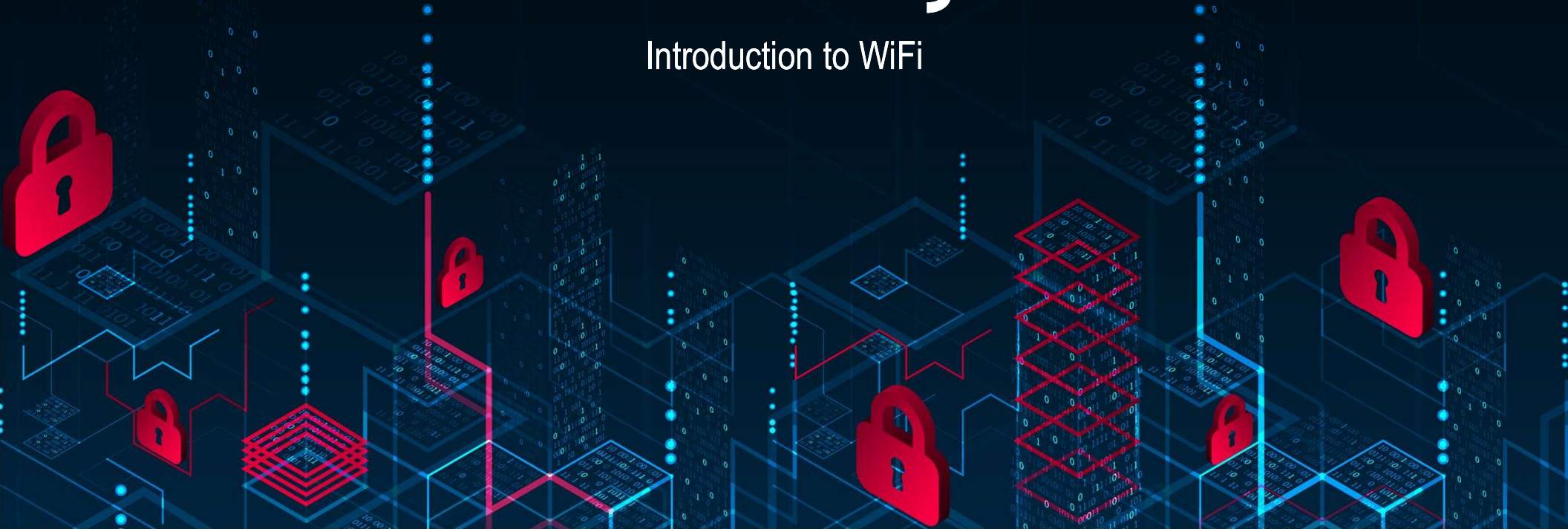


CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Wireless, IoT, and Cloud Security

Introduction to WiFi



Video summary

- WiFi History
- WiFi Standards
- WiFi Medium Access Control
- Advantages and Disadvantages
- Basic Security Strategies



Wi-Fi (WLAN)



- Wi-Fi is trademarked name for popular wireless technology that uses radio waves to provide high-speed Internet and network connections.
- The governing body that owns the term Wi-Fi, the **Wi-Fi Alliance**, defines it as any WLAN (wireless area network) products that are based on the **IEEE 802.11** standards.
- The way Wi-Fi works is through the use of radio signals like in phones. The wireless adapter card that is found inside of computers then uses the data that is being sent to change it into a radio signal to then be transmitted by the antenna.



① Internet
② Intranet

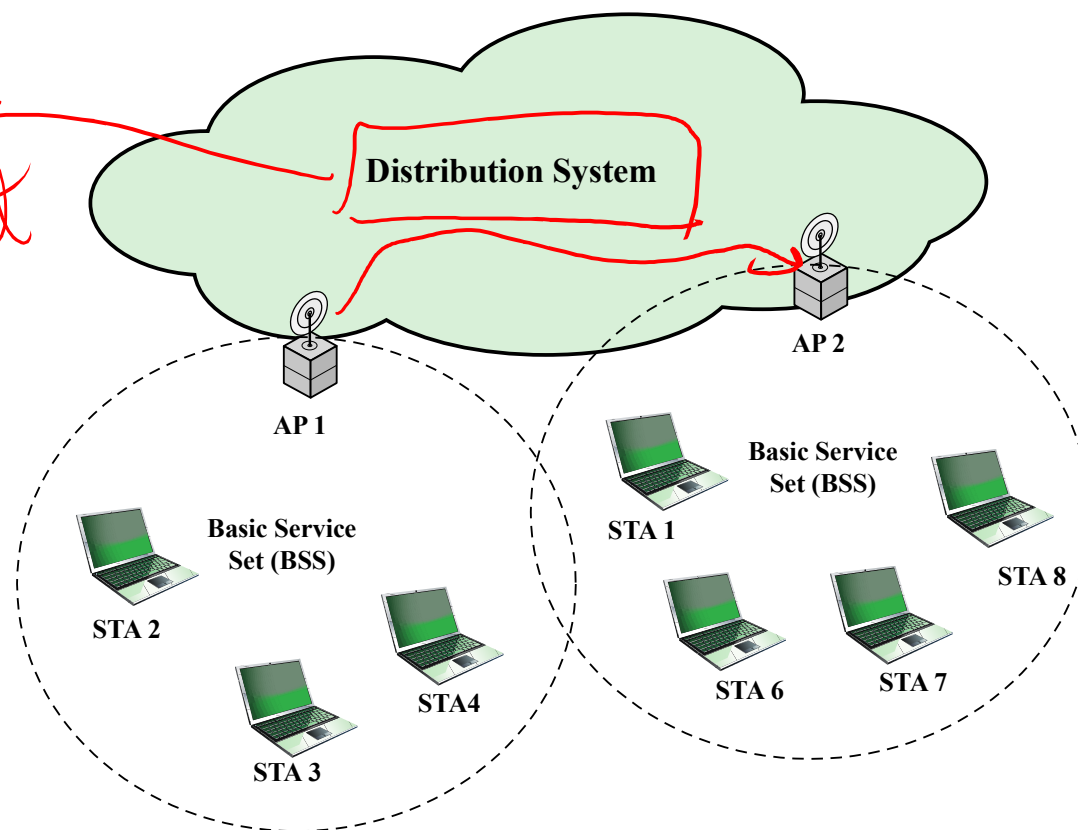
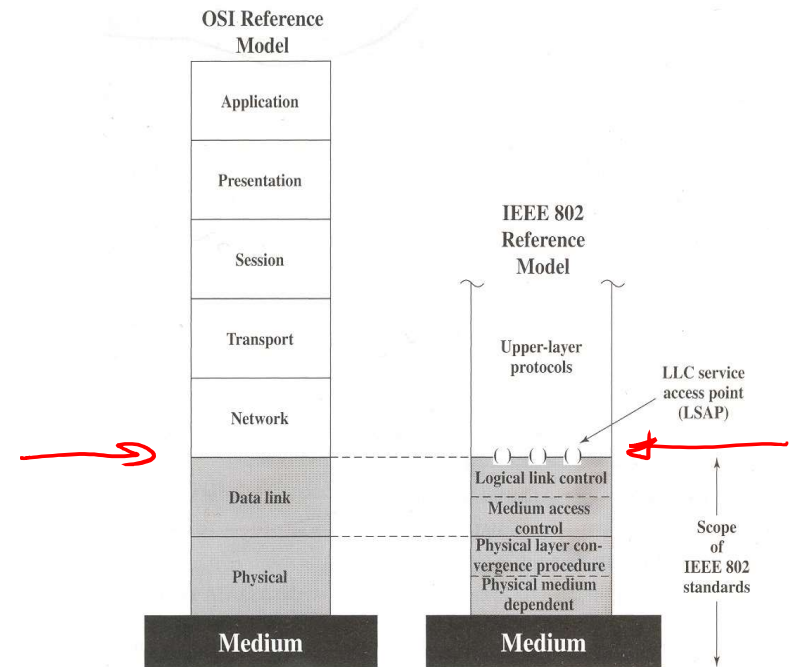


Figure 24.5 IEEE 802.11 Extended Service Set

802.11 Standard

- 802.11 is primarily concerned with the lower layers of the OSI model.
- Data Link Layer
 - Logical Link Control (LLC). ✓
 - Medium Access Control (MAC). ✓
- Physical Layer
 - Physical Layer Convergence Procedure (PLCP).
 - Physical Medium Dependent (PMD).



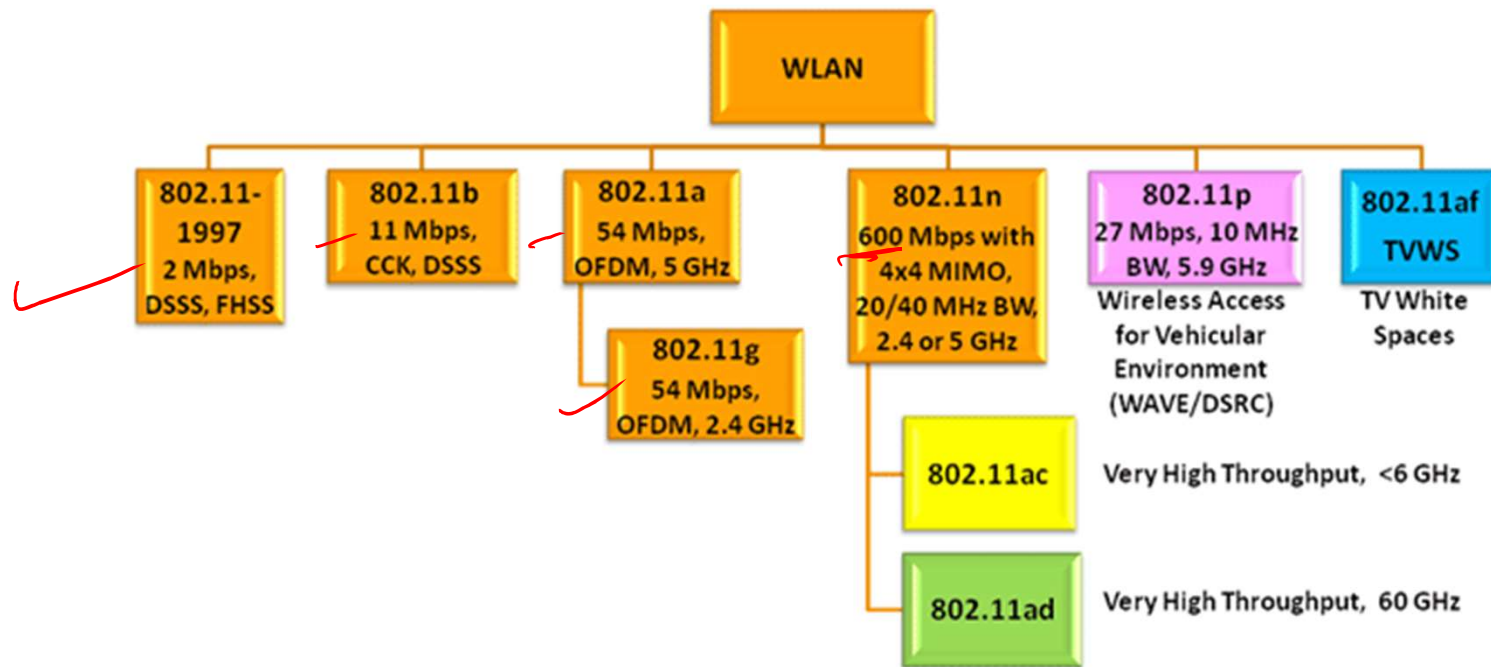
IEEE 802 Protocol Layers Compared to OSI Model

Specifications

- 802.11a
- 802.11b
- 802.11g
- 802.11n
- 802.11ac ✓
- 802.11ad ✗



Standardization (Extended)



DSRC = Dedicated Short-Range Communications

802.11 Medium Access Control (MAC)

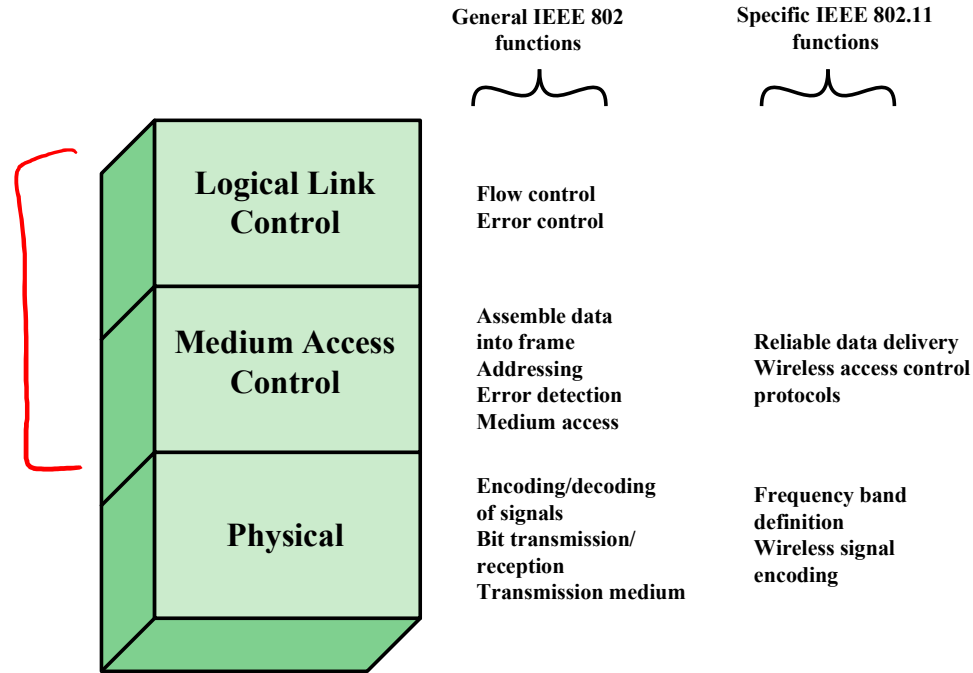
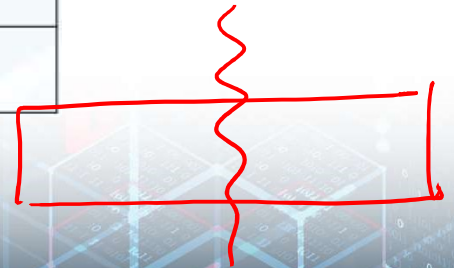


Figure 24.3 IEEE 802.11 Protocol Stack

802.11 Medium Access Control (MAC)



Function	Explanation
Scanning	Scanning of access points. Both active (probe) and passive (beacon) scanning are provided by the standard.
Authentication	Authentication is the process of proving identity between the client and the access point.
Association	Once authenticated, the client must associate with the access point before sending data frames.
Encryption	Encryption of payload
RTS/CTS	The optional request-to send and clear-to-send (RTS/CTS) function allows the access point to control use of the medium for stations activating RTS/CTS.
Power Save Mode	The power save mode enables the user to turn on or off enables the radio.
Fragmentation	The fragmentation function enables an 802.11 station to divide data packets into smaller frames.



802.11 Medium Access Control (MAC)

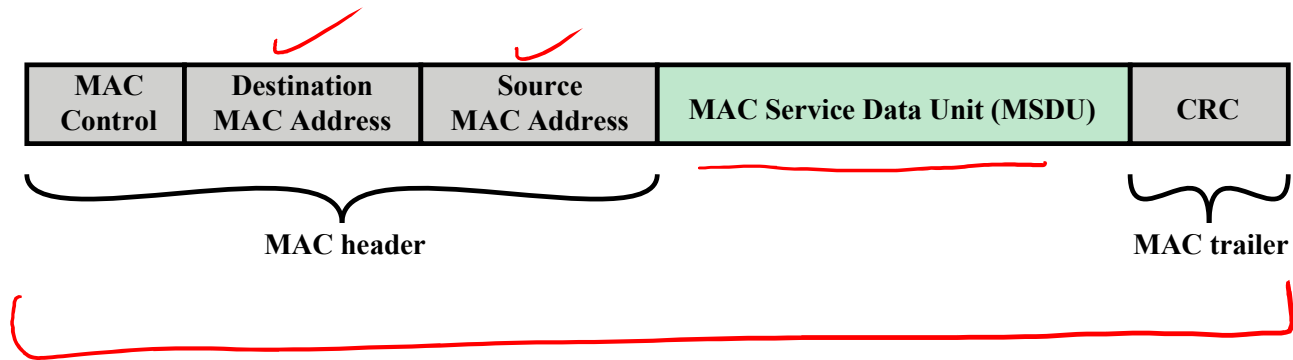


Figure 24.4 General IEEE 802 MPDU Format

MPDU: MAC Protocol Data Unit

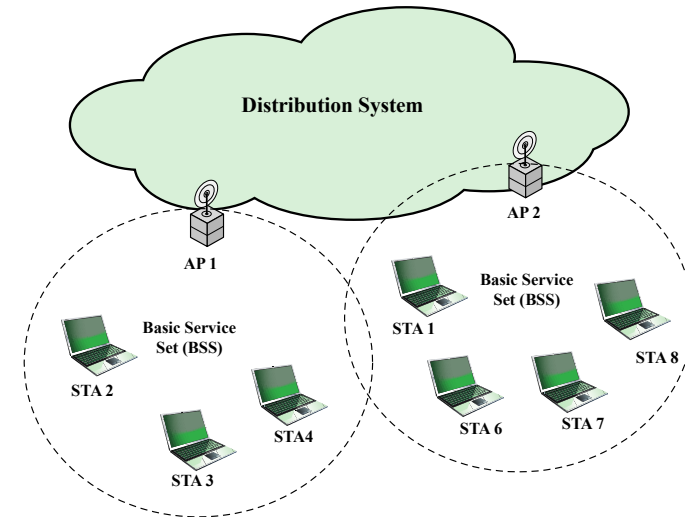
802.11 Infrastructure

AP – client services:

- Authentication : open, shared key or WPS
- De-authentication
- Privacy : WEP, WPA or WPA2

Distribution System services:

- Association : maps the client into the distribution system via access point
- Disassociation : release of association
- Distribution : used to deliver MAC frames across the distribution system
- Integration : enables delivery of MAC frames between DS and non 802.11
- Re-association : transition of association from one access point to an other



802.11b Standard

- Well-supported, stable, and cost effective, but runs in the 2.4 GHz range that makes it prone to interference from other devices (microwave ovens, cordless phones, etc) and also has security disadvantages.
- Limits the number of access points in range of each other to three.
- Has 11 channels, with 3 non-overlapping, and supports rates from 1 to 11 Mbps, but realistically about 4-5 Mbps max.



802.11g Standard

- Extension of 802.11b, with the same disadvantages (security and interference).
- Has a shorter range than 802.11b.
- Is backwards compatible with 802.11b so it allows or a smooth transition from 11b to 11g.
- Flexible because multiple channels can be combined for faster throughput.
- Runs at 54 Mbps, but realistically about 20-25 Mbps.



802.11a Standard

2.4 GHz / 5 GHz

- Completely different from 11b and 11g.
- Flexible because multiple channels can be combined for faster throughput and more access points can be co-located.
- Shorter range than 11b and 11g.
- Runs in the 5 GHz range, so less interference from other devices.
- Has 12 channels, 8 non-overlapping, and supports rates from 6 to 54 Mbps, but realistically about 27 Mbps max

WiFi Advantages

- Freedom – You can work from any location that you can get a signal.
- Setup Cost – No cabling required.
- Flexibility – Quick and easy to setup in temp or permanent space.
- Scalable – Can be expanded with growth.
- Mobile Access – Can access the network on the move.



Disadvantages

- Speed – Slower than cable.
- Range – Affected by various medium.
 - Travels best through open space.
 - Reduced by walls, glass, water, etc
- Security – Greater exposure to risks.
 - Unauthorized access.
 - Compromising data.
 - Denial of service.



Basic Security Strategies

- Block your Service Set Identifier (SSID) from being broadcast.
- Change the default network name in the access point.
- Change the default access point password.
- Center the access point in the middle of the building/house.



Media Access Control (MAC) Filtering

- Every network device has a unique MAC address
 - Allocated by the manufacturer.
- MAC Filtering only allows certain addresses access.
- Mostly for home use.
 - Tedious to implement on a large scale



Video summary

- WiFi History
- WiFi Standards
- WiFi Medium Access Control
- Advantages and Disadvantages
- Basic Security Strategies

