



Module 11: Network Communication Devices

CyberOps Associate v1.0



Module Objectives

Module Title: Network Communication Devices

Module Objective: Explain how network devices enable wired and wireless network communication.

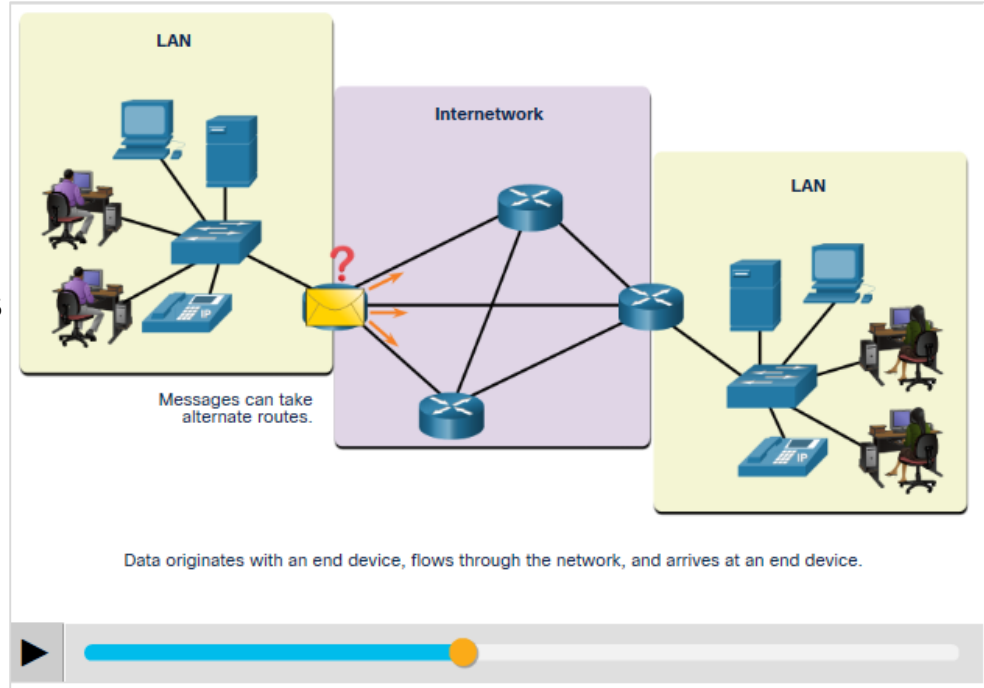
Topic Title	Topic Objective
Network Devices	Explain how network devices enable network communication.
Wireless Communications	Explain how wireless devices enable network communication.

11.1 Network Devices

Network Communication Devices

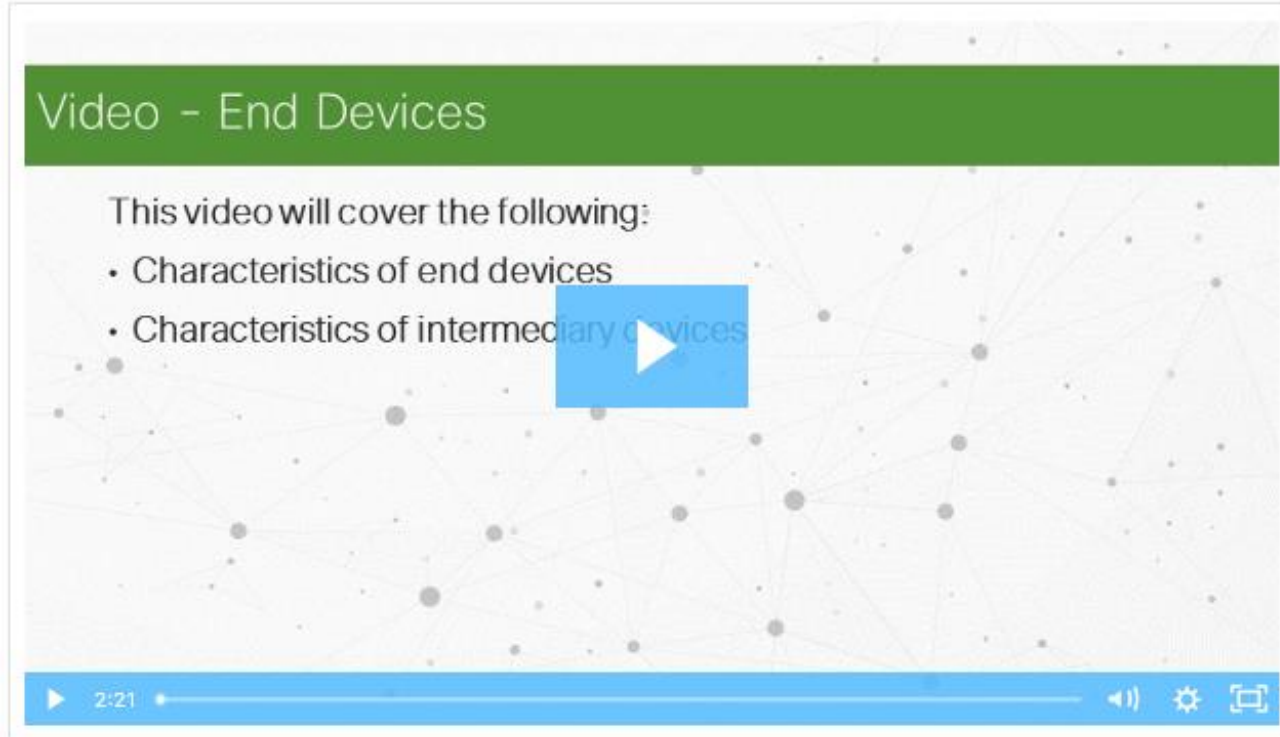
End Devices

- The most familiar network devices are end devices. An end device is either the source or destination of a message transmitted over the network.
- To distinguish one end device from another, each end device on a network has an address.
- When an end device initiates communication, it uses the address of the destination end device to specify where to deliver the message.
- Data originates with an end device, flows through the network, and arrives at an end device.



Video - End Devices

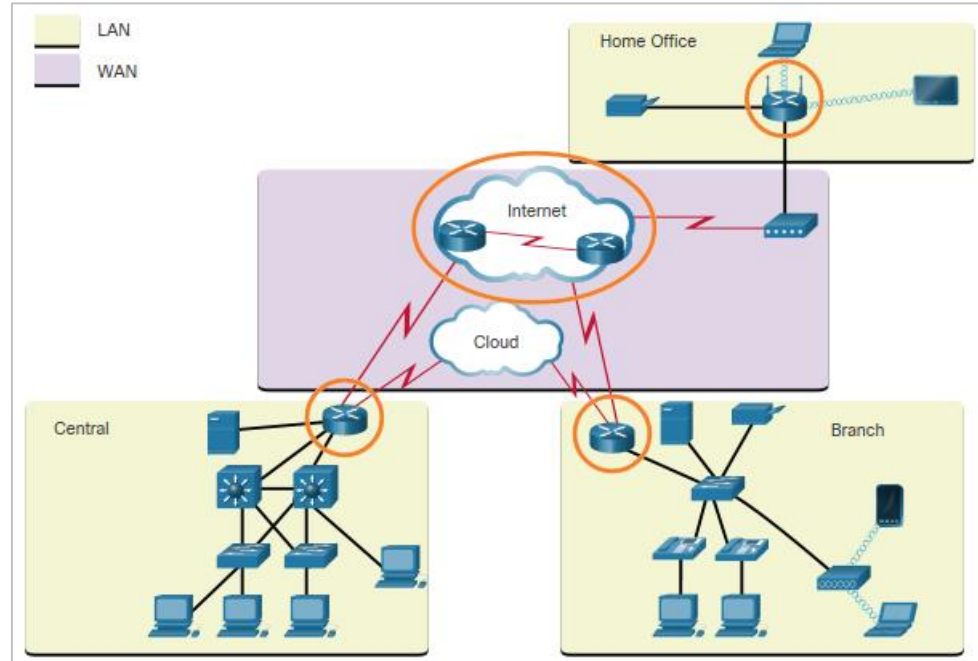
Watch the video to learn more about end devices.



Routers

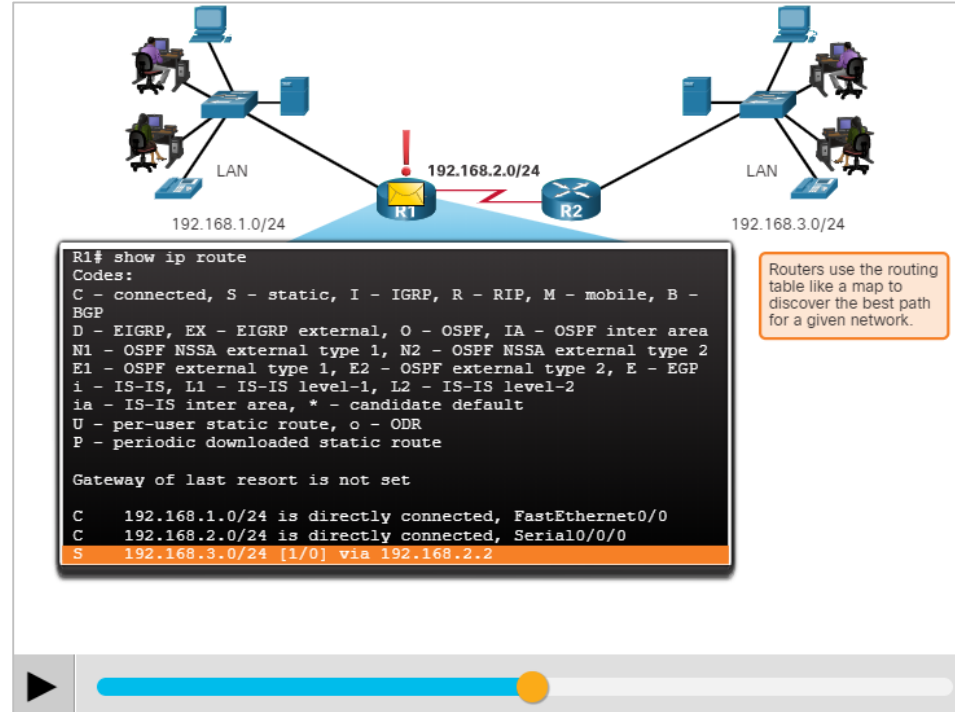
- Routers are devices that operate at the OSI network layer (Layer 3).
- As shown in the figure, routers are used to interconnect remote sites. They use the process of routing to forward data packets between networks.
- The routing process uses network routing tables, protocols, and algorithms to determine the most efficient path for forwarding an IP packet.
- Routers gather routing information and update other routers about changes in the network.

The Router Connection



Routers (Contd.)

- Routers have two primary functions: path determination and packet forwarding.
- To perform path determination, each router builds and maintains a routing table which is a database of known networks and how to reach them.
- The routing table can be built manually and contain static routes or can be built using a dynamic routing protocol.
- Packet forwarding is accomplished by using a switching function.
- Switching is the process used by a router to accept a packet on one interface and forward it out of another interface.
- A primary aim of the switching function is to encapsulate packets in the appropriate data link frame type for the outgoing data link.



Routers (Contd.)

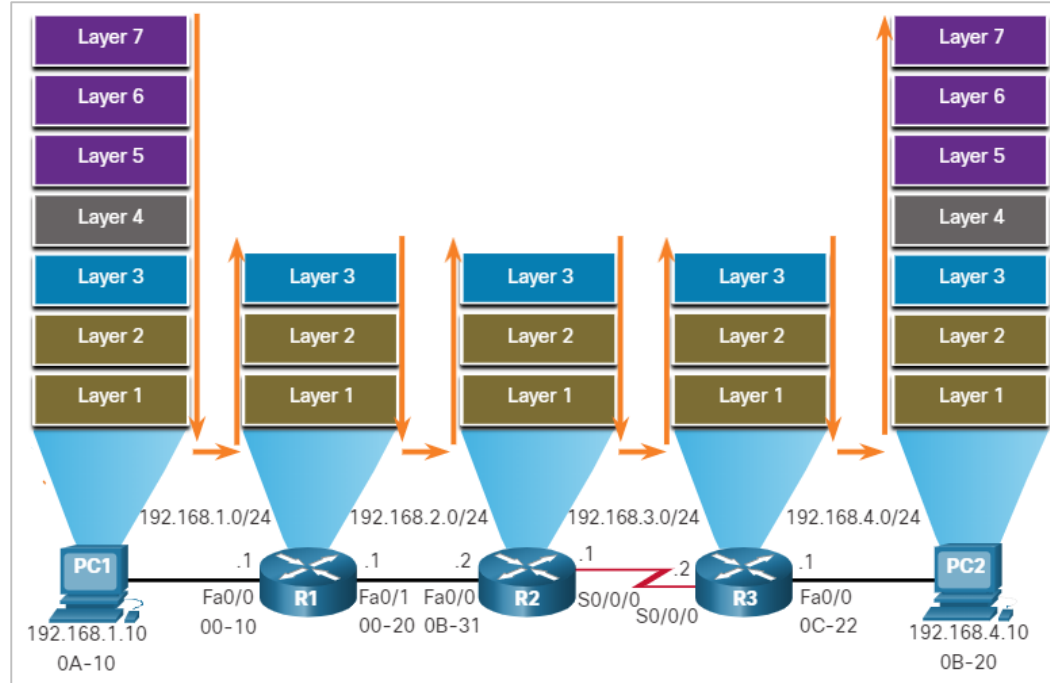
- After the router has determined the exit interface using path determination, the router must encapsulate the packet into the data link frame of the outgoing interface.
- When a packet received from one network and destined for another network, the router performs the following three major steps:
 - It de-encapsulates the Layer 2 frame header and trailer to expose the Layer 3 packet.
 - It examines the destination IP address of the IP packet to find the best path in the routing table.
 - If the router finds a path to the destination, it encapsulates the Layer 3 packet into a new Layer 2 frame and forwards that frame out the exit interface.

Network Communication Devices

Routers (Contd.)

- As shown in the figure, devices have Layer 3 IPv4 addresses, while Ethernet interfaces have Layer 2 data link addresses. The MAC addresses are shortened to simplify the illustration.
- As a packet travels from the source device to the final destination device, the Layer 3 IP addresses do not change as the Layer 3 PDU does not change.
- The Layer 2 data link addresses change at every router on the path to the destination, as the packet is de-encapsulated and re-encapsulated in a new Layer 2 frame.

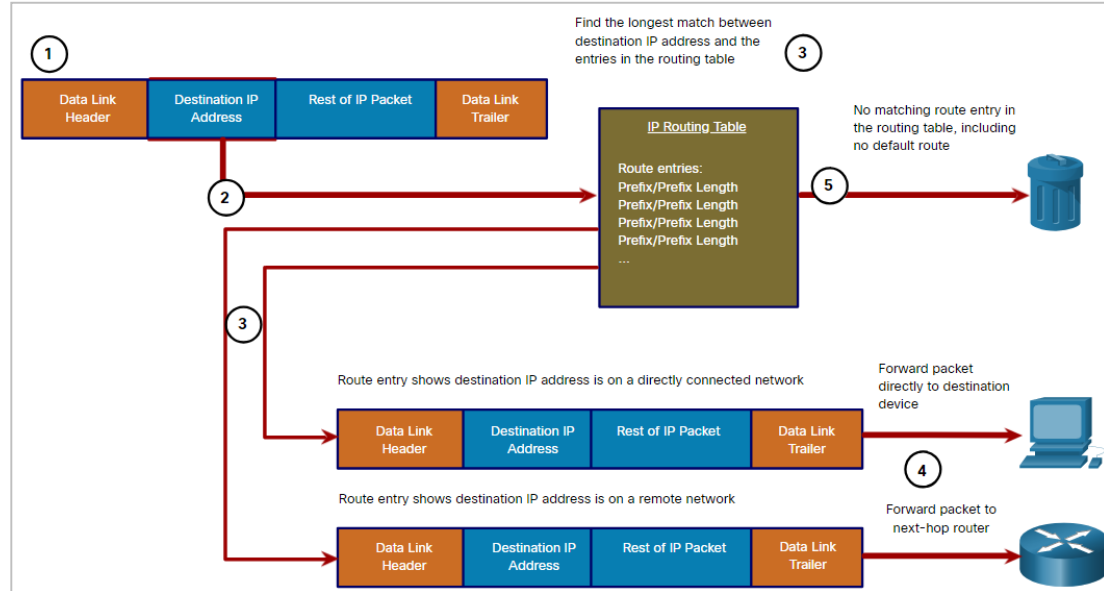
Encapsulating and De-Encapsulating Packets



Packet Forwarding Decision Process

Now, router must determine how to encapsulate the packet and forward it out the correct egress interface. The following steps describe the packet forwarding process shown in the figure:

- The data link frame with an encapsulated IP packet arrives on the ingress interface.
- The router examines the destination IP address in the packet header and consults its IP routing table.
- The router finds the longest matching prefix in the routing table.
- 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.
- If there is no matching route entry the packet is dropped.



Packet Forwarding Decision Process (Contd.)

The three actions a router can perform with a packet, after the best path is determined:

- Forwards the Packet to a Device on a Directly Connected Network
- Forwards the Packet to a Next-Hop Router
- Drops the Packet - No Match in Routing Table

Forwards the Packet to a Device on a Directly Connected Network

- If the route entry indicates that the egress interface is a directly connected network, this means that the destination IP address of the packet belongs to a device on the directly connected network.
- The packet can be forwarded directly to the destination device, an end device on an Ethernet LAN, which means the packet must be encapsulated in an Ethernet frame.
- To encapsulate the packet in the Ethernet frame, the router needs to determine the destination MAC address associated with the destination IP address of the packet.

Packet Forwarding Decision Process (Contd.)

The process varies based on whether the packet is an IPv4 or IPv6 packet.

IPv4 packet:

- The router checks its ARP table for the destination IPv4 address and an associated Ethernet MAC address.
- If there is no match, the router sends an ARP Request and the destination device will return an ARP Reply with its MAC address.
- The router can now forward the IPv4 packet in an Ethernet frame with the proper destination MAC address.

IPv6 packet:

- The router checks its neighbor cache for the destination IPv6 address and an associated Ethernet MAC address.
- If there is no match, the router sends an ICMPv6 Neighbor Solicitation (NS) message and the destination device will return an ICMPv6 Neighbor Advertisement (NA) message with its MAC address.
- The router can now forward the IPv6 packet in an Ethernet frame with the proper destination MAC address.

Packet Forwarding Decision Process (Contd.)

Forwards the Packet to a Next-Hop Router

- If the route entry indicates that the destination IP address is on a remote network, this means the destination IP address of the packet belongs to a device on network that is not directly connected.
- Therefore, the packet must be forwarded to another router, specifically a next-hop router. The next-hop address is indicated in the route entry.
- If the forwarding router and the next-hop router are on an Ethernet network, a similar process (ARP and ICMPv6 Neighbor Discovery) will occur for determining the destination MAC address of the packet. The difference is that the router will search for the IP address of the next-hop router in its ARP table or neighbor cache, instead of the destination IP address.

Drops the Packet - No Match in Routing Table

- If there is no match between the destination IP address and a prefix in the routing table, and if there is no default route, the packet will be dropped.

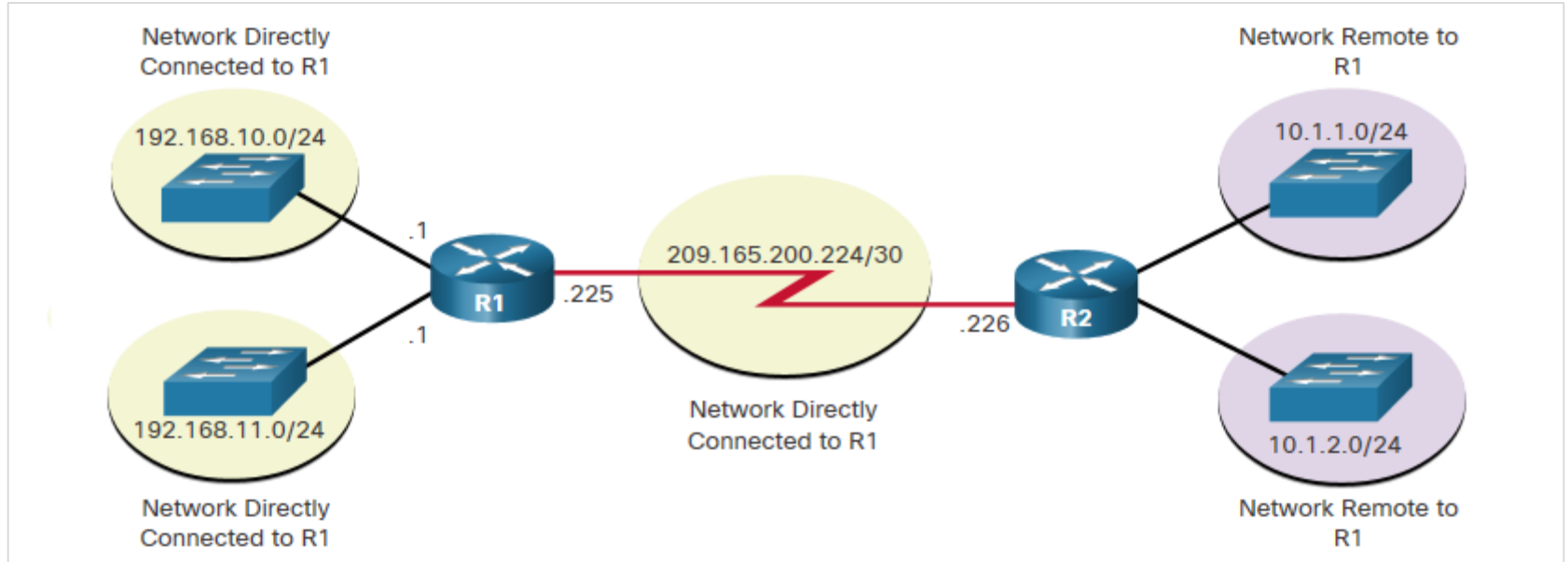
Routing Information

- The routing table stores the following information:
 - **Directly connected routes** - These routes come from the active router interfaces. Routers add a directly connected route when an interface is configured with an IP address and is activated.
 - **Remote routes** - These are remote networks connected to other routers.
- A routing table is a data file in RAM that is used to store route information about directly connected and remote networks.
- The routing table contains network or next hop associations. These associations tell a router that a particular destination can be optimally reached by sending the packet to a specific router that represents the next hop on the way to the final destination.
- The next hop association can also be the outgoing or exit interface to the next destination.

Routing Information (Contd.)

Directly Connected and Remote Network Routes

The figure identifies the directly connected networks and remote networks of router R1.



Routing Information (Contd.)

- The destination network entries in the routing table can be added in several ways:
 - **Local Route interfaces** – These are added when an interface is configured and active. This entry is only displayed in IOS 15 or newer for IPv4 routes, and all IOS releases for IPv6 routes.
 - **Directly connected interfaces** – These are added to the routing table when an interface is configured and active.
 - **Static routes** – These are added when a route is manually configured and the exit interface is active.
 - **Dynamic routing protocol** – This is added when routing protocols that dynamically learn about the network, such as EIGRP or OSPF, are implemented and networks are identified.
- Dynamic routing protocols exchange network reachability information between routers and dynamically adapt to network changes.

Routing Information (Contd.)

- One of the first dynamic routing protocols was RIP. RIPv1 was released in 1988.
- To address the needs of larger networks, two advanced routing protocols Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) were developed.
- Cisco developed the Interior Gateway Routing Protocol (IGRP) and Enhanced IGRP (EIGRP) which also scales well in larger network implementations.
- The Border Gateway Protocol (BGP) is now used between Internet Service Providers (ISPs) and their larger private clients to exchange routing information.
- The following table classifies the protocols:

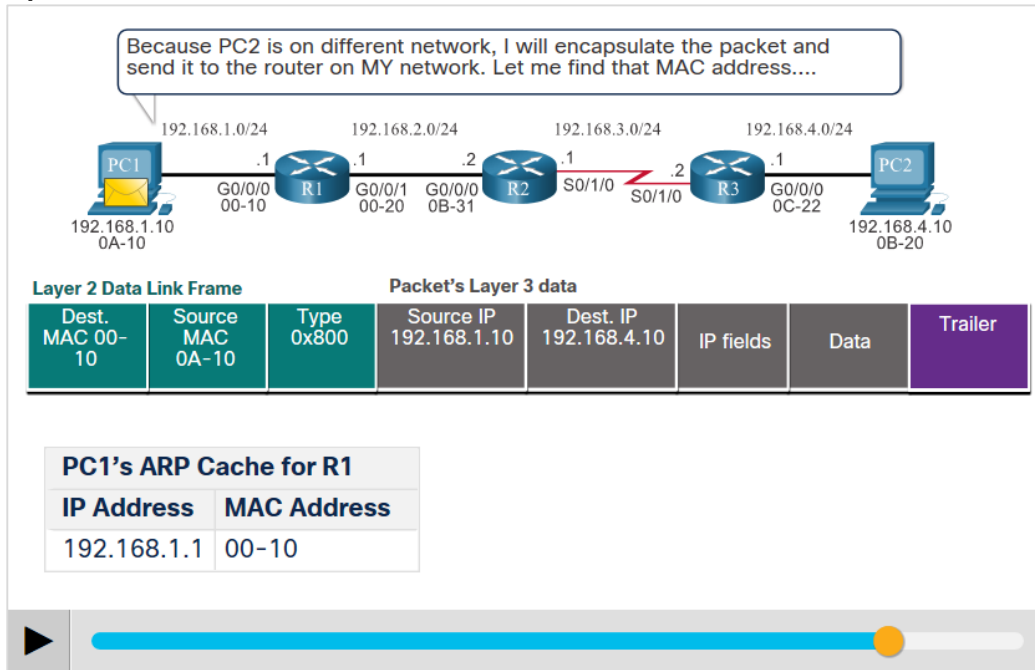
Protocol	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector		Link State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP

End-to-End Packet Forwarding

The primary responsibility of the packet forwarding function is to encapsulate packets in the appropriate data link frame type for the outgoing interface. The process of packet forwarding is described through the following example.

PC1 Sends Packet to PC2

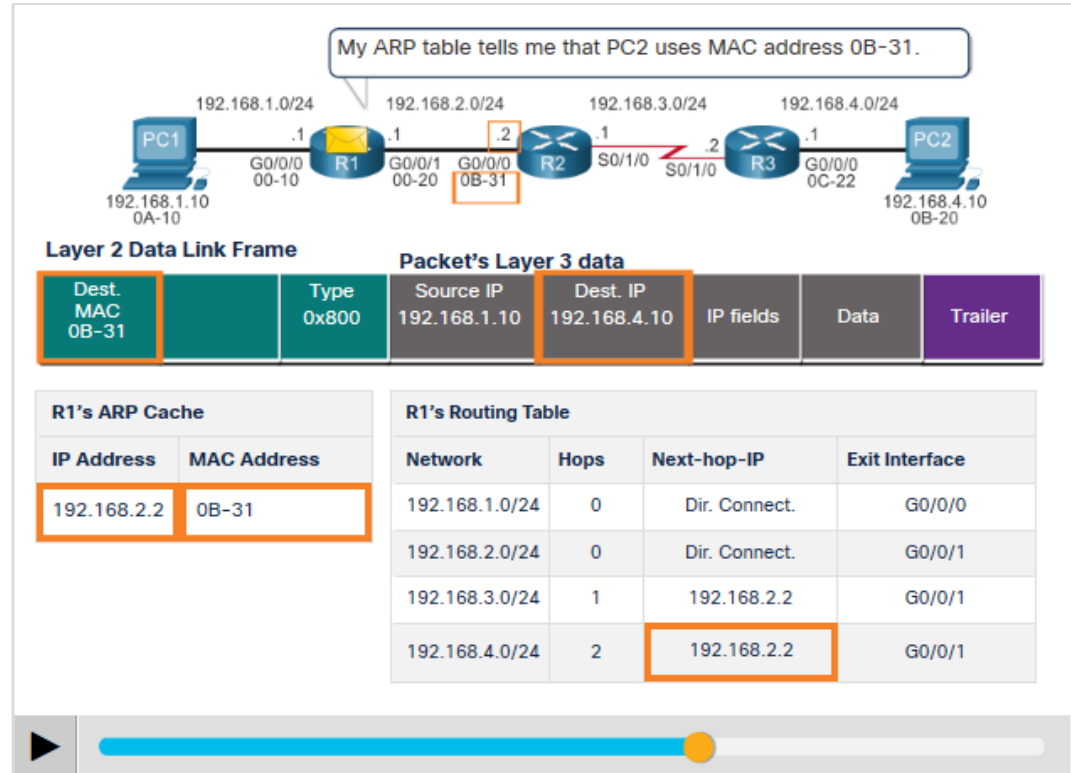
- In the first animation, PC1 sends a packet to PC2.
- Note that if an ARP entry does not exist in the ARP table for the default gateway of 192.168.1.1, PC1 sends an ARP request.
- Router R1 then return an ARP reply.



End-to-End Packet Forwarding (Contd.)

R1 Forwards the Packet to PC2

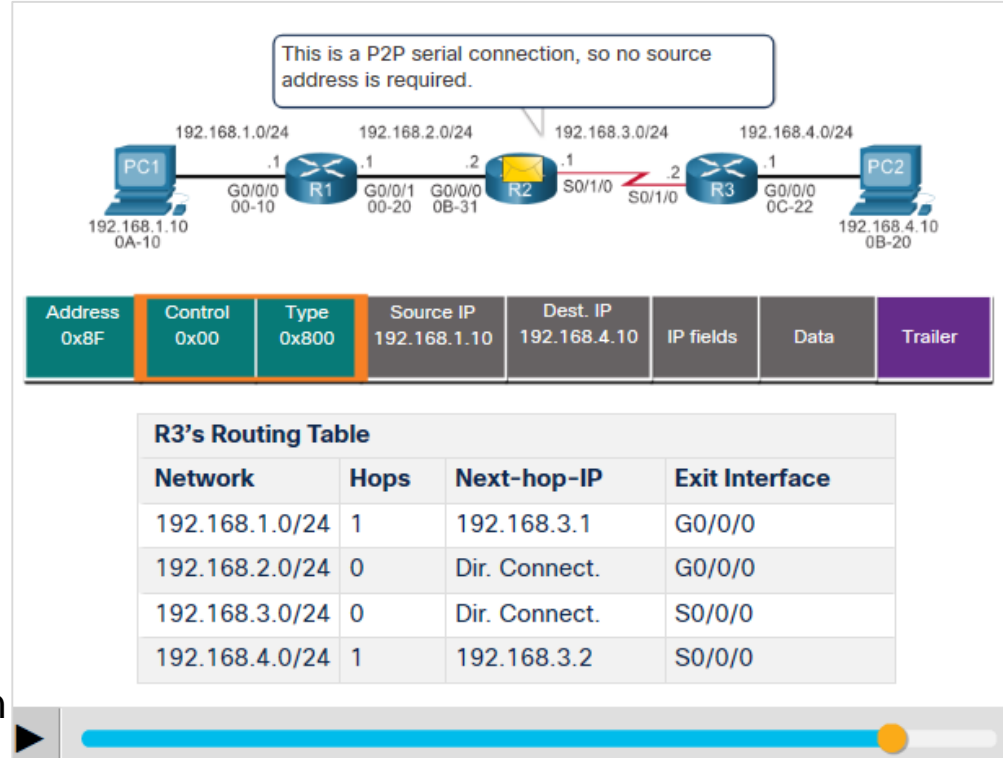
- R1 now forwards the packet to PC2.
- Because the exit interface is on an Ethernet network, R1 must resolve the next-hop IPv4 address with a destination MAC address using its ARP table.
- If an ARP entry does not exist in the ARP table for the next-hop interface of 192.168.2.2, R1 sends an ARP request.
- R2 would then return an ARP Reply.



End-to-End Packet Forwarding (Contd.)

R2 Forwards the Packet to R3

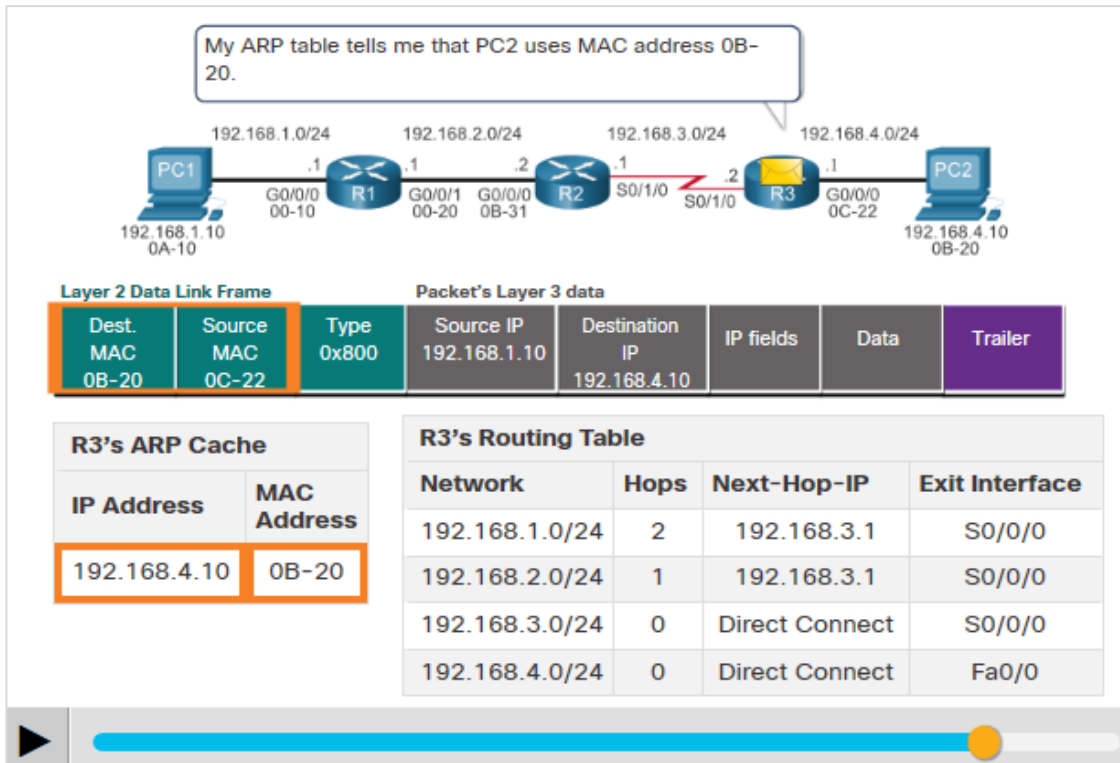
- R2 now forwards the packet to R3.
- As the exit interface is not an Ethernet network, R2 does not have to resolve the next-hop IPv4 address with a destination MAC address.
- When the interface is a point-to-point (P2P) serial connection, the router encapsulates the IPv4 packet into the proper data link frame format used by the exit interface.
- As there are no MAC addresses on serial interfaces, R2 sets the data link destination address to an equivalent of a broadcast.



End-to-End Packet Forwarding (Contd.)

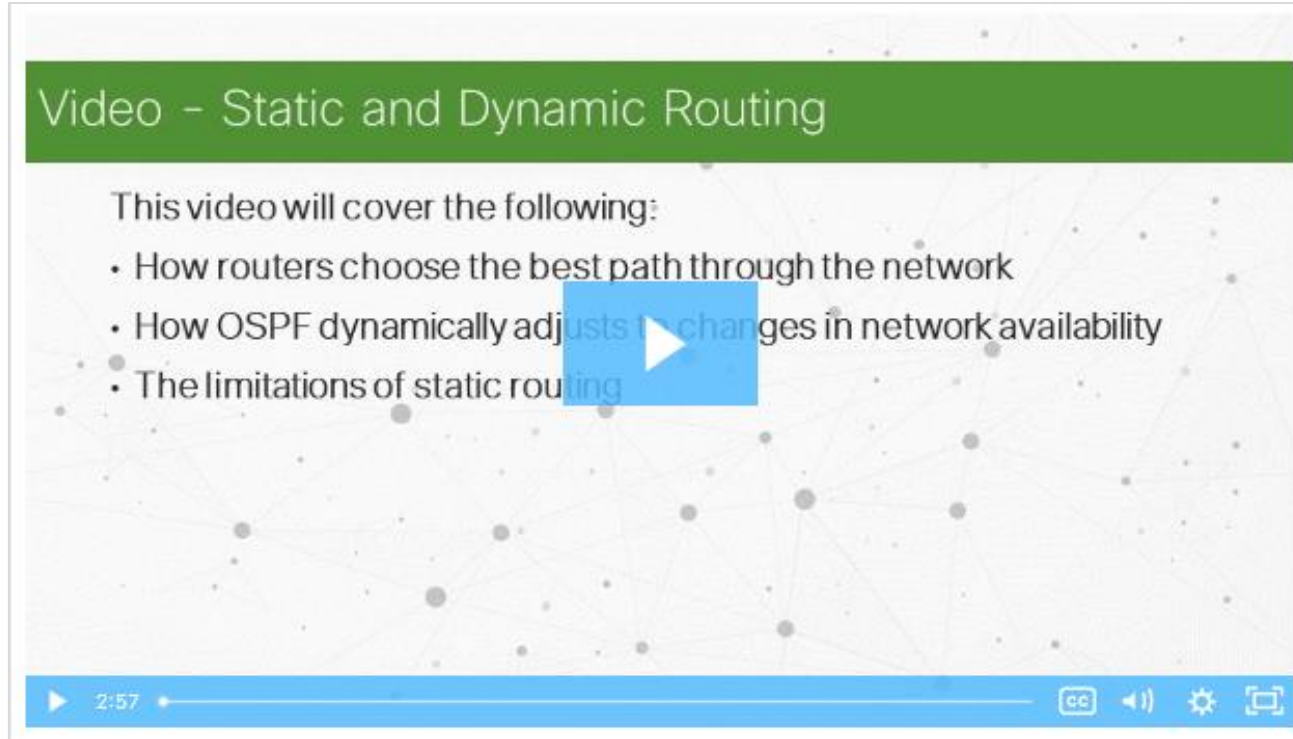
R3 Forwards the Packet to PC2

- R3 now forwards the packet to PC2.
- As the destination IPv4 address is on a directly connected Ethernet network, R3 must resolve the destination IPv4 address of the packet with its associated MAC address.
- If the entry is not in the ARP table, R3 sends an ARP request out of its FastEthernet 0/0 interface.
- PC2 would then return an ARP reply with its MAC address.



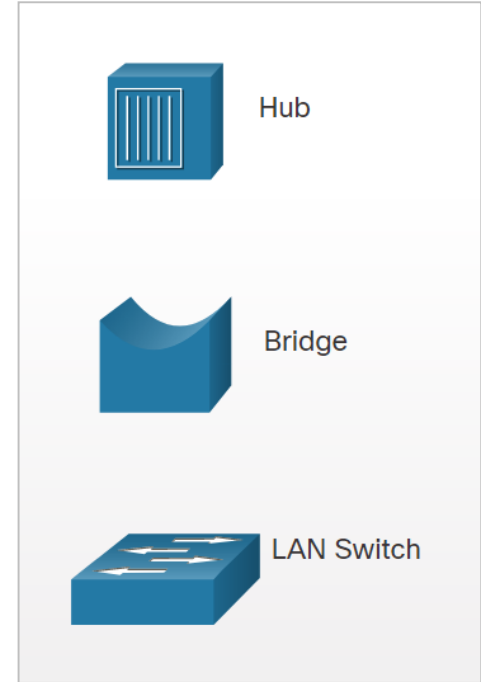
Video - Static and Dynamic Routing

Play the video to learn about static and dynamic routing.



Hubs, Bridges, LAN Switches

- The topology icons for hubs, bridges, and LAN switches are shown in the figure.
- An Ethernet hub acts as a multiport repeater that receives an incoming electrical signal (data) on a port. It then immediately forwards a regenerated signal out all other ports. Hubs use physical layer processing to forward data.
- Bridges have two interfaces and are connected between hubs to divide the network into multiple collision domains. Each collision domain can have only one sender at a time.
- LAN switches are multiport bridges that connect devices into a star topology. Switches also segment a LAN into separate collision domains, one for each switch port. A switch makes forwarding decisions based on Ethernet MAC addresses.



Switching Operation

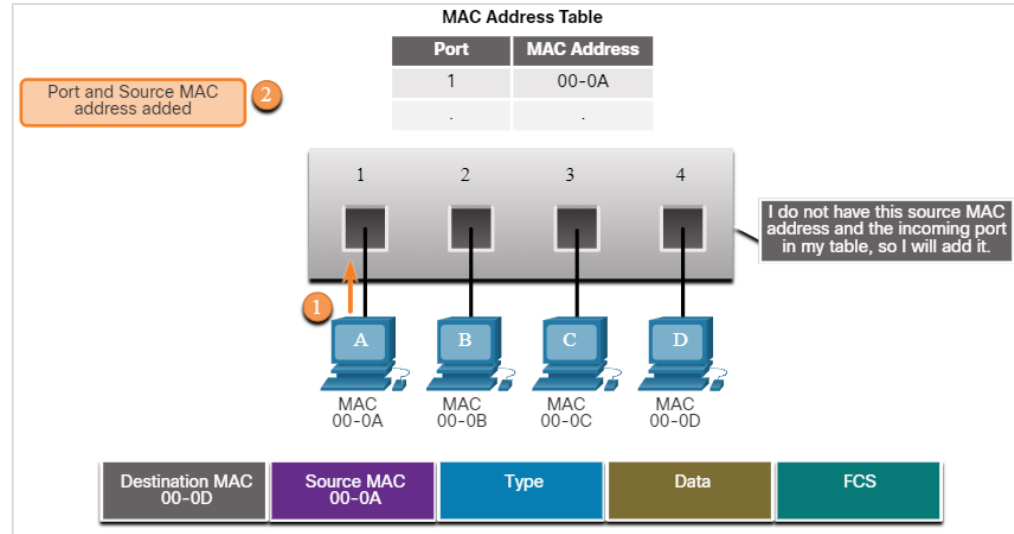
- Switches use MAC addresses to direct network communications through the switch, to the appropriate port, and toward the destination.
- A switch is made up of integrated circuits and the accompanying software that controls the data paths through the switch.
- For a switch to know the port to transmit a frame, it must first learn the devices existing on each port. As the switch learns the relationship of ports to devices, it builds a table called a MAC address table, or content addressable memory (CAM) table which is a special type of memory used in high-speed searching applications.
- LAN switches determine how to handle incoming data frames by maintaining the MAC address table.
- The switch uses the information in the MAC address table to send frames destined for a specific device out of the port to which the device is connected.

Switching Operation (Contd.)

The following two-step process is performed on every Ethernet frame that enters a switch.

Learn – Examining the Source MAC Address

- Every frame that enters a switch is checked for new MAC address information by examining the frame's source MAC address and the port number where the frame entered the switch.
- If the source MAC address is not in the table, it is added to the MAC address table along with the incoming port number.
- If the source MAC address does exist in the table, the switch updates the refresh timer for that entry. By default, most Ethernet switches keep an entry in the table for five minutes.



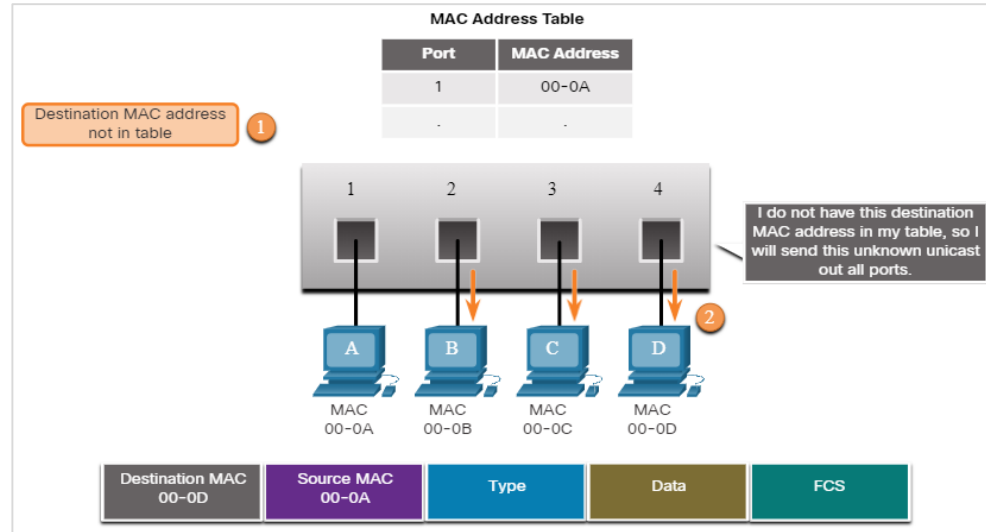
Note: If the source MAC address does exist in the table but on a different port, the switch treats this as a new entry. The entry is replaced using the same MAC address, but with the more current port number.

Switching Operation (Contd.)

Forward – Examining the Destination MAC Address

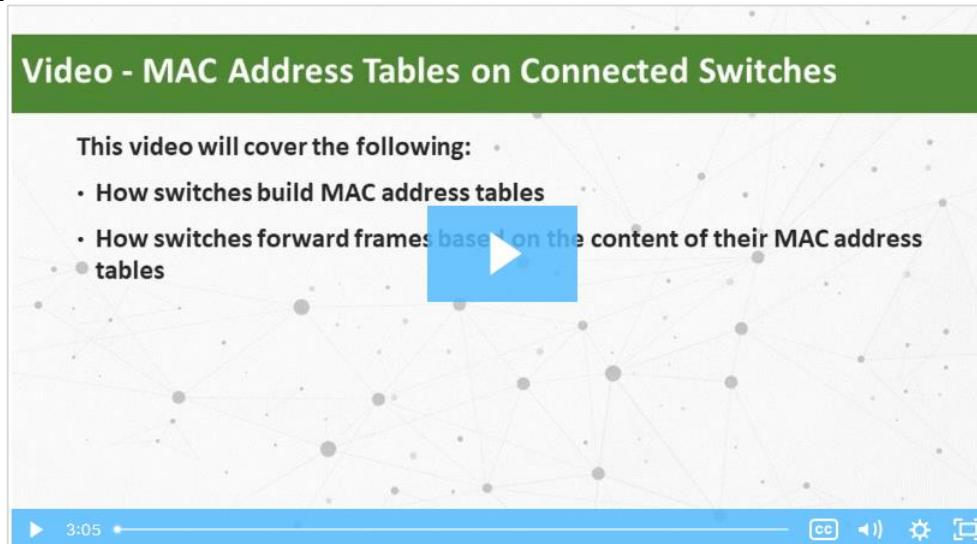
- If the destination MAC address is a unicast address, the switch will look for a match between the destination MAC address of the frame and an entry in its MAC address table.
- If the destination MAC address is in the table, it will forward the frame out the specified port.
- If the destination MAC address is not in the table, the switch will forward the frame out all ports except the incoming port. This is called an unknown unicast.

Note: If the destination MAC address is a broadcast or a multicast, the frame is also flooded out all ports except the incoming port.



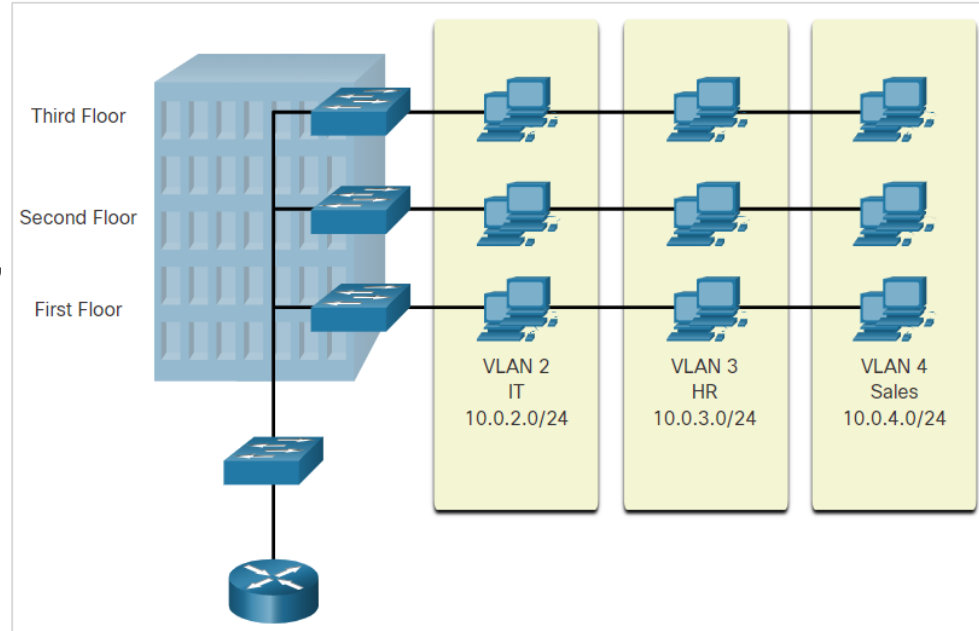
Video - MAC Address Tables on Connected Switches

- A switch can have multiple MAC addresses associated with a single port. This is common when the switch is connected to another switch. The switch will have a separate MAC address table entry for each frame received with a different source MAC address.
- Play the video to see a demonstration of how two connected switches build their MAC address tables.



VLANs

- VLANs provide a way to group devices within a LAN.
- It provides segmentation and organizational flexibility within a switched internetwork.
- It allows an administrator to segment networks based on factors such as function, project team, or application, without regard for the physical location of the user or device.
- It creates a logical broadcast domain that can span multiple physical LAN segments.
- It prevent users on different VLANs from snooping on each other's traffic.



STP

- The Spanning Tree Protocol is used to maintain one loop-free path in the Layer 2 network, at any time.
- Loops and duplicate frames have severe consequences for a switched network. STP was developed to address these issues.
- It ensures that there is one logical path between all destinations on the network by blocking redundant paths.
- A port is considered blocked when user data is prevented from entering or leaving that port. This does not include bridge protocol data unit (BPDU) frames that are used by STP to prevent loops.
- If the path is ever needed to compensate for a network cable or switch failure, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active.

Multilayer Switching

Multilayer switches (Layer 3 switches) perform Layer 2 switching and also forward frames based on Layer 3 and 4 information.

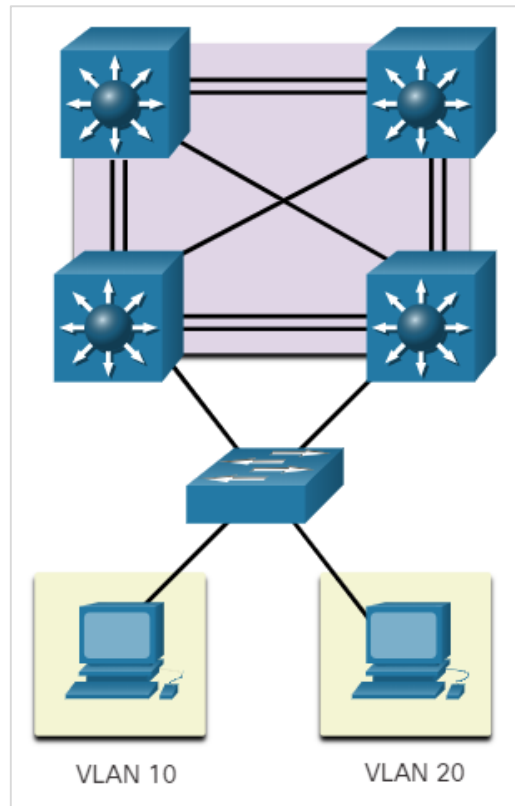
All Cisco Catalyst multilayer switches support the following types of Layer 3 interfaces:

- **Routed port** - A pure Layer 3 interface similar to a physical interface on a Cisco IOS router.
- **Switch virtual interface (SVI)** - A virtual VLAN interface for inter-VLAN routing. In other words, SVIs are the virtual-routed VLAN interfaces.

Multilayer Switching (Contd.)

Routed Ports

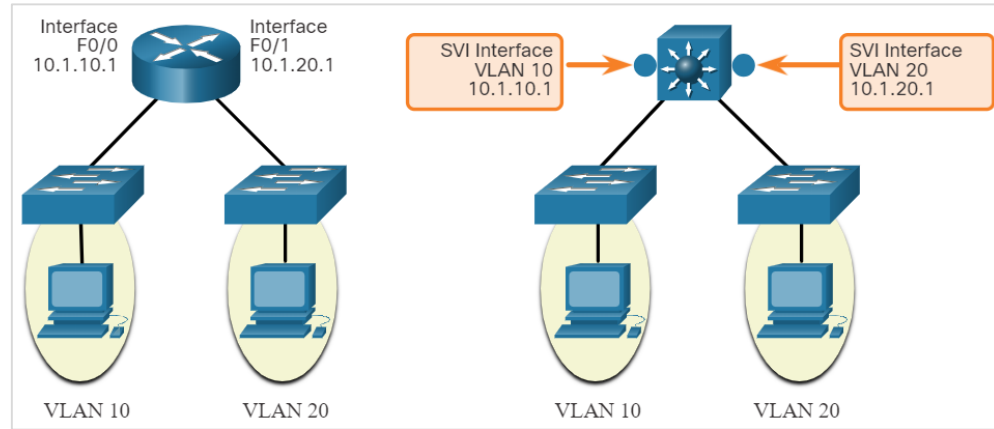
- A routed port is a physical port that acts similarly to an interface on a router.
- Unlike an access port, a routed port is not associated with a particular VLAN. It behaves like a regular router interface.
- Also, as Layer 2 functionality has been removed, Layer 2 protocols, such as STP, do not function on a routed interface.
- Some protocols, such as LACP and EtherChannel, do function at Layer 3. Unlike Cisco IOS routers, routed ports on a Cisco IOS switch do not support sub interfaces.



Multilayer Switching (Contd.)

Switch Virtual Interface

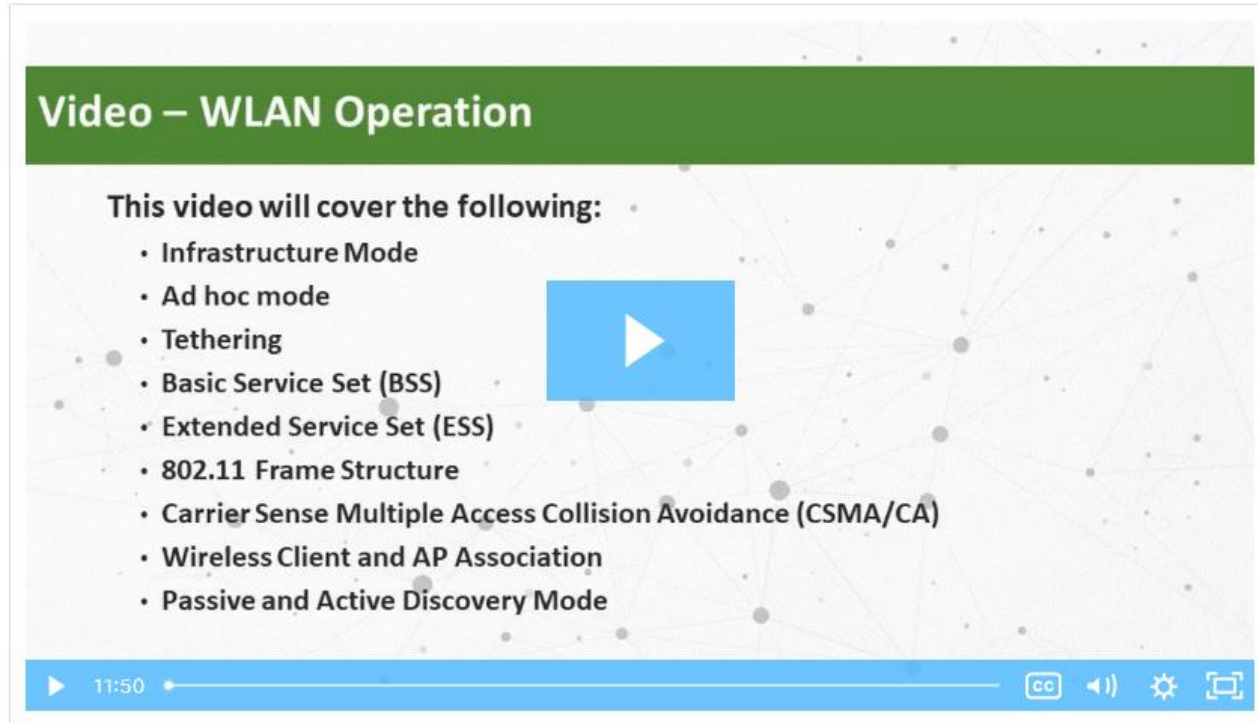
- An SVI is a virtual interface that is configured within a multilayer switch. Unlike the basic Layer 2 switches, a multilayer switch can have multiple SVIs. An SVI can be created for any VLAN that exists on the switch.
- An SVI is considered to be virtual as there is no physical port dedicated to the interface. It can perform the same functions for the VLAN as a router interface and can be configured in much the same way as a router interface.
- The SVI for the VLAN provides Layer 3 processing for packets to or from all switch ports associated with that VLAN.



11.2 Wireless Communications

Video - Wireless Communications

Watch the video to learn about Wireless LAN (WLAN) operation.



Video – WLAN Operation

This video will cover the following:

- Infrastructure Mode
- Ad hoc mode
- Tethering
- Basic Service Set (BSS)
- Extended Service Set (ESS)
- 802.11 Frame Structure
- Carrier Sense Multiple Access Collision Avoidance (CSMA/CA)
- Wireless Client and AP Association
- Passive and Active Discovery Mode

11:50

CC

Speaker icon

Settings icon

Fullscreen icon

Wireless versus Wired LANs

- WLANs use Radio Frequencies (RF) instead of cables at the physical layer and MAC sublayer of the data link layer.
- The IEEE has adopted the 802 LAN/MAN portfolio of computer network architecture standards which includes two dominant working groups 802.3 Ethernet, which defined Ethernet for wired LANs and 802.11 which defined Ethernet for WLANs.
- WLANs also differ from wired LANs as follows:
 - WLANs connect clients to the network through a wireless access point (AP) or wireless router, instead of an Ethernet switch.
 - WLANs connect mobile devices that are often battery powered, as opposed to plugged-in LAN devices. Wireless NICs tend to reduce the battery life of a mobile device.
 - WLANs support hosts that contend for access on the RF media (frequency bands).
 - WLANs use a different frame format than wired Ethernet LANs. WLANs require additional information in the Layer 2 header of the frame.
 - WLANs raise more privacy issues because radio frequencies can reach outside the facility.

Wireless versus Wired LANs (Contd.)

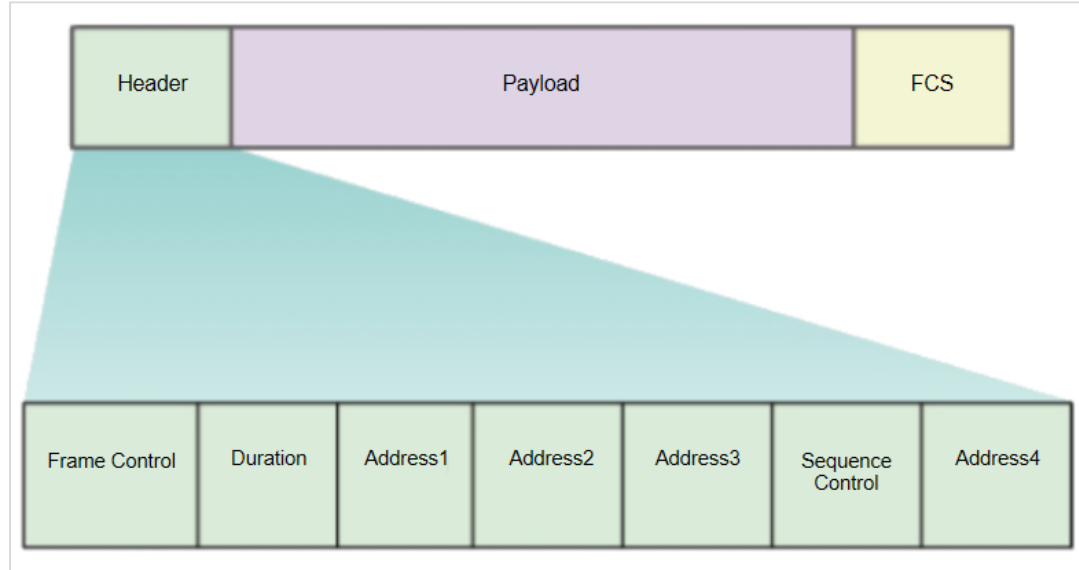
The difference between WLAN and Wired LAN is summarized in the following table.

Characteristic	802.11 Wireless LAN	802.3 Wired Ethernet LANs
Physical Layer	Radio frequency (RF)	Physical cables
Media Access	Collision avoidance	Collision detection
Availability	Anyone with a wireless NIC in range of an access point	Physical cable connection required
Signal Interference	Yes	Minimal
Regulation	Different regulations by country	IEEE standard dictates

802.11 Frame Structure

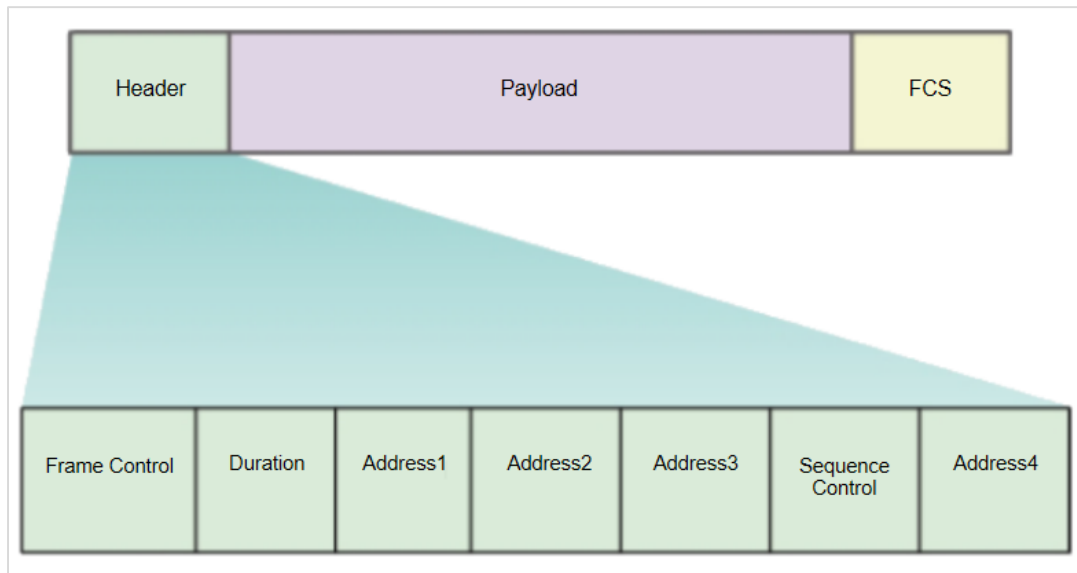
All 802.11 wireless frames contain the following fields:

- **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 used to indicate the remaining duration needed to receive the next frame transmission.
- **Address1** – This contains the MAC address of the receiving wireless device or AP.
- **Address2** – This contains the MAC address of the transmitting wireless device or AP.



802.11 Frame Structure (Contd.)

- **Address3** - This contains the MAC address of the destination, such as the router interface with AP attached.
- **Sequence Control** – This contains information to control sequencing and fragmented frames.
- **Address4** - This is usually missing as it is used only in ad hoc mode.
- **Payload** – This contains the data for transmission.
- **FCS** – This is used for Layer 2 error control.



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) method to determine how and when to send data on the network.

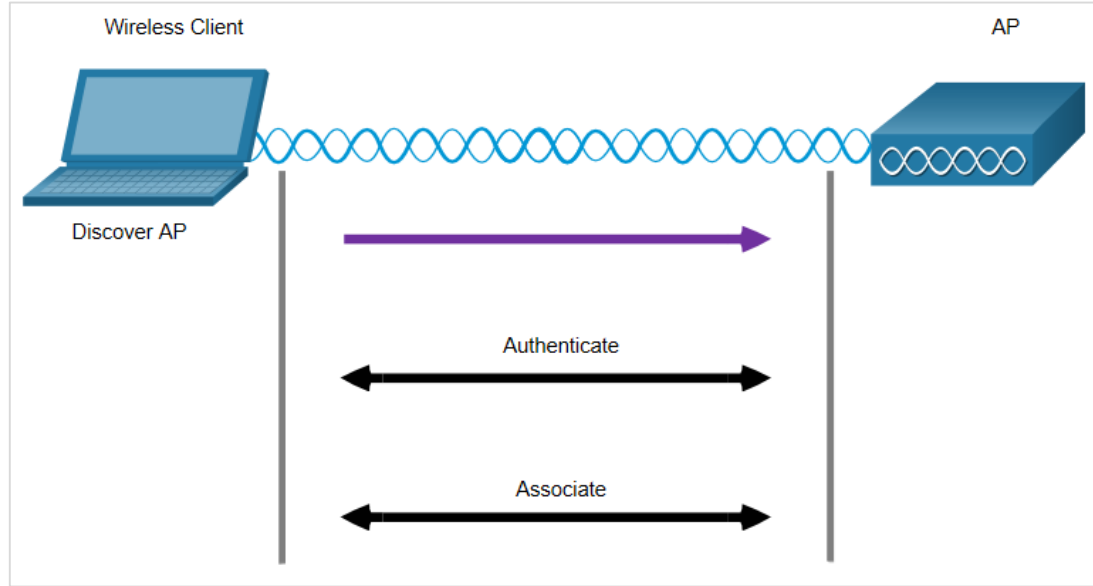
CSMA/CA (Contd.)

A wireless client does the following:

- Listens to the channel to see if it is idle. The channel is also called the carrier.
- Sends a Ready 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.

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, as shown in the figure:
 - Discover a wireless AP
 - Authenticate with AP
 - Associate with AP



Wireless Client and AP Association (Contd.)

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. The configurable wireless parameters include:

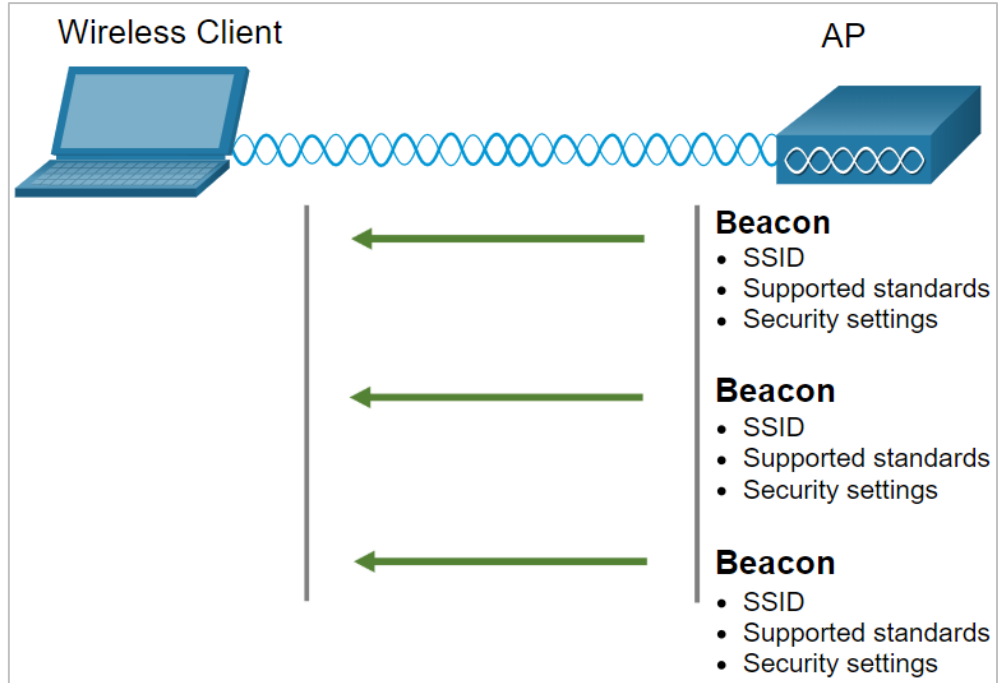
- **SSID** -The SSID name appears in the list of available wireless networks on a client.
- **Password** – This is required from the wireless client to authenticate to the AP.
- **Network mode** - This refers to the 802.11a/b/g/n/ac/ad WLAN standards.
- **Security mode** - This refers to the security 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.

Passive and Active Discover Mode

Wireless devices must discover and connect to an AP or wireless router. Wireless clients connect to the AP using a scanning (probing) process such as passive and active.

Passive Mode

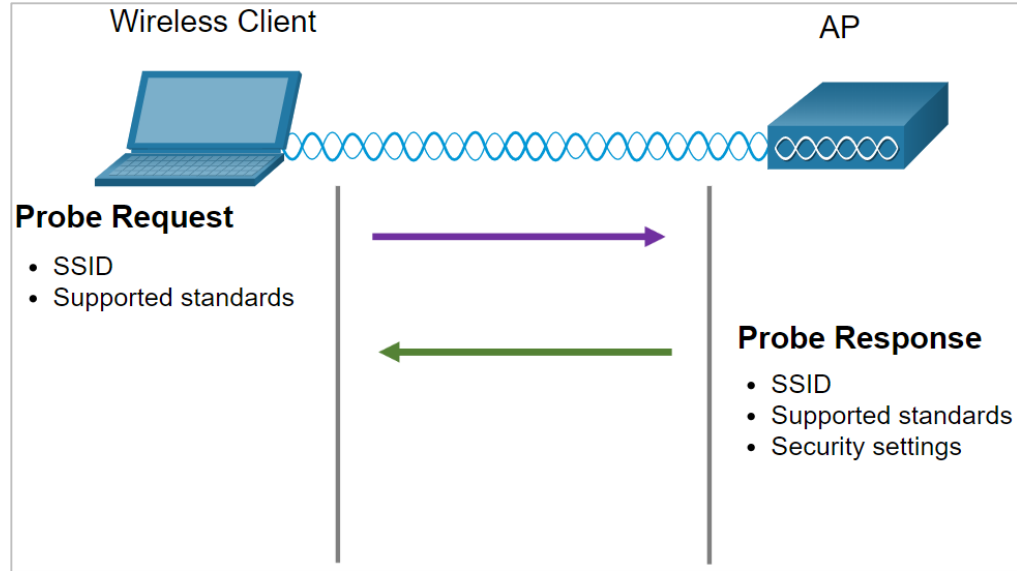
- In this mode, the AP openly advertises its service by periodically sending broadcast beacon frames containing the SSID, supported standards, and security settings.
- The primary purpose of the beacon is to allow wireless clients to learn which networks and APs are available in a given area.
- This allows the wireless clients to choose which network and AP to use.



Passive and Active Discover Mode (Contd.)

Active Mode

- In this 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 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 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.



- 

Wireless Devices - AP, LWAP, and WLC (Contd.)

- All of the control and management functions of the APs on a network can be centralized into a Wireless LAN Controller (WLC).
- When using a WLC, the APs no longer act autonomously, but instead act as lightweight APs (LWAPs).
- LWAPs only forward data between the wireless LAN and the WLC.
- All management functions, such as defining SSIDs and authentication are conducted on the centralized WLC rather than on each individual AP.
- A major benefit of centralizing the AP management functions in the WLC is simplified configuration and monitoring of numerous access points, among many other benefits.

11.3 Network Communication Devices Summary

What Did I Learn in this Module?

- End devices that are connected to a LAN connect to other LANs using an internetwork of intermediary devices such as routers and switches.
- Routers are network layer (i.e., Layer 3) devices and use the process of routing to forward data packets between networks or sub networks.
- Routers provide Path determination and Packet forwarding services.
- Switches segment a LAN into separate collision domains, one for each switch port.
- A switch makes forwarding decisions based on Ethernet MAC addresses that are contained in the Ethernet frame.
- Switches are configured with the Spanning Tree Protocol (STP) to maintain a loop-free Layer 2 path by intentionally blocking redundant paths that could cause a loop.
- Multilayer switches (also known as Layer 3 switches) not only perform Layer 2 switching, but also forward frames based on Layer 3 and 4 information.

What Did I Learn in this Module? (Contd.)

- A Cisco Catalyst multilayer switch supports routed ports and switch virtual interfaces (SVIs).
- Wireless networking devices connect to an Access Point (AP) or Wireless LAN Controller (WLC) using the 802.11 standard.
- The 802.11 frame format is similar to the Ethernet frame format, except that it contains additional fields.
- WLAN devices use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the method to determine how and when to send data on the network.
- To connect to the WLAN, wireless devices complete a three-stage process to discover a wireless AP, to authenticate with the AP, and to associate with the AP.
- APs can be configured autonomously (individually) or by using a WLC to simplify the configuration and monitoring of numerous access points.

