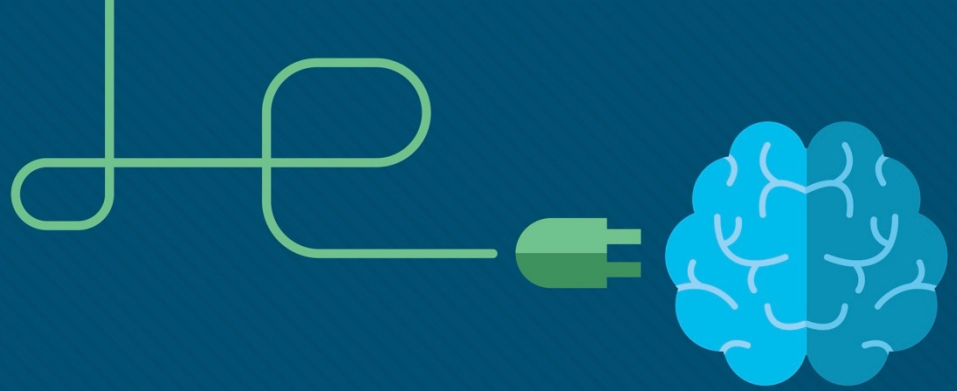


Chapter 4: Network Infrastructure

Information Security

Dr. Ayman Aljarbouh

4.2 Network Communication Devices

Module Objectives

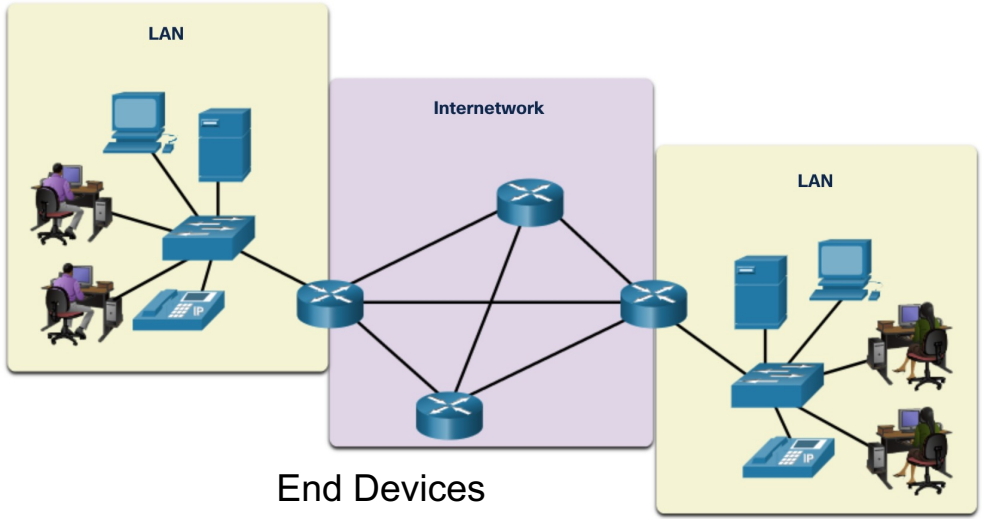
Module Title: Network Communication Devices

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

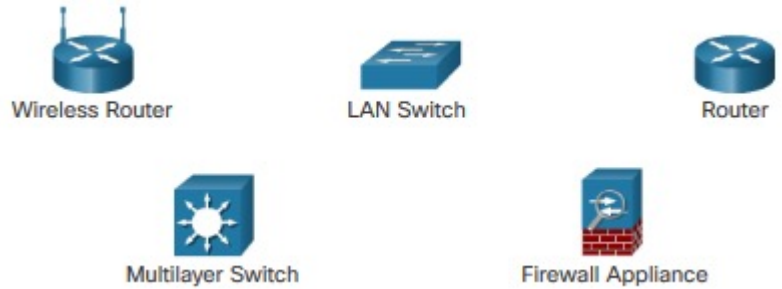
Topic Title	Topic Objective
Network Devices	Explain how network devices enable network communication.
Wireless Communications	Explain how wireless devices enable network communication.

End Devices

- End device is any device on the network that initiates communication, either source or destination.
- End Devices:
  - Computers, laptops, servers, printers, smart devices, and mobile devices.
  - Individual end devices are connected to the network by intermediary devices.
- Intermediary Devices:
  - Connect the individual end devices to the network and form an internetwork.
  - Provide connectivity and ensure that data flows across the network.



End Devices

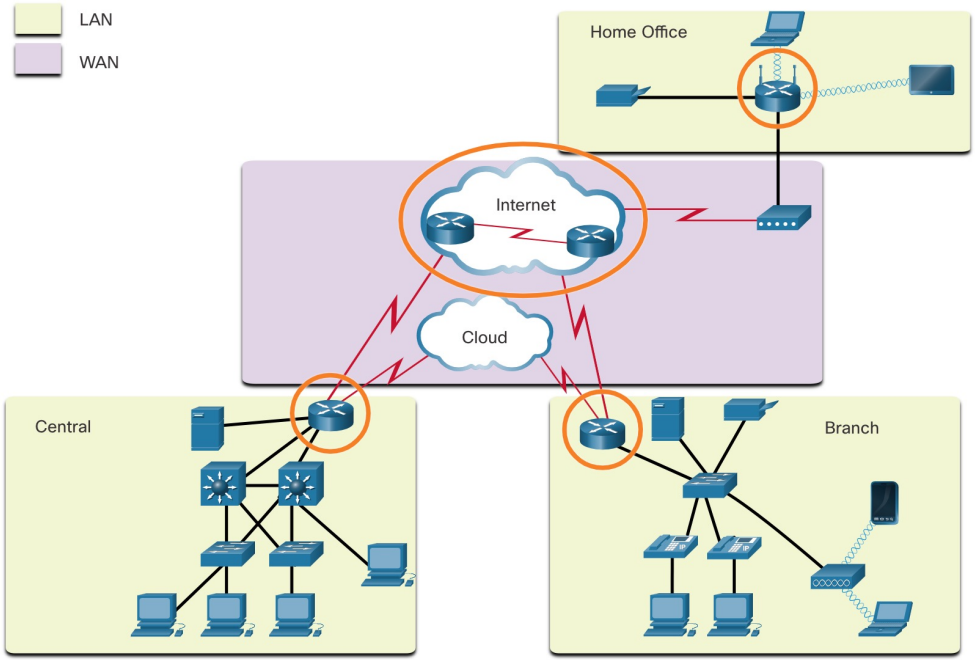


Intermediary Devices

Routers

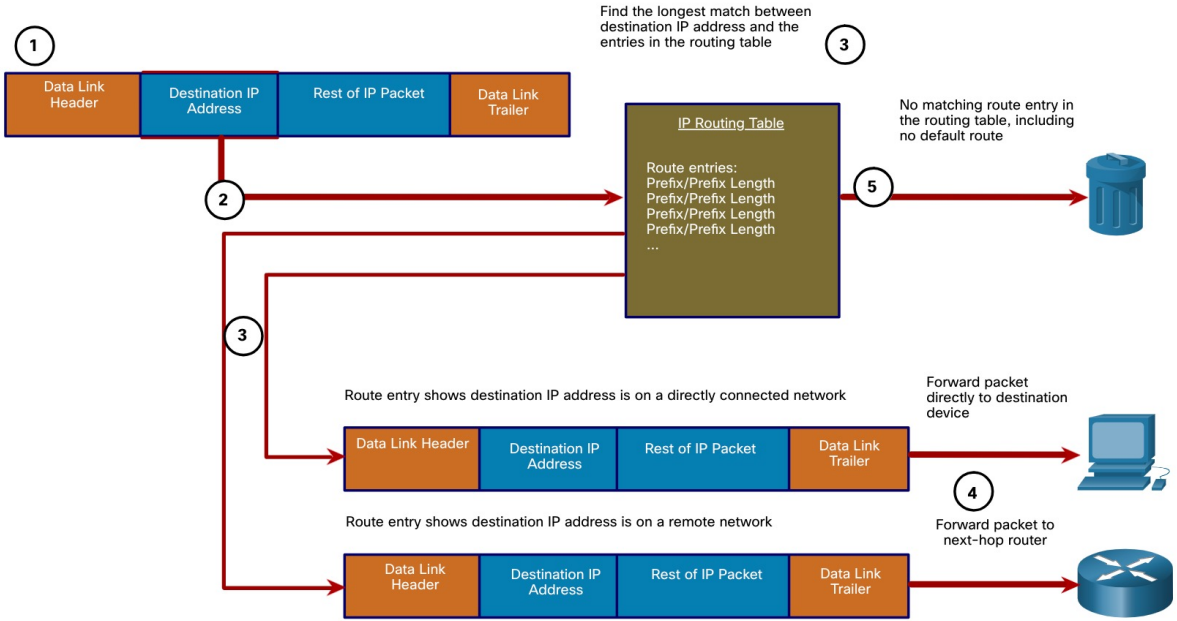
- Function of a Router:
  - Provides path determination and packet forwarding.
  - Responsible for encapsulating and de-encapsulating packets.
  - Uses a routing table to determine the best path to use to send packets to a specified network.
- Routing Table:
  - Contains directly connected routes and remote routes.
  - Router searches its routing table for a network address that matches the destination IP address of a packet.
  - Switching is the process used by a router to accept a packet on one interface and forward it out of another interface.

The Router Connection



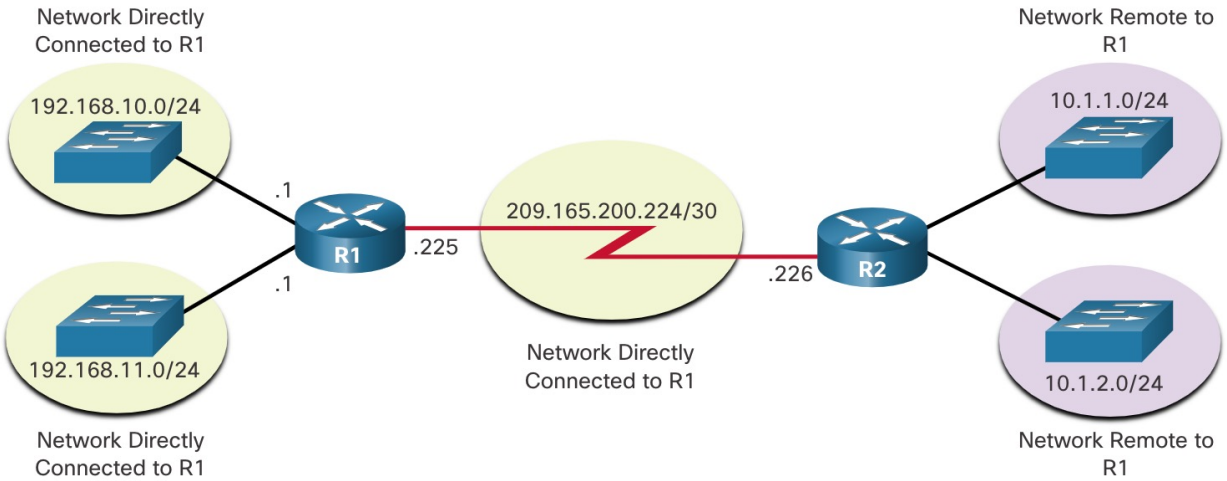
Packet Forwarding Decision Process

- To determine the best path, the router searches its routing table for a network address that matches the destination IP address of the packet.
- The routing table search results in one of three path determinations:
  - **Directly connected network**
  - **Remote network**
  - **No route determined**



Routing Information

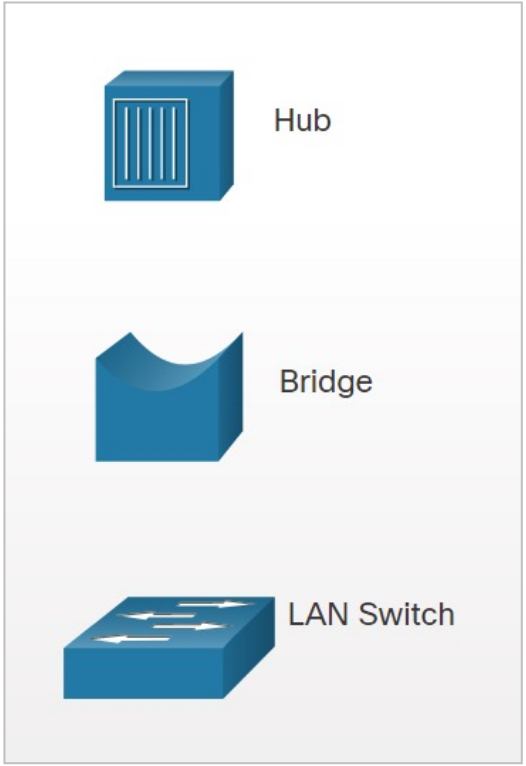
- The routing table of a router stores the following information:
  - **Directly connected routes** – These routes come from the active router interfaces.
  - **Remote routes** – These are remote networks connected to other routers.



https://www.youtube.com/watch?v=YRzr56cwgCg

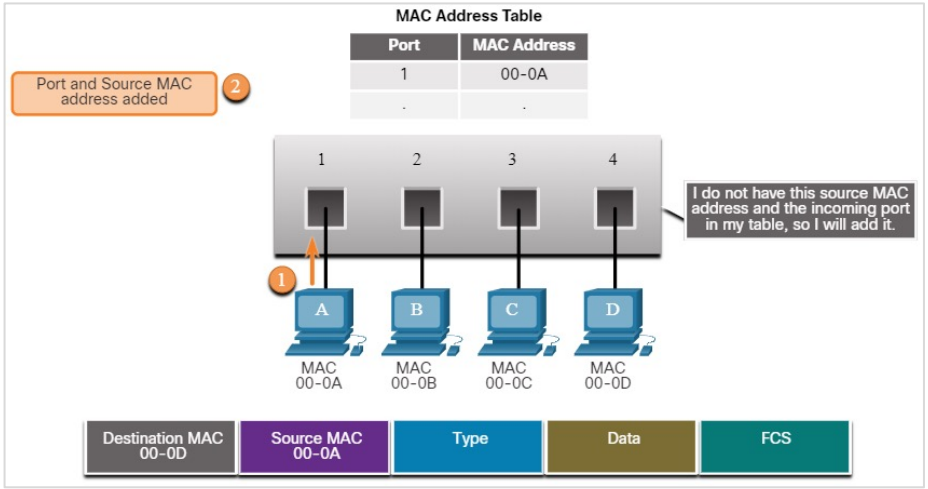
Hubs, Bridges, LAN Switches

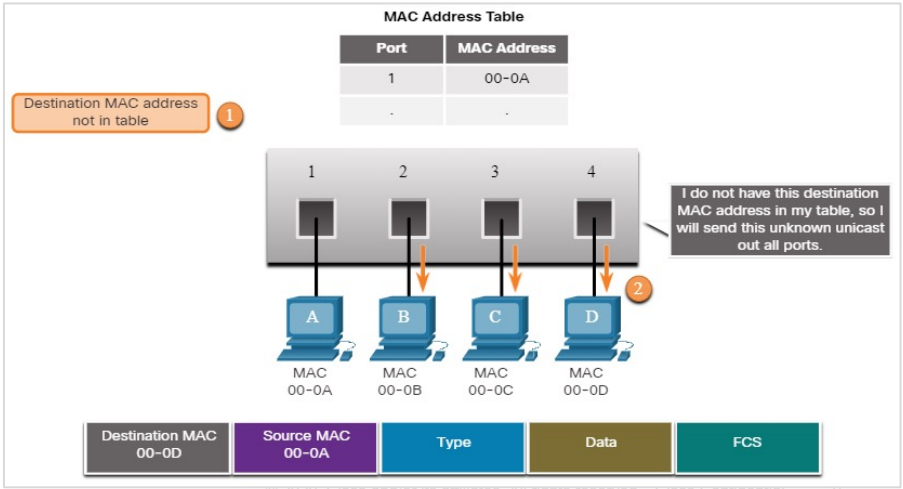
- The topology icons for hubs, bridges, and LAN switches are shown in the figure.
- An Ethernet hub acts as a multiport repeater that receives an incoming electrical signal (data) on a port. It then immediately forwards a regenerated signal out all other ports. Hubs use physical layer processing to forward 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

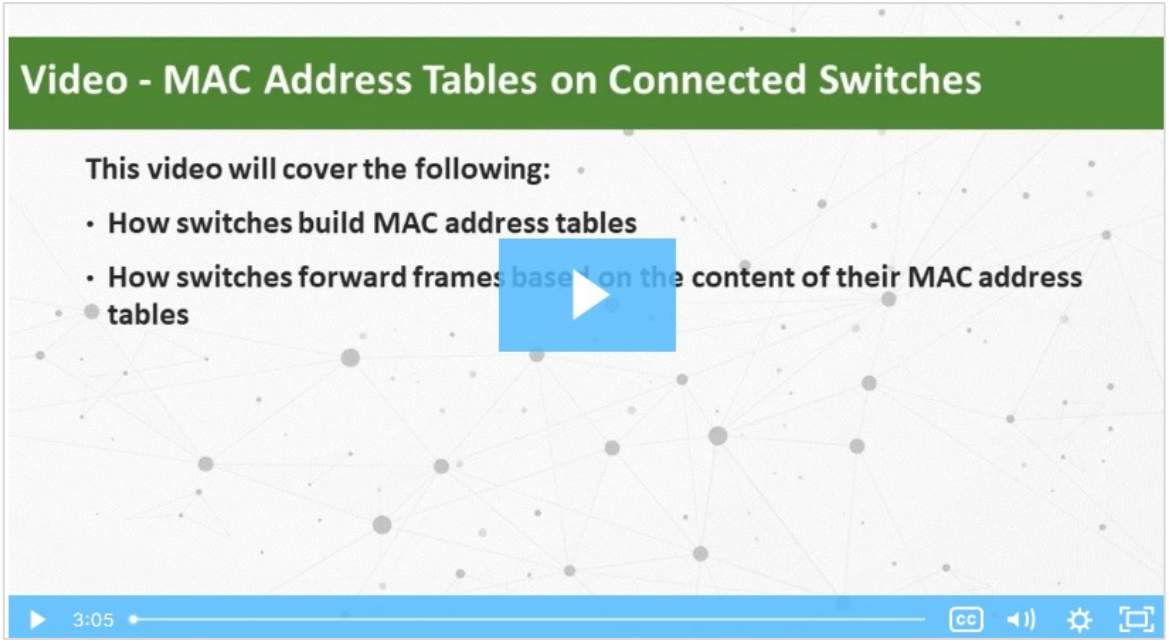
- Switches use MAC addresses to direct network communications through the switch, to the appropriate port, and toward the destination.
- The following two-step process is performed on every Ethernet frame that enters a switch:
  - Learn – Examining the Source MAC Address.
  - Forward – Examining the Destination MAC Address.





Video - MAC Address Tables on Connected Switches

- Play the video to see a demonstration of how two connected switches build their MAC address tables.



https://www.youtube.com/watch?v=epX5ED7rLiw

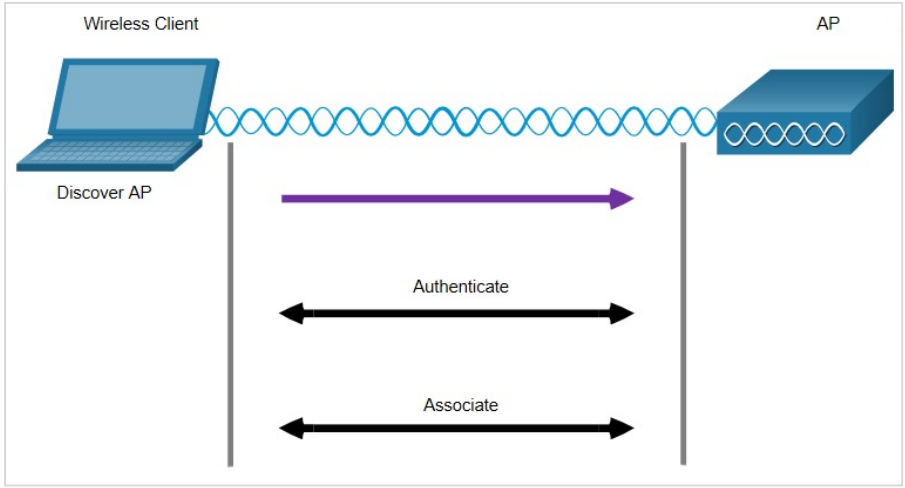
Protocols and Features

- Wireless LANs (WLANs):
  - Use Radio Frequencies (RF) instead of cables at the physical layer and MAC sublayer of the data link layer.
  - Connect clients to a network through a wireless access point (AP) or wireless router, instead of an Ethernet switch.
- 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

Wireless Client and AP Association

- Wireless client association process with AP includes discovering a new wireless AP, authenticating with that AP, then associating with that AP.



- Common configurable wireless parameters include:
  - **Network mode**
  - **SSID**
  - **Channel settings**
  - **Security mode**
  - **Encryption**
  - **Password**

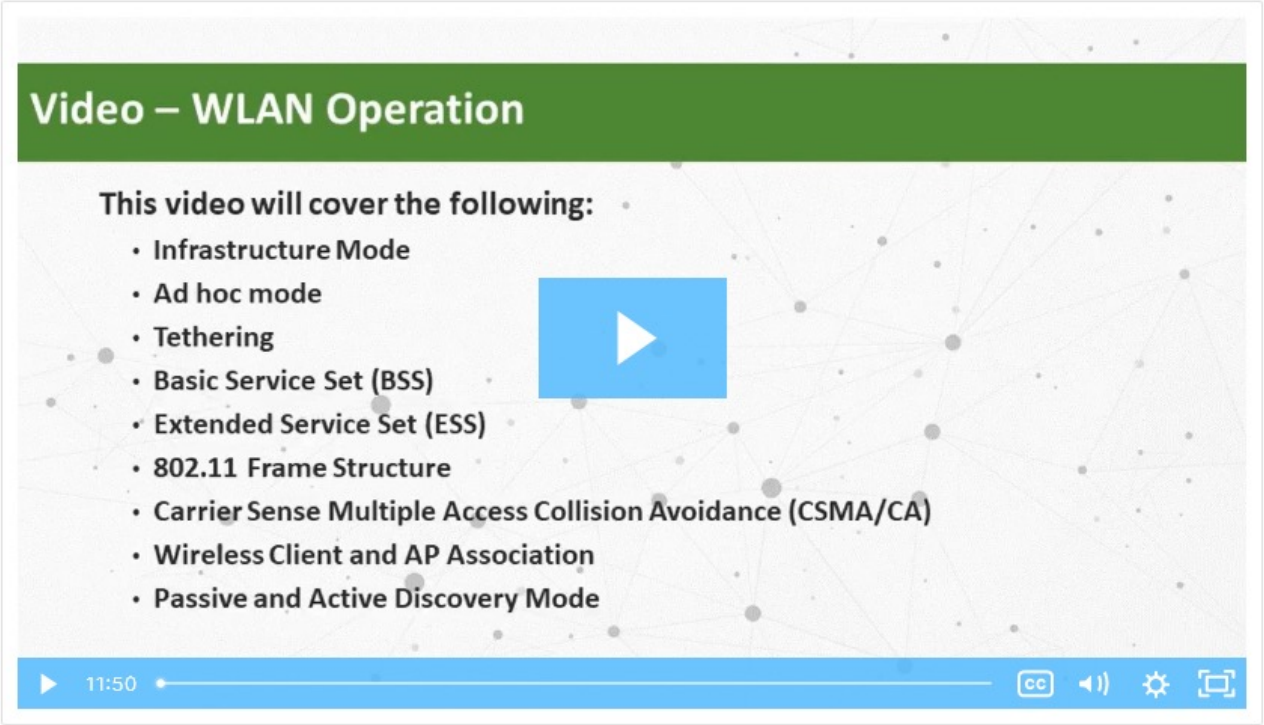
- Wireless devices must discover and connect to an AP or wireless router. This process can be passive or active.
- The 802.11 standard was originally developed with two authentication mechanisms: **open authentication** provides wireless connectivity to any wireless device, and the **shared key authentication** technique is based on a key that is pre-shared between the client and the AP.

Wireless Devices - AP, LWAP, and WLC

- Access Point (AP):
  - **Small network** – usually a wireless router that integrates the functions of a router.
  - **Large network** – can be many APs.
- Wireless LAN Controller (WLC):
  - Controls and manages the functions of the APs on a network.
  - Simplifies configuration and monitoring of numerous APs.
- Lightweight AP (LWAP):
  - Centralized management by WLC.
  - No longer acts autonomously.

Video - Wireless Communications

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



https://www.youtube.com/watch?v=gwoHhGcyQHQ

New Terms and Commands

• Wireless LAN Controller (WLC) • Access Point (AP)	• Lightweight AP (LWAP)

Lab 18 - ACL Demonstration

In this lab, you will observe the following:

- How an ACL can be used to prevent a ping from reaching hosts on remote networks.
- After removing the ACL from the configuration, the pings will be successful.