Wireless & Mobile Computing

First Semester 3rd Class

Lecture Eight & Nine

2025/2024

CHANNEL MANAGEMENT

- **Frequency Channel Saturation**
- Wireless LAN devices have transmitters and receivers tuned to specific frequencies of radio waves to communicate.
- A common practice is for frequencies to be allocated as ranges.
- Such ranges are then split into smaller ranges called channels. If the demand for a specific channel is too high, that channel is likely to become oversaturated.
- The saturation of the wireless medium degrades the quality of the communication.
- Over the years, a number of techniques have been created to improve wireless communication and alleviate saturation.
- These techniques mitigate channel saturation by using the channels in a more efficient way.

CHANNEL MANAGEMENT

- **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.

Accessing Channel

- Accessing a communication channel involves mechanisms and protocols that enable devices or nodes to transmit and receive data over a shared medium.
- The specific method depends on the type of communication system (wired, wireless, or optical) and the network's design.
- Channel Types:
- Dedicated Channel: Allocated exclusively to a single user or session (e.g., leased lines).
- Shared Channel: Multiple users share the same channel, requiring coordination to avoid collisions (e.g., Ethernet, Wi-Fi).

Accessing Channel

- **Channel Access Methods**:
- **Time Division Multiple Access (TDMA)**:
  - Time slots are allocated to different users, who transmit during their assigned slots.
  - Used in GSM networks and some satellite systems.
- **Frequency Division Multiple Access (FDMA)**:
  - Different users are assigned different frequency bands.
  - Common in analog cellular systems and FM radio.
- **Code Division Multiple Access (CDMA)**:
  - Signals are spread using unique codes, allowing multiple users to share the same frequency simultaneously.
  - Used in 3G mobile networks and GPS.
- **Carrier Sense Multiple Access (CSMA)**:
  - Devices sense the channel for activity before transmitting to avoid collisions.
  - Variants include CSMA/CD (collision detection, used in Ethernet) and CSMA/CA (collision avoidance, used in Wi-Fi).

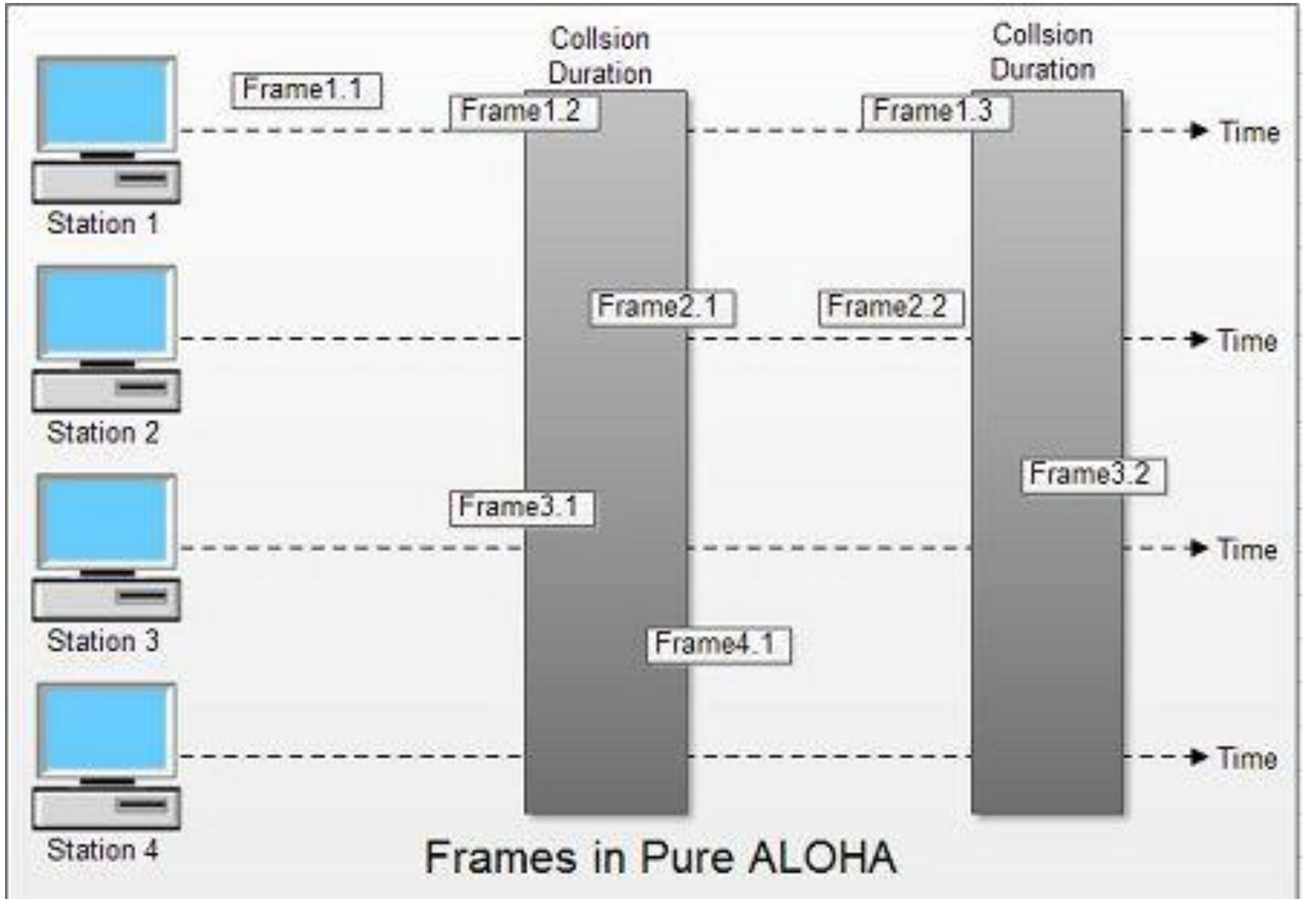
Accessing Channel

- **Access Protocols**:
- **ALOHA**: Basic protocol where users transmit whenever they have data, with potential collisions requiring retransmission.
- **Slotted ALOHA**: Divides time into slots to reduce collisions, improving efficiency.
- **Polling**: A central controller grants channel access to devices in a predetermined sequence.
- **Token Passing**: A "token" circulates through the network, and only the node with the token can transmit.

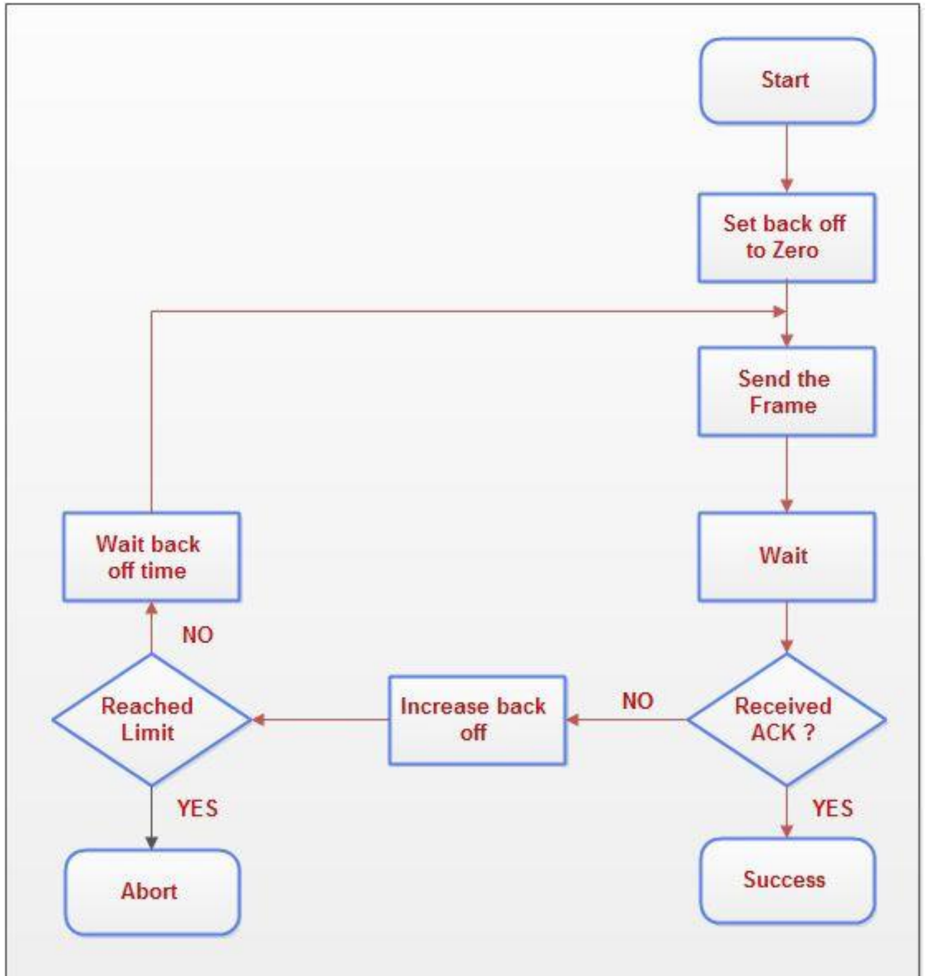
Accessing Channel

- **Aloha**
- is a random access protocol used for network communication, specifically in wireless networks, that allows multiple users to access a shared communication channel.
- This protocol helps manage data transmission by employing a simple approach where users transmit data whenever they have it, leading to potential collisions.
- Aloha is foundational in understanding how devices can communicate in a non-scheduled manner, influencing later protocols designed to improve efficiency and reduce collision rates.

Accessing Channel



Accessing Channel



Protocol flow chart for ALOHA

Accessing Channel

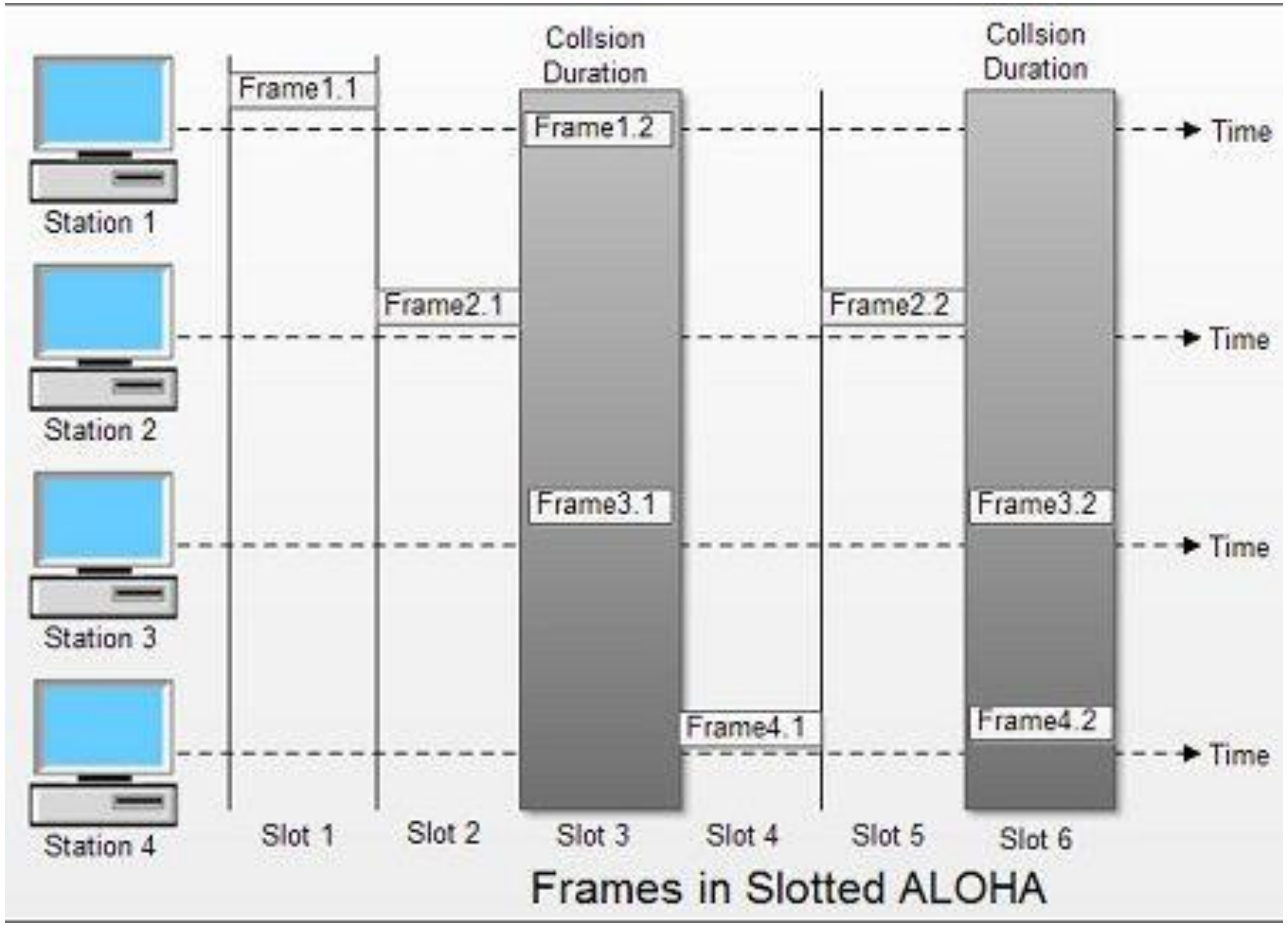
- Slotted ALOHA is a medium access control (MAC) protocol designed to improve the efficiency of the earlier Pure ALOHA protocol.
- It works by dividing time into equal-length slots, with each slot long enough to send one frame.
- A station can only begin transmission at the start of a time slot, reducing the chances of collisions compared to Pure ALOHA, where transmissions could start at any time.

Accessing Channel

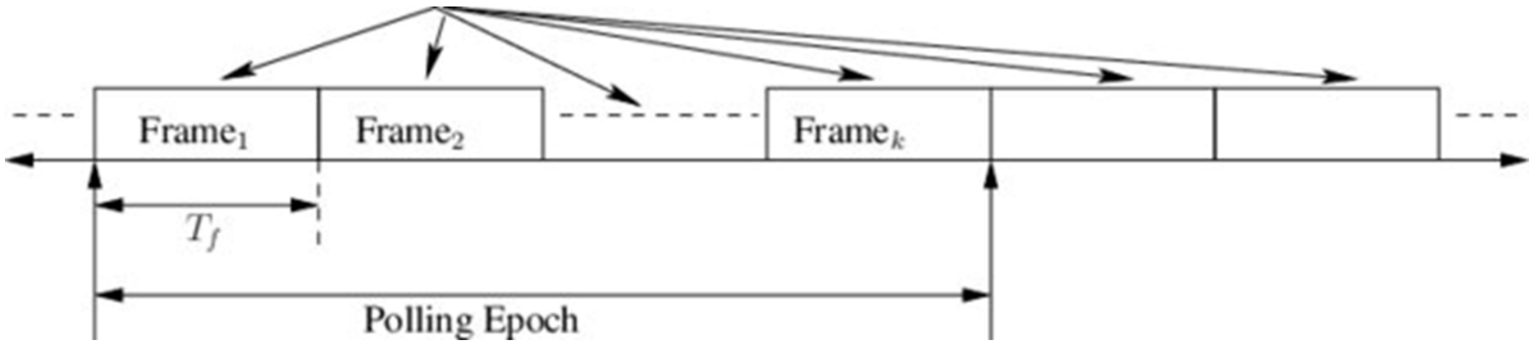
- **How it Works:**

1. **Time Synchronization:** All stations in the network agree on slot boundaries, typically synchronized using a clock signal.
2. **Transmission:** A station waits for the start of the next available time slot to send its data frame.
3. **Collisions:** If two or more stations try to transmit in the same slot, a collision occurs. In this case, the stations involved retransmit their data in subsequent slots, using a random backoff mechanism.
4. **Vulnerable Period:** The vulnerable period, or the time when collisions might occur, is limited to the duration of one slot, unlike Pure ALOHA, where it spans two frame durations.

Accessing Channel



Accessing Channel



- Polling is a controlled access protocol used in networking to regulate communication in environments where multiple devices share a communication medium.
- It relies on a **primary station** (controller) to manage communication with multiple **secondary stations** (devices).
- **How Polling Works:**

1. **Primary Station Initiates Communication**: The primary station sends polling requests to each secondary station in turn.
2. **Station Responses**:
    1. If a station has data to transmit, it responds to the poll and begins transmission.
    2. If a station has no data to send, it sends a negative acknowledgment (NAK), and the primary moves to the next station.
3. **Transmission**: Once data transmission begins, the primary station ensures orderly communication by acknowledging successful transfers before polling the next station.

Accessing Channel

- **Token Passing**
- is a controlled access protocol designed to prevent collisions in a network.
- It operates by passing a special control message, called a **token**, among network nodes arranged in a logical ring structure

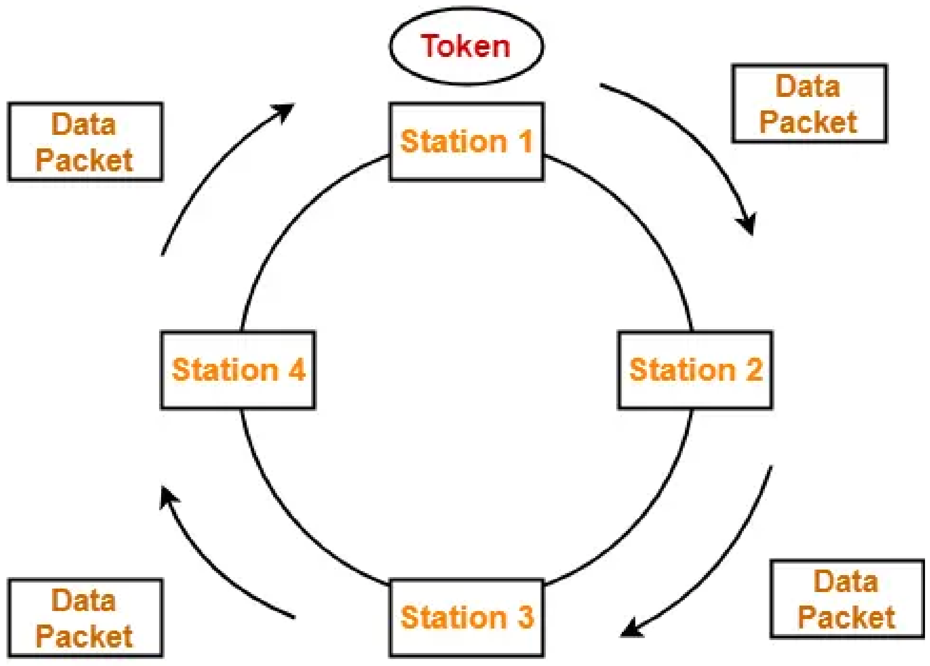
Accessing Channel

- How it works:

1. **Logical Ring Structure**: Even though the physical layout can vary (e.g., star or bus topology), the network maintains a logical ring. Each node has a predecessor and successor.
2. **Token Circulation**: The token is a small data packet that grants the right to transmit. Only the node holding the token can send data, ensuring that only one node communicates at a time.
3. **Data Transmission**:
    1. When a node receives the token and has data to send, it converts the token into a data frame, transmits its message, and waits for acknowledgment.
    2. Once the data is successfully transmitted and acknowledged, the node regenerates the token and passes it to the next node.
4. **No Data to Send**: If a node does not have data to send when it receives the token, it simply forwards the token to the next node in the ring.
5. **Token Monitoring**: A designated node (active monitor) ensures the token's integrity. If the token is lost (e.g., due to node failure), the monitor regenerates it to maintain network functionality.

Accessing Channel

- In a token ring network, the token-passing mechanism enables efficient channel access by regulating data transmission in a ring topology. The data frame in a token-passing protocol includes specific fields for managing this process.



Accessing Channel

1. Token Frame:

- Starting Delimiter (SD): Indicates the start of a frame.
- Access Control (AC): Specifies priority levels and distinguishes between a token frame and a data frame.
- Ending Delimiter (ED): Marks the end of the frame.

2. Data Frame (for actual data transmission):

- Frame Control (FC): Indicates the type of frame being transmitted.
- Destination Address (DA): Specifies the intended receiver.
- Source Address (SA): Identifies the sender.
- Information (INFO): Contains the actual data payload.
- Frame Check Sequence (FCS): A CRC used for error detection.
- Frame Status (FS): Communicates actions performed on the frame by recipient stations.

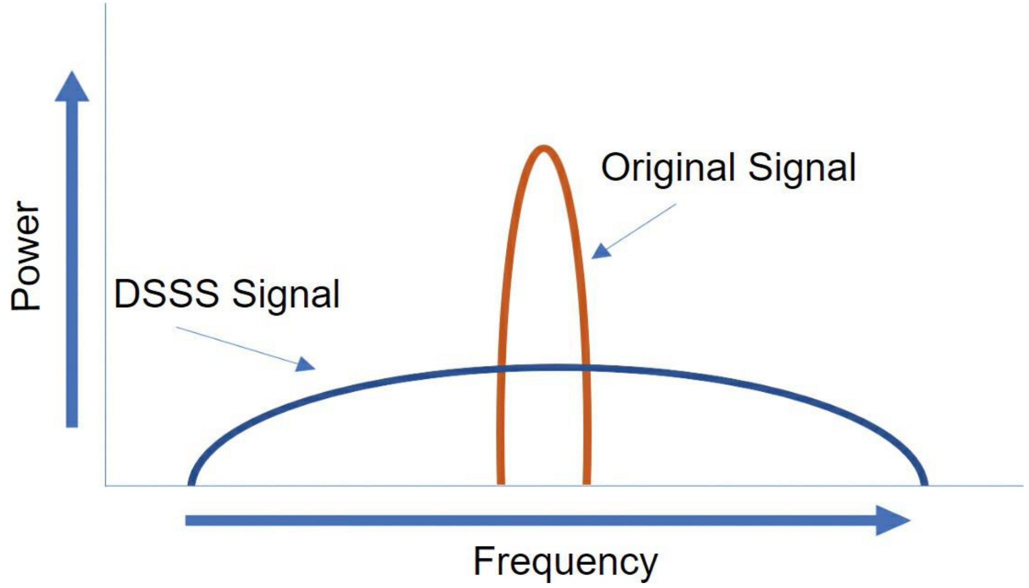
CHANNEL MANAGEMENT

- *Direct-Sequence Spread Spectrum (DSSS)*:
- This is a modulation technique designed to spread a signal over a larger frequency band.
- Spread spectrum techniques were developed during wartime to make it more difficult for enemies to intercept or jam a communication signal.
- It does this by spreading the signal over a wider frequency, which effectively hides the discernable peak of the signal, as shown in Figure.
- This spreading enhances the signal's resistance to interference, and jamming.
- A properly configured receiver can reverse the DSSS modulation and reconstruct the original signal.
- DSSS is used by 802.11b devices to avoid interference from other devices using the same 2.4 GHz frequency.

CHANNEL MANAGEMENT

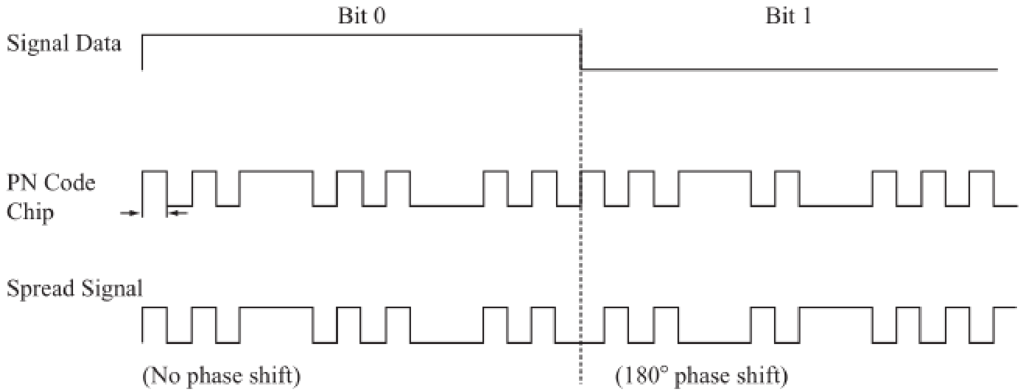
How DSSS Works Data Signal:

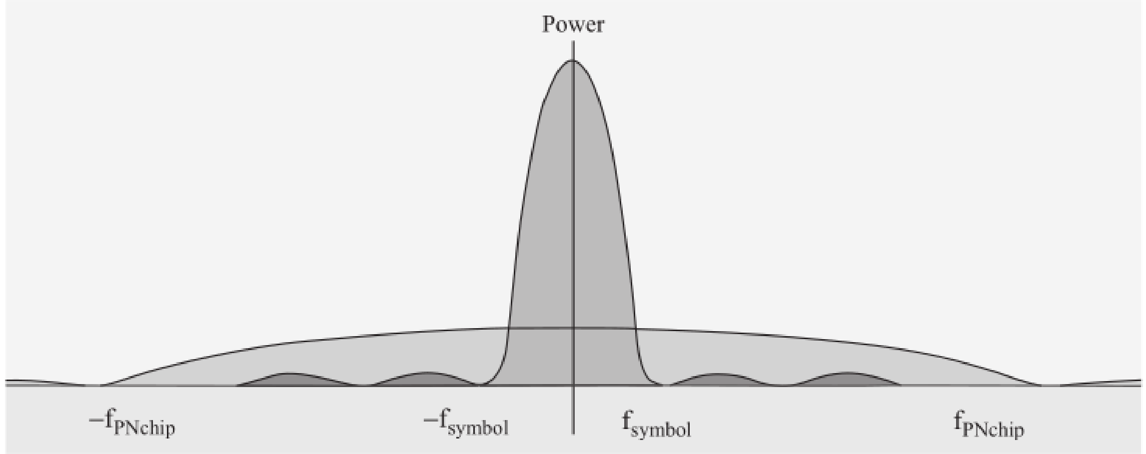
- The original data to be transmitted is represented as a low-rate digital signal (e.g., a sequence of bits).
- Spreading Code: DSSS uses a high-rate pseudo-random noise (PN) sequence, often called a spreading code or chip sequence.
- This sequence has a much higher frequency (chip rate) than the data signal.
- The spreading code is unique to each transmitter or communication channel and is shared between the transmitter and receiver.



- Spreading the Signal: The data signal is XORed (multiplied in binary) with the spreading code. This operation "spreads" the signal over a much wider frequency range.
- Each bit of the original signal is spread into multiple "chips" (shorter bits), increasing the signal's bandwidth.
- Transmission: The spread signal is transmitted over the channel, occupying a much broader bandwidth than the original signal.
- Despreading at the Receiver: The receiver uses the same spreading code to reverse the spreading process. It correlates the received signal with the spreading code, recovering the original data signal.

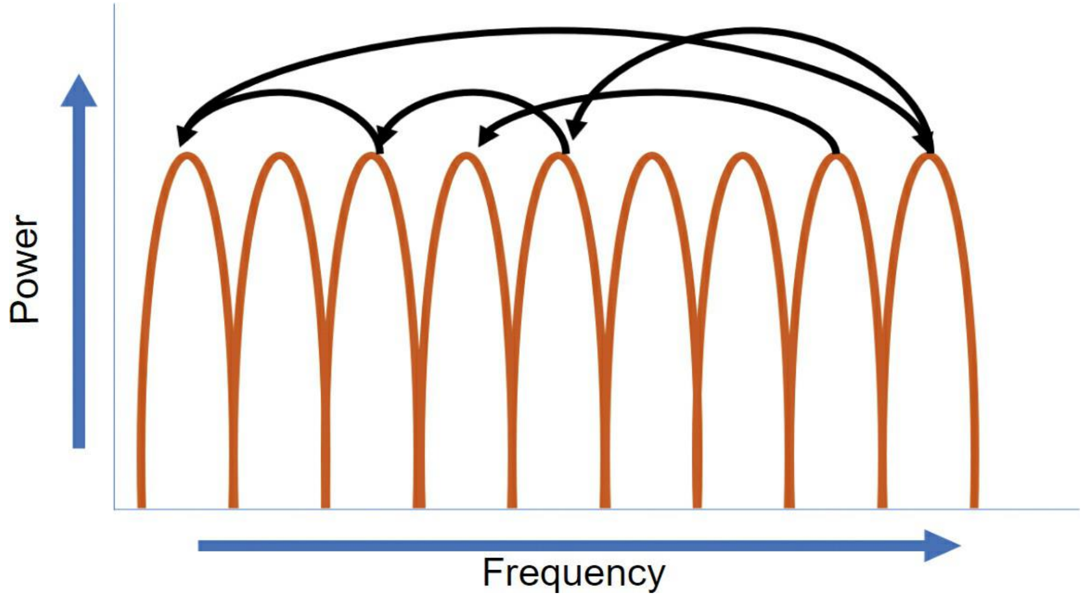
CHANNEL MANAGEMENT



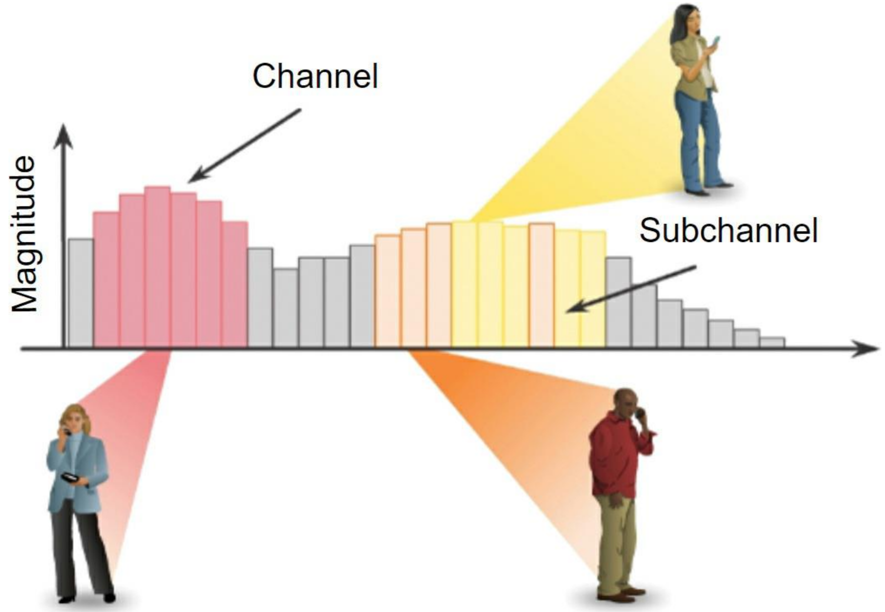


CHANNEL MANAGEMENT

- *Frequency-Hopping Spread Spectrum (FHSS)*:
- This relies on spread spectrum methods to communicate.
- It transmits radio signals by switching a carrier signal among many frequency
- channels, as shown in Figure.
- With FHSS, the sender and receiver must be synchronized to “know” which channel to jump to.
- This channel-hopping proc the channels, decreasing channel congestion. FHSS was used by the
- original 802.11 standard.



CHANNEL MANAGEMENT



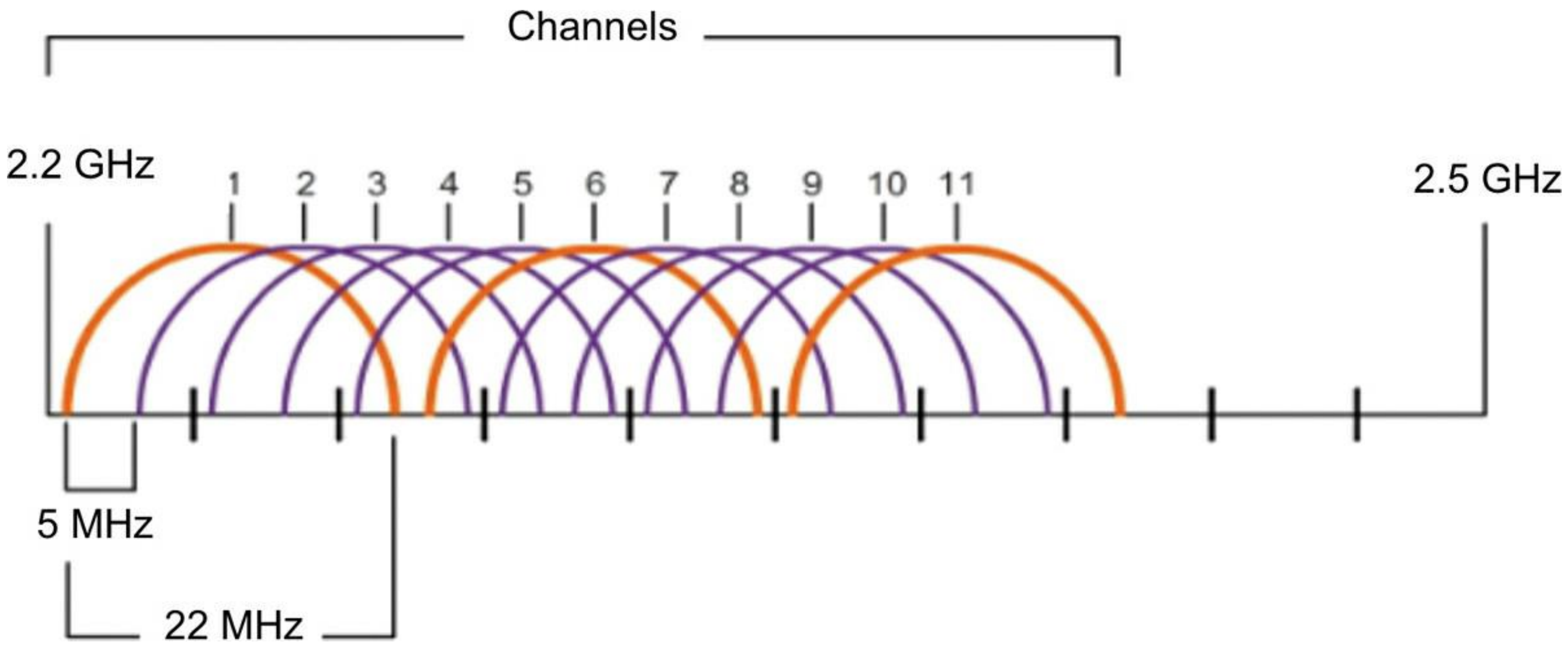
- *Orthogonal Frequency-Division Multiplexing (OFDM)*:

- This is a subset of frequency division multiplexing in which a single channel uses multiple subchannels on adjacent frequencies, as shown in Figure.
- Subchannels in an OFDM system are precisely orthogonal to one another, which allows the subchannels to overlap without interfering.
- OFDM is used by a number of communication systems, including 802.11a/g/n/ac.
- The new 802.11ax uses a variation of OFDM called orthogonal frequency-division multiaccess (OFDMA).

CHANNEL MANAGEMENT

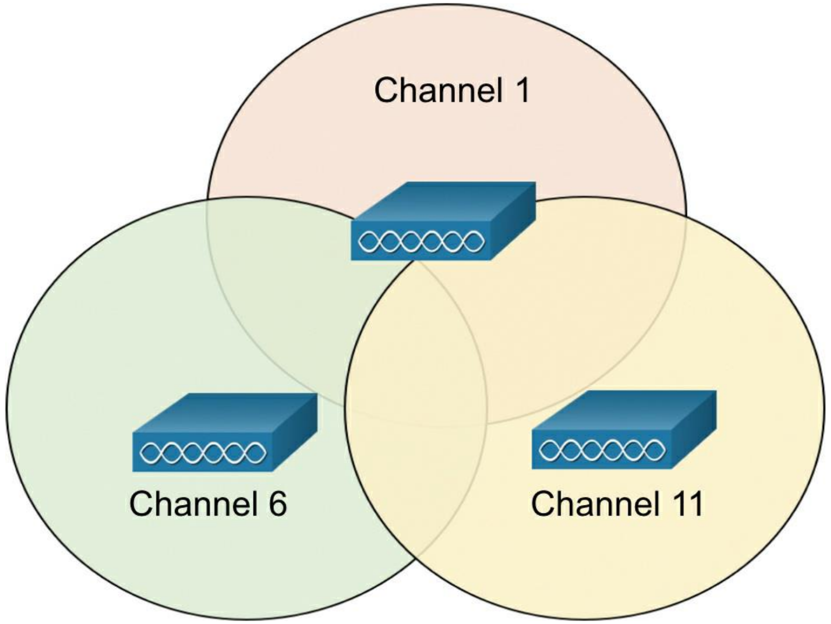
- **Channel Selection**
- A best practice for WLANs requiring multiple APs is to use nonoverlapping channels.
- For example, the 802.11b/g/n standards operate in the 2.4 GHz to 2.5 GHz spectrum.
- The 2.4 GHz band is subdivided into multiple channels.
- Each channel is allotted 22 MHz bandwidth and is separated from the next channel by 5
- MHz.
- The 802.11b standard identifies 11 channels for North America, as shown in Figure (13 in Europe and 14 in Japan).

CHANNEL MANAGEMENT



CHANNEL MANAGEMENT

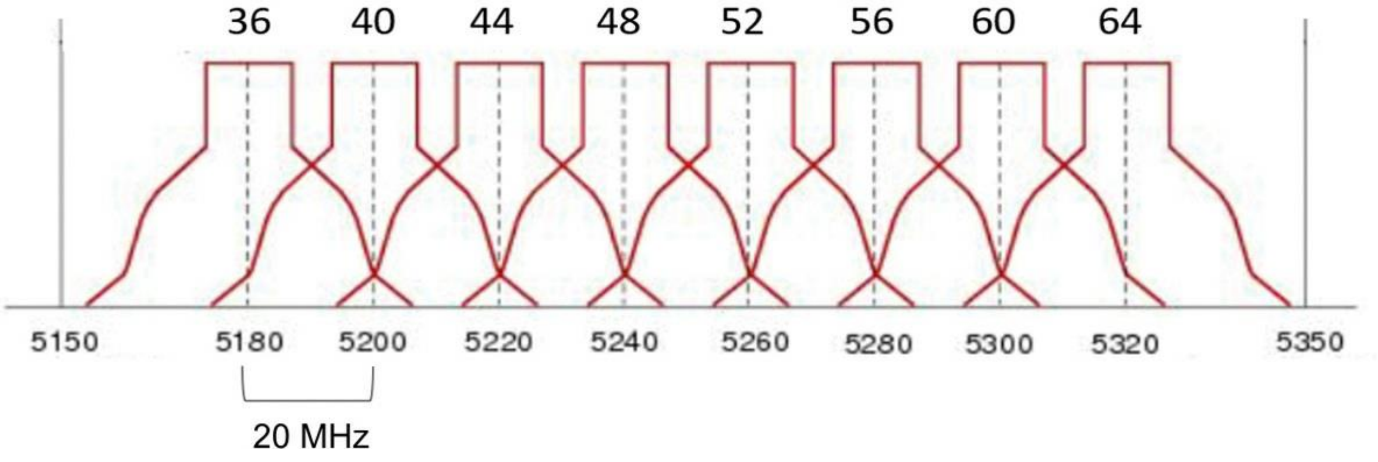
- Interference occurs when one signal overlaps a channel reserved for another signal, causing possible distortion.
- The best practice for 2.4 GHz WLANs that require multiple APs is to use non-overlapping channels, although most modern APs will do this automatically.
- If there are three adjacent APs, use channels 1, 6, and 11, as shown in Figure.



CHANNEL MANAGEMENT

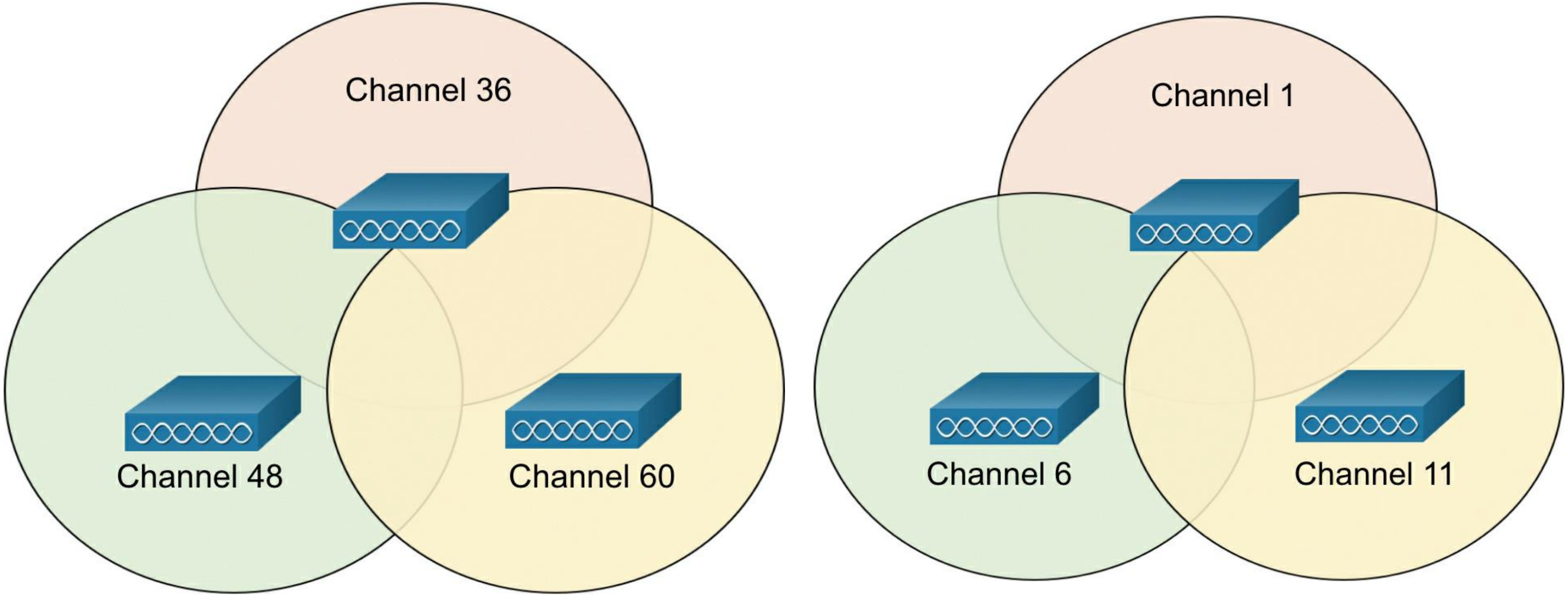
- For the 5 GHz standards 802.11a/n/ac, there are 24 channels.
- The 5 GHz band is divided into three sections.
- Each channel is separated from the next channel by 20 MHz. Figure shows the first section of eight channels for the 5 GHz band. Although there is a slight overlap, the channels do not interfere with one another.
- 5 GHz wireless can provide faster data transmission for wireless clients in heavily populated wireless networks because of the large amount of non-overlapping wireless channels.

5GHz Channel Identifiers



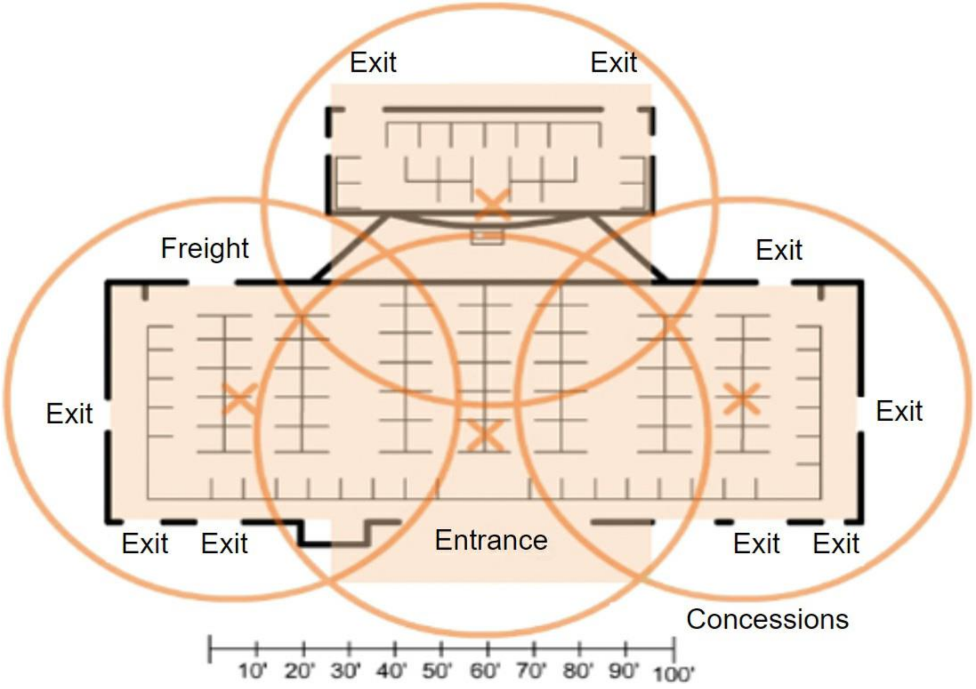
CHANNEL MANAGEMENT

As with 2.4 GHz WLANs, choose non-interfering channels when configuring multiple 5 GHz APs that are adjacent to each other, as shown in



CHANNEL MANAGEMENT

- **Plan a WLAN Deployment**
- The number of users supported by a WLAN depends on the geographical layout of the facility, including the number of bodies and devices that can fit in a space, the data rates users expect, the use of non-overlapping channels by multiple APs in an ESS, and transmit power settings.
- When planning the location of APs, the approximate circular coverage area is important, as shown in Figure



CHANNEL MANAGEMENT

- However, there are some additional recommendations:
- If APs are to use existing wiring, or if there are locations where Aps cannot be placed, note these locations on the map.
- Note all potential sources of interference, which can include microwave ovens, wireless video cameras, lights, motion detectors, or any other device that uses the 2.4 GHz range.
- Position APs above obstructions.
- Position APs vertically near the ceiling in the center of each coverage area, if possible.
- Position APs in locations where users are expected to be. For example, conference rooms are typically a better location for Aps than a hallway.
- If an IEEE 802.11 network has been configured for mixed mode, the wireless clients may experience slower than normal speeds to support the older wireless standards.

CHANNEL MANAGEMENT

- When an IEEE 802.11 network is configured in mixed mode, it operates to support both older and newer wireless standards (e.g., 802.11b, 802.11g, 802.11n, etc.) at the same time.
- This configuration allows devices that use older standards to connect to the network, but it may result in slower-than-normal speeds for all clients. Here's why:
- Reasons for Slower Speeds:
- Compatibility Overhead: To ensure compatibility with older devices, the network may need to include additional signaling and control mechanisms, such as sending management frames using the older standard's data rates.
- Protection Mechanisms: RTS/CTS (Request-to-Send/Clear-to-Send) or CTS-to-Self mechanisms are used to avoid collisions between devices operating on different standards. These protections introduce extra delays.
- Shared Medium: The wireless channel is shared among all connected devices. If an older device (e.g., 802.11b) joins, the access point may spend more time transmitting data at the slower rates of that device, reducing overall throughput for others.
- Reduced Spectrum Efficiency: Older standards, such as 802.11b, use less efficient modulation techniques, which can affect the network's ability to fully utilize available bandwidth.

CHANNEL MANAGEMENT

- **Example:**
- If an **802.11ac** (Wi-Fi 5) access point is operating in mixed mode with 802.11n (Wi-Fi 4) and 802.11g (Wi-Fi 3) devices, the high-speed 802.11ac devices may need to wait longer for access to the medium, reducing their effective speeds.