLAAC) can be used as an alternative to DHCPv6. In this approach, a router provides global routing prefix, prefix length, default gateway, and DNS server information to a host. The host is not provided with a global unicast address by SLAAC. Instead, SLAAC suggests that the host create its own global unicast address based on the supplied global routing prefix. ARP is not used in IPv6. ICMPv6 messages are used by SLAAC to provide addressing and other configuration information. EUI-64 is a process in which a host will create an Interface ID from its 48-bit MAC address.

Question 9

A company implements the stateless DHCPv6 method for configuring IPv6 addresses on employee workstations. After a workstation receives messages from multiple DHCPv6 servers to indicate their availability for DHCPv6 service, which message does it send to a server for configuration information?

DHCPv6 INFORMATION-REQUEST

Topic 8.3.0 - In stateless DHCPv6 configuration, a client configures its IPv6 address by using the prefix and prefix length in the RA message, combined with a self-generated interface ID. It then contacts a DHCPv6 server for additional configuration information via an INFORMATION-REQUEST message. The DHCPv6 SOLICIT message is used by a client to locate a DHCPv6 server. The DHCPv6 ADVERTISE message is used by DHCPv6 servers to indicate their availability for DHCPv6 service. The DHCPv6 REQUEST message is used by a client, in the stateful DHCPv6 configuration, to request ALL configuration information from a DHCPv6 server.

Question 10

What process is used in ICMPv6 for a host to verify that an IPv6 address is unique before configuring it on an interface?

DAD

Topic 8.2.0 - Before an IPv6 host can enable and use an assigned IPv6 address, the host must verify that the address is unique on the network. To verify that no other hosts are using the IPv6 address, the host performs the duplicate address detection (DAD) process by sending a Neighbor Solicitation (NS) message to the IPv6 address.

Question 11

What are two characteristics of the SLAAC method for IPv6 address configuration? (Choose two.)

The default gateway of an IPv6 client on a LAN will be the link-local address of the router interface attached to the LAN.

IPv6 addressing is dynamically assigned to clients through the use of ICMPv6.

Topic 8.2.0 - With SLAAC, the default gateway for IPv6 clients will be the link-local address of the router interface that is attached to the client LAN. The IPv6 addressing is dynamically assigned via the ICMPv6 protocol. SLAAC is a stateless method of acquiring an IPv6 address, a method that requires no servers. When a client is configured to obtain its addressing information automatically via SLAAC, the client sends a router solicitation message to the IPv6 all-routers multicast address FF02::2. The router advertisement messages are sent by routers to provide addressing information to clients.

Question 12

After booting, a client receives an ICMPv6 RA message with the M flag set to 0 and the O flag set to 1. What does this indicate?

The client should automatically configure an IPv6 address and then contact a DHCPv6 server for more information.

Topic 8.3.0 - The Managed Address Configuration (M) flag and the Other Configuration (O) flag in ICMPv6 RA messages are used to indicate to an IPv6 client how it should configure its IPv6 addresses. If the M flag is set to 0 it means that the host should automatically configure its own IPv6 interface address rather than asking for one from a DHCPv6 server. If the O flag is set to 1, it means that the client can find additional addressing information, such as a DNS server address, by contacting a DHCPv6 server after it has automatically configured its own address.

Question 13

A network administrator is entering the command ipv6 unicast-routing to start configuring DHCPv6 operation on a router. Which statement describes the function of this command?

It is required for sending ICMPv6 RA messages.

Topic 8.2.0 - The ipv6 unicast-routing command is required to enable IPv6 routing on a router. This command is not necessary for the router to be a stateless or stateful DHCPv6 server, but is required for sending ICMPv6 RA messages.

**9.0 FHRP (First Hop Redundancy Protocols)**

9.1.1 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. That mechanism is provided by first hop redundancy protocols (FHRPs).

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.

9.1.1 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. That mechanism is provided by first hop redundancy protocols (FHRPs).

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.

End devices are typically configured with a single IPv4 address for a default gateway. This address does not change when the network topology changes. If that default gateway IPv4 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.

Note: IPv6 devices receive their default gateway address dynamically from the ICMPv6 Router Advertisement. However, IPv6 devices benefit with a faster failover to the new default gateway when using FHRP.

9.1.2 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. 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.

9.1.3 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:

* The standby router stops seeing Hello messages from the forwarding router.
* The standby router assumes the role of the forwarding router.

Because the new forwarding router assumes both the IPv4 and MAC addresses of the virtual router, the host devices see no disruption in service.

9.1.4 FHRP Options

The FHRP used in a production environment largely depends on the equipment and needs of the network. The table lists all the options available for FHRPs.

9.1.5 Check Your Understanding - First Hop Redundancy Protocols

Question 1

What type of device routes traffic destined to network segments beyond the source network segment for which the sending node may not have explicit routing information?

Default gateway

Question 2

What device presents the illusion of a single router to hosts on a LAN segment but actually represents a set of routers working together?

Virtual router

Question 3

What device is part of a virtual router group assigned the role of alternate default gateway?

Standby router

Question 4

What device that is part of a virtual router group assigned to the role of default gateway?

Forwarding router

Question 5

Which FHRPs are Cisco-proprietary? (Choose two.)

HSRP

HSRP for IPv6

9.2 HSRP

9.2.1 HSRP Overview

Cisco provides HSRP and HSRP for IPv6 as a way to avoid losing outside network access if your default router fails.

HSRP is a Cisco-proprietary FHRP that is designed to allow for transparent failover of a first-hop IP device.

HSRP ensures high network availability by providing first-hop routing redundancy for IP hosts on networks configured with an IP 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.

9.2.2 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 to take place when a higher priority router comes online, 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.

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.

9.2.3 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 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.

9.2.4 Check Your Understanding - HSRP

Question 1

What is the default HSRP priority?

100

Question 2

True or False? If a router with a higher HSRP priority joins the network, it will take over the active router roll from an existing active router which has a lower priority.

False

Question 3

During which HSRP state does an interface begin sending periodic hello messages?

Speak

Question 4

Which is a characteristic of the HSRP learn state?

The router has not determined the virtual IP address

The FHRP used in a production environment largely depends on the equipment and needs of the network. These are the options available for FHRPs:

HSRP and HSRP for IPv6

VRRPv2 and VRRPv3

GLBP and GLBP for IPv6

IRDP

HSRP

9.3.2 Module Quiz - FHRP Concepts

Question 1

What is the purpose of HSRP?

It provides a continuous network connection when a router fails.

Topic 9.2.0 - HSRP is a first hop redundancy protocol and allows hosts to use multiple gateways through the use of a single virtual router.

Question 2

Which nonproprietary protocol provides router redundancy for a group of routers which support IPv4 LANs?

VRRPv2

Topic 9.1.0 - The only nonproprietary FHRP used for router redundancy listed in the options is VRRPv2. HSRP and GLBP are both Cisco proprietary FHRPs. IOS SLB is a Cisco-based solution used to load balance traffic across multiple servers.

Question 3

A network administrator is analyzing first-hop router redundancy protocols. What is a characteristic of VRRPv3?

It supports IPv6 and IPv4 addressing.

Topic 9.1.0 - VRRPv3 is a non-proprietary, first-hop router redundancy protocol. It provides features for both IPv4 and IPv6 addressing. HSRP and GLBP are both Cisco-proprietary protocols. GLBP provides load balancing between a group of redundant routers.

Question 4

What is a potential disadvantage when implementing HSRP as compared to GLBP?

HSRP does not provide load balancing with multiple active routers.

Topic 9.1.0 - HSRP is a first-hop redundancy protocol that can utilize a group of routers, where a single router is acting as the default gateway and all other HSRP routers will maintain a backup status. GLBP supports load balancing, where multiple active routers can share the traffic load at a single time. Both HSRP and GLBP are Cisco proprietary. HSRP provides default gateway failover when pre-set conditions are met or when the active router fails, and HSRP can support IPv6 addressing.

Question 5

A network engineer is configuring a LAN with a redundant first hop to make better use of the available network resources. Which protocol should the engineer implement?

GLBP

Topic 9.1.0 - Gateway Load Balancing Protocol (GLBP) provides load sharing between a group of redundant routers while also protecting data traffic from a failed router or circuit.

Question 6

When first hop redundancy protocols are used, which two items will be shared by a set of routers that are presenting the illusion of being a single router? (Choose two.)

IP address

MAC address

Topic 9.1.0 - In order for a set of routers to present the illusion of being a single router, they must share both an IP address and MAC address. A static route, BID, or hostname does not have to be shared in this context.

Question 7

In FHRP terminology, what represents a set of routers that present the illusion of a single router to hosts?

Virtual router

Topic 9.1.0 - In FHRP multiple routers are configured to work together to present to hosts a single gateway router. This single gateway router is a virtual router which has a virtual IP address that is used by hosts as a default gateway.

Question 8

A user needs to add redundancy to the routers in a company. What are the three options the user can use? (Choose three.)

HSRP

VRRP

GLBP

Topic 9.1.0 - Three protocols that provide default gateway redundancy include VRRP, GLBP, and HSRP.

Question 9

Which two protocols provide gateway redundancy at Layer 3? (Choose two.)

VRRP

HSRP

Topic 9.1.0 - HSRP (Hot Standby Routing Protocol) and VRRP (Virtual Router Redundancy Protocol) are both Layer 3 redundancy protocols. Both protocols allow multiple physical routers to act as a single virtual gateway router for hosts.

Question 10

A network administrator is overseeing the implementation of first hop redundancy protocols. Which two protocols are Cisco proprietary? (Choose two.)

HSRP

GLBP

Topic 9.1.0 - The first hop redundancy protocols HSRP and GLBP are Cisco proprietary and will not function in a multivendor environment.

Question 11

Which statement describes a characteristic of GLBP?

It provides automatic rerouting if any router in the group fails.

Topic 9.1.0 - GLBP provides support for IPv6. It provides one virtual IP address and multiple virtual MAC addresses, and there is no such limit of four gateways to provide load balancing.

Question 12

A network administrator is analyzing the features that are supported by different first-hop router redundancy protocols. Which statement is a feature that is associated with GLBP?

GLBP allows load balancing between routers.

Topic 9.1.0 - The GLBP first-hop router redundancy protocol is Ciscoproprietary and supports load balancing between a group of redundant routers. VRRPv2 and VRRPv3 are nonproprietary protocols and use a virtual router master.

Checkpoint Exam:

Question 1

After a host has generated an IPv6 address by using the DHCPv6 or SLAAC process, how does the host verify that the address is unique and therefore usable?

The host sends an ICMPv6 neighbor solicitation message to the DHCP or SLAAC-learned address and if no neighbor advertisement is returned, the address is considered unique.

Before a host can actually configure and use an IPv6 address learned through SLAAC or DHCP, the host must verify that no other host is already using that address. To verify that the address is indeed unique, the host sends an ICMPv6 neighbor solicitation to the address. If no neighbor advertisement is returned, the host considers the address to be unique and configures it on the interface.

Question 2

Match the DHCP message types to the order of the DHCPv4 process.

Step 1 – DHCPDISCOVER - A message that is used to locate any available DHCP server on a network.

Step 2 – DHCPOFFER - A message that is used to suggest a lease to a client

Step 3 – DHCPREQUEST - A message that is used to identify the explicit server and lease offer to accept.

Step 4 – DHCPACK - A message that is used to acknowledge that the lease is successful.

Question 3

Which statement describes HSRP?​

It is used within a group of routers for selecting an active device and a standby device to provide gateway services to a LAN.

It is VRRP that elects one router as the virtual router master, with the other routers acting as backups in case the virtual router master fails. HSRP is a Cisco-proprietary protocol. IRDP uses ICMP messages to allow IPv4 hosts to locate routers that provide IPv4 connectivity to other (nonlocal) IP networks. HSRP selects active and standby routers to provide gateway services to hosts on a LAN.

Question 5

A host PC is attempting to lease an address through DHCP. What message is sent by the server to let the client know it is able to use the provided IP information?

DHCPACK

When a host uses DHCP to automatically configure an IP address, the typically sends two messages: the DHCPDISCOVER message and the DHCPREQUEST message. These two messages are usually sent as broadcasts to ensure that all DHCP servers receive them. The servers respond to these messages using DHCPOFFER, DHCPACK, and DHCPNACK messages, depending on the circumstance.

Question 7

What is one indication that a Windows computer did not receive an IPv4 address from a DHCP server?

The computer receives an IP address that starts with 169.254.

When a Windows PC cannot communicate with an IPv4 DHCP server, the computer automatically assigns an IP address in the 169.254.0.0/16 range. Any other device on the same network that receives an address in the same range is reachable.​

Question 8

What is the reason that an ISP commonly assigns a DHCP address to a wireless router in a SOHO environment?

easy IP address management

In a SOHO environment, a wireless router connects to the ISP via a DSL or cable modem. The IP address between the wireless router and ISP site is typically assigned by the ISP through DHCP. This method facilitates the IP addressing management in that IP addresses for clients are dynamically assigned so that if a client is dropped, the assigned IP address can be easily reassigned to another client.

Question 9

Which set of commands will configure a router as a DHCP server that will assign IPv4 addresses to the 192.168.100.0/23 LAN while reserving the first 10 and the last addresses for static assignment?

ip dhcp excluded-address 192.168.100.1 192.168.100.10

ip dhcp excluded-address 192.168.101.254

ip dhcp pool LAN-POOL-100

network 192.168.100.0 255.255.254.0

default-router 192.168.100.1

The /23 prefix is equivalent to a network mask of 255.255.254.0. The network usable IPv4 address range is 192.168.100.1 to 192.168.101.254 inclusive.

Question 10

What is an advantage of configuring a Cisco router as a relay agent?

It can provide relay services for multiple UDP services.

By default, the ip helper-address command forwards the following eight UDP services:

Port 37: Time

Port 49: TACACS

Port 53: DNS

Port 67: DHCP/BOOTP client

Port 68: DHCP/BOOTP server

Port 69: TFTP

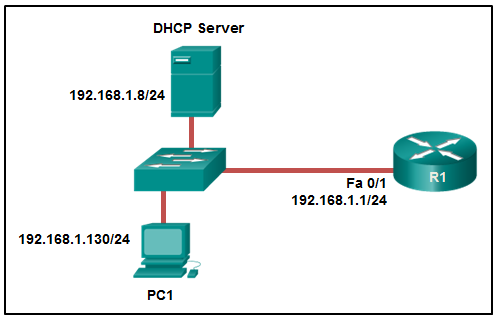
Port 137: NetBIOS name service

Port 138: NetBIOS datagram service

Question 11

Refer to the exhibit. PC1 is configured to obtain a dynamic IP address from the DHCP server. PC1 has been shut down for two weeks. When PC1 boots and tries to request an available IP address, which destination IP address will PC1 place in the IP header?

255.255.255.255



When a host boots and has been configured for dynamic IP addressing, the device tries to obtain a valid IP address. It sends a DHCPDISCOVER message. This is a broadcast message because the DHCP server address is unknown (by design). The destination IP address in the IP header is 255.255.255.255 and the destination MAC address is FF:FF:FF:FF:FF:FF.

Question 12

Which DHCPv4 message will a client send to accept an IPv4 address that is offered by a DHCP server?

broadcast DHCPREQUEST

When a DHCP client receives DHCPOFFER messages, it will send a broadcast DHCPREQUEST message for two purposes. First, it indicates to the offering DHCP server that it would like to accept the offer and bind the IP address. Second, it notifies any other responding DHCP servers that their offers are declined.

Question 13

What information can be verified through the show ip dhcp binding command?

the IPv4 addresses that are assigned to hosts by the DHCP server

The show ip dhcp binding command shows a list of IPv4 addresses and the MAC addresses of the hosts to which they are assigned. Using this information an administrator can determine which host interfaces have been assigned to specific hosts.

Question 15

Which command, when issued in the interface configuration mode of a router, enables the interface to acquire an IPv4 address automatically from an ISP, when that link to the ISP is enabled?

ip address dhcp

The ip address dhcp interface configuration command configures an Ethernet interface as a DHCP client. The service dhcp global configuration command enables the DHCPv4 server process on the router. The ip helper-address command is issued to enable DHCP relay on the router. The ip dhcp pool command creates the name of a pool of addresses that the server can assign to hosts.

Question 16

Which statement is true about DHCP operation?​

When a device that is configured to use DHCP boots, the client broadcasts a DHCPDISCOVER message to identify any available DHCP servers on the network.​

The client broadcasts a DHCPDISCOVER message to identify any available DHCP servers on the network. A DHCP server replies with a DHCPOFFER message. This message offers to the client a lease that contains such information as the IP address and subnet mask to be assigned, the IP address of the DNS server, and the IP address of the default gateway. After the client receives the lease, the received information must be renewed through another DHCPREQUEST message prior to the lease expiration.

Question 17

Which message does an IPv4 host use to reply when it receives a DHCPOFFER message from a DHCP server?

DHCPREQUEST

When the client receives the DHCPOFFER from the server, it sends back a DHCPREQUEST broadcast message. On receiving the DHCPREQUEST message, the server replies with a unicast DHCPACK message.

Question 18

Which kind of message is sent by a DHCP client when its IP address lease has expired?​

a DHCPREQUEST unicast message​

When the IP address lease time of the DHCP client expires, it sends a DHCPREQUEST unicast message directly to the DHCPv4 server that originally offered the IPv4 address.

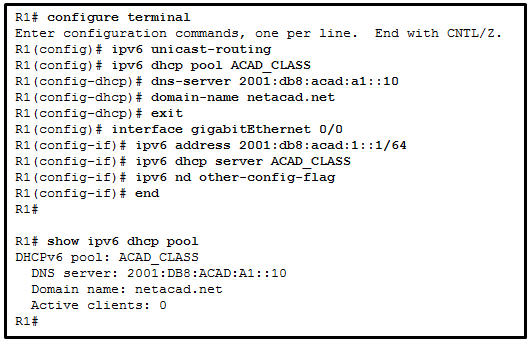
Question 19

Which command will allow a network administrator to check the IP address that is assigned to a particular MAC address?

Router# show ip dhcp binding

The show ip dhcp binding command will show the leases, including IP addresses, MAC addresses, lease expiration, type of lease, client ID, and user name.

Question 20

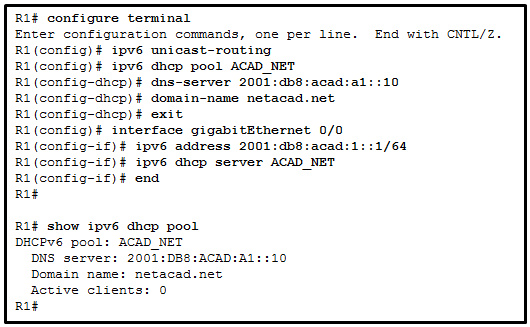


Refer to the exhibit. A network administrator is configuring a router as a DHCPv6 server. The administrator issues a show ipv6 dhcp pool command to verify the configuration. Which statement explains the reason that the number of active clients is 0?

The state is not maintained by the DHCPv6 server under stateless DHCPv6 operation.

Under the stateless DHCPv6 configuration, indicated by the command ipv6 nd other-config-flag, the DHCPv6 server does not maintain the state information, because client IPv6 addresses are not managed by the DHCP server. Because the clients will configure their IPv6 addresses by combining the prefix/prefix-length and a self-generated interface ID, the ipv6 dhcp pool configuration does not need to specify the valid IPv6 address range. And because clients will use the link-local address of the router interface as the default gateway address, the default gateway address is not necessary.

Question 21



Refer to the exhibit. A network administrator is implementing the stateless DHCPv6 operation for the company. Clients are configuring IPv6 addresses as expected. However, the clients are not getting the DNS server address and the domain name information configured in the DHCP pool. What could be the cause of the problem?

The router is configured for SLAAC operation.

The router is configured for SLAAC operation because there is no configuration command to change the RAM and O flag value. By default, both M and O flags are set to 0. In order to permint stateless DHCPv6 operation, the interface command ipv6 nd other-config-flag should be issued. The GigabitEthernet interface is in working condition because clients can get RA messages and configure their IPv6 addresses as expected. Also, the fact that R1 is the DHCPv6 server and clients are getting RA messages indicates that clients can communicate with the DHCP server. The number of active clients is 0 because the DHCPv6 server does not maintain the state of clients IPv6 addresses (it is not configured for stateful DHCPv6 operation). The DNS server address issue is not relevant to the problem.

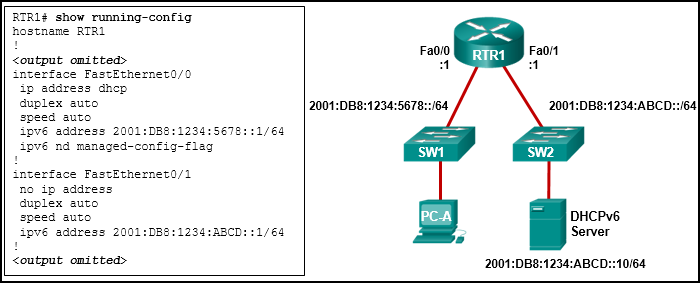
Question 22

A network administrator configures a router to send RA messages with M flag as 0 and O flag as 1. Which statement describes the effect of this configuration when a PC tries to configure its IPv6 address?

It should use the information that is contained in the RA message and contact a DHCPv6 server for additional information.

ICMPv6 RA messages contain two flags to indicate whether a workstation should use SLAAC, a DHCPv6 server, or a combination to configure its IPv6 address. These two flags are M flag and O flag. When both flags are 0 (by default), a client must only use the information in the RA message. When M flag is 0 and O flag is 1, a client should use the information in the RA message and look for the other configuration parameters (such as DNS server addresses) on DHCPv6 servers.

Question 23



Refer to the exhibit. What should be done to allow PC-A to receive an IPv6 address from the DHCPv6 server?

Add the ipv6 dhcp relay command to interface Fa0/0.

Client DHCPv6 messages are sent to a multicast address with link-local scope, which means that the messages will not be forwarded by routers. Because the client and server are on different subnets on different interfaces, the message will not reach the server. The router can be configured to relay the DHCPv6 messages from the client to the server by configuring the ipv6 dhcp relay command on the interface that is connected to the client.

Question 24

Match the DHCP message types to the order of the stateful DHCPv6 process when a client first connects to an IPv6 network.

Step 1 - DHCPv6 SOLICIT

Step 2 - DHCPv6 ADVERTISE

Step 3 - DHCPv6 REQUEST

Step 4 – DHCPv6 REPLY

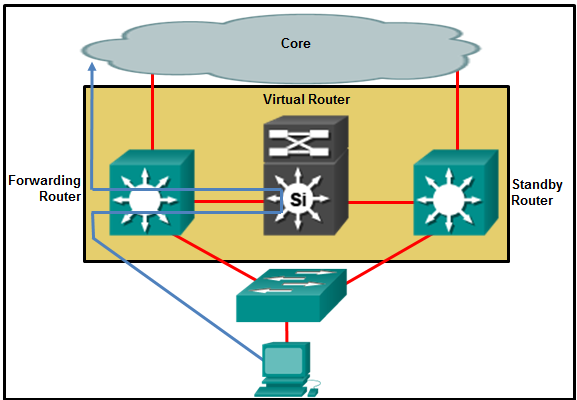
Question 25

A company uses the SLAAC method to configure IPv6 addresses for the employee workstations. Which address will a client use as its default gateway?​

the link-local address of the router interface that is attached to the network

When a PC is configured to use the SLAAC method for configuring IPv6 addresses, it will use the prefix and prefix-length information that is contained in the RA message, combined with a 64-bit interface ID (obtained by using the EUI-64 process or by using a random number that is generated by the client operating system), to form an IPv6 address. It uses the link-local address of the router interface that is attached to the LAN segment as its IPv6 default gateway address.

Question 26

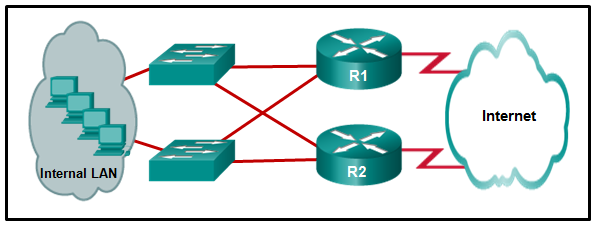


Refer to the exhibit. Which destination MAC address is used when frames are sent from the workstation to the default gateway?

MAC address of the virtual router

The IP address of the virtual router acts as the default gateway for all the workstations. Therefore, the MAC address that is returned by the Address Resolution Protocol to the workstation will be the MAC address of the virtual router.

Question 27



Refer to the exhibit. What protocol can be configured on gateway routers R1 and R2 that will allow traffic from the internal LAN to be load balanced across the two gateways to the Internet?

GLBP

GLBP, or Group Load Balancing Protocol, allows multiple routers to act as a single default gateway for hosts. GLBP load balances the traffic across the individual routers on a per host basis.

Question 28

Match the step number to the sequence of stages that occur during the HSRP failover process.

Step 1 - The forwarding router fails.

Step 2 - The standby router stops seeing hello messages from the forwarding router.

Step 3 - The standby router assumes the role of the forwarding router.

Step 4 - The new forwarding router assumes both the IP and MAC addresses of the virtual router.

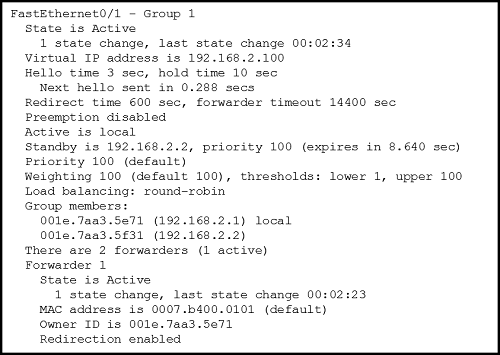
Question 29

A network administrator is analyzing the features that are supported by different first-hop router redundancy protocols. Which statement describes a feature that is associated with HSRP?

HSRP uses active and standby routers.

The HSRP first-hop router redundancy protocol is Cisco proprietary and supports standby and active devices. VRRPv2 and VRRPv3 are nonproprietary. GLBP is Cisco proprietary and supports load balancing between a group of redundant routers.

Question 30



Refer to the exhibit. A network engineer is troubleshooting host connectivity on a LAN that uses a first hop redundancy protocol. Which IPv4 gateway address should be configured on the host?

192.168.2.100

The host default gateway address should be the FHRP (in this case GLBP) virtual IP address.

Question 31

Match the FHRP protocols to the appropriate description.

HSRP - A Cisco proprietary FHRP that provides redundancy through use of an active device and standby device

VRRP - An open standard FHRP that provides redundancy through use of a virtual routers master and one or more backups

GLBP - A Cisco proprietary FHRP that provides load sharing in addition to redundancy

10.1 Endpoint Security

10.1.1 Network Attacks Today

Distributed Denial of Service (DDoS) - This is a coordinated attack from many devices, called zombies, with the intention of degrading or halting public access to an organization’s website and resources.

Data Breach - This is an attack in which an organization’s data servers or hosts are compromised to steal confidential information.

Malware - This is an attack in which an organization’s hosts are infected with malicious software that cause a variety of problems. For example, ransomware such as WannaCry, encrypts the data on a host and locks access to it until a ransom is paid.

10.1.2 Network Security Devices

Various network security devices are required to protect the network perimeter from outside access. These devices could include a virtual private network (VPN) enabled router, a next-generation firewall (NGFW), and a network access control (NAC) device.

* A VPN-enabled router provides a secure connection to remote users across a public network and into the enterprise network. VPN services can be integrated into the firewall.
* An NGFW provides stateful packet inspection, application visibility and control, a next-generation intrusion prevention system (NGIPS), advanced malware protection (AMP), and URL filtering.
* A NAC device includes authentication, authorization, and accounting (AAA) services. In larger enterprises, these services might be incorporated into an appliance that can manage access policies across a wide variety of users and device types. The Cisco Identity Services Engine (ISE) is an example of a NAC device.

10.1.3 Endpoint Protection

* Endpoints are hosts which commonly consist of laptops, desktops, servers, and IP phones, as well as employee-owned devices that are typically referred to as bring your own devices (BYODs).
* Endpoints are particularly susceptible to malware-related attacks that originate through email or web browsing. These endpoints have typically used traditional host-based security features, such as antivirus/antimalware, host-based firewalls, and host-based intrusion prevention systems (HIPSs).
* However, today endpoints are best protected by a combination of
  + NAC
  + host-based AMP software
  + an email security appliance (ESA)
  + a web security appliance (WSA).
  + Advanced Malware Protection (AMP) products include endpoint solutions such as Cisco AMP for Endpoints.

10.1.4 Cisco Email Security Appliance

The Cisco ESA is a device that is designed to monitor Simple Mail Transfer Protocol (SMTP). The Cisco ESA is constantly updated by real-time feeds from the Cisco Talos, which detects and correlates threats and solutions by using a worldwide database monitoring system. This threat intelligence data is pulled by the Cisco ESA every three to five minutes. These are some of the functions of the Cisco ESA:

Block known threats.

* Remediate against stealth malware that evaded initial detection.
* Discard emails with bad links (as shown in the figure).
* Block access to newly infected sites.
* Encrypt content in outgoing email to prevent data loss.

10.1.5 Cisco Web Security Appliance

The Cisco Web Security Appliance (WSA) is a mitigation technology for web-based threats. It helps organizations address the challenges of securing and controlling web traffic. The Cisco WSA combines advanced malware protection, application visibility and control, acceptable use policy controls, and reporting.

Cisco WSA provides complete control over how users access the internet. Certain features and applications, such as chat, messaging, video and audio, can be allowed, restricted with time and bandwidth limits, or blocked, according to the organization’s requirements. The WSA can perform blacklisting of URLs, URL-filtering, malware scanning, URL categorization, Web application filtering, and encryption and decryption of web traffic.

10.2 Access Control

10.2.1 Authentication with a Local Password

Many types of authentication can be performed on networking devices, and each method offers varying levels of security. The simplest method of remote access authentication is to configure a login and password combination on console, vty lines, and aux ports. This method is the easiest to implement, but it is also the weakest and least secure. This method provides no accountability and the password is sent in plaintext. Anyone with the password can gain entry to the device.

* R1(config)# line vty 0 4
* R1(config-line)# password ci5c0
* R1(config-line)# login

SSH is a more secure form of remote access:

It requires a username and a password, both of which are encrypted during transmission.

The username and password can be authenticated by the local database method.

It provides more accountability because the username is recorded when a user logs in.

The following example illustrates SSH and local database methods of remote access.

* R1(config)# ip domain-name example.com
* R1(config)# crypto key generate rsa general-keys modulus 2048
* R1(config)# username Admin secret Str0ng3rPa55w0rd
* R1(config)# ip ssh version 2
* R1(config)# line vty 0 4
* R1(config-line)# transport input ssh
* R1(config-line)# login local

The local database can be difficult to manage in a large enterprise

The local database also provides fallback authentication method. For example the admin forgets the password and username for the device.

The best solution is to have all the devices refer to the same database of usernames and passwords from a central server.

10.2.2.2 AAA Components

* Authentication – who is permitted to access
* Authorization – what they can do while they are there
* Accounting – audit actions they performed while accessing the network

10.2.3 Authentication

* Local and server-based are two common methods of implementing AAA authentication.
* Local AAA stores usernames and passwords locally in a network device such as the Cisco router.
* With server-based method, the router accesses a central AAA server. The server contains all the usernames and passwords for all users. The router uses either the Remote Authentication Dial-In User Service (RADIUS) or the Terminal Access Control Systsem (TACACS +) protocols to communicate with a AAA server.

10.2.4 Authorization

* It governs what the user can and cannot do on the network after the authentication
* It uses a set of attributes that describes the user’s access to the network. These attributes are used by the AAA server to determine privileges and restrictions for that user.

10.2.5 Accounting

* It collects and reports usage data.
* The data can be used for auditing or billing.
* Data can be start and stop connection times, executed commands, number of packets, and number of bytes.

10.2.6 802.1X

* The IEEE 802.1X standard is a port-based process control and authentication protocol.
* It 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.
* Client (Supplicant) – The device running 802.1X-compliant client software.
* Switch or wireless access point (Authenticator) – an intermediary between the client and the authentication server. It requests identity information from the client, verifies it and relays response to the client.
* Authentication server – validates the identity of the client and notifies the switch or the wireless access appoint that the client is authorized or not.

10.3.1 Layer 2 Security Threats

10.3.1 Layer 2 Attacks (Switch Attacks)

* MAC Table Attacks – includes MAC address flooding attacks
* VLAN Attacks – includes VLAN hopping and VLAN double-tagging attacks
* DHCP Attacks – includes DHCP starvation and DHCP spoofing attacks
* ARP Attacks – includes ARP spoofing and ARP poisoning attacks
* Address Spoofing Attacks – includes MAC address and IP address spoofing attacks
* STP Attacks – inc Spanning Tree Protocol Manipulation attacks

10.3.3 Switch Attacks Mitigation Techniques

* Port security – prevents MAC address flooding and DHCP starvation
* DHCP Snooping – prevents DHCP starvation and DHCP spoofing attacks
* Dynamic ARP inspection (DAI) – prevents ARP spoofing and ARP poisoning attacks.
* IP Source Guard (IPSG) – prevents MAC and IP address spoofing attacks.

The above solutions can only be effective if the management protocols are secured.

The management protocols include:

1. Syslog
2. Simple Network Management Protocol (SNMP)\
3. Trivial File Transfer Protocol (TFTP)

As a result, strategies such as;

* use of SSH, Secure Copy Protocol (SCP), Secure FTP (SFTP), and secure Socket Layer/Transport Layer Security (SSL/TLS).
* Using out-of-band management network to manage devices
* Use a dedicated management VLAN where nothing but management traffic resides.
* Use ACLs to filter unwanted access.

10.4 MAC Address Table Attack

* All MAC address tables have a fixed size (for example, a Catalyst 6500 switch can store 132,000 MAC addresses in its MAC address table) and consequently, a switch can run out of resources in which to store the MAC addresses.
* A tool such as macof, can flood a switch with up to 8,000 bogus frames per second.
* Attackers takes advantage of this by bombarding the switch with fake source MAC addresses until all the switch MAC address table is full.
* The switch will then turn the frames as an unknown unicast and begins flooding all the incoming traffic out of all ports on the same VLAN without referencing the MAC address table.
* This then allows the attacker to capture all the frames sent from one host to another on the local LAN or local VLAN.

10.5 LAN Attacks

VLAN and DHCP Attacks

VLAN Hopping Attacks

* Enables traffic from one VLAN to be seen by another VLAN without the aid of a router.
* The threat actor configures a host to act like a switch to take advantage of the automatic trunking port feature enabled by default on most switch ports.
* The threat actor configures the host to spoof 802.1Q signalling and Cisco-proprietary Dynamic Trunking protocol (DTP) signalling to trunk with the connecting switch.
* If successful, the switch establishes a trunk with the host.
* Hence the threat actor can access all the VLANs on the switch. The actor can send and receive traffic on any VLAN, effectively hopping between VLANs.

VLAN Double-Tagging Attack

* A threat actor could enable a hidden 802.1Q tag inside the frame that already has an 802.1Q tag.
* This tag allows the frame to go to a VLAN that the original 802.1Q did not specify.
* The double tagging allows the attacker to send data to hosts or servers on a VLAN that otherwise would be blocked by some type of access control configurations. Presumably the return traffic will also be permitted, thus giving the attacker the ability to communicate with the devices on the normally blocked VLAN.

Mitigating VLAN Hopping and VLAN double-tagging

* Disable trunking on all access ports
* Disable auto trunking on trunk links so that the trunk must be manually enabled.
* Be sure that the native VLAN is only used for trunk links.

10.5.5 DHCP Attacks

* DHCP starvation – creates a DoS for disconnecting clients. A tool such as Gobbler is used. The tool has the ability to look the entire scope of leasable IP address and tries to lease them all. Specifically, it creates DHCP discovery messages with bogus MAC addresses.
* DHCP spoofing – a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. The rogue server can provide misleading information such as wrong default gateway, wrong DNS server, and wrong IP address.

Step 1: Threat Actor Connects Rogue DHCP Server

A threat actor successfully connects a rogue DHCP server to a switch port on the same subnet and VLANs as the target clients. The goal of the rogue server is to provide clients with false IP configuration information.

Step 2: Client Broadcasts DHCP Discovery Messages

A legitimate client connects to the network and requires IP configuration parameters. Therefore, the client broadcasts a DHCP Discovery request looking for a response from a DHCP server. Both servers will receive the message and respond.

Step 3: Legitimate and Rogue DHCP Reply

The legitimate DHCP server responds with valid IP configuration parameters. However, the rogue server also responds with a DHCP offer containing IP configuration parameters defined by the threat actor. The client will reply to the first offer received.

Step 4: Client Accepts Rogue DHCP Offer

The rogue offer was received first, and therefore, the client broadcasts a DHCP request accepting the IP parameters defined by the threat actor. The legitimate and rogue server will receive the request.

Step 5: Rogue Server Acknowledges

The rogue server unicasts a reply to the client to acknowledge its request. The legitimate server will cease communicating with the client.

10.5.6 ARP Attacks, STP Attacks, and CDP Reconnaissance

* Recall that hosts broadcast ARP Requests to determine the MAC address of a host with a particular IPv4 address. This is typically done to discover the MAC address of the default gateway. All hosts on the subnet receive and process the ARP Request. The host with the matching IPv4 address in the ARP Request sends an ARP Reply.
* According to the ARP RFC, a client is allowed to send an unsolicited ARP Request called a “gratuitous ARP.” When a host sends a gratuitous ARP, other hosts on the subnet store the MAC address and IPv4 address contained in the gratuitous ARP in their ARP tables.
* The problem is that an attacker can send a gratuitous ARP message containing a spoofed MAC address to a switch, and the switch would update its MAC table accordingly. Therefore, any host can claim to be the owner of any IP and MAC address combination they choose. In a typical attack, a threat actor can send unsolicited ARP Replies to other hosts on the subnet with the MAC Address of the threat actor and the IPv4 address of the default gateway.
* There are many tools available on the internet to create ARP man-in-the-middle attacks including dsniff, Cain & Abel, ettercap, Yersinia, and others. IPv6 uses ICMPv6 Neighbor Discovery Protocol for Layer 2 address resolution. IPv6 includes strategies to mitigate Neighbor Advertisement spoofing, similar to the way IPv6 prevents a spoofed ARP Reply.
* ARP spoofing and ARP poisoning are mitigated by implementing DAI.

10.5.8 Address Spoofing Attack

IP addresses and MAC addresses can be spoofed for a variety of reasons. IP address spoofing is when a threat actor hijacks a valid IP address of another device on the subnet, or uses a random IP address. IP address spoofing is difficult to mitigate, especially when it is used inside a subnet in which the IP belongs.

MAC address spoofing attacks occur when the threat actors alter the MAC address of their host to match another known MAC address of a target host. The attacking host then sends a frame throughout the network with the newly-configured MAC address. When the switch receives the frame, it examines the source MAC address. The switch overwrites the current MAC table entry and assigns the MAC address to the new port.

When the target host sends traffic, the switch will correct the error, realigning the MAC address to the original port. To stop the switch from returning the port assignment to its correct state, the threat actor can create a program or script that will constantly send frames to the switch so that the switch maintains the incorrect or spoofed information. There is no security mechanism at Layer 2 that allows a switch to verify the source of MAC addresses, which is what makes it so vulnerable to spoofing.

IP and MAC address spoofing can be mitigated by implementing IPSG.

10.5.9 STP Attack

Network attackers can manipulate the Spanning Tree Protocol (STP) to conduct an attack by spoofing the root bridge and changing the topology of a network. Attackers can make their hosts appear as root bridges; and therefore, capture all traffic for the immediate switched domain.

To conduct an STP manipulation attack, the attacking host broadcasts STP bridge protocol data units (BPDUs) containing configuration and topology changes that will force spanning-tree recalculations. The BPDUs sent by the attacking host announce a lower bridge priority in an attempt to be elected as the root bridge.

10.5.10 CDP Reconnaissance

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 a periodic, unencrypted multicast. 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 a threat actor to discover network infrastructure vulnerabilities.

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) is 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.

Question 1

A threat actor changes the MAC address of the threat actor's device to the MAC address of the default gateway. What type of attack is this?

Address spoofing

Question 2

A threat actor sends a BPDU message with priority 0. What type of attack is this?

STP attack

Question 3

A threat actor leases all the available IP addresses on a subnet. What type of attack is this?

DHCP starvation

Question 4

A threat actor sends a message that causes all other devices to believe the MAC address of the threat actor's device is the default gateway. What type of attack is this?

ARP spoofing

Question 5

A threat actor configures a host with the 802.1Q protocol and forms a trunk with the connected switch. What type of attack is this?

VLAN hopping

Question 6

A threat actor discovers the IOS version and IP addresses of the local switch. What type of attack is this?

CDP reconnaissance

10.6.2 Module Quiz - LAN Security Concepts

Question 1

What two protocols are supported on Cisco devices for AAA communications? (Choose two.)

RADIUS

TACACS+

Topic 10.2.0 - Two AAA protocols are supported on Cisco devices, TACACS+ and RADIUS. Hot Standby Router Protocol (HSRP) is used on Cisco routers to allow for gateway redundancy. Link Layer Discovery Protocol (LLDP) is a protocol for neighbor discovery. VLAN trunking protocol (VTP) is used on Cisco switches to manage VLANs on a VTP-enabled server switch.

Question 2

Which service is enabled on a Cisco router by default that can reveal significant information about the router and potentially make it more vulnerable to attack?

CDP

Topic 10.5.0 - CDP is a Cisco proprietary protocol that gathers information from other connected Cisco devices, and is enabled by default on Cisco devices

Question 3

When security is a concern, which OSI Layer is considered to be the weakest link in a network system?​

Layer 2

Topic 10.3.0 - Security is only as strong as the weakest link in the system, and Layer 2 is considered to be that weakest link. In addition to protecting Layer 3 to Layer 7, network security professionals must also mitigate attacks to the Layer 2 LAN infrastructure.

Question 4

Which Layer 2 attack will result in a switch flooding incoming frames to all ports?

MAC address overflow

Topic 10.4.0 - When an attacker rapidly sends frames with spoofed MAC addresses to a switch, the MAC address table of the switch becomes full. Once the MAC address table of the switch is full, the switch will flood all new incoming frames to all ports.

Question 5

Why is authentication with AAA preferred over a local database method?

It provides a fallback authentication method if the administrator forgets the username or password.

Topic 10.2.0 - The local database method of authentication does not provide a fallback authentication method if an administrator forgets the username or password. Password recovery will be the only option. When authentication with AAA is used, a fallback method can be configured to allow an administrator to use one of many possible backup authentication methods.

Question 6

In a server-based AAA implementation, which protocol will allow the router to successfully communicate with the AAA server?

RADIUS

Topic 10.2.0 - With a server-based method, the router accesses a central AAA server using either the Remote Authentication Dial-In User (RADIUS) or Terminal Access Controller Access Control System (TACACS+) protocol.

Question 7

Which Cisco solution helps prevent MAC and IP address spoofing attacks?

* Port Security - prevents many types of attacks including MAC table overflow attacks and DHCP starvation attacks
* DHCP Snooping - prevents DHCP starvation and SHCP spoofing attacks
* IP Source Guard - prevents MAC and IP address spoofing attacks
* Dynamic ARP Inspection - - prevents ARP spoofing and ARP poisoning attacks

Question 8

What is the purpose of AAA accounting?

To collect and report application usage

Topic 10.2.0 - AAA accounting collects and reports application usage data. This data can be used for such purposes as auditing or billing. AAA authentication is the process of verifying users are who they say they are. AAA authorization is what the users can and cannot do on the network after they are authenticated.

Question 9

Which Layer 2 attack will result in legitimate users not getting valid IP addresses?

DHCP starvation

Topic 10.5.0 - The DHCP starvation attack causes the exhaustion of the IP address pool of a DHCP server before legitimate users can obtain valid IP addresses.

Question 10

Which three Cisco products focus on endpoint security solutions? (Choose three.)

Web Security Appliance

Email Security Appliance

NAC Appliance

Topic 10.1.0 - The primary components of endpoint security solutions are Cisco Email and Web Security appliances, and Cisco NAC appliance.

Question 11

True or False?

In the 802.1X standard, the client attempting to access the network is referred to as the supplicant. True

Topic 10.2.0 - In 802.1X terminology the client workstation is known as the supplicant.

Question 12

What is involved in an IP address spoofing attack?

A legitimate network IP address is hijacked by a rogue node.

Topic 10.5.0 - In an IP address spoofing attack, the IP address of a legitimate network host is hijacked and used by a rogue node. This allows the rogue node to pose as a valid node on the network.

Question 13

What three services are provided by the AAA framework? (Choose three.)

Accounting

Authorization

Authentication

Topic 10.2.0 - The authentication, authorization, and accounting (AAA) framework provides services to help secure access to network devices.

Question 14

Because of implemented security controls, a user can only access a server with FTP. Which AAA component accomplishes this?

Authorization

Topic 10.2.0 - One of the components in AAA is authorization. After a user is authenticated through AAA, authorization services determine which resources the user can access and which operations the user is allowed to perform.

Question 15

What mitigation plan is best for thwarting a DoS attack that is creating a MAC address table overflow?

Enable port security.

Topic 10.3.0 - A MAC address (CAM) table overflow attack, buffer overflow, and MAC address spoofing can all be mitigated by configuring port security. A network administrator would typically not want to disable STP because it prevents Layer 2 loops. DTP is disabled to prevent VLAN hopping. Placing unused ports in an unused VLAN prevents unauthorized wired connectivity.

11.0 Switch Security Configurations

11.1 Implement Port Security

Secure Unused Ports - A simple method that many administrators use to help secure the network from unauthorized access is to disable all unused ports on a switch.

Switch(config)# interface range type module/first-number – last-number\

S1(config)# interface range fa0/8 - 24

S1(config-if-range)# shutdown

Mitigate MAC Address Table Attacks

The simplest and most effective method to prevent MAC address table overflow attacks is to enable port security.

Port security limits the number of valid MAC addresses allowed on a port. It allows an administrator to manually configure MAC addresses for a port or to permit the switch to dynamically learn a limited number of MAC 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 MAC addresses that were manually configured or dynamically learned on the port.

By limiting the number of permitted MAC addresses on a port to one, port security can be used to control unauthorized access to the network.

11.1.3 Enable Port Security - port security can only be configured on manually configured access ports or manually configured trunk ports.

* S1(config)# interface f0/1
* S1(config-if)# switchport port-security
* Command rejected: FastEthernet0/1 is a dynamic port.
* S1(config-if)# switchport mode access
* S1(config-if)# switchport port-security
* S1(config-if)# end
* S1#

Use the show port-security interface command to display the current port security settings

S1(config-if)# switchport port-security ?

* aging Port-security aging commands
* mac-address Secure mac address
* maximum Max secure addresses
* violation Security violation mode

11.1.4 Limit and Learn MAC Addresses

To set the maximum number of MAC addresses allowed on a port, use the following command:

Switch(config-if)# switchport port-security maximum value

S1(config)# interface f0/1

S1(config-if)# switchport port-security maximum ?

<1-8192> Maximum addresses

S1(config-if)# switchport port-security maximum

The switch can be configured to learn about MAC addresses on a secure port in one of three ways:

1. Manually Configured - The administrator manually configures a static MAC address(es) by using the following command for each secure MAC address on the port:

Switch(config-if)# switchport port-security mac-address mac-address

2. Dynamically Learned - When the switchport port-security command is entered, the current source MAC for the device connected to the port is automatically secured but is not added to the startup configuration. If the switch is rebooted, the port will have to re-learn the device’s MAC address.

3. Dynamically Learned – Sticky - The administrator can enable the switch to dynamically learn the MAC address and “stick” them to the running configuration by using the following command:

Switch(config-if)# switchport port-security mac-address sticky

11.1.5 Port Security Aging

Port security aging can be used to set the aging time for static and dynamic secure addresses on a port. Two types of aging are supported per port:

Absolute - The secure addresses on the port are deleted after the specified aging time.

Inactivity - The secure addresses on the port are deleted only if they are inactive for the specified aging time.

Use aging to remove secure MAC addresses on a secure port without manually deleting the existing secure MAC addresses. Aging time limits can also be increased to ensure past secure MAC addresses remain, even while new MAC addresses are added. Aging of statically configured secure addresses can be enabled or disabled on a per-port basis.

Use the switchport port-security aging command to enable or disable static aging for the secure port, or to set the aging time or type.

Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}

11.1.6 Port Security Violation Modes

If the MAC address of a device attached to the port differs from the list of secure addresses, then a port violation occurs. By default, the port enters the error-disabled state.

To set the port security violation mode, use the following command:

Switch(config-if)# switchport port-security violation { protect | restrict | shutdown}

11.1.7 Ports in error-disabled State

What happens when the port security violation is shutdown and a port violation occurs? The port is physically shutdown and placed in the error-disabled state, and no traffic is sent or received on that port.

11.1.8 Verify Port Security

* Port Security for All Interfaces - show port-security
* Port Security for a Specific Interface - show port-security interface fastethernet 0/1
* Verify Learned MAC Addresses - show run interface fa0/1
* Verify Secure MAC Addresses - show port-security address

Practice Exercise

You are currently logged into S1. Configure FastEthernet 0/5 for port security by using the following requirements:

* Use the interface name fa0/5 to enter interface configuration mode.
* Enable the port for access mode.
* Enable port security.
* Set the maximum number of MAC address to 3.
* Statically configure the MAC address aaaa.bbbb.1234.
* Configure the port to dynamically learn additional MAC addresses and dynamically add them to the running configuration.
* Return to privileged EXEC mode.

S1(config)#interface fa0/5

S1(config-if)#switchport mode access

S1(config-if)#switchport port-security

S1(config-if)#switchport port-security maximum 3

S1(config-if)#switchport port-security mac-address aaaa.bbbb.1234

S1(config-if)#switchport port-security mac-address sticky

S1(config-if)#end

Enter the command to verify port security for all interfaces.

S1#show port-security

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

(Count) (Count) (Count)

---------------------------------------------------------------------------

Fa0/5 3 2 0 Shutdown

---------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 8192

Enter the command to verify port security on FastEthernet 0/5. Use fa0/5 for the interface name.

S1#show port-security interface fa0/5

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 3

Total MAC Addresses : 2

Configured MAC Addresses : 1

Sticky MAC Addresses : 1

Last Source Address:Vlan : 0090.2135.6B8C:1

Security Violation Count : 0

Enter the command that will display all of the addresses to verify that the manually configured and dynamically learned MAC addresses are in the running configuration.

S1#show port-security address

Secure Mac Address Table

-----------------------------------------------------------------------------

Vlan Mac Address Type Ports Remaining Age

(mins)

---- ----------- ---- ----- -------------

1 0090.2135.6b8c SecureSticky Fa0/5 -

1 aaaa.bbbb.1234 SecureConfigured Fa0/5 -

-----------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 8192

You have successfully configured and verified port security for the interface.

11.2 Mitigate VLAN Attacks

11.2.2 Steps to Mitigate VLAN Hopping Attacks

Use the following steps to mitigate VLAN hopping attacks:

* Step 1: Disable DTP (auto trunking) negotiations on non-trunking ports by using the switchport mode access interface configuration command.
* Step 2: Disable unused ports and put them in an unused VLAN.
* Step 3: Manually enable the trunk link on a trunking port by using the switchport mode trunk command.
* Step 4: Disable DTP (auto trunking) negotiations on trunking ports by using the switchport nonegotiate command.
* Step 5: Set the native VLAN to a VLAN other than VLAN 1 by using the switchport trunk native vlan vlan\_number command.

For example, assume the following:

FastEthernet ports 0/1 through fa0/16 are active access ports

FastEthernet ports 0/17 through 0/20 are not currently in use

FastEthernet ports 0/21 through 0/24 are trunk ports.

VLAN hopping can be mitigated by implementing the following configuration.

S1(config)# interface range fa0/1 - 16

S1(config-if-range)# switchport mode access

S1(config-if-range)# exit

S1(config)#

S1(config)# interface range fa0/17 - 20

S1(config-if-range)# switchport mode access

S1(config-if-range)# switchport access vlan 1000

S1(config-if-range)# shutdown

S1(config-if-range)# exit

S1(config)#

S1(config)# interface range fa0/21 - 24

S1(config-if-range)# switchport mode trunk

S1(config-if-range)# switchport nonegotiate

S1(config-if-range)# switchport trunk native vlan 999

S1(config-if-range)# end

S1#

FastEthernet ports 0/1 to 0/16 are access ports and therefore trunking is disabled by explicitly making them access ports.

FastEthernet ports 0/17 to 0/20 are unused ports and are disabled and assigned to an unused VLAN.

FastEthernet ports 0/21 to 0/24 are trunk links and are manually enabled as trunks with DTP disabled. The native VLAN is also changed from the default VLAN 1 to an unused VLAN 999.

11.3 Mitigate DHCP Attacks

DHCP spoofing attacks can be mitigated by using DHCP snooping on trusted ports.

11.3.2 DHCP Snooping

DHCP snooping does not rely on source MAC addresses. Instead, DHCP snooping determines whether DHCP messages are from an administratively configured trusted or untrusted source. It then filters DHCP messages and rate-limits DHCP traffic from untrusted sources.

Devices under your administrative control, such as switches, routers, and servers, are trusted sources. Any device beyond the firewall or outside your network is an untrusted source. In addition, all access ports are generally treated as untrusted sources

A DHCP table is built that includes the source MAC address of a device on an untrusted port and the IP address assigned by the DHCP server to that device. The MAC address and IP address are bound together. Therefore, this table is called the DHCP snooping binding table.

11.3.3 Steps to Implement DHCP Snooping

Use the following steps to enable DHCP snooping:

* Step 1. Enable DHCP snooping by using the ip dhcp snooping global configuration command.
* Step 2. On trusted ports, use the ip dhcp snooping trust interface configuration command.
* Step 3. Limit the number of DHCP discovery messages that can be received per second on untrusted ports by using the ip dhcp snooping limit rate interface configuration command.
* Step 4. Enable DHCP snooping by VLAN, or by a range of VLANs, by using the ip dhcp snooping vlan global configuration command.

Use the show ip dhcp snooping privileged EXEC command to verify DHCP snooping and show ip dhcp snooping binding to view the clients that have received DHCP information

Practice Exercise

You are currently logged into S1. Enable DHCP snooping globally for the switch.

S1(config)#ip dhcp snooping

Enter interface configuration mode for g0/1 - 2, trust the interfaces, and return to global configuration mode.

S1(config)#interface range g0/1 - 2

S1(config-if-range)#ip dhcp snooping trust

S1(config-if-range)#exit

Enter interface configuration mode for f0/1 - 24, limit the DHCP messages to no more than 10 per second, and return to global configuration mode.

S1(config)#interface range f0/1 - 24

S1(config-if-range)#ip dhcp snooping limit rate 10

S1(config-if-range)#exit

Enable DHCP snooping for VLANs 10,20,30-49.

S1(config)#ip dhcp snooping vlan 10,20,30-49

S1(config)# exit

Enter the command to verify DHCP snooping.

S1#show ip dhcp snooping

Enter the command to verify the current DHCP bindings logged by DHCP snooping

S1#show ip dhcp snooping binding

MacAddress IpAddress Lease(sec) Type VLAN Interface

------------------ --------------- ---------- ------------- ---- --------------------

00:03:47:B5:9F:AD 10.0.0.10 193185 dhcp-snooping 5 FastEthernet0/1

S1#

You have successfully configured and verified DHCP snooping for the switch.

11.4 Mitigate ARP Attacks

11.4.1 Dynamic ARP Inspection

In a typical ARP attack, a threat actor can send unsolicited ARP requests to other hosts on the subnet with the MAC Address of the threat actor and the IP address of the default gateway. To prevent ARP spoofing and the resulting ARP poisoning, a switch must ensure that only valid ARP Requests and Replies are relayed.

Dynamic ARP inspection (DAI) requires DHCP snooping and helps prevent ARP attacks by:

* Not relaying invalid or gratuitous ARP Requests out to other ports in the same VLAN.
* Intercepting all ARP Requests and Replies on untrusted ports.
* Verifying each intercepted packet for a valid IP-to-MAC binding.
* Dropping and logging ARP Requests coming from invalid sources to prevent ARP poisoning.
* Error-disabling the interface if the configured DAI number of ARP packets is exceeded.

11.4.2 DAI Implementation Guidelines

To mitigate the chances of ARP spoofing and ARP poisoning, follow these DAI implementation guidelines:

* Enable DHCP snooping globally.
* Enable DHCP snooping on selected VLANs.
* Enable DAI on selected VLANs.
* Configure trusted interfaces for DHCP snooping and ARP inspection.

It is generally advisable to configure all access switch ports as untrusted and to configure all uplink ports that are connected to other switches as trusted.

11.4.3 DAI Configuration Example

You are currently logged into S1. Enable DHCP snooping globally for the switch.

S1(config)#ip dhcp snooping

Enter interface configuration mode for g0/1 - 2, trust the interfaces for both DHCP snooping and DAI, and then return to global configuration mode.

S1(config)#interface range g0/1 - 2

S1(config-if-range)#ip dhcp snooping trust

S1(config-if-range)#ip arp inspection trust

S1(config-if-range)#exit

Enable DHCP snooping and DAI for VLANs 10,20,30-49.

S1(config)#ip dhcp snooping vlan 10,20,30-49

S1(config)#ip arp inspection vlan 10,20,30-49

S1(config)#

You have successfully configured DAI for the switch.

11.5 Mitigate STP Attacks

11.5.1 PortFast and BPDU Guard

Recall that network attackers can manipulate the Spanning Tree Protocol (STP) to conduct an attack by spoofing the root bridge and changing the topology of a network. To mitigate Spanning Tree Protocol (STP) manipulation attacks, use PortFast and Bridge Protocol Data Unit (BPDU) Guard:

* PortFast - PortFast immediately brings an interface configured as an access port to the forwarding state from a blocking state, bypassing the listening and learning states. Apply to all end-user ports. PortFast should only be configured on ports attached to end devices. PortFast can be enabled on an interface by using the spanning-tree portfast interface configuration command. Alternatively, Portfast can be configured globally on all access ports by using the spanning-tree portfast default global configuration command. To verify if PortFast is enabled an interface, use the show running-config interface type/number command
* BPDU Guard - BPDU guard immediately error disables a port that receives a BPDU. Like PortFast, BPDU guard should only be configured on interfaces attached to end devices. BPDU Guard can be enabled on a port by using the spanning-tree bpduguard enable interface configuration command. Alternatively, Use the spanning-tree portfast bpduguard default global configuration command to globally enable BPDU guard on all PortFast-enabled ports. To display information about the state of spanning tree, use the show spanning-tree summary command.

Practice Example

You are currently logged into S1. Complete the following steps to implement PortFast and BPDU Guard on all access ports:

* Enter interface configuration mode for fa0/1 - 24.
* Configure the ports for access mode.
* Return to global configuration mode.
* Enable PortFast by default for all access ports.
* Enable BPDU Guard by default for all access ports.

S1(config)#interface range fa0/1 - 24

S1(config-if-range)#switchport mode access

S1(config-if-range)#exit

S1(config)#spanning-tree portfast default

S1(config)#spanning-tree portfast bpduguard default

S1(config)# exit

Verify that PortFast and BPDU Guard is enabled by default by viewing STP summary information.

S1#show spanning-tree summary

You have successfully configured and verified PortFast and BPDU Guard for the switch.

11.6.4 Module Quiz - Switch Security Configuration

Question 1

What is a recommended best practice when dealing with the native VLAN?

Assign it to an unused VLAN.

Topic 11.2.0 - Port security cannot be enabled on a trunk and trunks are the only types of ports that have a native VLAN. Even though turning DTP off on a trunk is a best practice, it does not have anything to do with native VLAN risks. To prevent security breaches that take advantage of the native VLAN, place the native VLAN in an unused VLAN other than VLAN 1. The management VLAN should also be an unused VLAN that is different from the native VLAN and something other than VLAN 1.

Question 2

On what switch ports should PortFast be enabled to enhance STP stability?

All end-user ports

Topic 11.5.0 - PortFast will immediately bring an interface configured as an access or trunk port to the forwarding state from a blocking state, bypassing the listening and learning states. If configured on a trunk link, immediately transitioning to the forwarding state could lead to the formation of Layer 2 loops.

Question 3

Which command would be best to use on an unused switch port if a company adheres to the best practices as recommended by Cisco?

shutdown

Topic 11.1.0 - Unlike router Ethernet ports, switch ports are enabled by default. Cisco recommends disabling any port that is not used. The ip dhcp snooping command globally enables DHCP snooping on a switch. Further configuration allows defining ports that can respond to DHCP requests. The switchport port-security command is used to protect the network from unidentified or unauthorized attachment of network devices.

Question 4

Which two features on a Cisco Catalyst switch can be used to mitigate DHCP starvation and DHCP spoofing attacks? (Choose two.)

Port security

DHCP snooping

Topic 11.3.0 - In DHCP starvation attacks, an attacker floods the DHCP server with DHCP requests to use up all the available IP addresses that the DHCP server can issue. In DHCP spoofing attacks, an attacker configures a fake DHCP server on the network so that it provides clients with false DNS server addresses. The port security feature can limit the number of dynamically learned MAC addresses per port or allow only known valid NICs to be connected via their specific MAC addresses. The DHCP snooping feature can identify the legitimate DHCP servers and block fake DHCP servers from issuing IP address information. These two features can help fight against DHCP attacks.

Question 5

What is the best way to prevent a VLAN hopping attack?

Disable trunk negotiation for trunk ports and statically set nontrunk ports as access ports.

Topic 11.2.0 - VLAN hopping attacks rely on the attacker being able to create a trunk link with a switch. Disabling DTP and configuring user-facing ports as static access ports can help prevent these types of attacks.

Question 6

Which procedure is recommended to mitigate the chances of ARP spoofing?

Enable DHCP snooping on selected VLANs.

Topic 11.4.0 - To mitigate the chances of ARP spoofing, these procedures are recommended:

- Implement protection against DHCP spoofing by enabling DHCP snooping globally.

- Enable DHCP snooping on selected VLANs.

- Enable DAI on selected VLANs.

- Configure trusted interfaces for DHCP snooping and ARP inspection. Untrusted ports are configured by default.​

Question 7

What are two types of switch ports that are used on Cisco switches as part of the defense against DHCP spoofing attacks? (Choose two.)

- Trusted DHCP ports - switch ports connecting to upstream DHCP servers

- Untrusted ports - switch ports connecting to hosts that should not be providing DHCP server messages

Question 8

Which two commands can be used to enable PortFast on a switch? (Choose two.)

S1(config-if)# spanning-tree portfast

S1(config)# spanning-tree portfast default

Topic 11.5.0 - PortFast can be configured on all nontrunking ports using the spanning-tree portfast default global configuration command. Alternatively, PortFast can be enabled on an interface using the spanning-tree portfast interface configuration command.

Question 9

An administrator who is troubleshooting connectivity issues on a switch notices that a switch port configured for port security is in the err-disabled state. After verifying the cause of the violation, how should the administrator re-enable the port without disrupting network operation?

Issue the shutdown command followed by the no shutdown command on the interface.

Topic 11.1.0 - If an interface that has been protected with port security goes into the err-disabled state, then a violation has occurred and the administrator should investigate the cause of the violation. Once the cause is determined, the administrator can issue the shutdown command followed by the no shutdown command to enable the interface.

Question 10

A network administrator is configuring DHCP snooping on a switch. Which configuration command should be used first?

ip dhcp snooping

Topic 11.3.0 - The steps to enable DHCP snooping include these:

* Step 1. Enable DHCP snooping using the ip dhcp snooping global configuration command.
* Step 2. On trusted ports, use the ip dhcp snooping trust interface configuration command.
* Step 3. Enable DHCP snooping by VLAN, or by a range of VLANs.

Question 11

A network administrator is configuring DAI on a switch with the command ip arp inspection validate dst-mac. What is the purpose of this configuration command?

To check the destination MAC address in the Ethernet header against the target MAC address in the ARP body

Topic 11.4.0 - DAI can be configured to check for both destination or source MAC and IP addresses:

* Destination MAC - Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body.
* Source MAC - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body.
* IP address - Checks the ARP body for invalid and unexpected IP addresses including addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Question 12

Which security feature should be enabled in order to prevent an attacker from overflowing the MAC address table of a switch?

Port security

Topic 11.1.0 - Port security limits the number of source MAC addresses allowed through a switch port. This feature can prevent an attacker from flooding a switch with many spoofed MAC addresses.

Question 13

What Layer 2 attack is mitigated by disabling Dynamic Trunking Protocol?

VLAN hopping

Topic 11.2.0 - Mitigating a VLAN hopping attack can be done by disabling Dynamic Trunking Protocol (DTP) and by setting the native VLAN of trunk links to VLANs not in use.

Question 14

A network administrator is configuring DAI on a switch. Which command should be used on the uplink interface that connects to a router?

ip arp inspection trust

Topic 11.4.0 - In general, a router serves as the default gateway for the LAN or VLAN on the switch. Therefore, the uplink interface that connects to a router should be a trusted port for forwarding ARP requests.

Question 15

Where are dynamically learned MAC addresses stored when sticky learning is enabled with the switchport port-security mac-address sticky command?

RAM

Topic 11.1.0 - When MAC addresses are automatically learned by using the sticky command option, the learned MAC addresses are added to the running configuration, which is stored in RAM.

12.0 WLAN Concepts

12.1.2 Types of Wireless Networks

Wireless Personal-Area Networks (WPAN) - Uses low powered transmitters for a short-range network, usually 20 to 30 ft. (6 to 9 meters). Bluetooth and ZigBee based devices are commonly used in WPANs. WPANs are based on the 802.15 standard and a 2.4-GHz radio frequency.

Wireless LANs (WLAN) - Uses transmitters to cover a medium-sized network, usually up to 300 feet. WLANs are suitable for use in a home, office, and even a campus environment. WLANs are based on the 802.11 standard and a 2.4-GHz or 5-GHz radio frequency.

Wireless MANs (WMAN) - Uses transmitters to provide wireless service over a larger geographic area. WMANs are suitable for providing wireless access to a metropolitan city or specific district. WMANs use specific licensed frequencies.

Wireless Wide-Area Networks (WWANs) - Uses transmitters to provide coverage over an extensive geographic area. WWANs are suitable for national and global communications. WWANs also use specific licensed frequencies.

12.1.3 Wireless Technologies

Bluetooth - An IEEE 802.15 WPAN standard that uses a device-pairing process to communicate over distances up to 300 ft. (100m). It can be found in smart home devices, audio connections, automobiles, and other devices that require a short distance connection. There are two types of Bluetooth radios:

* Bluetooth Low Energy (BLE) - This supports multiple network technologies including mesh topology to large scale network devices.
* Bluetooth Basic Rate/Enhanced Rate (BR/EDR) - This supports point to point topologies and is optimized for audio streaming.

WiMAX (Worldwide Interoperability for Microwave Access) - WiMAX is an alternative to broadband wired internet connections, competing with DSL and cable. However, it is typically used in areas that are not yet connected to a DSL or cable provider. It is an IEEE 802.16 WWAN standard that provides high-speed wireless broadband access of up to 30 miles (50 km). 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. WiMAX transmitters and cellular transmitters may share space on the same tower.

Cellular Broadband - Cellular 4G/5G are wireless mobile networks primarily used by cellular phones but can be used in automobiles, tablets, and laptops. Cellular networks are multi-access networks carrying both data and voice communications. A cell site is created by a cellular tower transmitting signals in a given area. Interconnecting cell sites form the cellular network. The two types of cellular networks are Global System for Mobile (GSM) and Code Division Multiple Access (CDMA). GSM is internationally recognized, while CDMA is primarily used in the US.

The 4th Generation mobile network (4G) is the current mobile network. 4G delivers speeds that are 10 times the previous 3G networks. The new 5G holds the promise of delivering 100 times faster speeds than 4G and connecting more devices to the network than ever before.

Satellite Broadband - Provides network access to remote sites through the use of a directional satellite dish that is aligned with a specific geostationary Earth orbit satellite. It is usually more expensive and requires a clear line of sight. Typically, it is used by rural homeowners and businesses where cable and DSL are not available.

12.1.4 802.11 Standards

The world of wireless communications is vast. However, for particular job-related skills, we want to focus on specific aspects of Wi Fi. The best place to start is with the IEEE 802.11 WLAN standards. These standards define how radio frequencies are used for wireless links. Most of the standards specify that wireless devices have one antenna to transmit and receive wireless signals on the specified radio frequency (2.4 GHz or 5 GHz). Some of the newer standards that transmit and receive at higher speeds require access points (APs) and wireless clients to have multiple antennas using the multiple-input and multiple-output (MIMO) technology. MIMO uses multiple antennas as both the transmitter and receiver to improve communication performance. Up to eight transmit and receive antennas can be used to increase throughput.

|  |  |  |
| --- | --- | --- |
| IEEE WLAN Standard | Radio Frequency | Description |
| 802.11 | 2.4 GHz | Speeds of up to 2Mbps |
| 802.11a | 5GHz | Speed of up to 54 Mbps  Small coverage area  Less effective penetrating building structures  Not interoperable with the 802.11b and 802.11g |
| 802.11b | 2.4 GHz | Speeds of up to 11 Mbps  Longer range than 802.11a  Better able to penetrate building structures |
| 802.11g | 2.4GHz | 54 Mbps  Backward compatible with 802.11b |
| 802.11n | 2.4GHz 5GHz | 150 Mbps – 600Mbps  70m distance  APs and wireless clients require MIMO technology  Backward compatible with 802.11a/b/g |
| 802.11ac | 5GHz | 450 Mbps – 1.3 Gbps  Up to 8 antennas  Backward compatible with 802.11a/n |
| 802.11ax | 2.4GHz 5GHz | Latest  Also known as Wi-Fi 6 or High-Efficiency Wireless (HEW)  Higher data rates, improved power efficiency, increased capacity, many connected devices. |

12.1.6 Wireless Standards Organizations

* The International Telecommunication Union (ITU) regulates the allocation of the radio frequency spectrum and satellite orbits through the ITU-R. ITU-R stands for the ITU Radiocommunication Sector.
* The IEEE specifies how a radio frequency is modulated to carry information. It maintains the standards for local and metropolitan area networks (MAN) with the IEEE 802 LAN/MAN family of standards. The dominant standards in the IEEE 802 family are 802.3 Ethernet and 802.11 WLAN.
* The Wi-Fi Alliance is a global, non-profit, industry trade association devoted to promoting the growth and acceptance of WLANs. It is an association of vendors whose objective is to improve the interoperability of products that are based on the 802.11 standard by certifying vendors for conformance to industry norms and adherence to standards.

Quiz

Question 1

Which of the following wireless networks typically uses lower powered transmitters for short ranges?

WPAN

Question 2

Which of the following wireless networks are specified in the IEEE 802.11 standards for the 2.4 GHz and 5 GHz radio frequencies?

WLAN

Question 3

Which of the following is an IEEE 802.15 WPAN standard that uses a device-pairing process to communicate?

Bluetooth

Question 4

Which 802.11 standards exclusively use the 5 GHz radio frequency? (Choose 2)

802.11a

802.11ac

Question 5

Which standards organization is responsible for allocating radio frequencies?

ITU-R

12.2 WLAN Components

12.2.2 Wireless NICs

Wireless deployments require a minimum of two devices that have a radio transmitter and a radio receiver tuned to the same radio frequencies:

* End devices with wireless NICs
* A network device, such as a wireless router or wireless AP

To communicate wirelessly, laptops, tablets, smart phones, and even the latest automobiles include integrated wireless NICs that incorporate a radio transmitter/receiver. However, if a device does not have an integrated wireless NIC, then a USB wireless adapter can be used.

USB Wireless Adapter

12.2.3 Wireless Home Router

The type of infrastructure device that an end device associates and authenticates with varies based on the size and requirement of the WLAN.

For example, a home user typically interconnects wireless devices using a small, wireless router. The wireless router serves as an:

* Access point - This provides 802.11a/b/g/n/ac wireless access.
* Switch - This provides a four-port, full-duplex, 10/100/1000 Ethernet switch to interconnect wired devices.
* Router - This provides a default gateway for connecting to other network infrastructures, such as the internet

A wireless router is commonly implemented as a small business or residential wireless access device. The wireless router advertises its wireless services by sending beacons containing its shared service set identifier (SSID). Devices wirelessly discover the SSID and attempt to associate and authenticate with it to access the local network and internet.

Most wireless routers also provide advanced features, such as high-speed access, support for video streaming, IPv6 addressing, quality of service (QoS), configuration utilities, and USB ports to connect printers or portable drives.

Additionally, home users who want to extend their network services can implement Wi-Fi range extenders. A device can connect wirelessly to the extender, which boosts its communications to be repeated to the wireless router.

12.2.4 Wireless Access Points

While range extenders are easy to set up and configure, the best solution would be to install another wireless access point to provide dedicated wireless access to the user devices. Wireless clients use their wireless NIC to discover nearby APs advertising their SSID. Clients then attempt to associate and authenticate with an AP. After being authenticated, wireless users have access to network resources.

12.2.5 AP Categories

Autonomous APs

These are standalone devices configured using a command line interface or a GUI. Autonomous APs are useful in situations where only a couple of APs are required in the organization. A home router is an example of an autonomous AP because the entire AP configuration resides on the device. If the wireless demands increase, more APs would be required. Each AP would operate independent of other APs and each AP would require manual configuration and management. This would become overwhelming if many APs were needed.

Controller-based APs

These devices require no initial configuration and are often called lightweight APs (LAPs). LAPs use the Lightweight Access Point Protocol (LWAPP) to communicate with a WLAN controller (WLC). Controller-based APs are useful in situations where many APs are required in the network. As more APs are added, each AP is automatically configured and managed by the WLC.

12.2.6 Wireless Antennas

Omnidirectional antennas provide 360-degree coverage and are ideal in houses, open office areas, conference rooms, and outside areas.

Directional antennas focus the radio signal in a given direction. This enhances the signal to and from the AP in the direction the antenna is pointing This provides a stronger signal strength in one direction and reduced signal strength in all other directions.

Multiple Input Multiple Output (MIMO) uses multiple antennas to increase available bandwidth for IEEE 802.11n/ac/ax wireless networks. Up to eight transmit and receive antennas can be used to increase throughput.

12.3 WLAN Operation

Ad hoc mode - This is when two devices connect wirelessly in a peer-to-peer (P2P) manner without using APs or wireless routers. Examples include wireless clients connecting directly to each other using Bluetooth or Wi-Fi Direct. The IEEE 802.11 standard refers to an ad hoc network as an independent basic service set (IBSS).

Infrastructure mode - This is when wireless clients interconnect via a wireless router or AP, such as in WLANs. APs connect to the network infrastructure using the wired distribution system, such as Ethernet.

Tethering - A variation of the ad hoc topology is when a smart phone or tablet with cellular data access is enabled to create a personal hotspot. This feature is sometimes referred to as tethering. A hotspot is usually a temporary quick solution that enables a smart phone to provide the wireless services of a Wi-Fi router. Other devices can associate and authenticate with the smart phone to use the internet connection.

12.3.3 BSS and ESS

Infrastructure mode defines two topology building blocks: A Basic Service Set (BSS) and an Extended Service Set (ESS).

Basic Service Set

A BSS consists of a single AP interconnecting all associated wireless clients. Basic Service Area (BSA) - If a wireless client moves out of its BSA, it can no longer directly communicate with other wireless clients within the BSA.

The Layer 2 MAC address of the AP is used to uniquely identify each BSS, which is called the Basic Service Set Identifier (BSSID). Therefore, the BSSID is the formal name of the BSS and is always associated with only one AP.

Extended Service Set

When a single BSS provides insufficient coverage, two or more BSSs can be joined through a common distribution system (DS) into an ESS. An ESS is the union of two or more BSSs interconnected by a wired DS. Each ESS is identified by a SSID and each BSS is identified by its BSSID.

Wireless clients in one BSA can now communicate with wireless clients in another BSA within the same ESS. Roaming mobile wireless clients may move from one BSA to another (within the same ESS) and seamlessly connect.

12.3.4 802.11 Frame Structure

All 802.11 wireless frames contain the following fields:

Frame Control - This identifies the type of wireless frame and contains subfields for protocol version, frame type, address type, power management, and security settings.

Duration - This is typically used to indicate the remaining duration needed to receive the next frame transmission.

From a wireless device:

* Address 1 Receiver Address - MAC address of the AP.
* Address 2 Transmitter Address - MAC address of the sender.
* Address 3 SA/DA/BSSID - MAC address of the destination which could be a wireless device or wired device.

From the AP:

* Address 1 Receiver Address - MAC address of the sender.
* Address 2 Transmitter Address - MAC address of the AP.
* Address 3 SA/DA/BSSID - MAC address of the wireless destination.
* Sequence Control - This contains information to control sequencing and fragmented frames.
* Address4 - This usually missing because it is used only in ad hoc mode.
* Payload - This contains the data for transmission.
* FCS - This is used for Layer 2 error control.

12.3.5 CSMA/CA

WLANs are half-duplex, shared media configurations. Half-duplex means that only one client can transmit or receive at any given moment. Shared media means that wireless clients can all transmit and receive on the same radio channel. This creates a problem because a wireless client cannot hear while it is sending, which makes it impossible to detect a collision.

To resolve this problem, WLANs use carrier sense multiple access with collision avoidance (CSMA/CA) as the method to determine how and when to send data on the network. A wireless client does the following:

* Listens to the channel to see if it is idle, which means that is senses no other traffic is currently on the channel. The channel is also called the carrier.
* Sends a request to send (RTS) message to the AP to request dedicated access to the network.
* Receives a clear to send (CTS) message from the AP granting access to send.
* If the wireless client does not receive a CTS message, it waits a random amount of time before restarting the process.
* After it receives the CTS, it transmits the data.
* All transmissions are acknowledged. If a wireless client does not receive an acknowledgment, it assumes a collision occurred and restarts the process.

12.3.6 Wireless Client and AP Association

For wireless devices to communicate over a network, they must first associate with an AP or wireless router. An important part of the 802.11 process is discovering a WLAN and subsequently connecting to it. Wireless devices complete the following three stage process

* Discover a wireless AP
* Authenticate with AP
* Associate with AP

In order to have a successful association, a wireless client and an AP must agree on specific parameters. Parameters must then be configured on the AP and subsequently on the client to enable the negotiation of a successful association.

* SSID -The SSID name appears in the list of available wireless networks on a client. In larger organizations that use multiple VLANs to segment traffic, each SSID is mapped to one VLAN. Depending on the network configuration, several APs on a network can share a common SSID.
* Password - This is required from the wireless client to authenticate to the AP.
* Network mode - This refers to the 802.11a/b/g/n/ac/ad WLAN standards. APs and wireless routers can operate in a Mixed mode meaning that they can simultaneously support clients connecting via multiple standards.
* Security mode - This refers to the security parameter settings, such as WEP, WPA, or WPA2. Always enable the highest security level supported.
* Channel settings - This refers to the frequency bands used to transmit wireless data. Wireless routers and APs can scan the radio frequency channels and automatically select an appropriate channel setting. The channel can also be set manually if there is interference with another AP or wireless device.

12.3.7 Passive and Active Discover Mode

In passive mode, the AP openly advertises its service by periodically sending broadcast beacon frames containing the SSID, supported standards, and security settings. The primary purpose of the beacon is to allow wireless clients to learn which networks and APs are available in a given area. This allows the wireless clients to choose which network and AP to use.

In active mode, wireless clients must know the name of the SSID. The wireless client initiates the process by broadcasting a probe request frame on multiple channels. The probe request includes the SSID name and standards supported. APs configured with the SSID will send a probe response that includes the SSID, supported standards, and security settings. Active mode may be required if an AP or wireless router is configured to not broadcast beacon frames.

A wireless client could also send a probe request without a SSID name to discover nearby WLAN networks. APs configured to broadcast beacon frames would respond to the wireless client with a probe response and provide the SSID name. APs with the broadcast SSID feature disabled do not respond.

Quiz

Question 1

Which wireless topology mode is used by two devices to connect in a peer-to-peer network?

Ad hoc

Question 2

True or False: An ESS is created when two or more BSSs need to be joined to support roaming clients.

True

Question 3

How many address fields are in the 802.11 wireless frame?

4

Question 4

What is the term for an AP that openly advertises its service periodically?

Passive

Question 5

What is the term for an AP that does not send a beacon, but waits for clients to send probes?

Active

12.4 CAPWAP Operation

CAPWAP (Control and Provisioning of Wireless Access Points) is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANs. CAPWAP is also responsible for the encapsulation and forwarding of WLAN client traffic between an AP and a WLC.

CAPWAP is based on LWAPP (Lightweight Access Point Protocol, is a protocol that facilitates communication between wireless access points (APs) and a central Wireless LAN Controller (WLC). Developed by Cisco, LWAPP allows APs to operate in "lightweight" mode, meaning the APs handle only basic functions like forwarding data, while all configuration, management, and security settings are managed centrally by the WLC. ) but adds additional security with Datagram Transport Layer Security (DTLS). CAPWAP establishes tunnels on User Datagram Protocol (UDP) ports. CAPWAP can operate either over IPv4 or IPv6.

IPv4 and IPv6 both use UDP ports 5246 and 5247. Port 5246 is for CAPWAP control messages used by the WLC to manage the AP. Port 5247 is used by CAPWAP to encapsulate data packets traveling to and from wireless clients. However, CAPWAP tunnels use different IP protocols in the packet header. IPv4 uses IP protocol 17 and IPv6 uses IP protocol 136.

12.4.3 Split MAC Architecture

A key component of CAPWAP is the concept of a split media access control (MAC). The CAPWAP split MAC concept does all of the functions normally performed by individual APs and distributes them between two functional components:

* AP MAC Functions
* WLC MAC Functions

AP MAC Functions

* Beacons and probe responses
* Packet acknowledgement and retransmissions
* Frame queuing and packet prioritization
* MAC layer data encryption and decryption.

WLC MAC Functions

* Authentication
* Association and re-association of roaming clients
* Frame translations to other protocols
* Termination of 802.11 traffic on a wired interface.

12.4.4 DTLS Encryption

DTLS is a protocol which provides security between the AP and the WLC. It allows them to communicate using encryption and prevents eavesdropping or tampering.

DTLS is enabled by default to secure the CAPWAP control channel but is disabled by default for the data channel, as shown in the figure. All CAPWAP management and control traffic exchanged between an AP and WLC is encrypted and secured by default to provide control plane privacy and prevent Man-In-the-Middle (MITM) attacks.

CAPWAP data encryption is optional and is enabled per AP. Data encryption requires a DTLS license to be installed on the WLC prior to being enabled on an AP. When enabled, all WLAN client traffic is encrypted at the AP before being forwarded to the WLC and vice versa.

12.4.5 FlexConnect APs

FlexConnect is a wireless solution for branch office and remote office deployments. It lets you configure and control access points in a branch office from the corporate office through a WAN link, without deploying a controller in each office.

There are two modes of operation for the FlexConnect AP.

* Connected mode - The WLC is reachable. In this mode the FlexConnect AP has CAPWAP connectivity with its WLC and can send traffic through the CAPWAP tunnel, as shown in the figure. The WLC performs all its CAPWAP functions.
* Standalone mode - The WLC is unreachable. The FlexConnect has lost or failed to establish CAPWAP connectivity with its WLC. In this mode, a FlexConnect AP can assume some of the WLC functions such as switching client data traffic locally and performing client authentication locally.

12.5 Channel Management

12.5.1 Frequency Channel Saturation

Wireless LAN devices have transmitters and receivers tuned to specific frequencies of radio waves to communicate. A common practice is for frequencies to be allocated as ranges. Such ranges are then split into smaller ranges called channels.

If the demand for a specific channel is too high, that channel is likely to become oversaturated. The saturation of the wireless medium degrades the quality of the communication. Over the years, a number of techniques have been created to improve wireless communication and alleviate saturation. These techniques mitigate channel saturation by using the channels in a more efficient way.

Direct-Sequence Spread Spectrum (DSSS) - This is a modulation technique designed to spread a signal over a larger frequency band. Spread spectrum techniques were developed during war time to make it more difficult for enemies to intercept or jam a communication signal. It does this by spreading the signal over a wider frequency which effectively hides the discernable peak of the signal, as shown in the figure. A properly configured receiver can reverse the DSSS modulation and re-construct the original signal. DSSS is used by 802.11b devices to avoid interference from other devices using the same 2.4 GHz frequency.

Frequency-Hopping Spread Spectrum (FHSS) - This relies on spread spectrum methods to communicate. It transmits radio signals by rapidly switching a carrier signal among many frequency channels. With the FHSS, the sender and receiver must be synchronized to “know” which channel to jump to. This channel hopping process allows for a more efficient usage of the channels, decreasing channel congestion. FHSS was used by the original 802.11 standard. Walkie-talkies and 900 MHz cordless phones also use FHSS, and Bluetooth uses a variation of FHSS.

Orthogonal Frequency-Division Multiplexing (OFDM) - This is a subset of frequency division multiplexing in which a single channel uses multiple sub-channels on adjacent frequencies. Sub-channels in an OFDM system are precisely orthogonal to one another which allow the sub-channels to overlap without interfering. OFDM is used by a number of communication systems including 802.11a/g/n/ac. The new 802.11ax uses a variation of OFDM called Orthogonal frequency-division multiaccess (OFDMA).

Quiz

Question 1

Which of the following modulation techniques rapidly switches a signal among frequency channels?

FHSS

Question 2

Which of the following modulation techniques spreads a signal over a larger frequency band?

DSSS

OFDMA

Question 3

Which of the following modulation techniques is used in the new 802.11ax standard?

OFDMA

Question 4

How many channels are available for the 2.4 GHz band in Europe?

13

Question 5

How many channels are available for the 5 GHz band?

24

12.6 WLAN **Threats**

Attacks can be generated by outsiders, disgruntled employees, and even unintentionally by employees. Wireless networks are specifically susceptible to several threats, including:

* Interception of data - Wireless data should be encrypted to prevent it from being read by eavesdroppers.
* Wireless intruders - Unauthorized users attempting to access network resources can be deterred through effective authentication techniques.
* Denial of Service (DoS) Attacks - Access to WLAN services can be compromised either accidentally or maliciously. Various solutions exist depending on the source of the DoS attack.
* Rogue APs - Unauthorized APs installed by a well-intentioned user or for malicious purposes can be detected using management software.

12.6.3 DoS Attacks

Wireless DoS attacks can be the result of:

* Improperly configured devices - Configuration errors can disable the WLAN. For instance, an administrator could accidently alter a configuration and disable the network, or an intruder with administrator privileges could intentionally disable a WLAN.
* A malicious user intentionally interfering with the wireless communication - Their goal is to disable the wireless network completely or to the point where no legitimate device can access the medium.
* Accidental interference - WLANs are prone to interference from other wireless devices including microwave ovens, cordless phones, baby monitors, and more, as shown in the figure. The 2.4 GHz band is more prone to interference than the 5 GHz band.

To minimize the risk of a DoS attack due to improperly configured devices and malicious attacks, harden all devices, keep passwords secure, create backups, and ensure that all configuration changes are incorporated off-hours.

Monitor the WLAN for any accidental interference problems and address them as they appear. Because the 2.4 GHz band is used by other devices types, the 5 GHz should be used in areas prone to interference.

12.6.4 Rogue Access Points

A rogue AP is an AP or wireless router that has been connected to a corporate network without explicit authorization and against corporate policy. Anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network resource.

Once connected, the rogue AP can be used by an attacker to capture MAC addresses, capture data packets, gain access to network resources, or launch a man-in-the-middle attack.

A personal network hotspot could also be used as a rogue AP. For example, a user with secure network access enables their authorized Windows host to become a Wi-Fi AP. Doing so circumvents the security measures and other unauthorized devices can now access network resources as a shared device.

12.6.5 Man-in-the-Middle Attack

In a man-in-the-middle (MITM) attack, the hacker is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties. There are many ways in which to create a MITM attack.

A popular wireless MITM attack is called the “evil twin AP” attack, where an attacker introduces a rogue AP and configures it with the same SSID as a legitimate AP.

12.7 Secure WLANs

12.7.2 SSID Cloaking and MAC Address Filtering

Wireless signals can travel through solid matter, such as ceilings, floors, walls, outside of the home, or office space. Without stringent security measures in place, installing a WLAN can be the equivalent of putting Ethernet ports everywhere, even outside.

To address the threats of keeping wireless intruders out and protecting data, two early security features were used and are still available on most routers and APs: SSID cloaking and MAC address filtering.

SSID Cloaking

APs and some wireless routers allow the SSID beacon frame to be disabled. Wireless clients must manually configure the SSID to connect to the network.

MAC Addresses Filtering

An administrator can manually permit or deny clients wireless access based on their physical MAC hardware address. Devices with different MAC addresses will not be able to join the 2.4GHz WLAN.

12.7.3 802.11 Original Authentication Methods

Although these two features would deter most users, the reality is that neither SSID cloaking nor MAC address filtering would deter a crafty intruder. SSIDs are easily discovered even if APs do not broadcast them and MAC addresses can be spoofed. The best way to secure a wireless network is to use authentication and encryption systems.

Two types of authentication were introduced with the original 802.11 standard:

* Open system authentication- Any wireless client should easily be able to connect and should only be used in situations where security is of no concern, such as those providing free internet access like cafes, hotels, and in remote areas. The wireless client is responsible for providing security such as using a virtual private network (VPN) to connect securely. VPNs provide authentication and encryption services. VPNs are beyond the scope of this topic.
* Shared key authentication- Provides mechanisms, such as WEP, WPA, WPA2, and WPA3 to authenticate and encrypt data between a wireless client and AP. However, the password must be pre-shared between both parties to connect.

12.7.5 Authenticating a Home User

Home routers typically have two choices for authentication: WPA and WPA2. WPA2 is the stronger of the two.

Personal - Intended for home or small office networks, users authenticate using a pre-shared key (PSK). Wireless clients authenticate with the wireless router using a pre-shared password. No special authentication server is required.

Enterprise - Intended for enterprise networks but requires a Remote Authentication Dial-In User Service (RADIUS) authentication server. Although more complicated to set up, it provides additional security. The device must be authenticated by the RADIUS server and then users must authenticate using 802.1X standard, which uses the Extensible Authentication Protocol (EAP) for authentication.

12.7.6 Encryption Methods

Encryption is used to protect data. If an intruder has captured encrypted data, they would not be able to decipher it in any reasonable amount of time.

The WPA and WPA2 standards use the following encryption protocols:

Temporal Key Integrity Protocol (TKIP) - TKIP is the encryption method used by WPA. It provides support for legacy WLAN equipment by addressing the original flaws associated with the 802.11 WEP encryption method. It makes use of WEP, but encrypts the Layer 2 payload using TKIP, and carries out a Message Integrity Check (MIC) in the encrypted packet to ensure the message has not been altered.

Advanced Encryption Standard (AES) - AES is the encryption method used by WPA2. It is the preferred method because it is a far stronger method of encryption. It uses the Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) that allows destination hosts to recognize if the encrypted and non-encrypted bits have been altered.

12.7.7 Authentication in the Enterprise

In networks that have stricter security requirements, an additional authentication or login is required to grant wireless clients such access. The Enterprise security mode choice requires an Authentication, Authorization, and Accounting (AAA) RADIUS server.

RADIUS Server IP address - This is the reachable address of the RADIUS server.

UDP port numbers - Officially assigned UDP ports 1812 for RADIUS Authentication, and 1813 for RADIUS Accounting, but can also operate using UDP ports 1645 and 1646.

Shared key - Used to authenticate the AP with the RADIUS server.

The shared key is not a parameter that must be configured on a wireless client. It is only required on the AP to authenticate with the RADIUS server. User authentication and authorization is handled by the 802.1X standard, which provides a centralized, server-based authentication of end users.

The 802.1X login process uses EAP to communicate with the AP and RADIUS server. EAP is a framework for authenticating network access. It can provide a secure authentication mechanism and negotiate a secure private key which can then be used for a wireless encryption session using TKIP or AES encryption.

12.7.8 WPA3

At the time of this writing, devices that support WPA3 authentication were not readily available. However, WPA2 is no longer considered secure. WPA3, if available, is the recommended 802.11 authentication method. WPA3 includes four features:

* WPA3-Personal
* WPA3-Enterprise
* Open Networks
* Internet of Things (IoT) Onboarding
* WPA3-Personal

In WPA2-Personal, threat actors can listen in on the “handshake” between a wireless client and the AP and use a brute force attack to try and guess the PSK. WPA3-Personal thwarts this attack by using Simultaneous Authentication of Equals (SAE), a feature specified in the IEEE 802.11-2016. The PSK is never exposed, making it impossible for the threat actor to guess.

WPA3-Enterprise

WPA3-Enterprise still uses 802.1X/EAP authentication. However, it requires the use of a 192-bit cryptographic suite and eliminates the mixing of security protocols for previous 802.11 standards. WPA3-Enterprise adheres to the Commercial National Security Algorithm (CNSA) Suite which is commonly used in high security Wi-Fi networks.

Open Networks

Open networks in WPA2 send user traffic in unauthenticated, clear text. In WPA3, open or public Wi-Fi networks still do not use any authentication. However, they do use Opportunistic Wireless Encryption (OWE) to encrypt all wireless traffic.yu

IoT Onboarding

Although WPA2 included Wi-Fi Protected Setup (WPS) to quickly onboard devices without configuring them first, WPS is vulnerable to a variety of attacks and is not recommended. Furthermore, IoT devices are typically headless, meaning they have no built-in GUI for configuration, and needed any easy way to get connected to the wireless network. The Device Provisioning Protocol (DPP) was designed to address this need. Each headless device has a hardcoded public key. The key is typically stamped on the outside of the device or its packaging as a Quick Response (QR) code. The network administrator can scan the QR code and quickly onboard the device. Although not strictly part of the WPA3 standard, DPP will replace WPS over time.

Quiz

Question 1

What are the best ways to secure WLANs? (Choose two.)

Authentication

Encryption

Question 2

Which of the following authentication methods does not use a password shared between the wireless client and the AP?

Open

Question 3

Which encryption method is used by the original 802.11 specification?

RC4

Question 4

Which of the following encryption methods uses CCMP to recognize if the encrypted and non-encrypted bits have been altered?

AES

Question 5

Which of the following authentication methods has the user enter a pre-shared password? (Choose two)

WPA Personal

WPA2 Personal

12.8.2 Module Quiz - WLAN Concepts

Question 1

In the context of mobile devices, what does the term tethering involve?

Connecting a mobile device to another mobile device or computer to share a network connection

Topic 12.3.0 - Tethering allows a laptop or PC to use the Internet connection of a mobile device such as a cell phone, usually through a cellular data connection. This allows devices to connect to the Internet in locations where there is no Wi-Fi or cabled connection, but where there is still a cellular data connection.

Question 2

Which feature of 802.11n wireless access points allows them to transmit data at faster speeds than previous versions of 802.11 Wi-Fi standards did?

MIMO

Topic 12.2.0 - Multiple-input multiple-output (MIMO) technology allows 802.11n devices to use multiple antennas in order to increase the available bandwidth for the wireless network. Single Point Setup (SPS) is a Cisco technology that makes AP deployment easier by supporting clustering from a single management interface. Wi-Fi Protected Setup (WPS) is used to simplify connecting clients to secure wireless networks. Man-in-the-middle (MITM) is a type of security attack where the attacker attempts to insert themselves into the middle of a data stream.

Question 3

Which method of wireless authentication is currently considered to be the strongest?

WPA2

Topic 12.7.0 - WPA2 can use the AES encryption standard, which is currently the strongest method of encrypting wireless data.

Question 4

Which parameter is commonly used to identify a wireless network name when a home wireless AP is being configured?

SSID

Topic 12.3.0 - The SSID is used to name a wireless network. This parameter is required in order for a wireless client to attach to a wireless AP.

Question 5

Which characteristic describes a wireless client operating in active mode?

Must know the SSID to connect to an AP

Topic 12.3.0 - A wireless client operating in active mode must know the name of the SSID. Probe requests are broadcast by a client across multiple channels and include the SSID name and supported standards. Active mode is used if an AP is configured to not broadcast beacon frames.

Question 6

Which IEEE standard operates at wireless frequencies in both the 5 GHz and 2.4 GHz ranges?

802.11n

Topic 12.1.0 - The 802.11n standard is backwards compatible with both the 802.11a and 802.11b standards and therefore operates at both 5 GHz and 2.4 GHz.

Question 7

Which statement describes an autonomous access point?

It is a standalone access point.

Topic 12.2.0 - An autonomous access point is used in environments that require a small number of access points. As network demands increase, more access points can be added to the environment with each access point acting independently of another. An autonomous access point can be configured using either a GUI or CLI.

Question 8

Which two roles are typically performed by a wireless router that is used in a home or small business? (Choose two.)

Access point

Ethernet switch

Topic 12.2.0 - In addition to its roles as router, a typical SOHO wireless router acts as both a wireless access point and an Ethernet switch. RADIUS authentication is provided by an external server. A WLAN controller is used in enterprise deployments to manage groups of lightweight access points. A repeater is a device that enhances an incoming signal and retransmits it.

Question 9

Which protocol and port numbers are used by both IPv4 and IPv6 CAPWAP tunnels? (Choose two.)

UDP

5246 and 5247

Topic 12.4.0 -

CAPWAP can operate either over IPv4 or IPv6 and can use UDP ports 5246 and 5247.

Question 10

If three 802.11b access points need to be deployed in close proximity, which three frequency channels should be used? (Choose three.)

1

6

11

Topic 12.5.0 - In order to minimize interference, one of the three non-overlapping channels should be used in 2.4GHz Wi-Fi networks: 1, 6, or 11.

Question 11

Which type of telecommunication technology is used to provide Internet access to vessels at sea?

Satellite

Topic 12.1.0 - Internet access by means of satellites is available across the world. Temporary installations, airplanes in flight, and naval vessels benefit from the use of satellite internet. Municipal Wi-Fi, WiMax, and cellular technology are not able to support the mobile requirements of naval vessels and airplanes in transit.

Question 12

Which wireless network topology is being configured by a technician who is installing a keyboard, a mouse, and headphones, each of which uses Bluetooth?

Ad hoc mode

Topic 12.3.0 - Tethering enables a wireless device such as a phone to provide wireless Internet connectivity to other devices, thus creating a hotspot. Infrastructure mode is the type of wireless network that is created when an access point is being used. Mixed mode allows older wireless NICs to attach to an access point that can use a newer wireless standard.

Question 13

Which type of wireless topology is created when two or more Basic Service Sets are interconnected by Ethernet?

ESS

Topic 12.3.0 - Wireless devices operate in either ad hoc or infrastructure modes. An ad hoc WLAN, also referred to as an independent basic service set (IBISS), operates on a peer-to-peer basis without a network. Infrastructure modes can consist of a single Basic Service Set (BSS) with an AP interconnecting associated stations, or an Extended Service Set (ESS), with two or more BSSes interconnected over a wire distribution system such as Ethernet. WiFi Direct is a compatibility certification unrelated to WLAN topologies.

Question 14

What Wi-Fi management frame is regularly broadcast by APs to announce their presence?

Beacon

Topic 12.3.0 - Beacon frames are broadcast periodically by the AP to advertise its wireless networks to potential clients. Probing, association, and authentication frames are only sent when a client is associating to the AP.

Checkpoint Exam

Question 1

Which access control component, implementation, or protocol audits what users actions are performed on the network?

Accounting

Question 2

While attending a conference, participants are using laptops for network connectivity. When a guest speaker attempts to connect to the network, the laptop fails to display any available wireless networks. The access point must be operating in which mode?

Active

Active is a mode used to configure an access point so that clients must know the SSID to connect to the access point. APs and wireless routers can operate in a mixed mode meaning that that multiple wireless standards are supported. Open is an authentication mode for an access point that has no impact on the listing of available wireless networks for a client. When an access point is configured in passive mode, the SSID is broadcast so that the name of wireless network will appear in the listing of available networks for clients.

Question 3

What two IEEE 802.11 wireless standards operate only in the 5 GHz range? (Choose two.)

802.11a

802.11ac

The 802.11a and 802.11ac standards operate only in the 5 GHZ range. The 802.11b and 802.11g standards operate only in the 2.4 GHz range. The 802.11n standard operates in both the 2.4 and 5 GHz ranges. The 802.11ad standard operates in the 2.4, 5, and 60 GHz ranges.

Question 4

A network administrator is configuring DAI on a switch with the command ip arp inspection validate src-mac. What is the purpose of this configuration command?

It checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body.

DAI can be configured to check for both destination or source MAC and IP addresses:

Destination MAC - Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body.

Source MAC - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body.

IP address - Checks the ARP body for invalid and unexpected IP addresses including addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Question 5

A technician is configuring the channel on a wireless router to either 1, 6, or 11. What is the purpose of adjusting the channel?

To avoid interference from nearby wireless devices

Channels 1, 6, and 11 are selected because they are 5 channels apart. thus minimizing the interference with adjacent channels. A channel frequency can interfere with channels on either side of the main frequency. All wireless devices need to be used on nonadjacent channels.

Question 6

What is the result of a DHCP starvation attack?

Legitimate clients are unable to lease IP addresses.

DCHP starvation attacks are launched by an attacker with the intent to create a DoS for DHCP clients. To accomplish this goal, the attacker uses a tool that sends many DHCPDISCOVER messages to lease the entire pool of available IP addresses, thus denying them to legitimate hosts.

Question 7

Which type of VLAN-hopping attack may be prevented by designating an unused VLAN as the native VLAN?

VLAN double-tagging

Spoofing DTP messages forces a switch into trunking mode as part of a VLAN-hopping attack, but VLAN double tagging works even if trunk ports are disabled. Changing the native VLAN from the default to an unused VLAN reduces the possibility of this type of attack. DHCP spoofing and DHCP starvation exploit vulnerabilities in the DHCP message exchange.​

Question 8

A network administrator of a college is configuring the WLAN user authentication process. Wireless users are required to enter username and password credentials that will be verified by a server. Which server would provide such service?

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a protocol and server software that provides user-based authentication for an organization. When a WLAN is configured to use a RADIUS server, users will enter username and password credentials that are verified by the RADIUS server before allowing to the WLAN.

Question 9

Which authentication method stores usernames and passwords in the router and is ideal for small networks?

Local AAA

In a small network with a few network devices, AAA authentication can be implemented with the local database and with usernames and passwords stored on the network devices. Authentication using the TACACS+ or RADIUS protocol will require dedicated ACS servers although this authentication solution scales well in a large network.

Question 10

As part of the new security policy, all switches on the network are configured to automatically learn MAC addresses for each port. All running configurations are saved at the start and close of every business day. A severe thunderstorm causes an extended power outage several hours after the close of business. When the switches are brought back online, the dynamically learned MAC addresses are retained. Which port security configuration enabled this?

Sticky secure MAC addresses

With sticky secure MAC addressing, the MAC addresses can be either dynamically learned or manually configured and then stored in the address table and added to the running configuration file. In contrast, dynamic secure MAC addressing provides for dynamically learned MAC addressing that is stored only in the address table.

Question 11

The company handbook states that employees cannot have microwave ovens in their offices. Instead, all employees must use the microwave ovens located in the employee cafeteria. What wireless security risk is the company trying to avoid?

Accidental interference

Denial of service attacks can be the result of improperly configured devices which can disable the WLAN. Accidental interference from devices such as microwave ovens and cordless phones can impact both the security and performance of a WLAN. Man-in-the-middle attacks can allow an attacker to intercept data. Rogue access points can allow unauthorized users to access the wireless network.

Question 12

A technician is troubleshooting a slow WLAN that consists of 802.11b and 802.11g devices. A new 802.11n/ac dual-band router has been deployed on the network to replace the old 802.11g router. What can the technician do to address the slow wireless speed?

Split the wireless traffic between the 802.11n 2.4 GHz band and the 5 GHz band.

Splitting the wireless traffic between the 802.11n 2.4 GHz band and the 5 GHz band will allow for the 802.11n to use the two bands as two separate wireless networks to help manage the traffic, thus improving wireless performance.

Question 13

A laptop cannot connect to a wireless access point. Which two troubleshooting steps should be taken first? (Choose two.)

Ensure that the wireless SSID is chosen.

Ensure that the wireless NIC is enabled.

A wireless laptop normally does not have an antenna attached unless a repair has recently been implemented. If the wireless NIC is enabled, the correct media, radio, will be used. When the NIC detects an access point, the correct frequency is automatically used.

Question 14

A network administrator is configuring port security on a Cisco switch. The company security policy specifies that when a violation occurs, packets with unknown source addresses should be dropped and no notification should be sent. Which violation mode should be configured on the interfaces?

Protect

On a Cisco switch, an interface can be configured for one of three violation modes, specifying the action to be taken if a violation occurs:

Protect - Packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased. There is no notification that a security violation has occurred.

Restrict - Packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased. In this mode, there is a notification that a security violation has occurred.

Shutdown - The interface immediately becomes error-disabled and the port LED is turned off.

Question 15

Which two Cisco solutions help prevent DHCP starvation attacks? (Choose two.)

DHCP Snooping

Port Security

Cisco provides solutions to help mitigate Layer 2 attacks including these:

IP Source Guard (IPSG) - prevents MAC and IP address spoofing attacks

Dynamic ARP Inspection (DAI) - prevents ARP spoofing and ARP poisoning attacks

DHCP Snooping - prevents DHCP starvation and SHCP spoofing attacks

Port Security - prevents many types of attacks including MAC table overflow attacks and DHCP starvation attacks

Web Security Appliance (WSA) is a mitigation technology for web-based threats.

Question 16

Which protocol can be used to monitor the network?

SNMP

Simple Network Management Protocol (SNMP) is used to monitor the network.

Question 17

Which type of management frame may regularly be broadcast by an AP?

Beacon

Beacons are the only management frame that may regularly be broadcast by an AP. Probing, authentication, and association frames are used only during the association (or reassociation) process.

Question 18

Which protocol should be used to mitigate the vulnerability of using Telnet to remotely manage network devices?

SSH

Telnet uses plain text to communicate in a network. The username and password can be captured if the data transmission is intercepted. SSH encrypts data communications between two network devices. TFTP and SCP are used for file transfer over the network. SNMP is used in network management solutions.

Question 19

What are three techniques for mitigating VLAN attacks? (Choose three.)

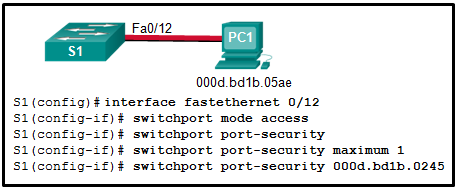
Disable DTP.

Enable trunking manually.

Set the native VLAN to an unused VLAN.

Mitigating a VLAN attack can be done by disabling Dynamic Trunking Protocol (DTP), manually setting ports to trunking mode, and by setting the native VLAN of trunk links to VLANs not in use.

Question 20



Refer to the exhibit. Port security has been configured on the Fa 0/12 interface of switch S1. What action will occur when PC1 is attached to switch S1 with the applied configuration?

Frames from PC1 will cause the interface to shut down immediately, and a log entry will be made.

Manual configuration of the single allowed MAC address has been entered for port fa0/12. PC1 has a different MAC address and when attached will cause the port to shut down (the default action), a log message to be automatically created, and the violation counter to increment. The default action of shutdown is recommended because the restrict option might fail if an attack is underway.

Question 21

What is the function provided by CAPWAP protocol in a corporate wireless network?

CAPWAP provides the encapsulation and forwarding of wireless user traffic between an access point and a wireless LAN controller.

Question 22

What are the two methods that are used by a wireless NIC to discover an AP? (Choose two.)

Receiving a broadcast beacon frame

Transmitting a probe request

Two methods can be used by a wireless device to discover and register with an access point: passive mode and active mode. In passive mode, the AP sends a broadcast beacon frame that contains the SSID and other wireless settings. In active mode, the wireless device must be manually configured for the SSID, and then the device broadcasts a probe request.

Question 23

A network administrator is working to improve WLAN performance on a dual-band wireless router. What is a simple way to achieve a split-the-traffic result?

Make sure that different SSIDs are used for the 2.4 GHz and 5 GHz bands.

By default, dual-band routers and APs use the same network name on both the 2.4 GHz band and the 5 GHz band. The simplest way to segment traffic is to rename one of the wireless networks.

Question 24

file\_download

PT Activity

Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.

Which event will take place if there is a port security violation on switch S1 interface Fa0/1?

Packets with unknown source addresses will be dropped.

The violation mode can be viewed by issuing the show port-security interface <int> command. Interface FastEthernet 0/1 is configured with the violation mode of protect. If there is a violation, interface FastEthernet 0/1 will drop packets with unknown MAC addresses.

Question 25

Which step is required before creating a new WLAN on a Cisco 3500 series WLC?

Create a new VLAN interface.

Each new WLAN configured on a Cisco 3500 series WLC needs its own VLAN interface. Thus it is required that a new VLAN interface to be created first before a new WLAN can be created.

Question 26

An IT security specialist enables port security on a switch port of a Cisco switch. What is the default violation mode in use until the switch port is configured to use a different violation mode?

Shutdown

If no violation mode is specified when port security is enabled on a switch port, then the security violation mode defaults to shutdown.

Question 27

Which component of AAA allows an administrator to track individuals who access network resources and any changes that are made to those resources?

Accounting

One of the components in AAA is accounting. After a user is authenticated through AAA, AAA servers keep a detailed log of exactly what actions the authenticated user takes on the device.

Question 28

Which service can be used on a wireless router to prioritize network traffic among different types of applications so that voice and video data are prioritized over email and web data?

QoS

Many wireless routers have an option for configuring quality of service (QoS). By configuring QoS, certain time-sensitive traffic types, such as voice and video, are prioritized over traffic that is not as time-sensitive, such as email and web browsing.

Question 29

A technician is about to install and configure a wireless network at a small branch office. What is the first security measure the technician should apply immediately upon powering up the wireless router?

Change the default user-name and password of the wireless router.

The first action a technician should do to secure a new wireless network is to change the default user-name and password of the wireless router. The next action would usually be to configure encryption. Then once the initial group of wireless hosts have connected to the network, MAC address filtering would be enabled and SSID broadcast disabled. This will prevent new unauthorized hosts from finding and connecting to the wireless network.

Question 30

Which type of wireless network is suitable for providing wireless access to a city or district?

Wireless metropolitan-area network

Question 31

Match each functional component of AAA with its description.

Authorization - Determines what resources users can access or the operations they are allowed to perform

Authentication - Proves that users are who they say they are

Accounting - Records what users do and what they access

Question 32

What device is considered a supplicant during the 802.1X authentication process?

The client that is requesting authentication

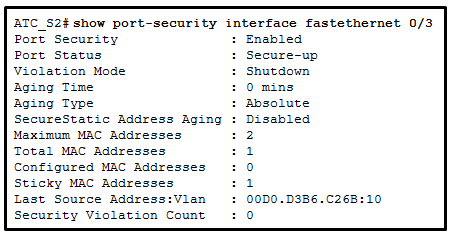
The devices involved in the 802.1X authentication process are as follows:

The supplicant, which is the client that is requesting network access

The authenticator, which is the switch that the client is connecting to and that is actually controlling physical network access

The authentication server, which performs the actual authentication

Question 33



Refer to the exhibit. What can be determined about port security from the information that is shown?

The port violation mode is the default for any port that has port security enabled.

The Port Security line simply shows a state of Enabled if the switchport port-security command (with no options) has been entered for a particular switch port. If a port security violation had occurred, a different error message appears such as Secure-shutdown. The maximum number of MAC addresses supported is 50. The Maximum MAC Addresses line is used to show how many MAC addresses can be learned (2 in this case). The Sticky MAC Addresses line shows that only one device has been attached and learned automatically by the switch. This configuration could be used when a port is shared by two cubicle-sharing personnel who bring in separate laptops.