CTS2145
Introduction to Networking

Module 6 – Wireless Networking Standards

Signaling Methods: FHSS or DSSS

- FHSS (Frequency Hopping Spread Spectrum)

FHSS uses a narrow frequency band and 'hops' data signals in a predictable sequence from frequency to frequency over a wide band of frequencies.

- DSSS (Direct-Sequence Spread Spectrum)

The transmitter breaks data into pieces and sends the pieces across multiple frequencies in a defined range. DSSS is more susceptible to interference and less secure then FHSS.

Topology: Ad hoc or Infrastructure

Ad hoc

Works in peer-to-peer mode without a WAP (the wireless NICs in each host communicates directly with another) using a physical mesh, logical bus topology

- Cheap and easy to set up.
- Cannot handle a large number of hosts.
- Requires special modifications to reach wired networks.

You will typically only use an ad hoc network to create a direct, temporary connection between two hosts.

Topology: Ad hoc or Infrastructure

Infrastructure

Employs a WAP that functions like a hub Ethernet network using a physical star, logical bus topology.

- You can easily add hosts without increasing administrative efforts (scalable).
- The access point can be easily connected to a wired network, allowing clients to access both wired and wireless hosts.
- The placement and configuration of access points require planning to implement effectively.

You should implement an infrastructure network for all but the smallest of wireless networks.

Media Access

Wireless networks use **CSMA/CA** (Carrier Sense Media Access /Collision Avoidance).

-If a host detects traffic on the network, it experiences a longer back-off time than hosts on a wired network before attempting to transmit again.

-May use RTS (Request to send) and CTS (Clear to send) packets. Without RTS/CTS, collisions are more likely.

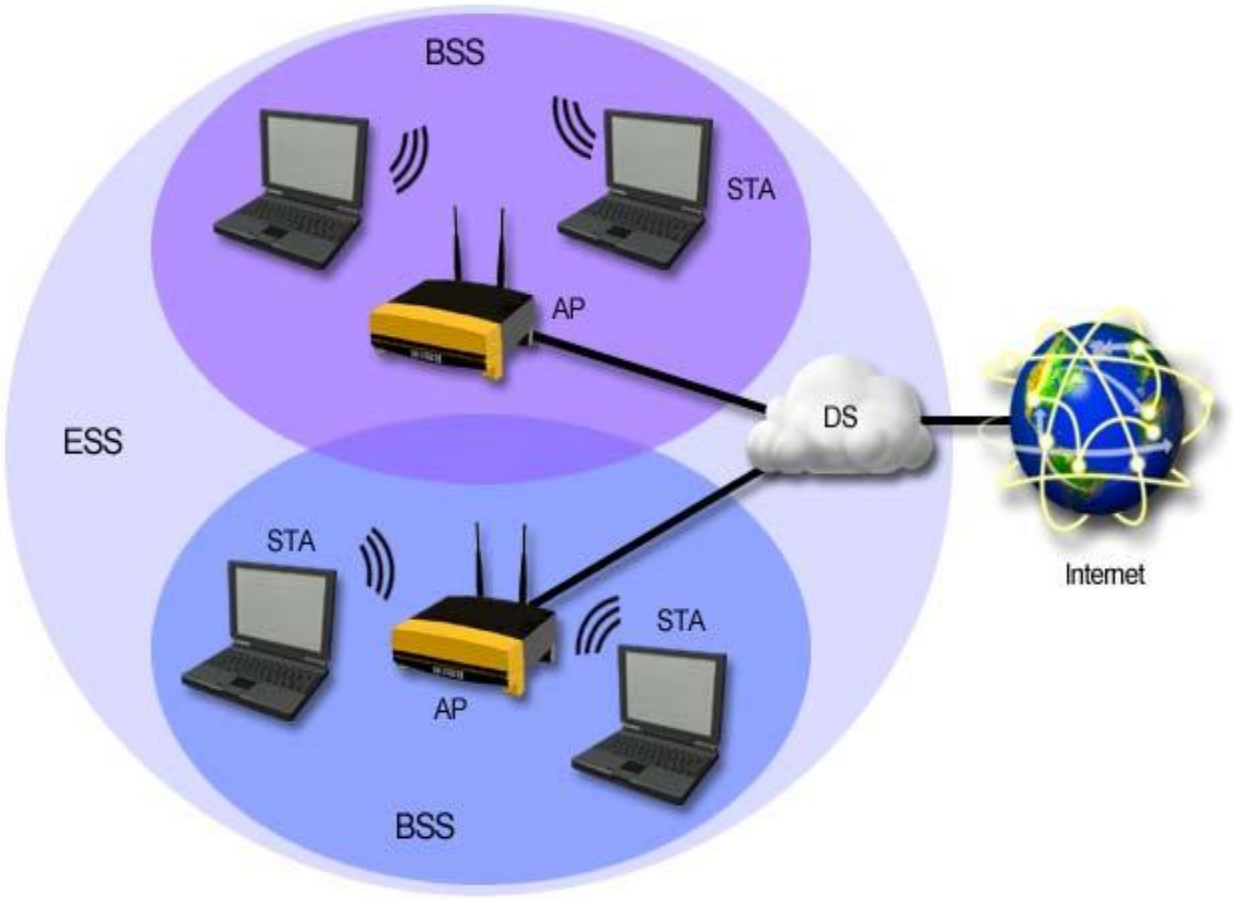
-Every transmission must be acknowledged.

- Wireless communication is *half-duplex*

Wireless Network Components

- **BSS** (Basic Service Set), also called a cell, is the smallest unit of a wireless network. All devices in the BSS can communicate with each other.
- **IBSS** (Independent Basic Service Set) : STAs configured in ad hoc mode.
- **ESS** (Extended Service Set) consists of multiple BSSs with a distribution system (DS). In an ESS, BSSs that have an overlapping transmission range use different frequencies.
- **DS** (Distribution System) is the backbone or LAN that connects multiple APs (and BSSs) together. The DS allows wireless clients to communicate with the wired network and with wireless clients in other cells.

Infrastructure Mode



Wireless network identifiers

SSID (Service Set ID), also called the network name

- Groups wireless devices together in a logical network.
- All devices on the same network must have the same SSID.
- The SSID is a 32-bit value in each frame. The SSID is case-sensitive.

BSSID (Basic Service Set Identifier)

- The BSSID is a 48-bit value that identifies an AP in an infrastructure network
- The BSSID allows devices to find a specific AP within an ESS that has multiple access points, and is used by STAs to keep track of APs when roaming.
- The BSSID is the MAC address of the access point and is set automatically.

Wireless Standards

	802.11a	802.11b	802.11g	802.11n
Frequency	5.75 GHz	2.4 GHz	2.4 GHz	2.4 GHz or 5.75 GHz
Maximum speed	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Maximum range	150’	300’	300’	1200’
Channels (non-overlapped)	23 (12)	11 (3)	11 (3)	2.4 GHz, 23 (12 or 6) 5.75 GHz, 11 (3 or 1)
Backwards compatibility	N/A	No	802.11b	802.11a/b/g, depending on implementation

802.11n

Multiple Input Multiple Output (MIMO)	**Multiple antennas both at the transmitter and receiver improves the performance (stronger signal and increased speed). Up to 4 sending and 4 receiving radios (above 3x3 offers little practical return).**
Channel bonding	**Two non-overlapping 20-MHz channels into a single 40-MHz channel, more than double the bandwidth.**
Frame composition	**802.11n changes the frame composition, resulting in increased efficiency of data transmissions (less overhead).**

Infrared Facts

IR data transfers occur at 4 Mbps and are insecure because the signals are not encrypted, and can be easily intercepted.

Line of Sight (LoS)	Devices must have a direct LoS (line-of-sight) connection. •The maximum distance between devices is 1 meter. •Communication signals are easily interrupted (eavesdropping).
Diffuse Mode	Diffuse mode (also called *scatter mode*) operates by broadcasting a large beam of light rather than a narrow beam. It does not require LOS connections. •Despite its advantages, diffuse mode still operates under range limitations. The IR access point and devices must be in the same room with each other. •Diffuse mode is also subject to signal disruptions (such as from obstructions).

Bluetooth

Bluetooth was designed to allow people to connect in PAN (personal area network) configurations using cell phones, PDAs and other Bluetooth equipped devices.

- Bluetooth uses a 128-bit proprietary encryption mechanism
- Bluetooth is a proposed standard of the IEEE 802.15 committee.

Frequency	2.45 GHz
Speed	Bluetooth 1.0--Up to 1 Mbps (practical rates: 720 Kbps) Bluetooth 2.0--Up to 3 Mbps (practical rates: 2 Mbps)
Range	30 Ft.
Signal	FHSS

Wired Equivalent Privacy (WEP)

WEP has the following weaknesses:

- Static Pre-shared Keys (PSK) are configured on the access point and the client and cannot be dynamically changed. As a result, every host on large networks uses the same key.
- Because it doesn't change, the key can be captured and easily broken. The key values are short, making it easy to predict.

Note: When using WEP, use open authentication.

If you use shared key authentication, WEP uses the same key for encryption and authentication.

Wi-Fi Protected Access (WPA)

WPA was intended as an intermediate measure to take the place of WEP while a fully secured system (802.11i) was prepared.

- Uses TKIP encryption (periodically rotating keys).
- Supports Pre-shared Key (WPA-PSK or WPA Personal) and 802.1x (WPA Enterprise) authentication.
- Can use dynamic keys or pre-shared keys.
- Can typically be implemented in WEP-capable devices through a software/firmware update.

Wi-Fi Protected Access 2 (WPA2) or 802.11i

WPA2 adheres to the 802.11i specifications and is intended to eventually replace both WEP and WPA.

- Uses Advanced Encryption Standard (AES) encryption. It is more secure than TKIP, but requires special hardware for performing encryption.
- Supports Pre-shared Key (WPA2-PSK or WPA2 Personal) and 802.1x (WPA2 Enterprise) authentication.
- Can use dynamic keys or pre-shared keys.

Note: WPA2 has the same advantages over WEP as WPA. While more secure than WPA, its main disadvantage is that it requires new hardware for implementation.

Additional Security Practices

- Change the administrator account name and password
- Change SSID from defaults and turn off SSID broadcast (SSID suppression or cloaking)
- Update the firmware
- Enable the firewall on the access point
- Disable DHCP (set static addresses)
- Enable MAC address filtering (Attackers can still use tools to capture packets and then retrieve valid MAC addresses)

Wireless Configuration Tasks

1. Set the SSID using a cryptic name
2. Configure the region (WAP only)
3. Configure the channel
4. Configure security
   - MAC access list, Disable SSID broadcast, Enable WEP, WPA or WPA2 (use a passphrase)
5. Configure the beacon

Wireless Network Considerations

Incorrect configuration	Verify that the correct SSID and WEP/WPA keys have been configured. Remember WEP/WPA keys are not case-sensitive, but passphrases are case-sensitive. Make sure you are using the same standard as the AP.
Range and Obstructions	Wireless standards have a limited range and have trouble transmitting through obstructions in the path.
Channel interference	To avoid interference, try changing the channel used on the access point.
Atmospheric and EMI conditions	Interference from atmospheric conditions or other sources of stray radio waves
AP placement	Place APs in central locations.
Antennae orientation	Directional antenna or Omni-directional antenna