## WIRELESS MEDIA

Wireless network systems use radio signals to transmit and receive, a system that hosts a wireless ***NIC*** is known as an ***end point***, the transceiver is known as the ***access point***. Wireless technologies use spread spectrum, that is a frequency hopping transmission that varies its frequencies over a certain band, there a three main types of spread spectrum technologies that exist today:

## OFDM: *ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING*

OFDM splits the signal into smaller subsignals that are transmitted together on varying frequencies. IEEE 802.11a and 802.11g networks can make use of OFDM.

## DSSS: *DIRECT SEQUENCE SPREAD SPECTRUM*

DSSS spreads the signal over the entire band at once, it is considered ***wideband*** for this reason. DSSS uses 802.11b and 802.11g networks.

## FHSS: *FREQUENCY HOPPING SPREAD SPECTRUM*

FHSS is a narrowband technology which changes the frequency for transmission at regular intervals, each frequency change is called a ***hop***, the client and server both coordinate the hops between frequencies. They retune with each other regularly agreeing on what frequency they will use for the next hop. FHSS is slower than DSSS and is considered an obsolete technology.

IEEE 802.11a , b, g are modes that exist for ad-hoc and infrastructure.

**AD-HOC –** Is where clients connect and communicate via their NICs this mode is decentralised and less secure.

**INFRASTRUCTURE -** Is where clients connect and communicate via a centralised access point (AP). This mode offers better control and protection because of its centralised administration.

## AP: *Access Point*

A centralised hub for connecting wireless devices.

## Wireless Cell

A wireless cell is a collection of wireless clients around a specific AP, these cells are sometimes referred to as a ‘Sphere of Influence’.

## BSSID: *Basic Service Set Identifier*

The BSSID differentiates one wireless cell from another, it provides no authentication information, it is usually the MAC address of the AP.

## SSID: *Service Set Identifier*

The SSID is the name given to an AP, this can be up to 32 characters long and can be also be encrypted.

The default channel for many AP’s is usually channel 11.

## WiFi Security Features

An AP allows for centralised control of the network and in doing so acts as a hub.

## WEP: *Wired Equivalent Privacy*

WEP is no longer secure, it was cracked in Nov 2008, its encryption can be 64bit, 128bit or 256bit, the 64bit and 128bit keys are weak and prone to hacking, WPA (*WiFi Protected Access*) is considered the strongest standard today. WPA2 is best.

## MAC Address Filtering

MAC filtering enables only allowed devices to access the network by means of their MAC address. ***Exclude by default*** allows only the devices with listed MAC addys, or you can set the AP to ***Include all*** and exclude those devices listed. Hackers are able to forge MAC addresses so MAC filtering is not the safest system for mitigating rogue systems attaching themselves to the network.

A Wifi Router or AP can be configured from an end point (NIC) and the general configuration mechanisms may be:

- Set the Admin password
- Configure WEP and MASC filtering
- Set the AP's IP address
- Upgrade its firmware
- Configure it to operate as a DHCP device

The wireless AP will be defaulted with an IP, you must first setup an end point to access this IP, and then commence reconfiguration to the networks IP.

Before installing a wireless LAN, a few things need to be considered:

- Security, WEP and MAC filtering, WPA2?
- Staff training
- Network management and integration

## TROUBLESHOOTING WIRELESS CONNECTIONS

- **POWER** – All cables and connecters and peripheral devices
- **ENCRYPTION** – Ensure all devices are using the same encryption method
- **SIDD** – Ensure SSID is correct (may change due admin)
- **MAC** Filtering – Include/Exclude all list (check table)

## CONFIGURING A WIRELESS NETWORK

1. **PLUG IN AND POWER ON THE AP** (ALL CABLES AND CONNECTORS)
2. **CONFIGURE AP'S SSID AND SHARED KEY WITH ENCRYPTION**
3. **INSERT WIFI NIC INTO COMPUTER OR CLIENT'S**
4. **SELECT A NETWORKING PROTOCOL** (TCP/IP)
5. **CONFIGURE EACH NIC TO USE THE CORRECT PROTOCOL AND AP'S ACCESS INFO**
6. **TEST THE CONNECTION**
7. **CONFIGURE SECURITY**
   (**MAC** FILTERING, ENCRYPTION, AUTHENTICATION, SHARED KEY)
8. **CONNECT AP TO WIRED NETWORK**

## NEXT-GENERATION 3G WIRELESS

3G Networks use additional access protocols for multiplexing:

- **CDMA** (Code-Division Multiple Access) originally had Data speeds of 144Kbps, now allows use of 8 channels and speeds of 115Kbps.
- **Wideband CDMA** – WAN speed 384Mbps, LAN speed 2Mbps.

All 2G and 3G networks are digital, there is no need for modulation and

demodulation.

## IEEE 802.11 WIFI

Wireless transmissions operating in the 2.4Ghz band using FHSS or DSSS, speeds of 1 -2 Mbps. 802.11 comes in several flavours: 802.11a, 802.11b, 802.11g, 802.111 and 802.11n.

**802.11A :**

5Ghz band, 54Mbps , OFDM.

**802.11B:**

2.4Ghz band, 11Mbps, DSSS.

**802.11G:**

2.5Ghz, 54Mbps, OFDM, DSSS.

**802.11I: (WPA2)**

Encryption mechanisms for 802.11a, b, g.

**802.1N:**

Fastest and most current, high bandwidth, increases speed and range, reduces 'dead spot' coverage and uses the following:

- **MIMO** – *Multiple Input, Multiple Output*, Uses multiple antennae to channel signals, simultaneously transmits three streams of data and receives on two.
- **Channel Bonding** – Two overlapping channels, increases data output.
- **Payload Optimization** – (*Packet Aggregation*), more data in each packet.

## **IEEE 802.11** WiFi Access Method (CSMA/CA)

**CSMA/CA** – *Carrier Sense Multiple Access/Collision Avoidance*

CSMA/CA specifies that each node transmit its intention to broadcast, if a node is transmitting no other node can transmit until it is finished. It's the "*listen before talking*" rule so no collisions exits on the network.