Wireless & Mobile Computing

First Semester 3rd Class

Lecture Five

2025/2024

Wi-Fi: 802.11 Wireless LANs

- The home, educational institutions, cafés, airports, and street corners, wireless LANs are now one of the most important access network technologies in the Internet today.
- One particular class of standards has clearly emerged as the winner: the IEEE 802.11 wireless LAN, also known as WiFi.
- There are several 802.11 standards [IEEE 802.11 2020].
- The 802.11 b, g, n, ac, ax are successive generations of 802.11 technology aimed for wireless local area networks (WLANs), typically less than 70 m range in a home office, workplace, or business setting.
- The 802.11 n, ac, and ax standards have recently been branded as WiFi 4, 5 and 6, respectively.
- The 802.11 af, ah standards operate over longer distances and are aimed at Internet of Things, sensor networks, and metering applications.

Wi-Fi: 802.11 Wireless LANs

- The different 802.11 b, g, n, ac, ax standards all share some common characteristics, including the 802.11 frame format.
- For example, that a mobile capable only of 802.11 g may still interact with a newer 802.11 ac or 802.11 ax base station.
- They also all use the same medium access protocol, *carrier sense multiple access with collision avoidance (CSMA/CA)*.

Wi-Fi: 802.11 Wireless LANs

- The standards have some major differences at the physical layer.
- 802.11 devices operate in two different frequency ranges:
- 2.4–2.485 GHz (referred to as the 2.4 GHz range) and 5.1–5.8 GHz (referred to as the 5 GHz range).
- The 2.4 GHz range is an unlicensed frequency band, where 802.11 devices may compete for frequency spectrum with 2.4 GHz phones and appliances such as microwave ovens.
- Devices that use this band, including 802.11 Wi-Fi standards (like 802.11b/g/n) and other electronics like cordless phones, Bluetooth devices, and microwave ovens, all compete for the limited available frequency spectrum.
- This competition can lead to signal interference and degraded performance in networks operating on this frequency

- At 5 GHz, 802.11 LANs have a shorter transmission distance for a given power level.
- The 802.11n, 802.11ac, and 802.11ax standards use multiple input multiple-output (MIMO) antennas; that is, two or more antennas on the sending side and two or more antennas on the receiving side that are transmitting/receiving different signals.

Wi-Fi: 802.11 Wireless LANs

- A **licensed frequency band** refers to portions of the radio frequency spectrum that require a government-issued license for use.
- These bands are regulated by national telecommunications authorities (such as the **FCC** in the United States or **Ofcom** in the UK) to ensure that usage is controlled, preventing interference between different services and users.
- Licensed spectrum is often used for **critical communication services**, such as cellular networks, television broadcasts, and emergency services, where reliable and interference-free communication is essential.

Wi-Fi: 802.11 Wireless LANs

IEEE 802.11 standard	Year	Max data rate	Range Frequency
802.11 b	1999	11 Mbps 30 m	2.4 Ghz
802.11 g	2003	54 Mbps 30 m	2.4 Ghz
802.11 n (WiFi 4)	2009	600 70 m	2.4, 5 Ghz
802.11 ac (WiFi 5)	2013	3.47 Gpbs 70 m	5 Ghz
802.11 ax (WiFi 6)	2020	14 Gbps 70 m	2.4, 5 Ghz
802.11 af	2014	35–560 Mbps	1 Km unused TV bands (54–790 MHz)
802.11 ah	2017	347 Mbps	1 Km 900 Mhz

Wi-Fi: 802.11 Wireless LANs

- **Wi-Fi 7** (also known as **802.11be** or **Extremely High Throughput (EHT)**) is the next-generation Wi-Fi standard, following Wi-Fi 6 (802.11ax), and is designed to significantly enhance wireless connectivity performance, capacity, and efficiency.
- It introduces several advanced technologies aimed at supporting increasingly demanding applications such as **virtual reality (VR)**, **augmented reality (AR)**, **8K streaming**, **cloud gaming**, and the massive growth of **IoT devices**.
- Wi-Fi 7 is expected to deliver **multi-gigabit speeds**, lower latency, and improved support for dense network environments.

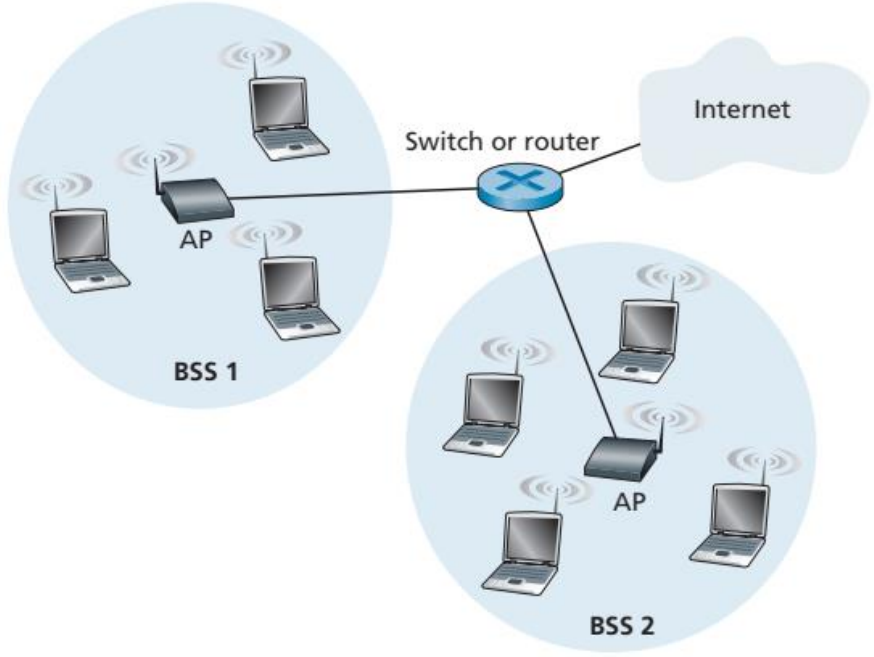
Wi-Fi: 802.11 Wireless LANs

- 802.11ac and 802.11ax base stations may transmit to multiple stations simultaneously,
- Use “smart” antennas to adaptively beamform to target transmissions in the direction of a receiver.
- This decreases interference and increases the distance reached at a given data rate.

Wi-Fi: 802.11 Wireless LANs

- The 802.11 Wireless LAN Architecture

- The fundamental building block of the 802.11 architecture is the **basic service set (BSS)**.
- A BSS contains one or more wireless stations and a central **base station**, known as an **access point (AP)** in 802.11. Figure shows the AP in each of two BSSs connecting to an interconnection device (such as a switch or router), which in turn leads to the Internet.

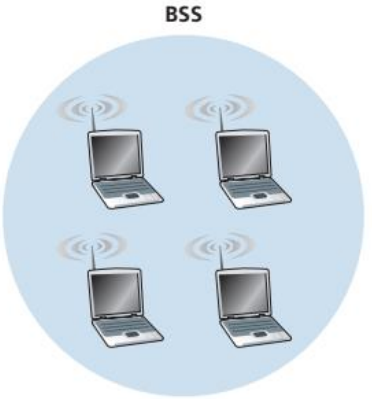


Wi-Fi: 802.11 Wireless LANs

- In a typical home network, there is one AP and one router (typically integrated together as one unit) that connects the BSS to the Internet.

- As with Ethernet devices, each 802.11 wireless station has a 6-byte MAC address that is stored in the firmware of the station's adapter (that is, 802.11 network interface card).
- Each AP also has a MAC address for its wireless interface.
- As with Ethernet, these MAC addresses are administered by IEEE and are (in theory) globally unique.

Wi-Fi: 802.11 Wireless LANs



- Wireless LANs that deploy APs are often referred to as infrastructure wireless LANs, with the “infrastructure” being the APs along with the wired Ethernet infrastructure that interconnects the APs and a router.
- Figure shows that IEEE 802.11 stations can also group themselves together to form an ad hoc network—a network with no central control and with no connections to the “outside world.”
- An ad hoc network might be formed when people with laptops get together (e.g., in a conference room, a train, or a car) and want to exchange data in the absence of a centralized AP

CSMA/CA

- WLANs are half-duplex, shared media configurations.
- Half-duplex means that only one client can transmit or receive at any given moment.
- Shared media means that wireless clients can all transmit and receive on the same radio channel.
- This creates a problem because a wireless client cannot hear while it is sending, which makes it impossible to detect a collision.
- To resolve this problem, WLANs use *carrier sense multiple access with collision avoidance (CSMA/CA)* as the method to determine how and when to send data on the network.
- A wireless client does the following:

1. Listens to the channel to see if it is idle, which means that it senses no other traffic is currently on the channel. The channel is also called the carrier.

2. Sends a ready to send (RTS) message to the AP to request dedicated access to the network.

CSMA/CA

3. Receives a clear to send (CTS) message from the AP granting access to send.
4. If the wireless client does not receive a CTS message, it waits a random amount of time before restarting the process.
5. After it receives the CTS, it transmits the data.
6. All transmissions are acknowledged. If a wireless client does not receive an acknowledgment, it assumes a collision occurred and restarts the process.

Wireless Client and AP Association

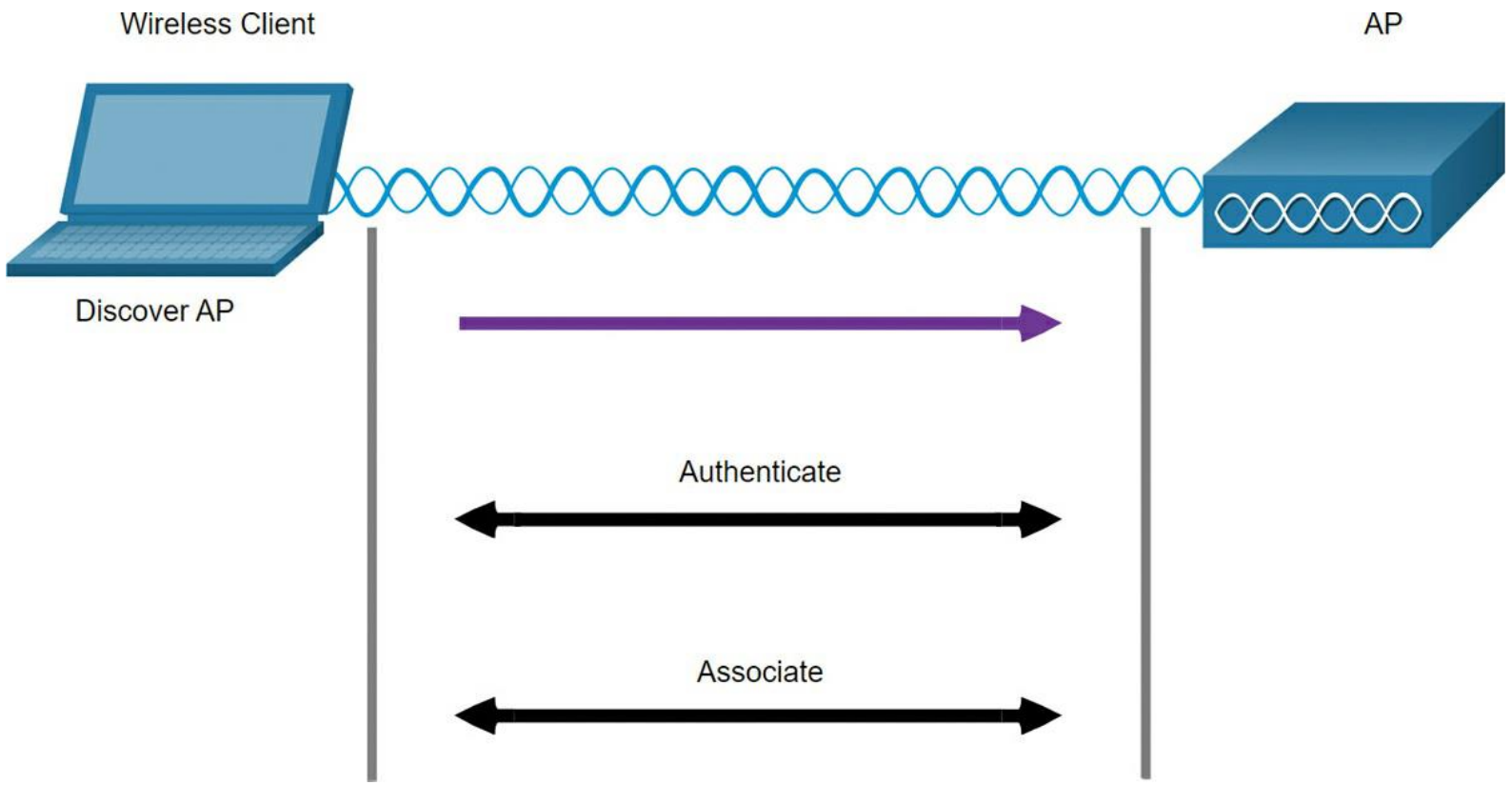
For wireless devices to communicate over a network, they must first associate with an AP or wireless router.

An important part of the 802.11 process is discovering a WLAN and subsequently connecting to it.

Wireless devices complete the three stage process.

Wireless Client and AP Association

1. Discover a wireless AP.
2. Authenticate with AP.
3. Associate with AP.



Wireless Client and AP Association

- To have a successful association, a wireless client and an AP must agree on specific parameters.
- Parameters must then be configured on the AP and subsequently on the client to enable the negotiation of a successful association.
- **SSID**
- The SSID name appears in the list of available wireless networks on a client.
- In larger organizations that use multiple VLANs to segment traffic, each SSID is mapped to one VLAN.
- Depending on the network configuration, several APs on a network can share a common SSID.
- **Password**
- This is required from the wireless client to authenticate to the AP.

Wireless Client and AP Association

- **Network mode**
- This refers to the 802.11a/b/g/n/ac/ad WLAN standards.
- APs and wireless routers can operate in a Mixed mode, meaning that they can at same time support clients connecting via multiple standards.
- **Security mode**
- This refers to the security parameter settings, such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, or WPA3. Always enable the highest security level supported.
- **Channel settings**
- This refers to the frequency bands used to transmit wireless data.
- Wireless routers and APs can scan the radio frequency channels and automatically select an appropriate channel setting.
- The channel can also be set manually if there is interference with another AP or wireless device.

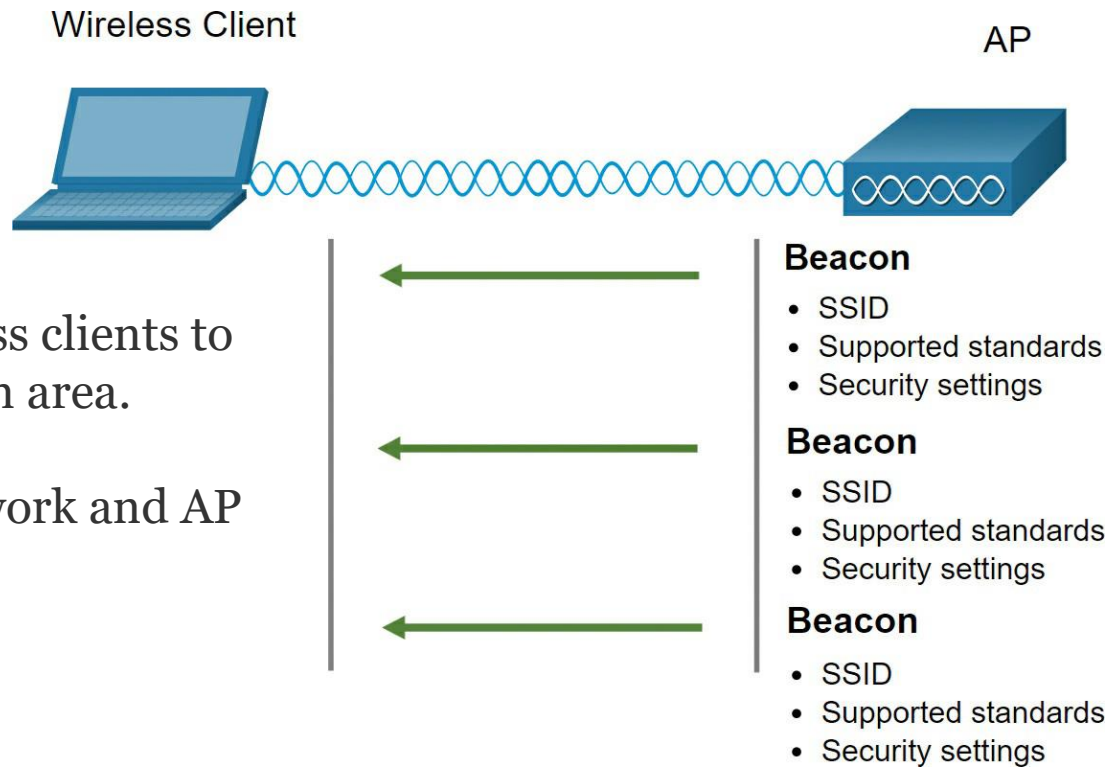
Passive and Active Discover Mode

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

- **Passive Mode**
- In passive mode, the AP openly advertises its service by periodically sending broadcast beacon frames containing the
- SSID, supported standards, and security settings.

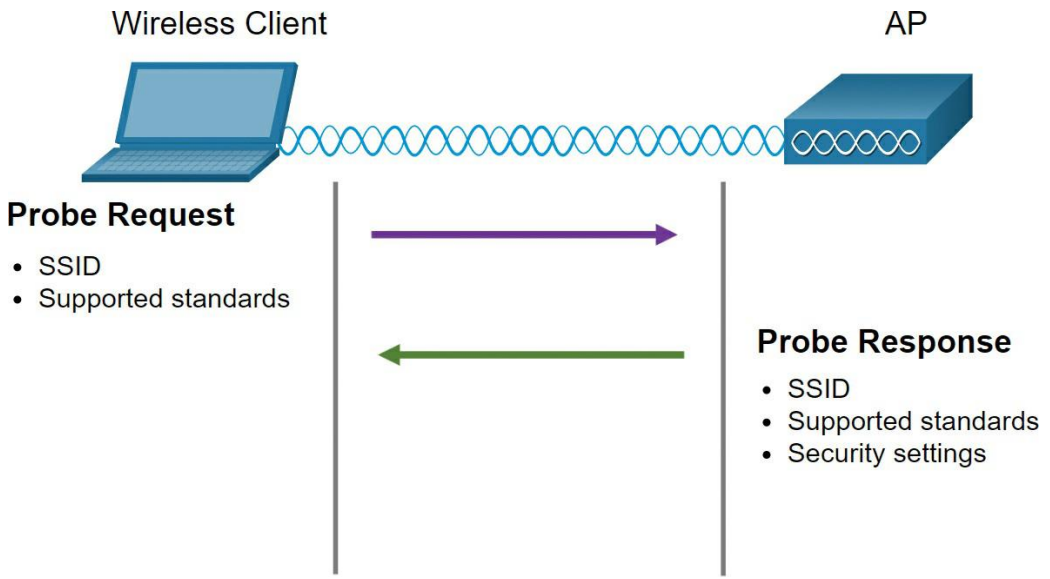
Passive and Active Discover Mode

- 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

- **Active Mode**
- In active mode, wireless clients must know the name of the SSID.
- The wireless client initiates the process by broadcasting a probe request frame on multiple channels,



Passive and Active Discover Mode

- The probe request includes the SSID name and standards supported.
- APs configured with the SSID will send a probe response that includes the SSID, supported standards, and security settings.
- Active mode may be required if an AP or wireless router is configured to not broadcast beacon frames.
- A wireless client could also send a probe request without a SSID name to discover nearby WLAN networks.
- APs configured to broadcast beacon frames would respond to the wireless client with a probe response and provide the SSID name.
- APs with the broadcast SSID feature disabled do not respond.