Wireless & Mobile Computing

First Semester 3rd Class

Lecture Four

2025/2024

WLAN COMPONENTS

1. Wireless NICs, Network Interface Card

- Wireless deployments require a minimum of two devices that have a radio transmitter and a radio receiver tuned to the same radio frequencies:
- End devices with wireless network interface cards (NICs)
- A network device, such as a wireless router or wireless access point (AP)

- To communicate wirelessly, laptops, tablets, smart phones, and even the latest automobiles include integrated wireless NICs that incorporate a radio transmitter/receiver.
- However, if a device does not have an integrated wireless NIC, a *USB wireless adapter* can be used.

WLAN COMPONENTS

2. Wireless Home Router

- The type of infrastructure device that an end device associates and authenticates with varies based on the size and requirement of the WLAN. For example, a home user typically interconnects wireless devices using a small, wireless router.

- *The wireless router serves as the following*:
- Access point: This provides 802.11a/b/g/n/ac wireless access.
- Switch: This provides a four-port, full-duplex, 10/100/1000 Ethernet switch to interconnect wired devices.
- Router: This provides a default gateway for connecting to other network infrastructures, such as the Internet.

WLAN COMPONENTS

- A wireless router is commonly implemented as a small business wireless access device.
- The wireless router advertises its wireless services by sending beacons containing
- its shared *service set identifier (SSID)*.
- Devices wirelessly discover the SSID and attempt to associate and authenticate with it to access the local network and Internet.
- Most wireless routers also provide advanced features, such as
- high-speed access, support for video streaming,
- IPv6 addressing, quality of service (QoS), configuration utilities,
- and USB ports to connect printers or portable drives.

WLAN COMPONENTS

- Additionally, home users who want to extend their network services can implement *Wi-Fi range extenders*.
- A device can connect wirelessly to the extender, which boosts its communications to be repeated to the wireless router.
- **Wireless Access Points**
- Although range extenders are easy to set up and configure, the best solution would be to install another wireless access point to provide dedicated wireless access to the user devices.
- 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.

WLAN COMPONENTS

- AP Categories
- APs can be categorized as either autonomous APs or controller based APs.

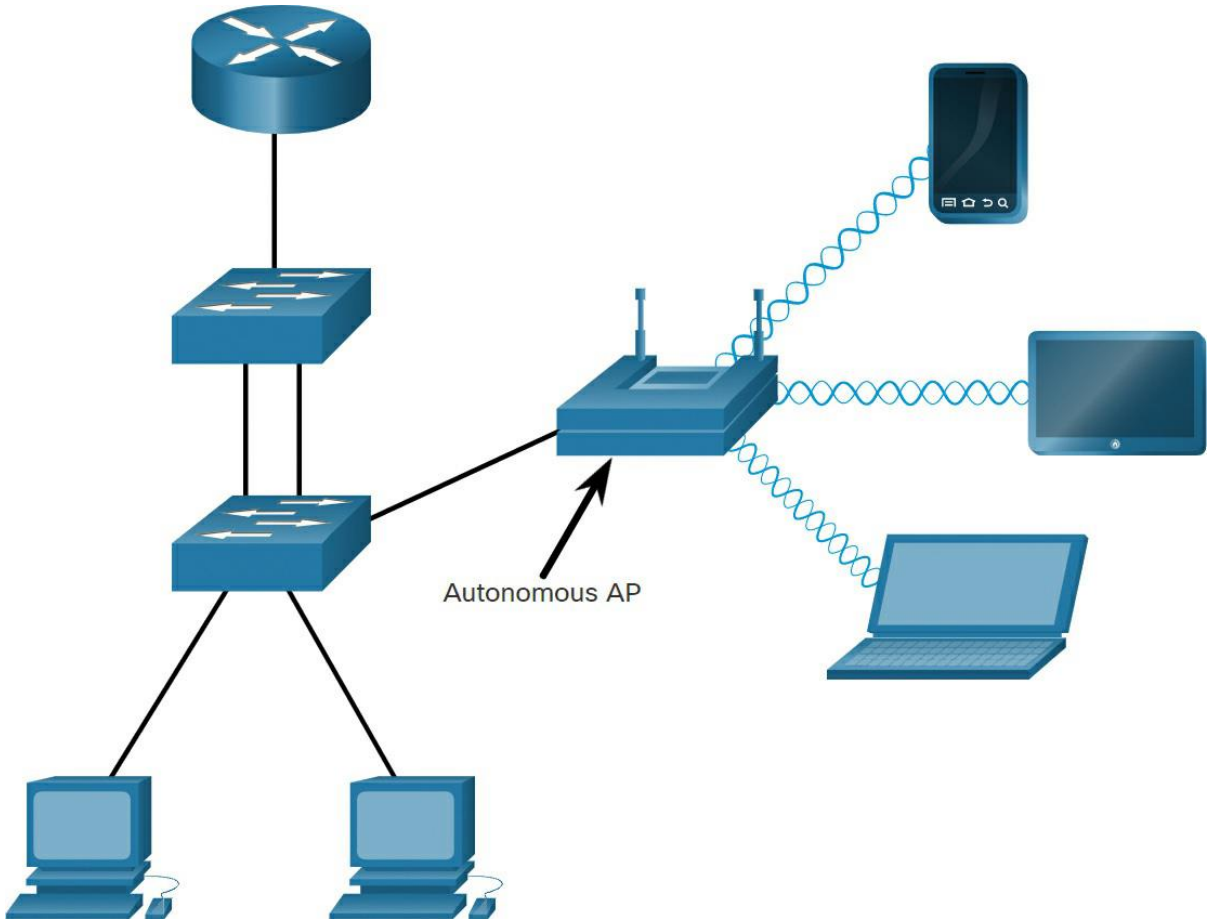
1. Autonomous APs

- These are standalone devices configured using a command line interface (CLI) or a graphical user interface (GUI).
- Autonomous APs are useful in situations where only a couple of APs are required in the organization.
- A home router is an example of an autonomous AP, because the entire AP configuration resides on the device.
- If the wireless demands increase, more APs would be required.
- Each AP would operate independently of other APs, and each AP would require manual
- configuration and management.
- This would become overwhelming (Wi-Fi Slowing Down) if many APs were needed.

WLAN COMPONENTS

- Having too many access points (APs) in close proximity can cause Wi-Fi performance issues due to factors like.
- Interference: When multiple APs operate on the same or overlapping channels, they can interfere with each other, leading to reduced throughput and increased latency. This is especially problematic in the 2.4 GHz band, where fewer non-overlapping channels are available.

Autonomous APs

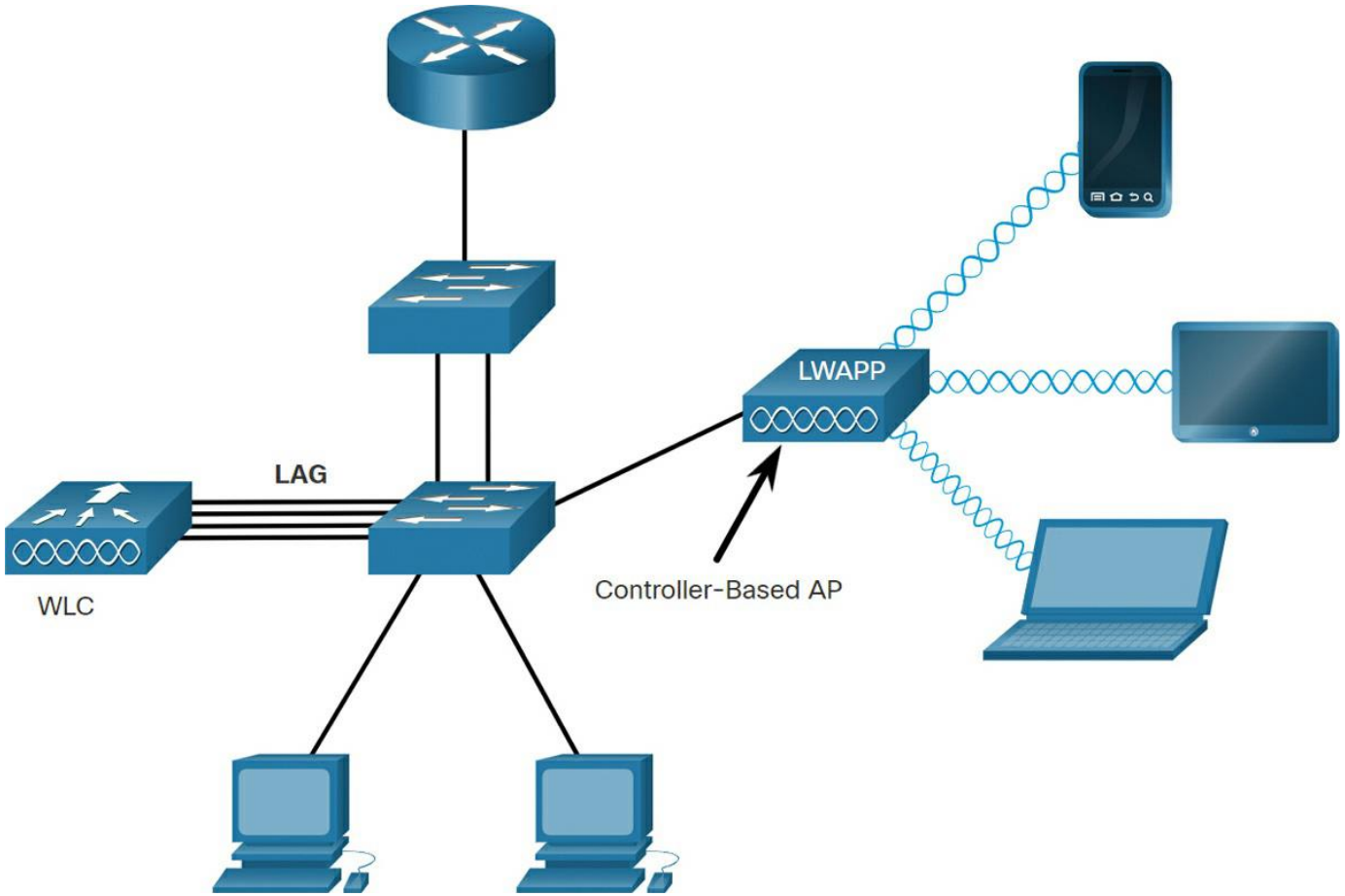


Controller-Based APs

2. Controller-Based APs

- These devices require no initial configuration and are often called lightweight APs (LAPs).
- LAPs use the Lightweight Access Point Protocol (LWAPP) to communicate with a WLAN
- controller (WLC).
- Controller-based APs are useful in situations where many APs are required in the network.
- As more APs are added, each AP is automatically configured and managed by the WLC.

Controller-Based APs



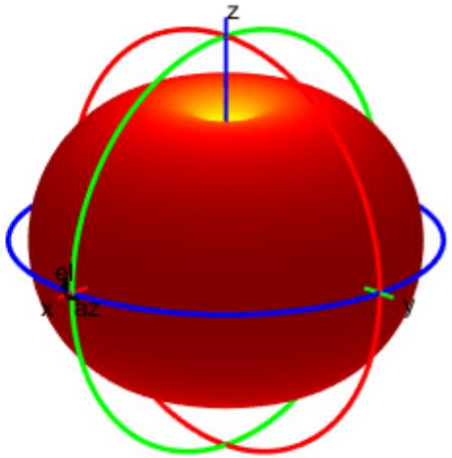
Controller-Based APs

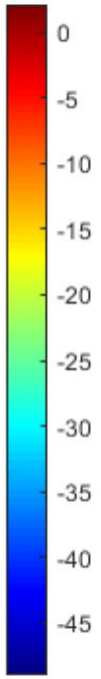
- Notice in the figure that the WLC has four ports connected to the switching infrastructure.
- These four ports are configured as a link aggregation group (LAG) to bundle them together.
- Much like how EtherChannel operates.
- LAG provides redundancy and load-balancing.
- All the ports on the switch that are connected to the WLC need to be trunking and configured with EtherChannel on. (Why?)
- to ensure that the switch ports are configured correctly for optimal performance and proper VLAN management. If you are using EtherChannel (or port aggregation) for link redundancy and increased bandwidth
- However, LAG does not operate exactly like EtherChannel !!!
- The WLC does not support Port Aggregation Protocol (PaGP) or Link Aggregation Control Protocol (LACP).
- PaGP Cisco proprietary protocol used to automate the creation of EtherChannel links.
- EtherChannel is a technology that allows multiple physical Ethernet links to be combined into one logical link to increase bandwidth and provide redundancy.

Wireless Antennas

- Most business class APs require external antennas to make them fully functioning units.

1. *Omnidirectional antennas*, provide 360-degree coverage and are ideal in houses, open office areas, conference rooms, and outside areas.





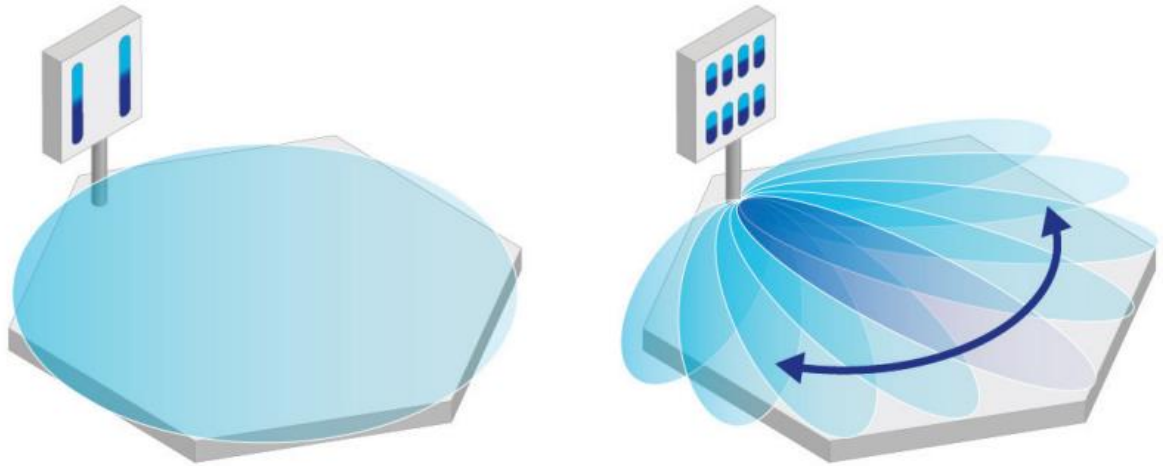
Wireless Antennas

2. *Directional antennas*

- focus the radio signal in a given direction.
- This enhances the signal to and from the AP in the direction the antenna is pointing.
- This provides a stronger signal strength in one direction and reduced signal strength in all other directions.
- Examples of directional Wi-Fi antennas include *Yagi antenna* and *parabolic dish antenna*.

Wireless Antennas

- *Multiple Input Multiple Output (MIMO)*
- uses multiple antennas to increase available bandwidth for IEEE 802.11n/ac/ax
- wireless networks.
- Up to eight transmit and receive antennas can be used to increase throughput.

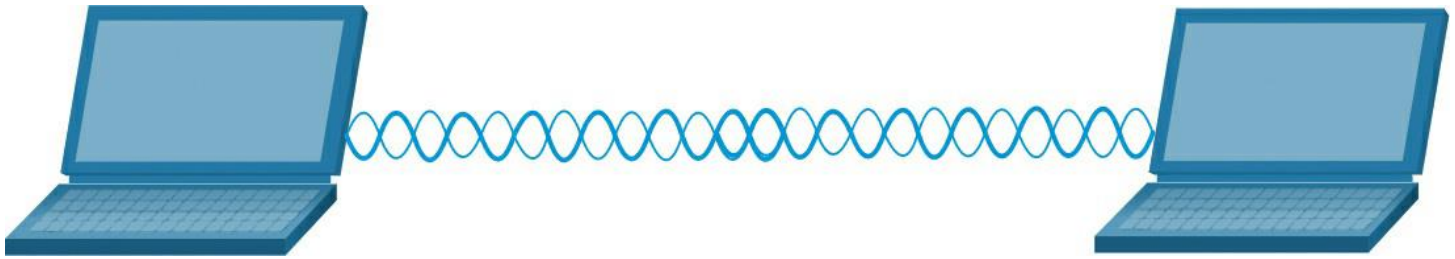


WLAN OPERATION

- *802.11 Wireless Topology Modes*
- Wireless LANs can accommodate various network topologies.
- The 802.11 standard identifies two main wireless topology modes:
- Ad hoc mode and Infrastructure mode

1. *Ad hoc mode*: This is when two devices connect wirelessly in a peer-to- peer (P2P) manner without using APs or wireless routers.

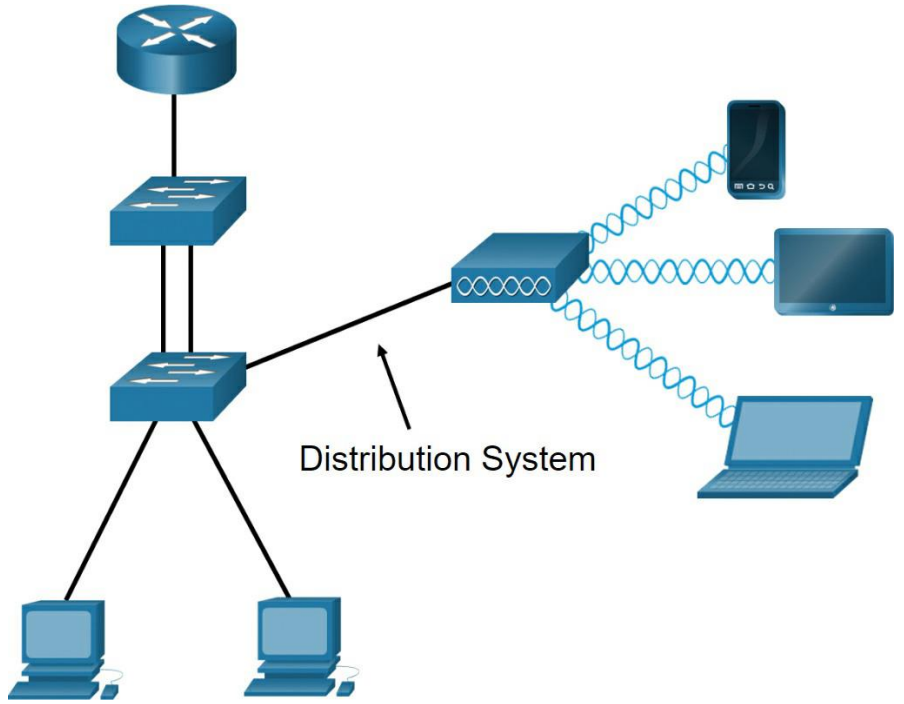
- Examples include wireless clients connecting directly to each other using Bluetooth or Wi-Fi Direct.
- The IEEE 802.11 standard refers to an ad hoc network as an *independent basic service set (IBSS)*.



WLAN OPERATION

2. *Infrastructure mode*:

- This is when wireless clients interconnect via a wireless router or AP, such as in WLANs.
- APs connect to the network infrastructure using the wired distribution system (WDS).
- WDS refers to the network infrastructure that uses wired connections (Ethernet, fiber optic, etc.) to distribute network services across different locations.



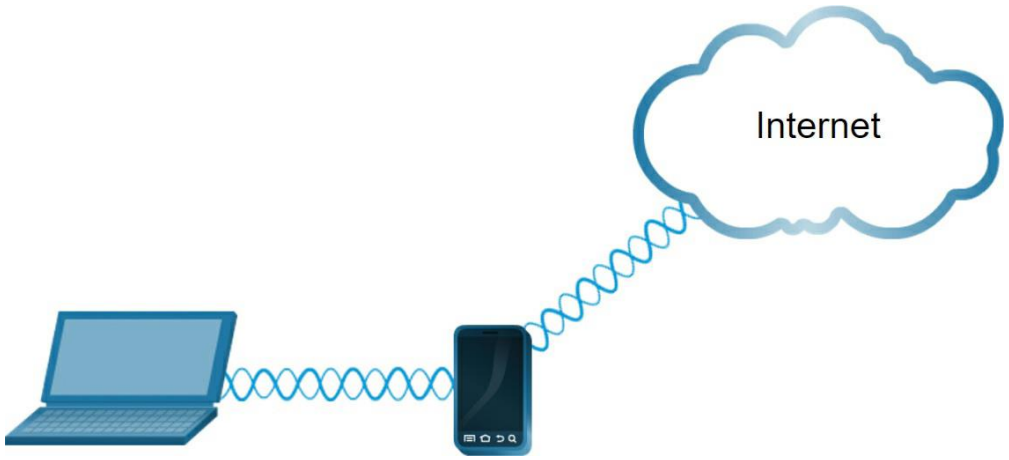
WLAN OPERATION

3. *Tethering*:

- A variation of the ad hoc topology is when a smart phone or tablet with cellular data access is enabled to create a personal *hotspot*.

This feature is sometimes referred to as tethering.

- A hotspot is usually a temporary, quick solution that enables a smart phone to provide the wireless services of a Wi-Fi router.
- Other devices can associate and authenticate with the smart phone to use the Internet connection.



WLAN OPERATION

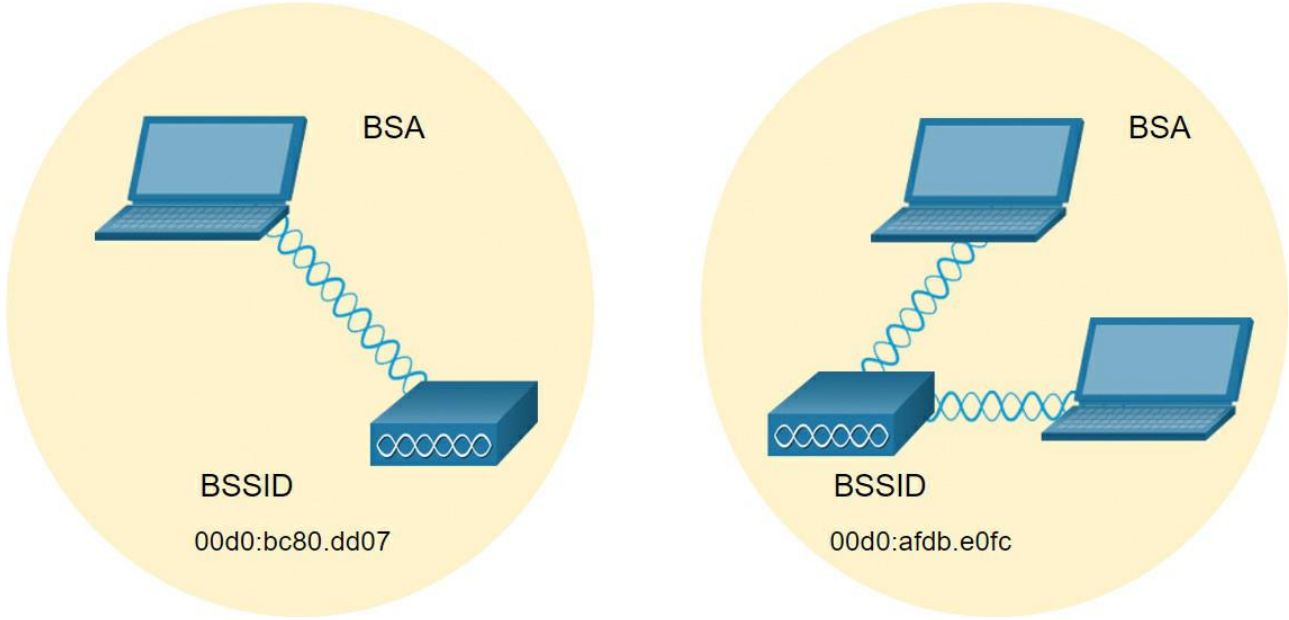
- Infrastructure mode defines two topology building blocks:-

1. *Basic Service Set (BSS).*
2. *Extended Service Set (ESS)*.

- *Basic Service Set BSS* consists of a single AP interconnecting all associated wireless clients.
- Two BSSs, whereas the circles depict the coverage area for the BSS, which is called the *Basic*
- *Service Area (BSA)*.
- If a wireless client moves out of its BSA, it can no longer directly communicate with other wireless clients within the BSA.

WLAN OPERATION

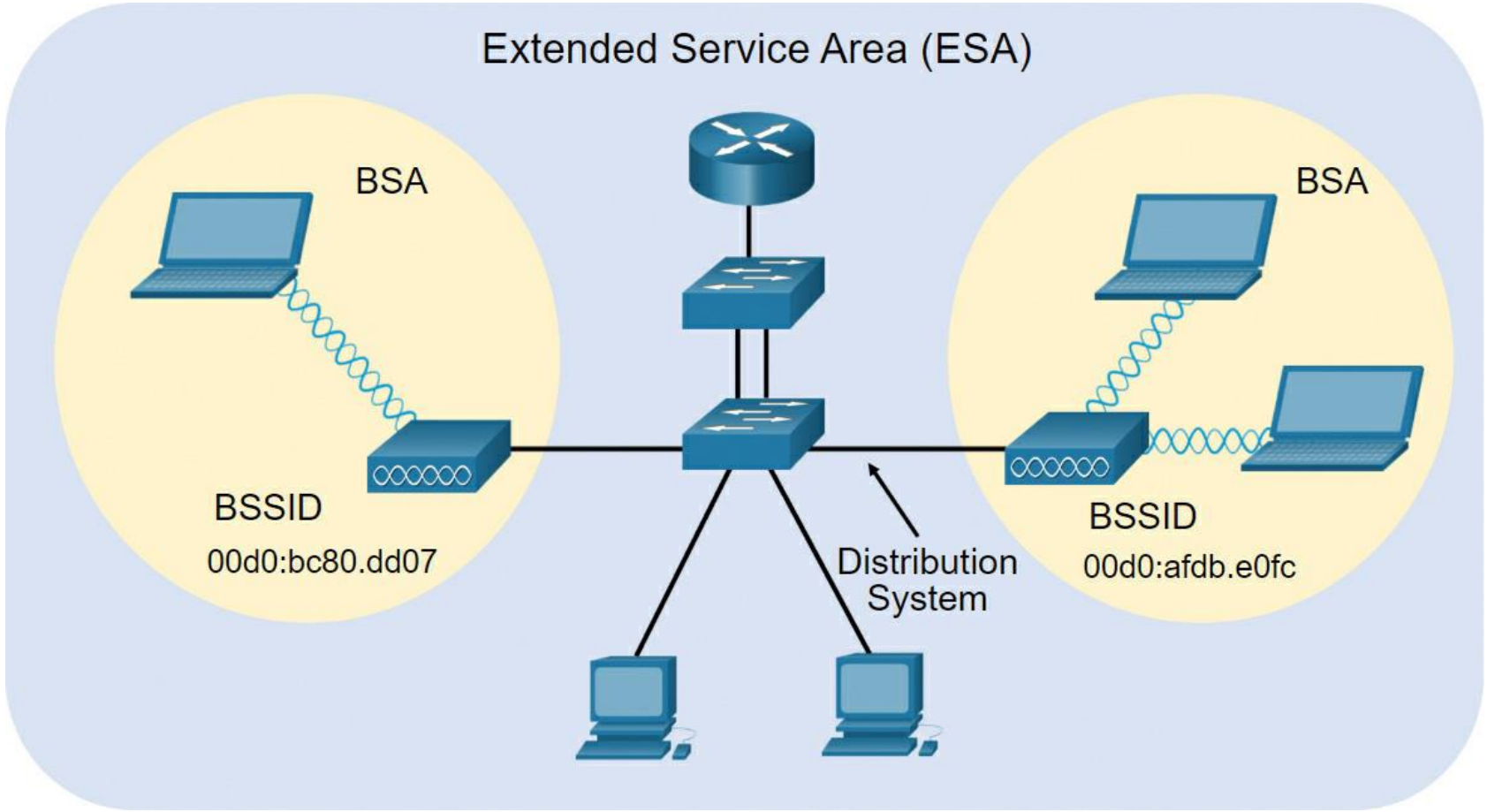
- The Layer 2 MAC address of the AP is used to uniquely identify each BSS, which is called the
- Basic Service Set Identifier (BSSID).
- Therefore, the BSSID is the formal name of the BSS and is always associated with only one AP.
- The BSSID is the unique identifier of the BSS and is derived from the MAC address of the AP's wireless interface. The BSSID is typically the MAC address of the AP itself or a virtual MAC address when using multiple SSIDs.



WLAN OPERATION

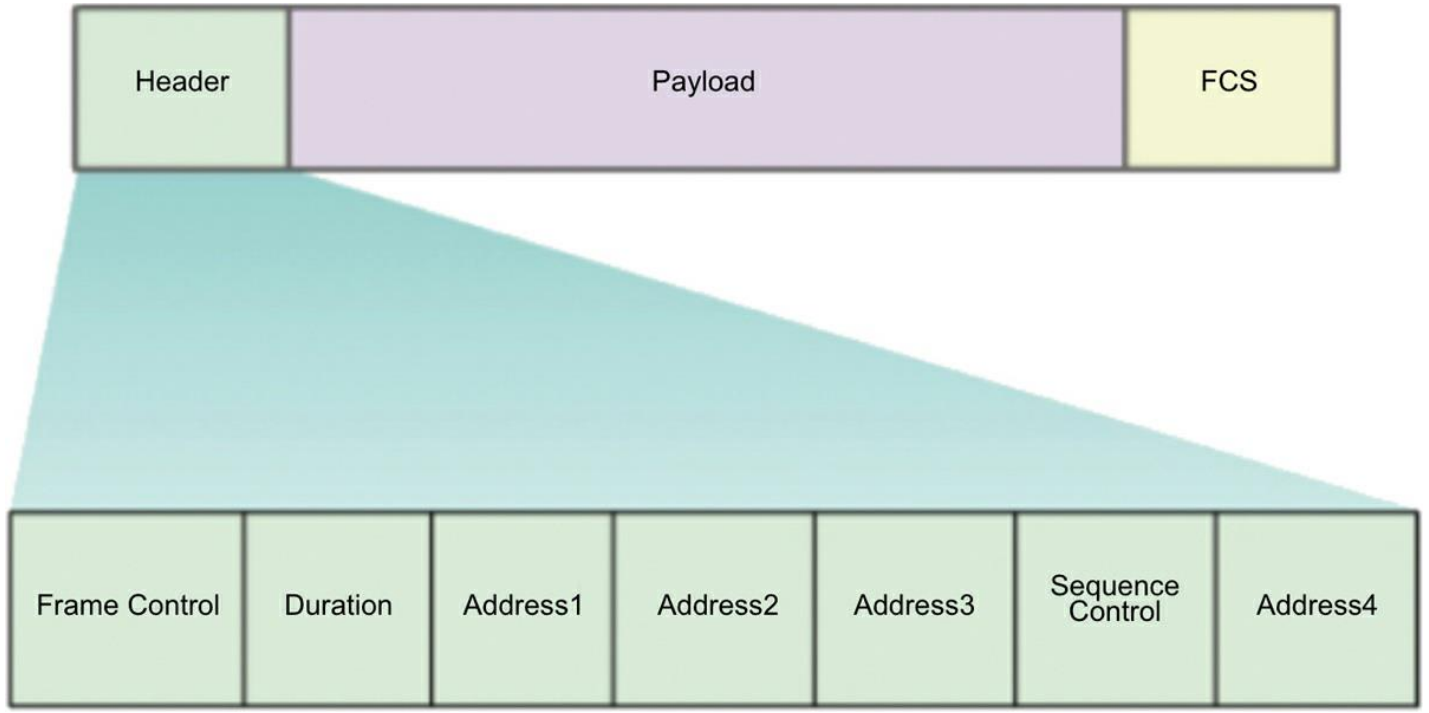
- Extended Service Set
- When a single BSS provides insufficient coverage, two or more *BSSs* can be joined through a common *distribution system (DS)* into an ESS.
- An *ESS* is the union of two or more *BSSs* interconnected by a wired *DS*.
- Each *ESS* is identified by a *SSID*, and each BSS is identified by its *BSSID*.
- Wireless clients in one *BSA* can now communicate with wireless clients in another *BSA* within the same *ESS*.
- Roaming mobile wireless clients may move from one *BSA* to another (within the same *ESS*) and seamlessly connect.
- The rectangular depicts the coverage area within which members of an *ESS* may communicate.
- This area is called the *Extended Service Area (ESA)*.

WLAN OPERATION



802.11 Frame Structure

- All Layer 2(MAC) frames consist of a header, payload, and Frame Check Sequence (FCS) section.
- The 802.11 frame format
- is similar to the Ethernet frame format, except that it contains more fields



802.11 Frame Structure

- All 802.11 wireless frame from a wireless device contains the following fields:

1. **Frame Control:** This identifies the type of wireless frame and contains subfields for protocol version, frame type, address type, power management, and security settings.
2. **Duration:** This is typically used to indicate the remaining duration needed to receive the next frame transmission.
3. **Address1:** This usually contains the MAC address of AP.
4. **Address2:** This usually contains the MAC address of the transmitting (that is, sending) wireless device.
5. **Address3:** This sometimes contains the MAC address of the destination, such as the router interface (default gateway) to which the AP is attached.
6. **Sequence Control:** This contains information to control sequencing and fragmented frames.
7. **Address4:** This is usually missing because it is used only in ad hoc mode.
8. **Payload:** This contains the data for transmission.
9. **FCS:** This is used for Layer 2 error control.