### **Switching, Routing and Wireless Essentials**

**Module 1**

**Configure a Switch with Initial Settings**

After a Cisco switch is powered on, it goes through a five-step boot sequence. The BOOT environment variable is set using the **boot system** global configuration mode command. The IOS is located in a distinct folder and the folder path is specified. Use the switch LEDs to monitor switch activity and performance: SYST, RPS, STAT, DUPLX, SPEED, and PoE. The boot loader provides access into the switch if the operating system cannot be used because of missing or damaged system files. The boot loader has a command line that provides access to the files stored in flash memory. To prepare a switch for remote management access, the switch must be configured with an IP address and a subnet mask. To manage the switch from a remote network, the switch must be configured with a default gateway. To configure the switch SVI, you must first configure the management interface, then configure the default gateway, and finally, verify your configuration.

**Configure Switch Ports**

Full-duplex communication increases effective bandwidth by allowing both ends of a connection to transmit and receive data simultaneously. Half-duplex communication is unidirectional. Switch ports can be manually configured with specific duplex and speed settings. Use auto negotiation when the speed and duplex settings of the device connecting to the port are unknown or may change. When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately. There are several **show** commands to use when verifying switch configurations. Use the **show running-config** command and the **show interfaces** command to verify a switch port configuration. The output from the **show interfaces** command is also useful for detecting common network access layer issues because it displays the line and data link protocol status. The reported input errors from the **show interfaces** command include: runt frames, giants, CRC errors, along with collisions and late collisions. Use **show interfaces** to determine if your network has no connection or a bad connection between a switch and another device.

**Secure Remote Access**

Telnet (using TCP port 23) 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 (using TCP port 22) is a secure protocol that provides an encrypted management connection to a remote device. SSH provides security for remote connections by providing strong encryption when a device is authenticated (username and password) and also for the transmitted data between the communicating devices. 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 features and capabilities. To configure SSH you must verify that the switch supports it, configure the IP domain, generate RSA key pairs, configure use authentication, configure the VTY lines, and enable SSH version 2. To verify that SSH is operational, use the **show ip ssh** command to display the version and configuration data for SSH on the device.

**Basic Router Configuration**

The following initial configuration tasks should always be performed: name the device to distinguish it from other routers and configure passwords, configure a banner to provide legal notification of unauthorized access, and save the changes on a router. One distinguishing feature between switches and routers is the type of interfaces supported by each. For example, Layer 2 switches support LANs and, therefore, have multiple Fast Ethernet or Gigabit Ethernet ports. The dual stack topology is used to demonstrate the configuration of router IPv4 and IPv6 interfaces. Routers support LANs and WANs and can interconnect different types of networks; therefore, they support many types of interfaces. For example, G2 ISRs have one or two integrated Gigabit Ethernet interfaces and High-Speed WAN Interface Card (HWIC) slots to accommodate other types of network interfaces, including serial, DSL, and cable interfaces. The IPv4 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.

**Verify Directly Connected Networks**

Use the following commands to quickly identify the status of an interface: **show ip interface brief** and **show ipv6 interface brief** to see summary all interfaces (IPv4 and IPv6 addresses and operational status), **show running-config interface interface-id** to see the commands applied to a specified interface, and **show ip route** and **show ipv6 route** to see the contents of the IPv4 or IPv6 routing table stored in RAM. The output of the **show ip interface brief** and **show ipv6 interface brief** commands can be used to quickly reveal the status of all interfaces on the router. The **show ipv6 interface gigabitethernet 0/0/0** command displays the interface status and all of the IPv6 addresses belonging to the interface. Along with the link local address and global unicast address, the output includes the multicast addresses assigned to the interface. The output of the **show running-config interface** command displays the current commands applied to a specified interface. The **show interfaces** command displays interface information and packet flow count for all interfaces on the device. Verify interface configuration using the **show ip interface** and **show ipv6 interface** commands, which display the IPv4 and IPv6 related information for all interfaces on a router. Verify routes using the **show ip route** and **show ipv6 route** commands. Filter show command output using the pipe (|) character. Use filter expressions: section, include, exclude, and begin. By default, command history is enabled, and the system captures the last 10 command lines in its history buffer. Use the **show history** privileged EXEC command to display the contents of the buffer.

**Module 2**

**Frame Forwarding**

The decision on how a switch forwards traffic is based on the flow of that traffic. The term ingress describes the port where a frame enters a device. The term egress describes the port that frames will use when leaving the device. An Ethernet frame will never be forwarded out the port where it entered. For a switch to know which port to use to transmit a frame, it must first learn which devices exist on each port. As the switch learns the relationship of ports to devices, it builds a table called a MAC address table. Every frame that enters a switch is checked for new information to learn by examining the source MAC address of the frame and port number where the frame entered the switch. If the destination MAC address 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. Switch forwarding methods include store-and-forward and cut-through. Store-and-forward uses error-checking and automatic buffering. Cut-through does not error check. Instead it performs rapid frame switching. This means the switch can make a forwarding decision as soon as it has looked up the destination MAC address of the frame in its MAC address table.

**Switching Domains**

If an Ethernet switch port is operating in half-duplex, each segment is in its own collision domain. There are no collision domains when switch ports are operating in full-duplex. By default, Ethernet switch ports will autonegotiate full-duplex when the adjacent device can also operate in full-duplex. A collection of interconnected switches forms a single broadcast domain. Only a network layer device, such as a router, can divide a Layer 2 broadcast domain. The Layer 2 broadcast domain is referred to as the MAC broadcast domain. The MAC broadcast domain consists of all devices on the LAN that receive broadcast frames from a host. When a switch receives a broadcast frame, it forwards the frame out each of its ports, except the ingress port where the broadcast frame was received. Each device connected to the switch receives a copy of the broadcast frame and processes it. Switches can: interconnect LAN segments, use a MAC address table to determine egress ports, and can lessen or eliminate collisions entirely. Characteristics of switches that alleviate network congestion are fast port speeds, fast internal switching, large frame buffers, and high port density.

**Module 3**

**Overview of VLANs**

Virtual LANs (VLANs) are a group of devices that can communicate as if each device was attached to the same cable. VLANs are based on logical instead of physical connections. Administrators use VLANs to segment networks based on factors such as function, team, or application. Each VLAN is considered a separate logical network. Any switch port can belong to a VLAN. A VLAN creates a logical broadcast domain that can span multiple physical LAN segments. VLANs improve network performance by separating large broadcast domains into smaller ones. Each VLAN in a switched network corresponds to an IP network; therefore, VLAN design must use a hierarchical network-addressing scheme. Types of VLANs include the default VLAN, data VLANs, the native VLAN, management VLANs. and voice VLANs.

**VLANs in a Multi-Switched Environment**

A VLAN trunk does not belong to a specific VLAN. It is a conduit for multiple VLANs between switches and routers. A VLAN trunk is a point-to-point link between two network devices that carries more than one VLAN. A VLAN trunk extends VLANs across an entire network. When VLANs are implemented on a switch, the transmission of unicast, multicast, and broadcast traffic from a host in a particular VLAN are restricted to the devices that are in that VLAN. VLAN tag fields include the type, user priority, CFI and VID. Some devices add a VLAN tag to native VLAN traffic. If an 802.1Q trunk port receives a tagged frame with the VID that is the same as the native VLAN, it drops the frame. A separate voice VLAN is required to support VoIP. QoS and security policies can be applied to voice traffic. Voice VLAN traffic must be tagged with an appropriate Layer 2 CoS priority value.

**VLAN Configuration**

Different Cisco Catalyst switches support various numbers of VLANs including normal range VLANs and extended range VLANs. When configuring normal range VLANs, the configuration details are stored in flash memory on the switch in a file called vlan.dat. Although it is not required, it is good practice to save running configuration changes to the startup configuration. After creating a VLAN, the next step is to assign ports to the VLAN. There are several commands for defining a port to be an access port and assigning it to a VLAN. VLANs are configured on the switch port and not on the end device. An access port can belong to only one data VLAN at a time. However, a port can also be associated to a voice VLAN. For example, a port connected to an IP phone and an end device would be associated with two VLANs: one for voice and one for data. After a VLAN is configured, VLAN configurations can be validated using Cisco IOS **show** commands. If the switch access port has been incorrectly assigned to a VLAN, then simply re-enter the **switchport access** **vlan** *vlan-id* interface configuration command with the correct VLAN ID. The **no vlan** *vlan-id* global configuration mode command is used to remove a VLAN from the switch vlan.dat file.

**VLAN Trunks**

A VLAN trunk is an OSI Layer 2 link between two switches that carries traffic for all VLANs. There are several commands to configure the interconnecting ports. To verify VLAN trunk configuration use the **show interfaces** *interface-ID* **switchport** command. Use the **no switchport trunk allowed vlan** and the **no switchport trunk native vlan** commands to remove the allowed VLANs and reset the native VLAN of the trunk.

**Dynamic Trunking Protocol**

An interface can be set to trunking or nontrunking, or to negotiate trunking with the neighbor interface. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which operates on a point-to-point basis only, between network devices. DTP is a Cisco proprietary protocol that manages trunk negotiation only if the port on the neighbor switch is configured in a trunk mode that supports DTP. To enable trunking from a Cisco switch to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration mode commands. The **switchport mode** command has additional options for negotiating the interface mode including access, dynamic auto, dynamic desirable, and trunk. To verify the current DTP mode, issue the **show dtp interface** command.

**Module 4**

**Inter-VLAN Routing Operation**

Hosts in one VLAN cannot communicate with hosts in another VLAN unless there is a router or a Layer 3 switch to provide routing services. Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN. Three options include legacy, router-on-a-stick, and Layer 3 switch using SVIs. Legacy used a router with multiple Ethernet interfaces. Each router interface was connected to a switch port in different VLANs. Requiring one physical router interface per VLAN quickly exhausts the physical interface capacity of a router. The ‘router-on-a-stick’ inter-VLAN routing method 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. The router interface is configured using subinterfaces to identify routable VLANs. The configured subinterfaces are software-based virtual interfaces, associated with a single physical Ethernet interface. The modern method is Inter-VLAN routing on a Layer 3 switch using SVIs. The SVI is created for a VLAN that exists on the switch. The SVI performs the same functions for the VLAN as a router interface. It provides Layer 3 processing for packets being sent to or from all switch ports associated with that VLAN.

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

To configure a switch with VLANs and trunking, complete the following steps: create and name the VLANs, create the management interface, configure access ports, and configure trunking ports. The router-on-a-stick method requires a subinterface to be created for each VLAN to be routed. A subinterface is created using the **interface** *interface\_id subinterface\_id* global configuration mode command. Each router subinterface must be assigned an IP address on a unique subnet for routing to occur. When all subinterfaces have been created, the physical interface must be enabled using the **no shutdown** interface configuration command. From a host, verify connectivity to a host in another VLAN using the **ping** command. Use **ping** to verify connectivity with the host and the switch. To verify and troubleshoot use the **show ip route**, **show ip interface brief**, **show interfaces**, and **show interfaces trunk** commands.

**Inter-VLAN Routing using Layer 3 Switches**

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. Capabilities of a Layer 3 switch include routing from one VLAN to another using multiple switched virtual interfaces (SVIs) and converting a Layer 2 switchport to a Layer 3 interface (i.e., a routed port). 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. To configure a switch with VLANS and trunking, complete the following steps: create the VLANS, create the SVI VLAN interfaces, configure access ports, and enable IP routing. From a host, verify connectivity to a host in another VLAN using the **ping** command. Next, verify connectivity with the host using the **ping** Windows host command. VLANs 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. The interface can be configured with an IPv4 configuration to connect to a router or another Layer 3 switch. To configure a Layer 3 switch to route with a router, follow these steps: configure the routed port, enable routing, configure routing, verify routing, and verify connectivity.

**Troubleshoot Inter-VLAN Routing**

There are a number of reasons why an inter-VAN configuration may not work. All are related to connectivity issues such as missing VLANs, switch trunk port issues, switch access port issues, and router configuration issues. A VLAN could be missing if it was not created, it was accidently deleted, or it is not allowed on the trunk link. Another issue for inter-VLAN routing includes misconfigured switch ports. In a legacy inter-VLAN solution, a misconfigured switch port could be caused when the connecting router port is not assigned to the correct VLAN. With a router-on-a-stick solution, the most common cause is a misconfigured trunk port. When a problem is suspected with a switch access port configuration, use **ping** and **show interfaces** *interface-id* **switchport** commands to identify the problem. Router configuration problems with router-on-a-stick configurations are usually related to subinterface misconfigurations. Verify the subinterface status using the **show ip interface brief** command.

**Module 5**

**Purpose of STP**

Redundant paths in a switched Ethernet network may cause both physical and logical Layer 2 loops. A Layer 2 loop can result in MAC address table instability, link saturation, and high CPU utilization on switches and end-devices. This results in the network becoming unusable. Unlike the Layer 3 protocols, IPv4 and IPv6, Layer 2 Ethernet does not include a mechanism to recognize and eliminate endlessly looping frames. Ethernet LANs require a loop-free topology with a single path between any two devices. STP is a loop-prevention network protocol that allows for redundancy while creating a loop-free Layer 2 topology. Without STP, Layer 2 loops can form, causing broadcast, multicast and unknown unicast frames to loop endlessly, bringing down a network. 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. STP is based on an algorithm invented by Radia Perlman. Her spanning tree algorithm (STA) creates a loop-free topology by selecting a single root bridge where all other switches determine a single least-cost path.

**STP Operations**

Using the STA, STP builds a loop-free topology in a four-step process: elect the root bridge, elect the root ports, elect designated ports, and elect alternate (blocked) ports. During STA and STP functions, switches use 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 BID that identifies the switch that sent the BPDU. The BID is involved in making many of the STA decisions including root bridge and port roles. The BID contains a priority value, the MAC address of the switch, and an extended system ID. The lowest BID value is determined by the combination of these three fields. The switch with the lowest BID will become the root bridge. Because the default BID is 32,768 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. When the root bridge has been elected for a given spanning tree instance, the STA determines 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. After the root bridge has been determined the STA algorithm selects the root port. The root port is the port closest to the root bridge in terms of overall cost, which is called the internal root path cost. After each switch selects a root port, switches will select designated ports. The designated port is a port on the segment (with two switches) that has the internal root path cost to the root bridge. 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 loops. When a switch has multiple equal-cost paths to the root bridge, the switch will determine a port using the following criteria: lowest sender BID, then the lowest sender port priority, and finally the lowest sender port ID. STP convergence requires three timers: the hello timer, the forward delay timer, and the max age timer. Port states are blocking, listening, learning, forwarding, and disabled. In 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.

**Evolution of STP.**

The term Spanning Tree Protocol and the acronym STP can be misleading. STP is often used to refer to the various implementations of spanning tree, such as RSTP and MSTP. RSTP is an evolution of STP that provides faster convergence than STP. RSTP port states are learning, forwarding and discarding. PVST+ is a Cisco enhancement of STP that provides a separate spanning tree instance for each VLAN configured in the network. PVST+ supports PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard, and loop guard. Cisco switches running IOS 15.0 or later, run PVST+ by default. Rapid PVST+ is a Cisco enhancement of RSTP that uses PVST+ and provides a separate instance of 802.1w per VLAN. When a switch port is configured with PortFast, that port transitions from blocking to forwarding state immediately, bypassing the STP listening and learning states and avoiding a 30 second delay. Use PortFast on access ports to allow devices connected to these ports, such as DHCP clients, to access the network immediately, rather than waiting for STP to converge on each VLAN. Cisco switches support a feature called BPDU guard which immediately puts the switch port in an error-disabled state upon receipt of any BPDU to protect against potential loops. Over the years, Ethernet LANs went from a few interconnected switches that were connected to a single router, to a sophisticated hierarchical network design. Depending on the implementation, Layer 2 may include not only the access layer, but also the distribution or even the core layers. These designs may include hundreds of switches, with hundreds or even thousands of VLANs. STP has adapted to the added redundancy and complexity with enhancements as part of RSTP and MSTP. Layer 3 routing allows for redundant paths and loops in the topology, without blocking ports. For this reason, some environments are transitioning to Layer 3 everywhere except where devices connect to the access layer switch.

**Module 6**

**EtherChannel Operation**

To increase bandwidth or redundancy, multiple links could be connected between devices. However, STP will block redundant links to prevent switching loops. EtherChannel is a link aggregation technology that allows redundant links between devices that will not be blocked by STP. EtherChannel groups multiple physical Ethernet links together into one single logical link. It provides fault-tolerance, load sharing, increased bandwidth, and redundancy between switches, routers, and servers. When an EtherChannel is configured, the resulting virtual interface is called a port channel. EtherChannel has several advantages, as well as some restrictions to implementation. EtherChannels can be formed through negotiation using one of two protocols, PAgP or LACP. These protocols allow ports with similar characteristics to form a channel through dynamic negotiation with adjoining switches. When an EtherChannel link is configured using Cisco-proprietary PAgP, PAgP packets are sent between EtherChannel-capable ports to negotiate the forming of a channel. Modes for PAgP are On, PAgP desirable, and PAgP auto. LACP 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. Modes for LACP are On, LACP active, and LACP passive.

**Configure EtherChannel**

The following guidelines and restrictions are useful for configuring EtherChannel:

* **EtherChannel support** - All Ethernet interfaces on all modules must support EtherChannel with no requirement that interfaces be physically contiguous, or on the same module.
* **Speed and duplex** - Configure all interfaces in an EtherChannel to operate at the same speed and in the same duplex mode.
* **VLAN match** - All interfaces in the EtherChannel bundle must be assigned to the same VLAN or be configured as a trunk.
* **Range of VLANs** - An EtherChannel supports the same allowed range of VLANs on all the interfaces in a trunking EtherChannel.

Configuring EtherChannel with LACP requires three steps:

**Step 1.** Specify the interfaces that compose the EtherChannel group using the interface range interface global configuration mode command.

**Step 2.** Create the port channel interface with the channel-group identifier mode active command in interface range configuration mode.

**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.

**Verify and Troubleshoot EtherChannel.**

There are a number of commands to verify an EtherChannel configuration including **show interfaces port-channel**, **show etherchannel summary**, **show etherchannel port-channel**, and **show interfaces etherchannel**. Common EtherChannel issues include the following:

* Assigned ports in the EtherChannel are not part of the same VLAN, or not configured as trunks. Ports with different native VLANs cannot form an EtherChannel.
* Trunking was configured on some of the ports that make up the EtherChannel, but not all of them.
* If the allowed range of VLANs is not the same, the ports do not form an EtherChannel even when PAgP is set to the auto or desirable mode.
* The dynamic negotiation options for PAgP and LACP are not compatibly configured on both ends of the EtherChannel.

**Module 7**

**DHCPv4 Concepts**

The DHCPv4 server dynamically assigns, or leases, an IPv4 address to a client from a pool of addresses for a limited period of time chosen by the server, or until the client no longer needs the address. The DHCPv4 lease process begins with the client sending message requesting the services of a DHCP server. If there is a DHCPv4 server that receives the message it will respond with an IPv4 address and possible other network configuration information. 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 the client boots (or otherwise wants to join a network), it begins a four-step process to obtain a lease: DHCPDISCOVER, then DHCPOFFER, then DHCPREQUEST, and finally DHCPACK. Prior to lease expiration, the client begins a two-step process to renew the lease with the DHCPv4 server: DHCPREQUEST then DHCPACK.

**Configure a Cisco IOS DHCPv4 Server**

A Cisco router running Cisco IOS software can be configured to act as a DHCPv4 server. Use the following steps to configure a Cisco IOS DHCPv4 server: exclude IPv4 addresses, define a DHCPv4 pool name, and configure the DHCPv4 pool. Verify your configuration using the **show running-config | section dhcp**, **show ip dhcp binding**, and **show ip dhcp server statistics** commands. The DHCPv4 service is enabled, by default. To disable the service, use the **no service dhcp** global configuration mode command. 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. A PC is attempting to acquire an IPv4 address from a DHCPv4 server using a broadcast message. If the router is not configured as a DHCPv4 server, it will not forward the broadcast. If the DHCPv4 server is located on a different network, the PC cannot receive an IP address using DHCP. The router must be configured to relay DHCPv4 messages to the DHCPv4 server. The network administrator releases all current IPv4 addressing information using the **ipconfig /release** command. Next, the network administrator attempts to renew the IPv4 addressing information with the **ipconfig /renew** command. A better solution is to configure R1 with the **ip helper-address** *address interface* configuration command. The network administrator can use the **show ip interface** command to verify the configuration. The PC is now able to acquire an IPv4 address from the DHCPv4 server as verified with the **ipconfig /all** command. 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

**Configure a DHCPv4 Client**

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. Home routers are typically already set to receive IPv4 addressing information automatically from the ISP. The internet connection type is set to Automatic Configuration - DHCP. This selection is used when the router is connected to a DSL or cable modem and acts as a DHCPv4 client, requesting an IPv4 address from the ISP.

**Module 8**

**IPv6 GUA Assignment**

On a router, an IPv6 global unicast addresses (GUA) is manually configured using the **ipv6 address** *ipv6-address/prefix-length* interface configuration command. When automatic IPv6 addressing is selected, the host will attempt to automatically obtain and configure IPv6 address information on the interface. The IPv6 link-local address is automatically created by the host when it boots and the Ethernet interface is active. By default, an IPv6-enabled router advertises its IPv6 information enabling a host to dynamically create or acquire its IPv6 configuration. The IPv6 GUA can be assigned dynamically using stateless and stateful services. 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:

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

**SLAAC**

The SLAAC method enables hosts to create their own unique IPv6 global unicast address without the services of a DHCPv6 server. SLAAC, which is stateless, uses ICMPv6 RA messages to provide addressing and other configuration information that would normally be provided by a DHCP server. SLAAC can be deployed as SLAAC only, or SLAAC with DHCPv6. To enable the sending of RA messages, a router must join the IPv6 all-routers group using the **ipv6 unicast-routing** global config command. Use the **show ipv6 interface** command to verify if a router is enabled. 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 to create its own IPv6 GUA using the prefix advertised in the RA. The O =0 and M=0 flags instructs the client to use the information in the RA message exclusively. 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. 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, or EUI-64. The 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 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.

**DHCPv6**

The host begins the DHCPv6 client/server communications after stateless DHCPv6 or stateful DHCPv6 is indicated in the RA. Server to client DHCPv6 messages use UDP destination port 546, while client to server DHCPv6 messages use UDP destination port 547. The stateless DHCPv6 option informs the client to use the information in the RA message for addressing, but additional configuration parameters are available from a DHCPv6 server. This is called stateless DHCPv6 because the server is not maintaining any client state information. 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. In stateful DHCPv6, 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. It is called stateful because the DHCPv6 server maintains IPv6 state information. 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.

**Configure DHCPv6 Server**

A Cisco IOS router can be configured to provide DHCPv6 server services as one of the following three types: DHCPv6 server, DHCPv6 client, or DHCPv6 relay agent. The stateless DHCPv6 server option requires that the router advertise the IPv6 network addressing information in RA messages. A router can also be a DHCPv6 client and get an IPv6 configuration from a DHCPv6 server. The stateful DHCP server option requires that the IPv6-enabled router tells the host to contact a DHCPv6 server to acquire all required IPv6 network addressing information. For a client router to be a DHCPv6 router, it needs to **have ipv6 unicast-routing** enabled and an IPv6 link-local address to send and receive IPv6 messages. Use the **show ipv6 dhcp pool** and **show ipv6 dhcp binding** commands to verify DHCPv6 operation on a router. 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 using the **ipv6 dhcp relay destination** *ipv6-address [interface-type interface-number]* command. This command is configured on the interface facing the DHCPv6 clients and specifies the DHCPv6 server address and egress interface to reach the server. The egress interface is only required when the next-hop address is an LLA. Verify the DHCPv6 relay agent is operational with the **show ipv6 dhcp interface** and **show ipv6 dhcp binding** commands.

**Module 9**

**First Hop Redundancy Protocols**

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. FHRP provides alternate default gateways in switched networks where two or more routers are connected to the same VLANs. One way to prevent a single point of failure at the default gateway, is to implement a virtual router. With a virtual router, multiple routers are configured to work together to present the illusion of a single router to the hosts on the LAN. When the active router fails, the redundancy protocol transitions the standby router to the new active router role. These are the steps that take place when the active router fails:

1. The standby router stops seeing Hello messages from the forwarding router.
2. The standby router assumes the role of the forwarding router.
3. Because the new forwarding router assumes both the IPv4 and MAC addresses of the virtual router, the host devices see no disruption in service.

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**

HSRP is a Cisco-proprietary FHRP designed to allow for transparent failover of a first-hop IP device. 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. The router with the highest HSRP priority will become the active router. 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. HSRP states include initial, learn, listen, speak, and standby.

**Module 10**

Endpoints are particularly susceptible to malware-related attacks that originate through email or web browsing, such as DDOS, date breaches, and malware. These endpoints have typically used traditional host-based security features, such as antivirus/antimalware, host-based firewalls, and host-based intrusion prevention systems (HIPSs). Endpoints are best protected by a combination of NAC, host-based AMP software, an email security appliance (ESA), and a web security appliance (WSA). Cisco WSA can perform blacklisting of URLs, URL-filtering, malware scanning, URL categorization, Web application filtering, and encryption and decryption of web traffic.

AAA controls who is permitted to access a network (authenticate), what they can do while they are there (authorize), and to audit what actions they performed while accessing the network (accounting). Authorization uses a set of attributes that describes the user’s access to the network. Accounting is combined with AAA authentication. The AAA server keeps a detailed log of exactly what the authenticated user does on the device. The IEEE 802.1X standard is a port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports.

If Layer 2 is compromised, then all layers above it are also affected. The first step in mitigating attacks on the Layer 2 infrastructure is to understand the underlying operation of Layer 2 and the Layer 2 solutions: Port Security, DHCP Snooping, DAI, and IPSG. These won’t work unless management protocols are secured.

MAC address flooding attacks bombard the switch with fake source MAC addresses until the switch MAC address table is full. At this point, the switch treats the frame as an unknown unicast and begins to flood all incoming traffic out all ports on the same VLAN without referencing the MAC table. The threat actor can now capture all of the frames sent from one host to another on the local LAN or local VLAN. The threat actor uses **macof** to rapidly generate many random source and destination MAC and IP. To mitigate MAC table overflow attacks, network administrators must implement port security.

A VLAN hopping attack 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.

A VLAN double-tagging attack is unidirectional and works only when the threat actor is connected to a port residing in the same VLAN as the native VLAN of the trunk port. Double tagging allows the threat actor to send data to hosts or servers on a VLAN that otherwise would be blocked by some type of access control configuration. Return traffic will also be permitted, letting the threat actor communicate with devices on the normally blocked VLAN.

VLAN hopping and VLAN double-tagging attacks can be prevented by implementing the following trunk security guidelines:

* Disable trunking on all access ports.
* Disable auto trunking on trunk links so that trunks must be manually enabled.
* Be sure that the native VLAN is only used for trunk links.

DHCP Attack: DHCP servers dynamically provide IP configuration information including IP address, subnet mask, default gateway, DNS servers, and more to clients. Two types of DHCP attacks are DHCP starvation and DHCP spoofing. Both attacks are mitigated by implementing DHCP snooping.

ARP Attack: A threat actor sends a gratuitous ARP message containing a spoofed MAC address to a switch, and the switch updates its MAC table accordingly. Now the threat actor sends 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. ARP spoofing and ARP poisoning are mitigated by implementing DAI.

Address Spoofing Attack: 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. 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. IP and MAC address spoofing can be mitigated by implementing IPSG.

STP Attack: Threat actors manipulate STP to conduct an attack by spoofing the root bridge and changing the topology of a network. Threat actors make their hosts appear as root bridges; therefore, capturing all traffic for the immediate switched domain. This STP attack is mitigated by implementing BPDU Guard on all access ports

CDP Reconnaissance: 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. the information provided by CDP can also be used by a threat actor to discover network infrastructure vulnerabilities. To mitigate the exploitation of CDP, limit the use of CDP on devices or ports.

**Module 11**

All switch ports (interfaces) should be secured before the switch is deployed for production use. The simplest and most effective method to prevent MAC address table overflow attacks is to enable port security. By default, Layer 2 switch ports are set to dynamic auto (trunking on). The switch can be configured to learn about MAC addresses on a secure port in one of three ways: manually configured, dynamically learned, and dynamically learned – sticky. 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 and inactivity. 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. When a port is shutdown and placed in the error-disabled state, no traffic is sent or received on that port. To display port security settings for the switch, use the **show port-security** command.

To mitigate VLAN hopping attacks:

**Step 1.** Disable DTP negotiations on non-trunking ports.  
**Step 2.** Disable unused ports.  
**Step 3.** Manually enable the trunk link on a trunking port.  
**Step 4.** Disable DTP negotiations on trunking ports.  
**Step 5.** Set the native VLAN to a VLAN other than VLAN 1.

The goal of a DHCP starvation attack is to create a Denial of Service (DoS) for connecting clients. DHCP spoofing attacks can be mitigated by using DHCP snooping on trusted ports. 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. Use the following steps to enable DHCP snooping:

**Step 1.** Enable DHCP snooping.  
**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.  
**Step 4.** Enable DHCP snooping by VLAN, or by a range of VLANs.

Dynamic ARP inspection (DAI) requires DHCP snooping and helps prevent ARP attacks by:

* Not relaying invalid or gratuitous ARP Replies 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 Replies coming from invalid to prevent ARP poisoning.
* Error-disabling the interface if the configured DAI number of ARP packets is exceeded.

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.

As a general guideline, configure all access switch ports as untrusted and all uplink ports that are connected to other switches as trusted.

DAI can also 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 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.

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 or trunk 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 bypasses the STP listening and learning states to minimize the time that access ports must wait for STP to converge. If PortFast is enabled on a port connecting to another switch, there is a risk of creating a spanning-tree loop.
* **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.

**Module 12**

A Wireless LAN (WLAN) is a type of wireless network that is commonly used in homes, offices, and campus environments. Wireless networks are based on IEEE standards and can be classified into four main types: WPAN, WLAN, WMAN, and WWAN. Wireless LAN technologies uses the unlicensed radio spectrum to send and receive data. Examples of this technology are Bluetooth, WiMAX, Cellular Broadband, and Satellite Broadband. The IEEE 802.11 WLAN standards define how radio frequencies are used for wireless links. WLAN networks operate in the 2.4 GHz frequency band and the 5 GHz band. Standards ensure interoperability between devices that are made by different manufacturers. Internationally, the three organizations influencing WLAN standards are the ITU-R, the IEEE, and the Wi-Fi Alliance.

To communicate wirelessly, most devices include integrated wireless NICs that incorporate a radio transmitter/receiver. The wireless router serves as an access point, a switch, and a router. 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. APs can be categorized as either autonomous APs or controller-based APs. There are three types of antennas for business class APs: omnidirectional, directional, and MIMO.

The 802.11 standard identifies two main wireless topology modes: Ad hoc mode and Infrastructure mode. Tethering is used to provide quick wireless access. Infrastructure mode defines two topology building blocks: A Basic Service Set (BSS) and an Extended Service Set (ESS). All 802.11 wireless frames contain the following fields: frame control, duration, address 1, address 2, address 3, sequence control, address 4, payload, and FCS. WLANs use CSMA/CA as the method to determine how and when to send data on the network. Part of the 802.11 process is discovering a WLAN and subsequently connecting to it. Wireless devices discover a wireless AP, authenticate with it, and then associate with it. Wireless clients connect to the AP using a scanning process which may be passive or active.

CAPWAP is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANs. 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 and WLC MAC functions. DTLS is a protocol which provides security between the AP and the WLC. FlexConnect is a wireless solution for branch office and remote office deployments. 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 and standalone.

Wireless LAN devices have transmitters and receivers tuned to specific frequencies of radio waves to communicate. Frequencies are allocated as ranges. Ranges are then split into smaller ranges called channels: DSSS, FHSS, and OFDM. The 802.11b/g/n standards operate in the 2.4 GHz to 2.5GHz spectrum. The 2.4 GHz band is subdivided into multiple channels. Each channel is allotted 22 MHz bandwidth and is separated from the next channel by 5 MHz. When planning the location of APs, the approximate circular coverage area is important.

Wireless networks are susceptible to threats, including: data interception, wireless intruders, DoS attacks, and rogue APs. Wireless DoS attacks can be the result of: improperly configured devices, a malicious user intentionally interfering with the wireless communication, and accidental interference. A rogue AP is an AP or wireless router that has been connected to a corporate network without explicit authorization. When connected, a threat actor can use the rogue AP to capture MAC addresses, capture data packets, gain access to network resources, or launch a MITM attack. In a MITM attack, the threat actor is positioned in between two legitimate entities to read or modify the data that passes between the two parties. A popular wireless MITM attack is called the “evil twin AP” attack, where a threat actor introduces a rogue AP and configures it with the same SSID as a legitimate AP. To prevent the installation of rogue APs, organizations must configure WLCs with rogue AP policies.

To keep wireless intruders out and protect data, two early security features are still available on most routers and APs: SSID cloaking and MAC address filtering. There are four shared key authentication techniques available: WEP, WPA, WPA2, and WPA3 (Devices with WPA3 are not yet readily available). Home routers typically have two choices for authentication: WPA and WPA2. WPA2 is the stronger of the two. Encryption is used to protect data. The WPA and WPA2 standards use the following encryption protocols: TKIP and AES. In networks that have stricter security requirements, an additional authentication or login is required to grant wireless clients access. The Enterprise security mode choice requires an Authentication, Authorization, and Accounting (AAA) RADIUS server.

**Module 13**

Remote workers, small branch offices, and home networks often use a wireless router, which typically include a switch for wired clients, a port for an internet connection (sometimes labeled “WAN”), and wireless components for wireless client access. Most wireless routers are preconfigured to be connected to the network and provide services. The wireless router uses DHCP to automatically provide addressing information to connected devices. Your first priority should be to change the username and password of your wireless router. Use your router’s interface to complete basic network and wireless setup. If you want to extend the range beyond approximately 45 meters indoors and 90 meters outdoors, you can add wireless access points. The router will use a process called Network Address Translation (NAT) to convert private IPv4 addresses to Internet-routable IPv4 addresses. By configuring QoS, you can guarantee that certain traffic types, such as voice and video, are prioritized over traffic that is not as time-sensitive, such as email and web browsing.

Lightweight APs (LAPs) use the Lightweight Access Point Protocol (LWAPP) to communicate with a WLAN controller (WLC). Configuring a wireless LAN controller (WLC) is similar to configuring a wireless router except that a WLC controls APs and provides more services and management capabilities. Use the WLC interface to view an overall picture of the AP’s system information and performance, to access advanced settings and to configure a WLAN.

SNMP is used monitor the network. The WLC is set to forward all SNMP log messages, called traps, to the SNMP server. For WLAN user authentication, a RADIUS server is used for authentication, accounting, and auditing (AAA) services. Individual user access can be tracked and audited. Use the WLC interface to configure SNMP server and RADIUS server information, VLAN interfaces, DHCP scope, and a WPA2 Enterprise WLAN.

There are six steps to the troubleshooting process. When troubleshooting a WLAN, a process of elimination is recommended. Common problems are: no connectivity and poorly performing wireless connection when the PC is operational. To optimize and increase the bandwidth of 802.11 dual-band routers and APs, either: upgrade your wireless clients or split the traffic. Most wireless routers and APs offer upgradable firmware. Firmware releases may contain fixes for common problems reported by customers as well as security vulnerabilities. You should periodically check the router or AP for updated firmware.

**Module 14**

**Path Determination**

The primary functions of a router are to determine the best path to forward packets based on the information in its routing table, and to forward packets toward their destination. The best path in the routing table is also known as the longest match. The longest match is the route in the routing table that has the greatest number of far-left matching bits with the destination IP address of the packet. Directly connected networks are networks that are configured on the active interfaces of a router. A directly connected network is added to the routing table when an interface is configured with an IP address and subnet mask (prefix length) and is active (up and up). Routers learn about remote networks in two ways: static routes are added to the routing table when a route is manually configured, and with dynamic routing protocols. Using dynamic routing protocols such as EIGRP and OSPF, routes are added to the routing table when routing protocols dynamically learn about the remote network.

**Packet Forwarding**

After a router determines the correct path, it can forward the packet on a directly connected network, it can forward the packet to a next-hop router, or it can drop the packet. The primary responsibility of the packet forwarding function is to encapsulate packets in the appropriate data link frame type for the outgoing interface. Routers support three packet forwarding mechanisms: process switching, fast switching, and CEF. The following steps describe the packet forwarding process:

1. The data link frame with an encapsulated IP packet arrives on the ingress interface.
2. The router examines the destination IP address in the packet header and consults its IP routing table.
3. The router finds the longest matching prefix in the routing table.
4. The router encapsulates the packet in a data link frame and forwards it out the egress interface. The destination could be a device connected to the network or a next-hop router.
5. However, if there is no matching route entry the packet is dropped.

**Basic Router Configuration Review**

There are several configuration and verification commands for routers, including **show ip route**, **show ip interface**, **show ip interface brief** and **show running-config**. To reduce the amount of command output, use a filter. Filtering commands can be used to display specific sections of output. To enable the filtering command, enter a pipe (|) character after the **show** command and then enter a filtering parameter and a filtering expression. The filtering parameters that can be configured after the pipe include the following:

* **section** - Shows entire section that starts with the filtering expression
* **include** - Includes all output lines that match the filtering expression
* **exclude** - Excludes all output lines that match the filtering expression
* **begin** - Shows all the output lines from a certain point, starting with the line that matches the filtering expression

**IP Routing Table**

A routing table contains a list of routes known networks (prefixes and prefix lengths). The source of this information is derived from directly connected networks, static routes, and dynamic routing protocols. Common routing table codes include:

* **L** - Identifies the address assigned to a router interface. This allows the router to efficiently determine when it receives a packet for the interface instead of being forwarded.
* **C** - Identifies a directly connected network.
* **S** - Identifies a static route created to reach a specific network.
* **O** - Identifies a dynamically learned network from another router using the OSPF routing protocol.
* **\*** - This route is a candidate for a default route.

Every router makes its decision alone, based on the information it has in its own routing table. The information in a routing table of one router does not necessarily match the routing table of another router. Routing information about a path does not provide return routing information. Routing table entries include the route source, destination network, AD, metric, next-hop, route timestamp, and exit interface. To learn about remote networks, a router must have at least one active interface configured with an IP address and subnet mask (prefix length), called a directly connected network. Static routes are manually configured and define an explicit path between two networking devices. Dynamic routing protocols can discover a network, maintain routing tables, select a best path, and automatically discover a new best path if the topology changes. The default route specifies a next-hop router to use when the routing table does not contain a specific route that matches the destination IP address. A default route can be either a static route or learned automatically from a dynamic routing protocol. A default route has an IPv4 route entry of 0.0.0.0/0 or an IPv6 route entry of ::/0. IPv4 routing tables still have a structure based on classful addressing represented by levels of indentation. IPv6 routing tables do not use the IPv4 routing table structure. Cisco IOS uses what is known as the administrative distance (AD) to determine the route to install into the IP routing table. The AD represents the "trustworthiness" of the route. The lower the AD, the more trustworthy the route source.

**Static and Dynamic Routing**

Static routes are commonly used:

* As a default route forwarding packets to a service provider.
* For routes outside the routing domain and not learned by the dynamic routing protocol.
* When the network administrator wants to explicitly define the path for a specific network.
* For routing between stub networks.

Dynamic routing protocol are commonly used:

* In networks consisting of more than just a few routers
* When a change in the network topology requires the network to automatically determine another path
* For scalability. As the network grows, the dynamic routing protocol automatically learns about any new networks.

Current routing protocols include IGPs and EGPs. IGPs exchange routing information within a routing domain administered by a single organization. The only EGP is BGP. BGP exchanges routing information between different organizations. BGP is used by ISPs to route packets over the internet. Distance vector, link-state, and path vector routing protocols refer to the type of routing algorithm used to determine best path. The main components of dynamic routing protocols are data structures, routing protocol messages, and algorithms. The best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network. A metric is the quantitative value used to measure the distance to a given network. The best path to a network is the path with the lowest metric. When a router has two or more paths to a destination with equal cost metrics, then the router forwards the packets using both paths equally. This is called equal cost load balancing.

**Module 15**

**Static Routes**

Static routes can be configured for IPv4 and IPv6. Both protocols support the following types of static routes: standard static route, default static route, floating static route, and summary static route. Static routes are configured using the ip route and ipv6 route global configuration commands. When configuring a static route, the next hop can be identified by an IP address, exit interface, or both. How the destination is specified creates one of the three following types of static route: next-hop, directly connected, and fully specified. IPv4 static routes are configured using the following global configuration command: **ip route** *network-address subnet-mask* { *ip-address* | *exit-intf* [*ip=address*] } [**distance**]. IPv6 static routes are configured using the following global configuration command: **ipv6 route** *ipv6-prefix/prefix-length* { *ipv6-address* | *exit-intf* [*ipv6-address*]} [**distance**]. The command to start an IPv4 routing table is **show ip route** | **begin Gateway**. The command to start an IPv6 routing table is **show ipv6 route** | **begin C.**

**Configure IP Static Routes**

In a next-hop static route, only the next-hop IP address is specified. The exit interface is derived from the next hop. When configuring a static route, another option is to use the exit interface to specify the next-hop address. Directly connected static routes should only be used with point-to-point serial interfaces. In a fully specified static route, both the exit interface and the next-hop IP address are specified. This form of static route is used when the exit interface is a multi-access interface and it is necessary to explicitly identify the next hop. The next hop must be directly connected to the specified exit interface. In a fully specified IPv6 static route, both the exit interface and the next-hop IPv6 address are specified. Along with **show ip route**, **show ipv6 route**, **ping** and **traceroute**, other useful commands to verify static routes include: **show ip route static**, **show ip route** *network*, and **show running-config | section ip route**. Replace ip with ipv6 for the IPv6 versions of the command.

**Configure IP Default Static Routes**

A default route is a static route that matches all packets. A default route does not require any far-left bits to match between the default route and the destination IP address. Default static routes are commonly used when connecting an edge router to a service provider network, and a stub router. The command syntax for an IPv4 default static route is similar to any other IPv4 static route, except that the network address is 0.0.0.0 and the subnet mask is 0.0.0.0. The 0.0.0.0 0.0.0.0 in the route will match any network address. The command syntax for an IPv6 default static route is similar to any other IPv6 static route, except that the ipv6-prefix/prefix-length is ::/0, which matches all routes. To verify an IPv4 default static route, use the **show ip route static** command. For IPV6 use the **show ipv6 route static** command.

**Configure Floating Static Routes**

Floating static routes are static routes that are used to provide a backup path to a primary static or dynamic route in the event of a link failure. The floating static route is configured with a higher administrative distance than the primary route. By default, static routes have an administrative distance of 1, making them preferable to routes learned from dynamic routing protocols. The administrative distances of some common interior gateway dynamic routing protocols are EIGRP = 90, OSPF = 110, and IS-IS = 115. IP floating static routes are configured by using the **distance** argument to specify an administrative distance. If no administrative distance is configured, the default value (1) is used. The **show ip route** and **show ipv6 route** output verifies that the default routes to a router are installed in the routing table.

**Configure Static Host Routes**

A host route is an IPv4 address with a 32-bit mask or an IPv6 address with a 128-bit mask. There are three ways a host route can be added to the routing table: automatically installed when an IP address is configured on the router, configured as a static host route, or automatically obtained through other methods not covered in this module. Cisco IOS automatically installs a host route, also known as a local host route, when an interface address is configured on the router. A host route can be a manually configured static route to direct traffic to a specific destination device. For IPv6 static routes, the next-hop address can be the link-local address of the adjacent router; however, you must specify an interface type and an interface number when using a link-local address as the next hop. To do this, the original IPv6 static host route is removed, then a fully specified route is configured with the IPv6 address of the server and the IPv6 link-local address of the ISP router.

**Module 16**

**Packet Processing with Static Routes**

1. The packet arrives on the interface of R1.
2. R1 does not have a specific route to the destination network; therefore, R1 uses the default static route.
3. R1 encapsulates the packet in a new frame. Because the link to R2 is a point-to-point link, R1 adds an "all 1s" address for the Layer 2 destination address.
4. The frame is forwarded out of the appropriate interface. The packet arrives on the interface on R2.
5. R2 de-encapsulates the frame and looks for a route to the destination. R2 has a static route to the destination network out of one of its interfaces.
6. R2 encapsulates the packet in a new frame. Because the link to R3 is a point-to-point link, R2 adds an "all 1s" address for the Layer 2 destination address.
7. The frame is forwarded out of the appropriate interface. The packet arrives on the interface on R3.
8. R3 de-encapsulates the frame and looks for a route to the destination. R3 has a connected route to the destination network out of one of its interfaces.
9. R3 looks up the ARP table entry for the destination network to find the Layer 2 MAC address for PC3. If no entry exists, R3 sends an ARP request out of one of its interfaces, and PC3 responds with an ARP reply, which includes the PC3 MAC address.
10. R3 encapsulates the packet in a new frame with the MAC address of the appropriate interface as the source Layer 2 address and the MAC address of PC3 as the destination MAC address.
11. The frame is forwarded out of the appropriate interface. The packet arrives on the network interface card (NIC) interface of PC3.

**Troubleshoot IPv4 Static and Default Route Configuration**

Networks are frequently subject to events that can cause their status to change. An interface can fail, or a service provider drops a connection. Links can become oversaturated, or an administrator may enter a wrong configuration. Common IOS troubleshooting commands include the following:

* **ping**
* **traceroute**
* **show ip route**
* **show ip interface brief**
* **show cdp neighbors detail**