Wireless LANs

Slide Set 7

Wireless LANs

- The Big Thing in local area networking today
- Gives mobility to users within the corporate premises
- Not a competitor yet for wired Ethernet LAN but wireless speed increasing everyday; mostly used to extend the wired LAN's resources

Wireless vs Wired: Pros and Cons

Parameter	Wireless	Wired
Security	Less Secure	More Secure
Data Rate	Slower (300 Mbps)	Faster (10 Gbps)
Setup and Deployment Cost	Cheaper	More Expensive
Connection Reliability	Less Reliable	More Reliable
Mobility	Higher	Much Lower
Deployment Speed	Faster	Slower
Range and Coverage	Smaller*	Larger
Robustness	Better	Weaker
Flexibility to change	Higher	Lower

802.11x Wireless Access Point and Wireless LAN Adapters (PCMCIA, PCI & USB)

A 802.11g Access Point with two antennas

USB: Most popular and portable. Works with any device with USB ports

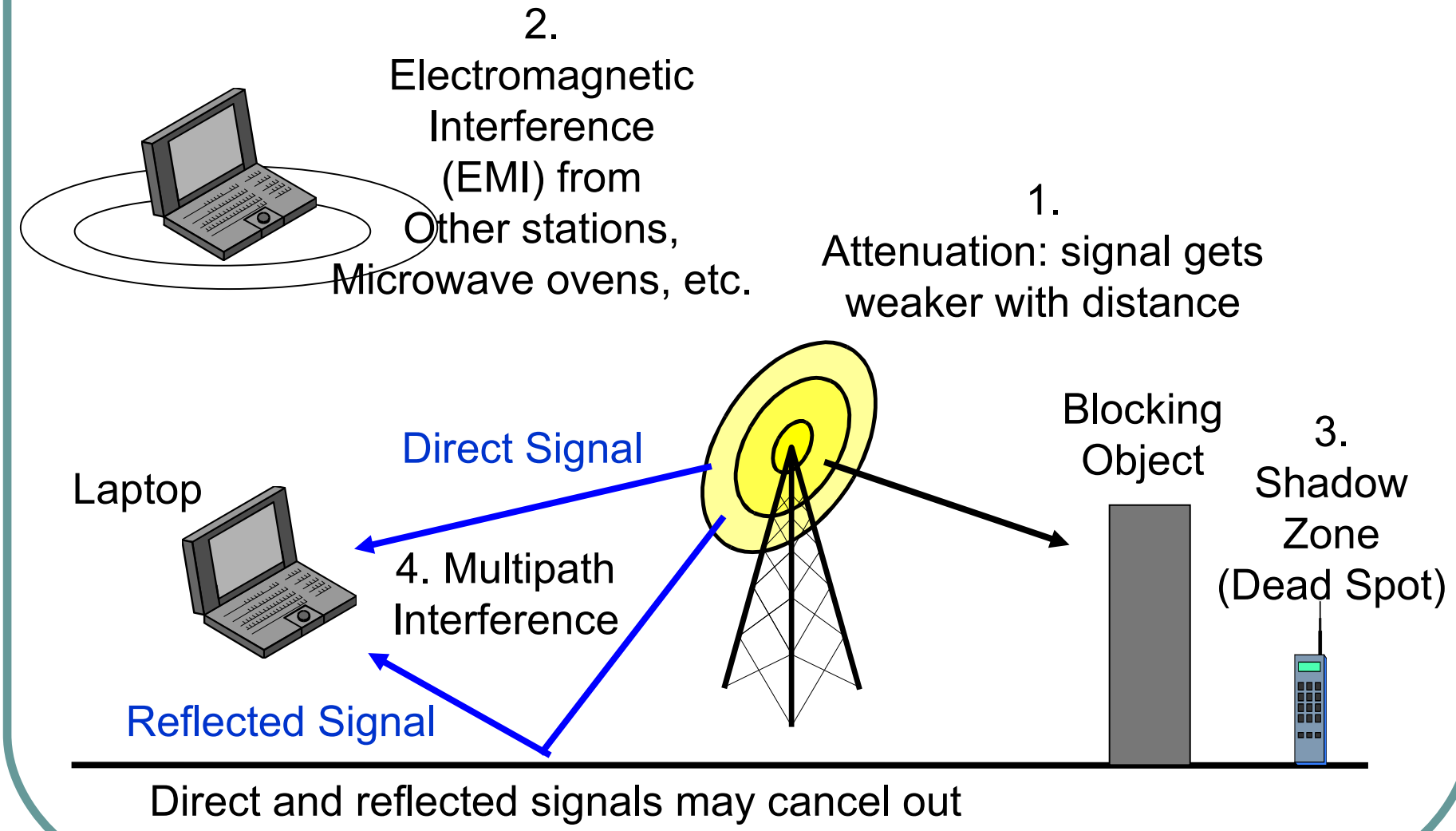
PCMCIA: used in
old laptops with no built-in WLAN Adapter

PCI: used in Desktop PCs

Some Terminologies

- An Access Point (AP) or wireless Access Point is usually a device that only allows wireless clients (stations) to connect to it. Examples of wireless clients (smartphone, laptops, PDAs, tablets, Smart TVs, etc...)
- A wireless router is an AP which also contains a number wired ethernet ports that allows wired clients to connect to it. Basically, it is an AP+network switch.
- A wireless gateway is usually a wireless router which integrates a modem to provide Internet access as well. Basically, it is an AP+Switch+Modem (This is the one most of us have at home (Residential Gateway).
- A Hotspot is usually the same thing as a wireless gateway.

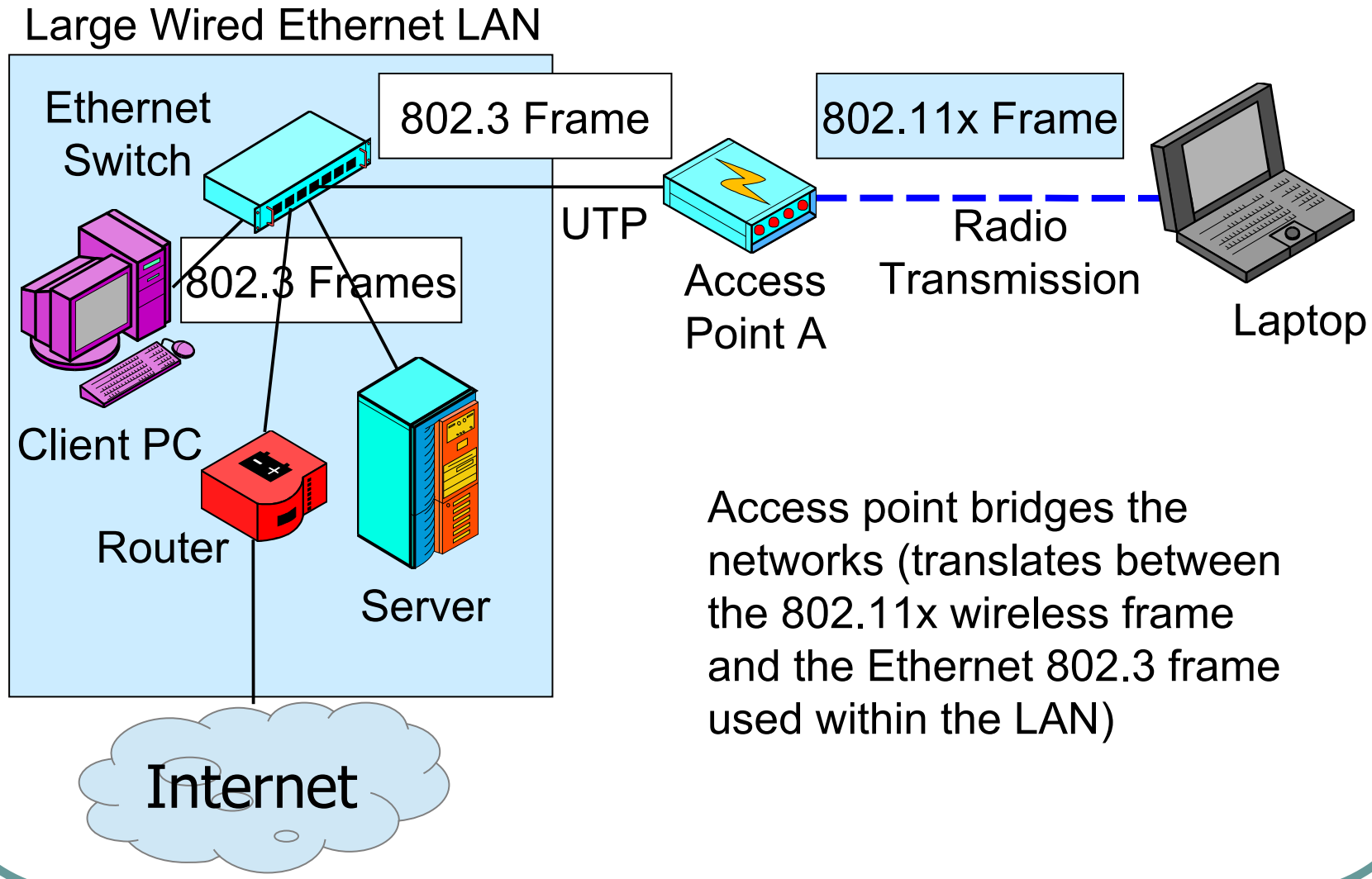
Wireless Propagation Problems



Wireless Propagation Problems

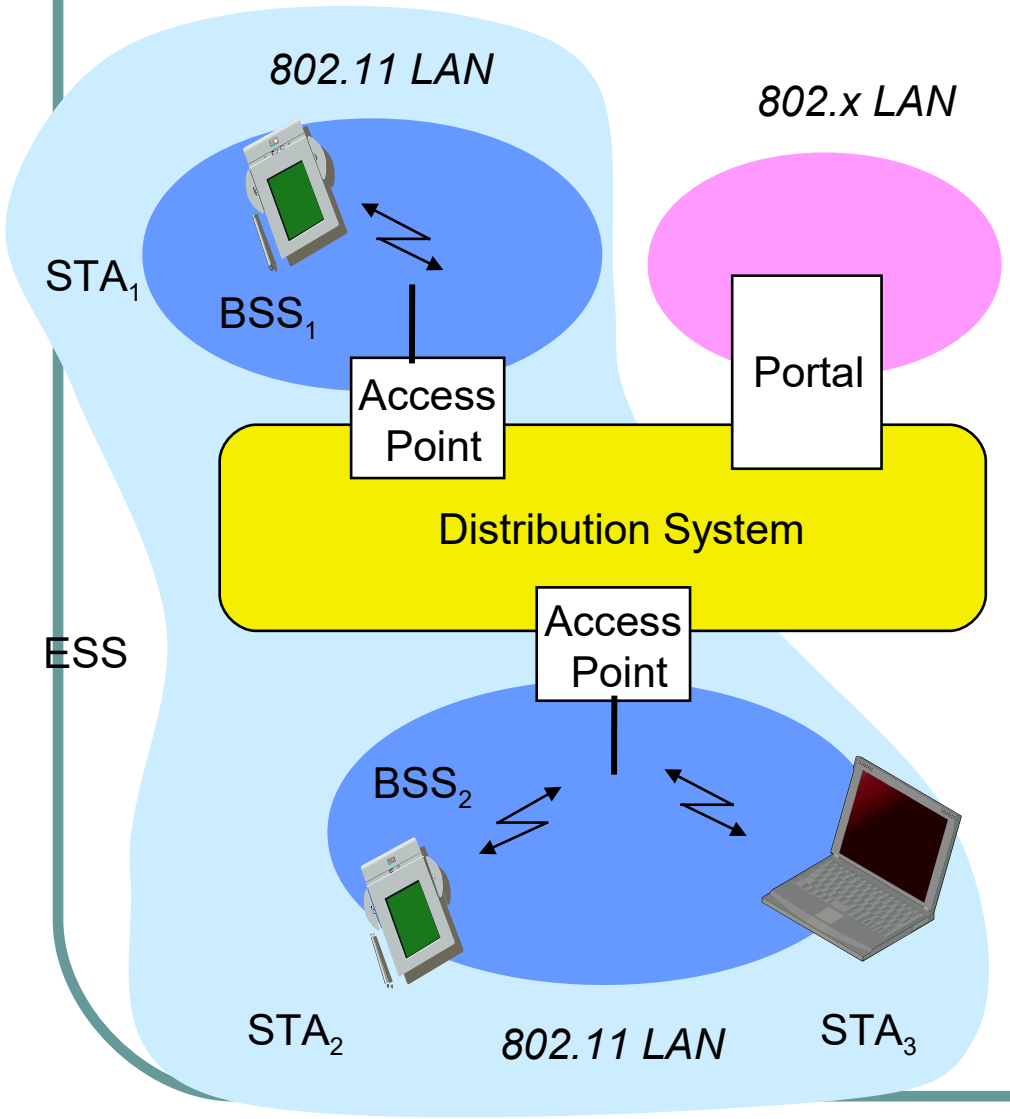
- Some problems are Frequency-Dependent
  - Higher-frequency signals attenuate faster
    - Absorbed more rapidly by moisture in the air
  - Higher-frequency signals blocked more by obstacles
    - At lower frequencies, signal refract (bend) around obstacles like an ocean wave hitting a buoy
    - At higher frequencies, signals do not refract; leave a complete shadow behind obstacles

Typical 802.11 Wireless LAN Operation with Access Points



Access point bridges the networks (translates between the 802.11x wireless frame and the Ethernet 802.3 frame used within the LAN)

Architecture of an wireless network



Station (STA)

- terminal with access mechanisms to the wireless medium and radio contact to the access point

Basic Service Set (BSS)

- group of stations using the same radio frequency

Access Point (AP)

- integrated into the wireless LAN and the distribution system

Portal

- bridge to other (wired) networks

Distribution System

- interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

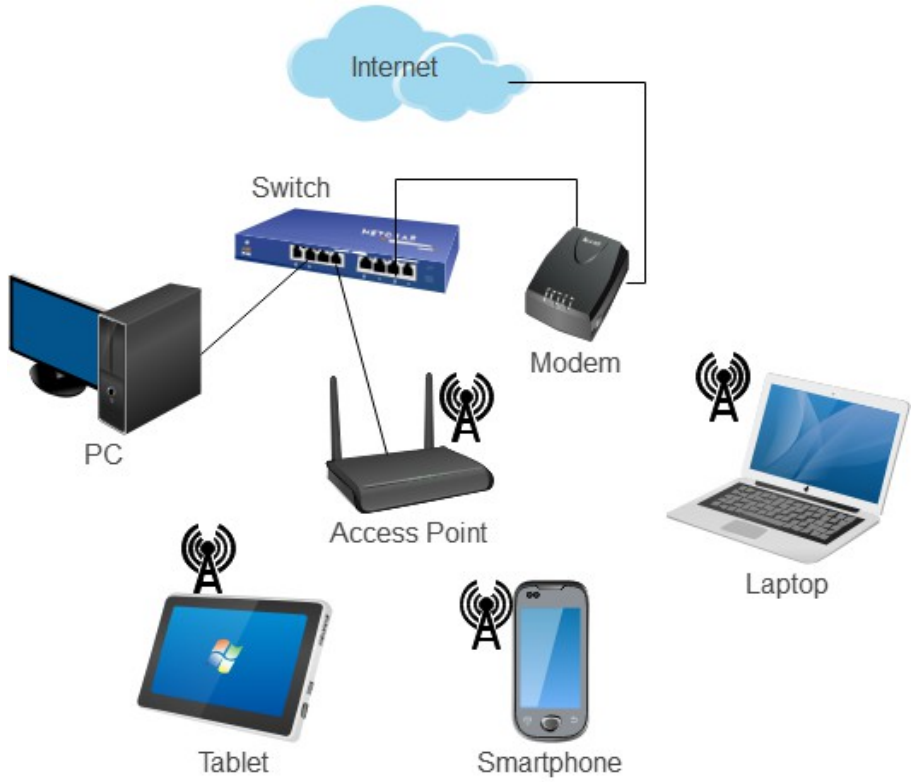
Typical AP modes of Operation

1. Infrastructure (Local/Managed) Mode
2. Client (Relay/Repeater) Mode ***
3. Sniffer (Monitor) Mode ***
4. Rogue Detector Mode ***
5. Bridge (Mesh) Mode ***

***(not available on all AP models)

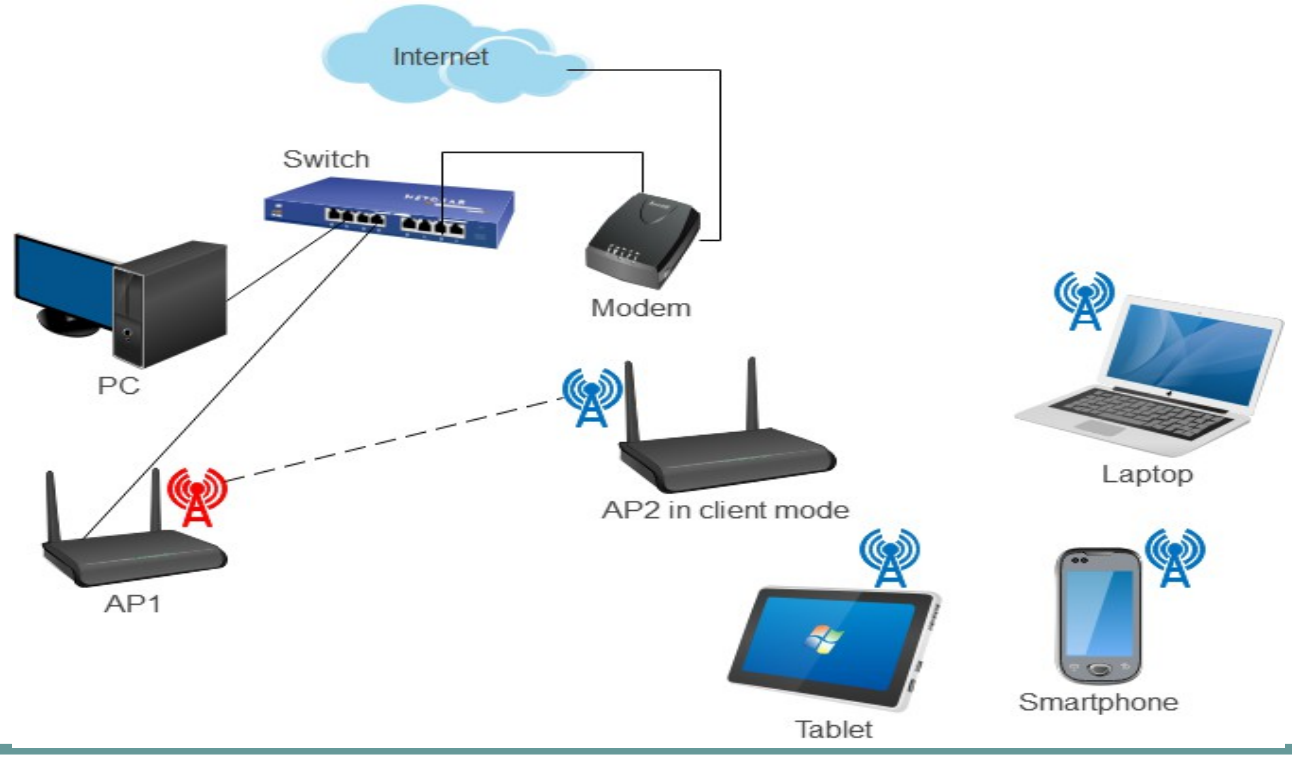
1. Infrastructure (Local/Managed) Mode

The tablet, smartphone and laptop all connect wirelessly to the AP.



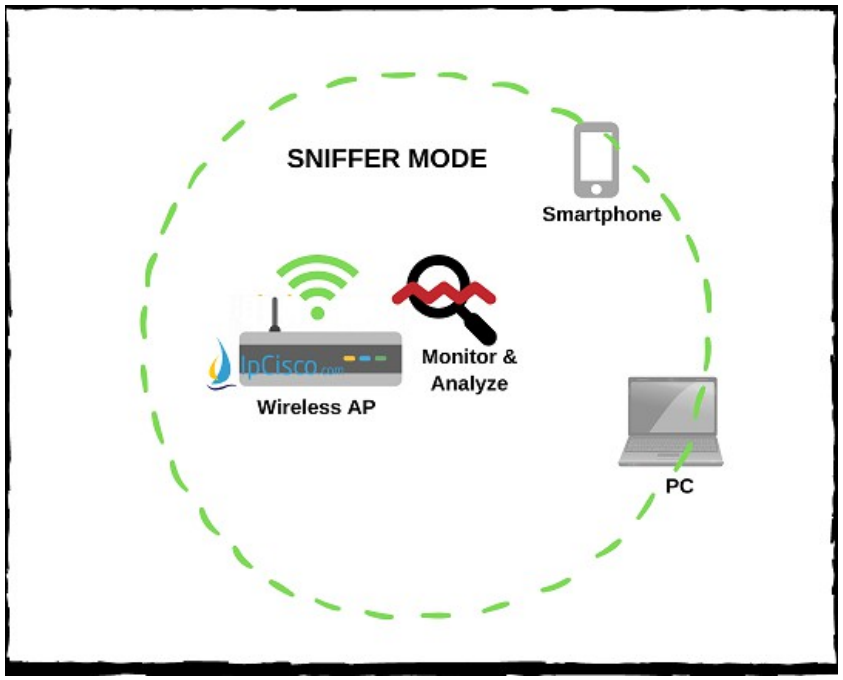
2. Client (Relay/Repeater) Mode

In this scenario, AP1 has internet connection, but the three stations are not in range to connect to it. AP2 is configured as client mode and connects to AP1 to allow the stations connected to the former to get internet access.



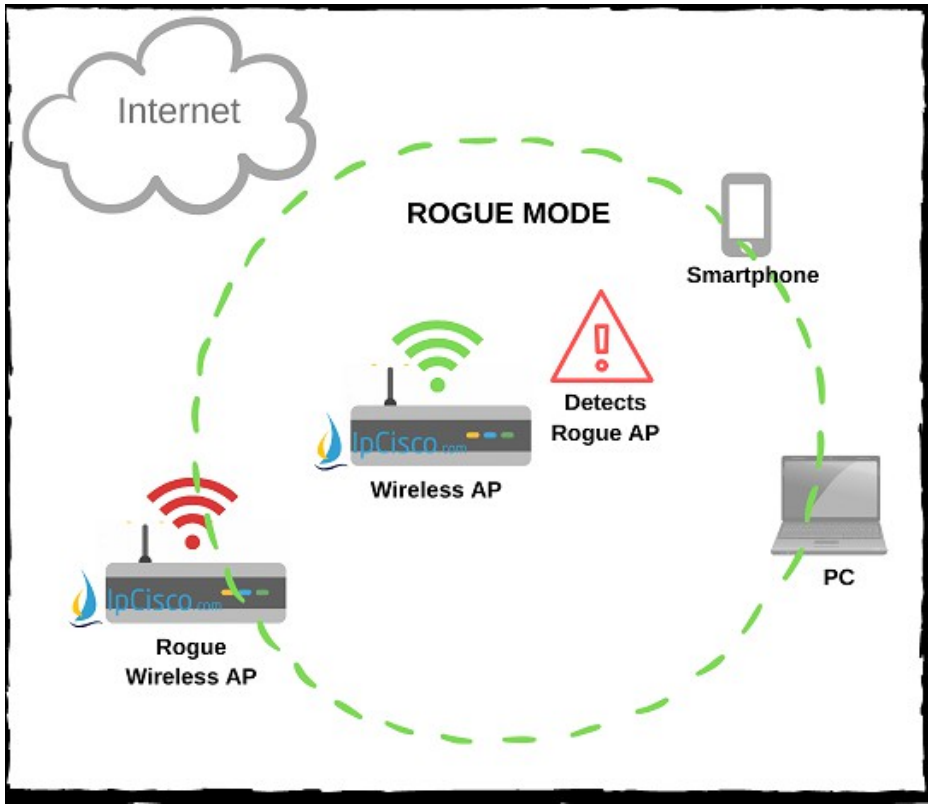
3. Sniffer (Monitor) Mode

In sniffer or monitor mode, the AP does not broadcast any SSID hence no wireless clients can connect to it but it can still receive wireless frames from stations. A laptop can connect remotely to the AP and perform sniffing with the appropriate software e.g. Wireshark



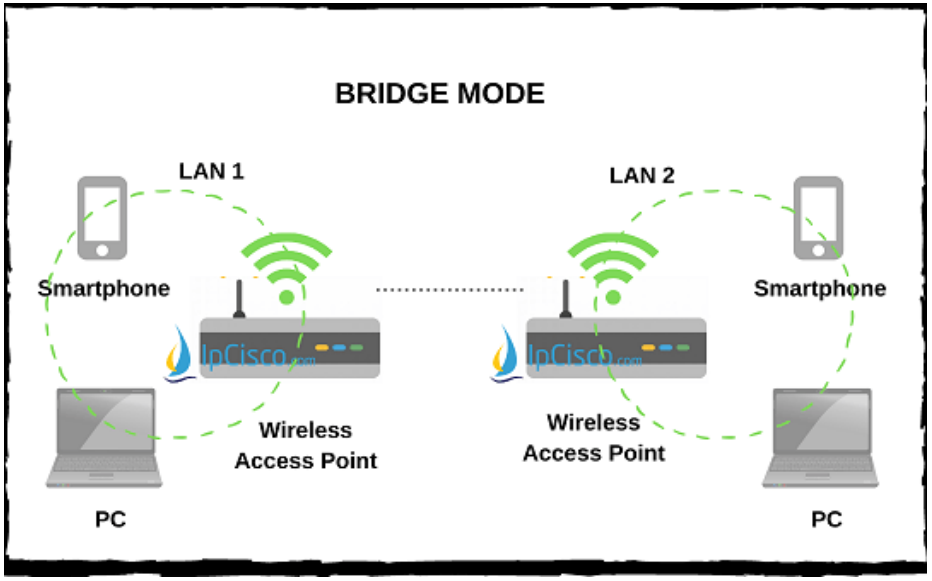
4. Rogue Detector Mode

In this mode, the AP is used to detect rogue devices. This detection is perform by inspecting the MAC address.



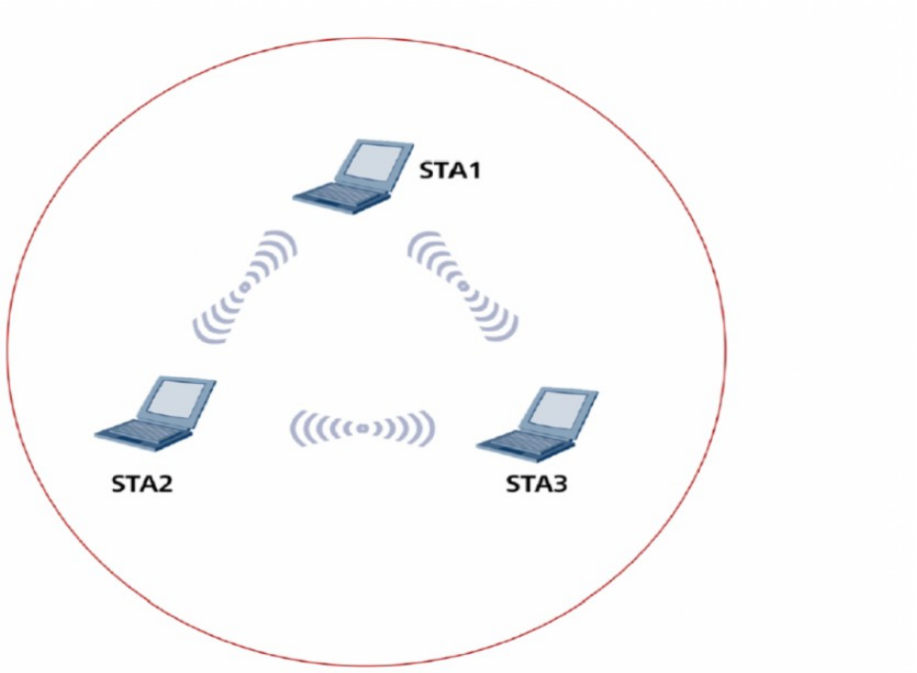
5. Bridge (Mesh) Mode

In Bridge mode, the two APs effectively establishes a point-to-point connection between themselves bridging 2 wireless LAN segments. If more than 2 APs are present, they can then establish point-to-multipoint connections effectively creating a mesh.



Ad-hoc or P2P Mode

In this mode, the stations connect to each other without the need of an access point (AP)



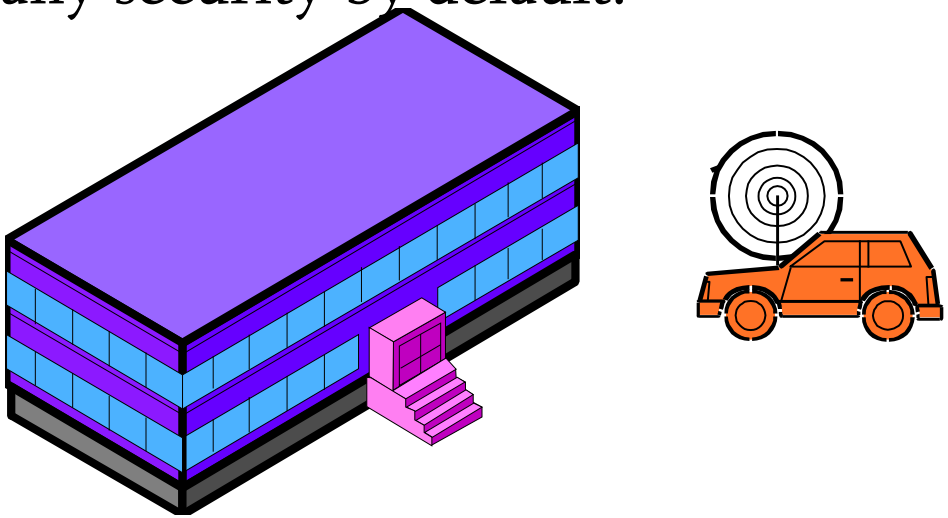
802.11 Wireless LAN Standards

802.11-Standard	Standard Year	Frequency (GHz)	Bandwidth (MHz)	Modulation Type	Max. Data Rate (Mbit/s)
802.11a	1999	5 GHz	20 MHz	OFDM	54 Mbit/s
802.11ac	2013	5 GHz	40/80/160	OFDM	6,93 Gbit/s
802.11ad	2012	60 GHz	2160	SC-OFDM	6,76 Gbit/s
802.11b	1999	2,4 GHz	20	DSSS	11 Mbit/s
802.11g	2003	2,4 GHz	20	DSSS/OFDM	54 Mbit/s
802.11n	2009	2,4/5 GHz	20/40	OFDM	600 Mbit/s

DSSS, direct sequence spread spectrum
FHSS, frequency hopping spread spectrum
OFDM, orthogonal frequency division multiplex
SC-OFDM, single carrier orthogonal frequency division multiplex

802.11x Security

- Automated Drive-By Hacking (War Driving)
  - Can read traffic from outside the corporate walls
  - Can also send malicious traffic into the network
  - This was possible as the first generation of APs did not have any security by default.

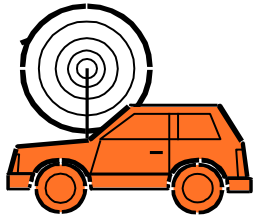


802.11 Security, Continued

- Wired Equivalent Privacy (WEP)
  - Initial flawed security method developed by the 802.11 Working Group for 802.11 devices in 1997.
  - All stations share the same encryption key with the access point. This key cannot be changed as it was a static key
  - Shared static keys means that a large volume of traffic is encrypted with the same key
  - With so much traffic generated with one unchanging key, cryptanalysts (code-breakers) can crack the key by collecting data for a few days
  - Once the key is cracked, the attacker can read all messages and send attack messages into the network without going through a firewall filter

802.11 Security, Continued

- Wired Equivalent Privacy (WEP)
  - Software that automates the hacking process is widely available e.g. AirSnort
    - Locate vulnerable access points by driving around (war driving)
    - Collect traffic and crack the key
    - **No longer recommended to use WEP nowadays**



802.11 Security, Continued

- Because of the security issues around WEP, the Wi-Fi Alliance developed Wi-Fi Protected Access (WPA) in 2003. Shortly afterward in 2004, they released WPA2 and in 2018 they released WPA3.

	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

802.11 Security, Continued

- Wireless Protected Access (WPA)
  - Stopgap security method introduced before full 802.11i security could be developed
  - It was often possible to upgrade older WEP products to WPA because the underlying hardware was the same as WEP.
  - It uses Temporal Key Integrity Protocol (TKIP). It addressed the two flaws present in WEP by using MIC instead of CRC-32 and increasing the IV of RC4 from 40 bits to 48 bits.

802.11 Security, Continued

- Wireless Protected Access 2 and 3
  - In WPA2, encryption and integrity check are performed within single logical block – CCM and both are based on AES.
  - In WPA3, both encryption and data integrity are enhanced even further from WPA2. The only downside is that more processing power is required. Not many wireless devices support WPA3 yet.

802.11 Security, Continued

- Ways to strengthen your Wireless LAN
  - **Do not use WEP**. Use WPA, WPA2 or WPA3 instead.
  - Enforce MAC address Association (i.e only allowed wireless adapters can join your wireless network)
  - Disable SSID broadcast once all permitted stations have been allowed to join the wireless network.
  - Enable Access Point firewall features to mitigate potential attacks.