Wireless & Mobile Computing

First Semester 3rd Class

Lecture Seven

2025/2024

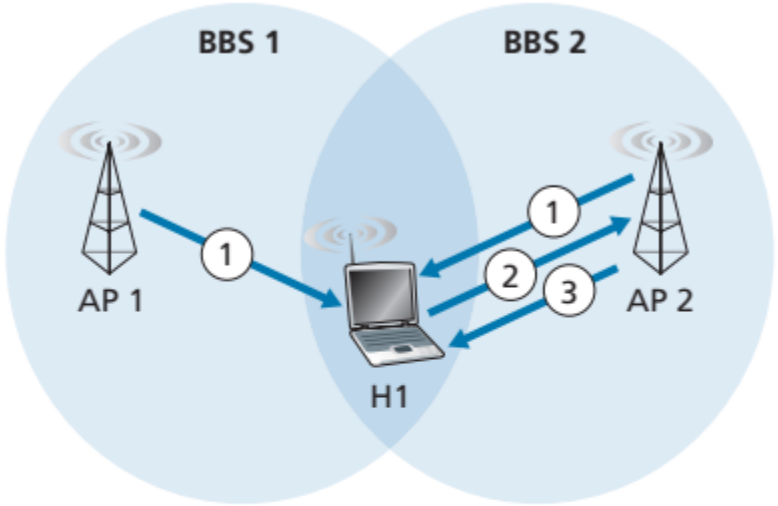
Wi-Fi: 802.11 Wireless LANs

- **How does your wireless device associate with a particular AP?**
- **How does your wireless device know which APs, if any, are out there in the jungle?**
- The 802.11 standard does not specify an algorithm for selecting which of the available APs to associate with;
- that algorithm is left up to the designers of the 802.11firmware and software in your wireless device.
- Typically, the device chooses the AP whose beacon frame is received with the highest signal strength.
- It’s possible that the selected AP may have a strong signal, but may be overloaded with other affiliated devices.

Wi-Fi: 802.11 Wireless LANs

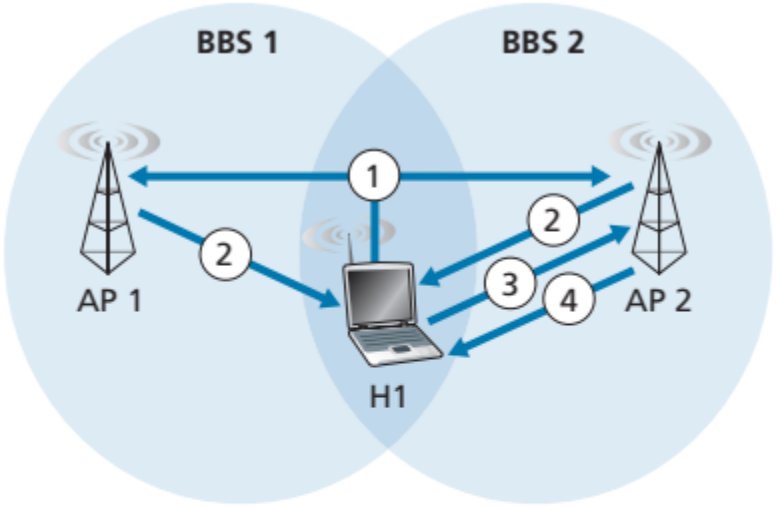
- The process of scanning channels and listening for beacon frames is known as passive scanning.
- A wireless device can also perform active scanning, by broadcasting a probe frame that will be received by all APs within the wireless device's range, as shown in Figure.
- APs respond to the probe request frame with a probe response frame.
- The wireless device can then choose the AP with which to associate from among the responding APs.

Wi-Fi: 802.11 Wireless LANs



a. Passive scanning

1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent: Selected AP to H1



a. Active scanning

1. Probe Request frame broadcast from H1
2. Probes Response frame sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent: Selected AP to H1

Wi-Fi: 802.11 Wireless LANs

- After selecting the AP with which to associate, the wireless device sends an association request frame to the AP, and the AP responds with an association response frame.
- Note that this second request/response handshake is needed with active scanning, since an AP responding to the initial probe request frame doesn't know which of the (possibly many) responding APs the device will choose to associate with.
- In order to create an association with a particular AP, the wireless device may be required to authenticate itself to the AP. 802.11 wireless LANs provide a number of alternatives for authentication and access.
- One approach, used by many companies, is to permit access to a wireless network based on a device's MAC address. A second approach, used by many Internet cafés, employs usernames and passwords.

Wi-Fi: 802.11 Wireless LANs

- Once a wireless device is associated with an AP, it can start sending and receiving data frames to and from the access point. But because multiple wireless devices, or the
- AP itself may want to transmit data frames at the same time over the same channel, a multiple access protocol is needed to coordinate the transmissions.
- we'll refer to the devices or the AP as wireless “stations” that share the multiple access channel.
-

The 802.11 MAC Protocol

- Once a wireless device is associated with an AP, it can start sending and receiving data frames to and from the access point.
- But because multiple wireless devices, or the AP itself may want to transmit data frames at the same time over the same channel,
- a multiple access protocol is needed to coordinate the transmissions.

- The designers of 802.11 chose a random access protocol for 802.11 wireless LANs.
- This random access protocol is referred to as CSMA with collision avoidance, or more succinctly as CSMA/CA.
- As with Ethernet's CSMA/CD, the "CSMA" in CSMA/CA stands for "carrier sense multiple access," meaning that each station senses the channel before transmitting, and refrains from transmitting when the channel is sensed busy.

The 802.11 MAC Protocol

- The random access protocol is referred to as CSMA with collision avoidance, or more succinctly as CSMA/CA.
- As with Ethernet's CSMA/CD, the "CSMA" in CSMA/CA stands for "carrier sense multiple access," meaning that each station senses the channel before transmitting, and refrains from transmitting when the channel is sensed busy.
- Although both Ethernet and 802.11 use carrier-sensing random access,
- the two MAC protocols have important differences.
- First, instead of using collision detection, 802.11 uses collision-avoidance techniques.
- Second, because of the relatively high bit error rates of wireless channels, 802.11 (unlike Ethernet) uses a link-layer acknowledgment/retransmission (ARQ) scheme.

The 802.11 MAC Protocol

- Although both Ethernet and 802.11 use carrier-sensing random access,
- the two MAC protocols have important differences.
- First, instead of using collision detection, 802.11 uses collision-avoidance techniques.
- Second, 802.11 (unlike Ethernet) uses a link-layer acknowledgment/retransmission (ARQ) scheme.
- Ethernet's collision-detection algorithm, an Ethernet station listens to the channel as it transmits. If, while transmitting, it detects that another station is also transmitting, it aborts its transmission and tries to transmit again after waiting a small, random amount of time.
- Unlike the 802.3 Ethernet protocol, the 802.11 MAC protocol does not implement collision-detection. WHY?

The 802.11 MAC Protocol

- There are two important reasons for this:
- The ability to detect collisions requires the ability to send (the station's own
- signal) and receive (to determine whether another station is also transmitting) at the same time.
- Because the strength of the received signal is typically very small compared to the strength of the transmitted signal at the 802.11 adapter, it is costly to build hardware that can detect a collision.
- In 802.11 Wi-Fi networks, the received signal strength at the adapter is usually significantly weaker than the strength of the transmitted signal due to signal attenuation over distance, interference, and obstacles in the environment.
- This low signal strength makes it challenging to detect a collision.

CSMA/CA

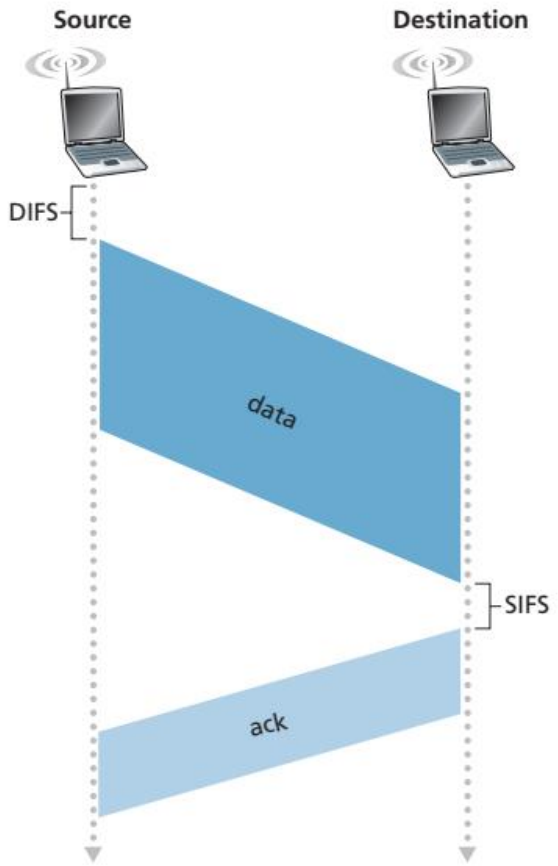
- WLANs are half-duplex, shared media configurations.
- Half-duplex means that only one client can transmit or receive at any given moment.
- Shared media means that wireless clients can all transmit and receive on the same radio channel.
- This creates a problem because a wireless client cannot hear 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

Because 802.11wireless LANs do not use collision detection, once a station begins to transmit a frame, it transmits the frame in its entirety; that is, once a station.
First need to examine 802.11's **link-layer acknowledgment** scheme.
When a station in a wireless LAN sends a frame, the frame may not reach the destination station intact for a variety of reasons.
To deal with this non-negligible chance of failure, the 802.11 MAC protocol uses link-layer acknowledgments.
As shown in Figure, when the destination station receives a frame that passes the **Cyclic Redundancy Check (CRC)**, it waits a short period of time known as the **Short Inter-frame Spacing (SIFS)** and then sends back an acknowledgment frame.
If the transmitting station does not receive an acknowledgment within a given amount of time, it assumes that an error has occurred and retransmits the frame, using the CSMA/CA protocol to access the channel.
If an acknowledgment is not received after some fixed number of retransmissions, the transmitting station gives up and discards the frame.



CSMA/CA

- Suppose that a station (wireless device or an AP) has a frame to transmit.
- 1. If initially the station senses the channel idle, it transmits its frame after a short period of time known as the Distributed Inter-frame Space (DIFS);
- 2. Otherwise, the station chooses a random backoff value using binary exponential and counts down this value after DIFS when the channel is sensed idle.
- While the channel is sensed busy, the counter value remains frozen.
- 3. When the counter reaches zero (note that this can only occur while the channel is sensed idle), the station transmits the entire frame and then waits for an acknowledgment.
- 4. If an acknowledgment is received, the transmitting station knows that its frame has been correctly received at the destination station.
- If the station has another frame to send, it begins the CSMA/CA protocol at step 2. If the acknowledgment isn’t received, the transmitting station reenters the backoff phase in step 2, with the random value chosen from a larger interval.

CSMA/CA

- Why do CSMA/CD and CDMA/CA take such different approaches here?
- Let’s consider a scenario in which two stations each have a data frame to transmit, but neither station transmits immediately because each senses that a third station is already transmitting.
- With Ethernet’s CSMA/CD, the two stations would each transmit as soon as they detect that the third station has finished transmitting.
- This would cause a collision, which isn’t a serious issue in CSMA/CD, since both stations would abort their transmissions and thus avoid the useless transmissions of the remainders of their frames.
- In 802.11, however, the situation is quite different.
- Because 802.11 does not detect a collision and abort transmission, a frame suffering a collision will be transmitted in its entirety.
- The goal in 802.11 is thus to avoid collisions whenever possible.
- In 802.11, if the two stations sense the channel busy, they both immediately enter random backoff, hopefully choosing different backoff values.
- If these values are indeed different, once the channel becomes idle, one of the two stations will begin transmitting before the other.

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

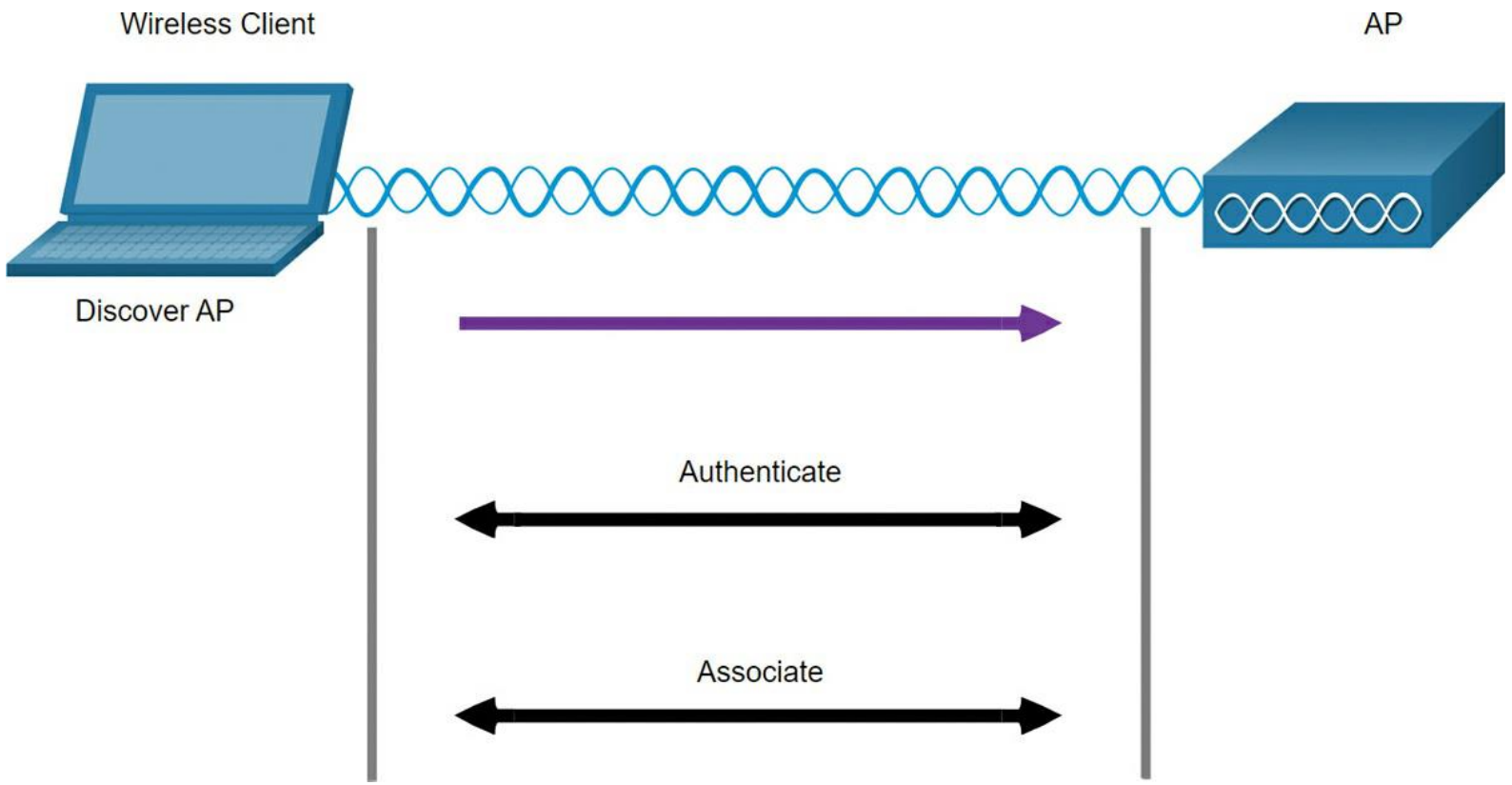
For wireless devices to communicate over a network, they must first associate with an AP or wireless router.

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.

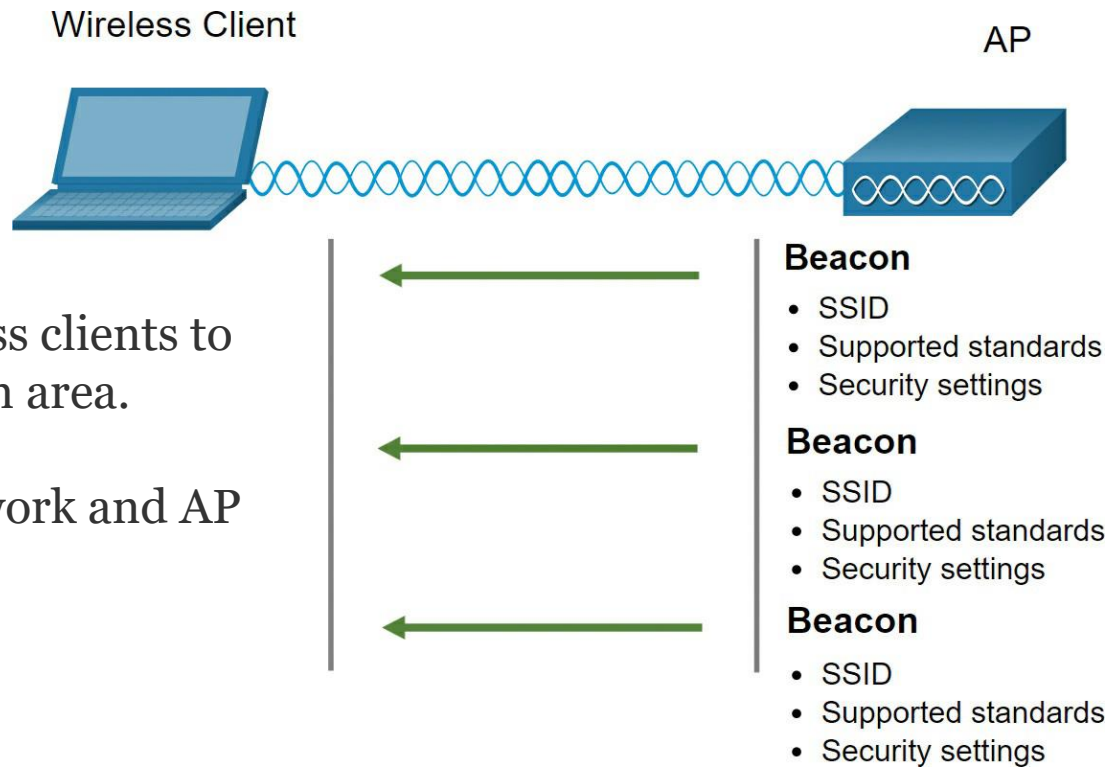
Passive and Active Discover Mode

- 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.

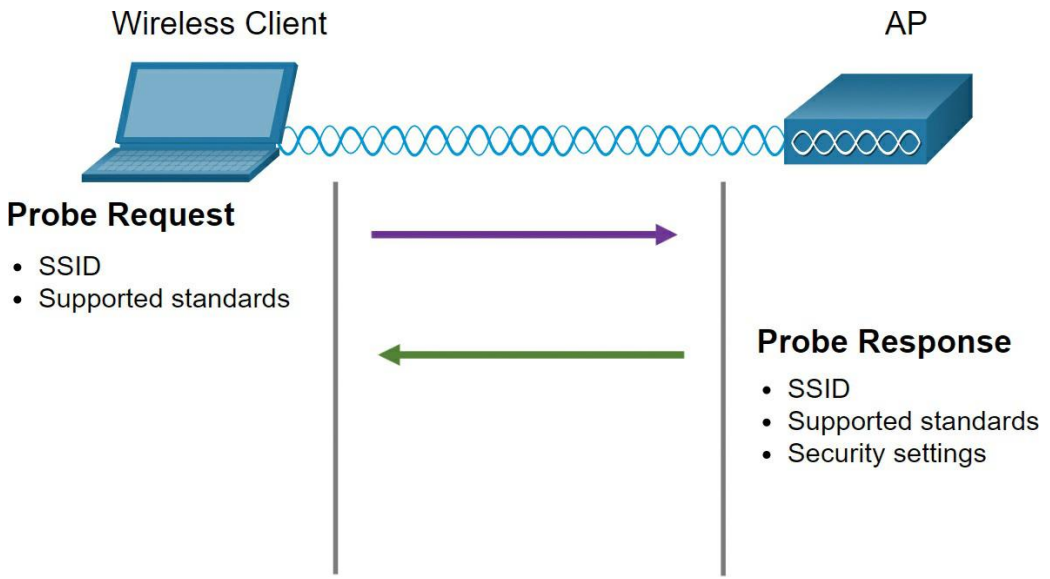
Passive and Active Discover Mode

- 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.