Installing Wireless and SOHO Networks

802.11 Networking Standards

- Standards managed by IEEE
- Most common wireless standard IEEE 802.11
- First standard for WLAN (in 1997)
- Over 20 standards within 802.11
- 802.11a, b, g, n, and ac
- Connect to a wireless router or wireless access point
- Client will need to know the SSID (service set identifier)
- Use CSMA/CA – Carrier Sense Multiple Access/Collision Avoidance not ethernet protocol CSMA/CD
- Packet collisions general avoided
  - Wait random period of time to resend (back-off time)

Modulation Techniques

- (FHSS) Frequency-Hopping Spread Spectrum
  - Communicates by hopping the transmission over a range of predefined frequencies.
  - Appears as a single channel at each end
  - Bluetooth hops 1600 times per second between the 79 defined channels
- (DSSS) Direct-Sequence Spread Spectrum
  - Adds data to the data to be sent
  - Protects against interference (inc. jamming)
  - Provides security if added data is unknown
  - Used by 802.11b and Zigbee
- (OFDM) Orthogonal Division Multiplexing
  - Data divided and each part sent over a different frequency at the same time
- www.telecomabc.com is an excellent resource if you want to know more about the above

802.11 – Original Standard

- 1Mbps or 2Mbps
- Using 2.4Ghz spectrum
- Data encoding using
  - FHSS – Frequency Hopping Spread Spectrum
  - DSSS – Direct Sequence Spread Spectrum
- Like the OSI 7 layer model, its a theoretical standard
  - All released devices will be post fixed with a number. e.g. 802.11g

802.11a

- 54Mbps
- 5GHz Spectrum
- OFDM – Orthogonal Frequency Division Multiplexing
- Ratified 1999
- Market availability 2001

802.11b

- Ratified in 1999
- Marketed very quickly – de-Facto standard for years
- 11Mbps
  - Can operate at 5.5, 2 and 1Mbps
- 2.4GHz range
- DSSS for data encoding
- Avoid and update to something faster!

802.11g

- Ratified 2003
- 54Mbps Bandwidth
- 2.4Ghz spectrum
- OFDM or DSSS
- Compatible with 802.11b (hence labels of 802.11b/g)
- Note: 802.11b cannot use OFDM
  - Unable to tell if 802.11g access point is free or busy
  - Access point reverts to DSSS (max 11Mbps)
  - Therefore upgrade all devices to 802.11g

2.4GHz Range

- 14 Channels (but can only use first 11)
- Channels are auto-configured
  - Two channels will not overlap
  - Three channels can only be 1, 6, and 11
  - Avoid overlap if setting manually
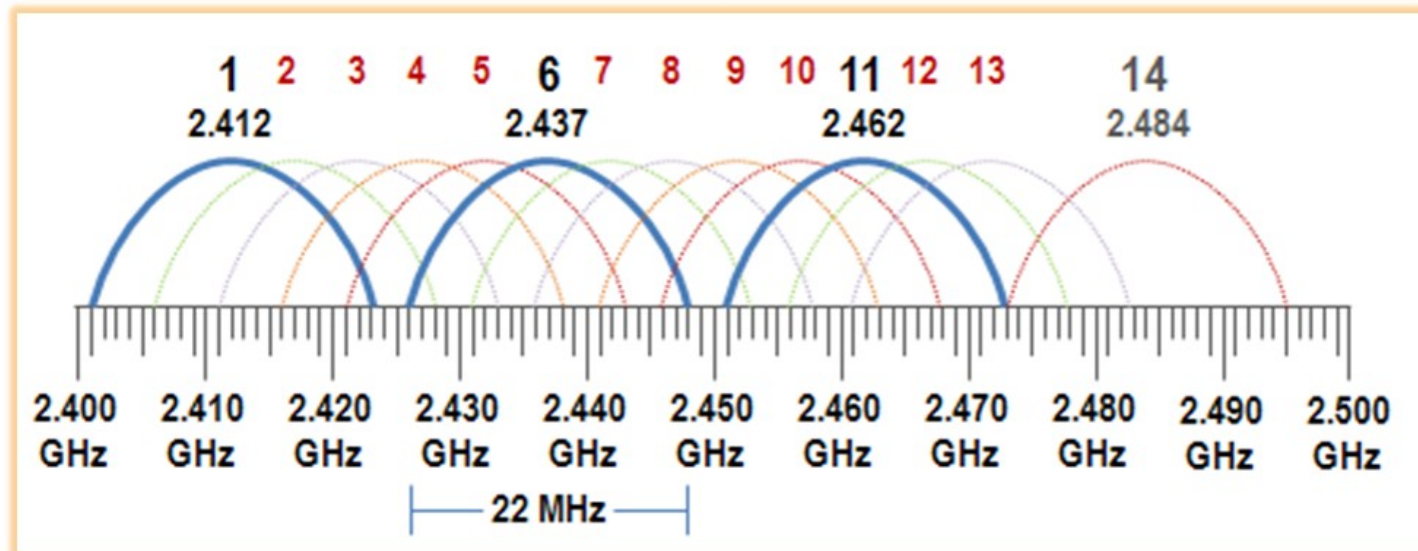
Frequencies

- Frequency use is defined by each country
- UK is managed by ofcom - http://static.ofcom.org.uk/static/spectrum/fat.html
- For example, on 5GHz, wi-fi is a secondary user. The Primary user is radar and weather satellites.
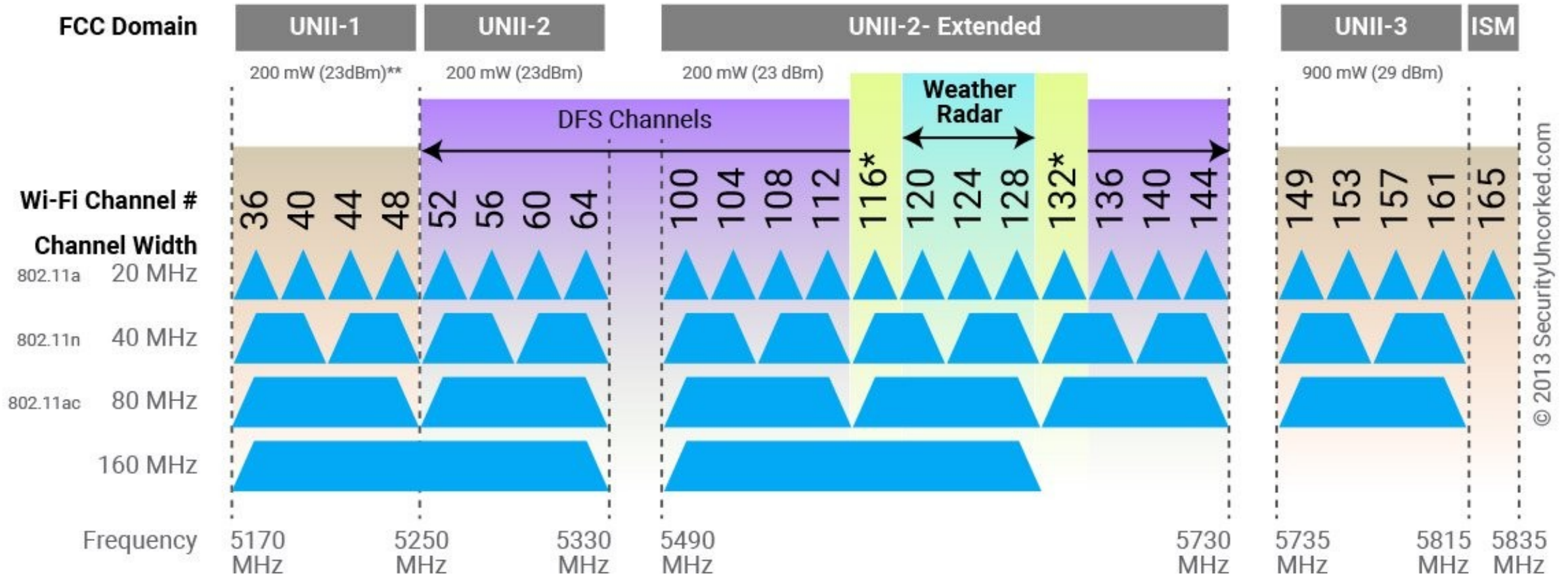
802.11n

- Ratified in 2010
- Bandwidth up to 600Mbps (reality 300Mbps - 450Mbps)
- In 2.4Ghz and 5GHz spectrum
- 40MHz Channels
  - MIMO – Multiple Input Multiple Output
  - Channel Bonding (Combines channels to double capacity)
  - Requires multiple antennas (Maximum of 8. Need some to send and some to receive)
  - Simultaneously at 2.4Ghz and 5GHz
- Backwards compatible with a/b/g

802.11ac

- January 2014
- Bonds up to 8 Channels (160MHz bandwidth)
- Theoretical Max speed of 6900Mbps (Common 800Mbps current device capability)
- Beam forming – send signals is specific direction
- 802.11ac is NOT backwards compatible to 802.11b

802.11ac Channel Allocation (N America)

FCC Domain	UNII-1	UNII-2	UNII-2- Extended	UNII-3	ISM
	200 mW (23dBm)**	200 mW (23dBm)	200 mW (23 dBm)	900 mW (29 dBm)	

DFS Channels

Weather Radar

Wi-Fi Channel #

36 40 44 48 | 52 56 60 64 | 100 104 108 112 | 116* 120 124 128 132* 136 140 144 | 149 153 157 161 | 165

Channel Width

802.11a	20 MHz
802.11n	40 MHz
802.11ac	80 MHz
	160 MHz

Frequency

5170 MHz | 5250 MHz | 5330 MHz | 5490 MHz | 5730 MHz | 5735 MHz | 5815 MHz | 5835 MHz

*Channels 116-144 used for Doppler radar. Channel 132-144 not yet available in USA

**Allowed Power for UNII-1 band increased by FCC from 40 mW to 200 mW in 2014

© 2013 SecurityUncorked.com

802.11 Standards (For information only)

IEEE 802.11	Release Date	Frequency (GHz)	Max Data Rate (Mbps)	Range (m)		Status and Comments
				Indoor	Outdoor	
-1997	1997	2.4	2	20	100	Obsolete
a	1999	5/3.7	54	35/-	120/5k	Legacy systems
b	1999	2.4	11	35	140	Legacy systems
g	2003	2.4	54	38	140	Legacy systems
n	2009	2.4/5	600	70	250	Current systems
ac	2013	2.4/5	450/7,000	35		Next generation – just starting to be deployed.
ad	2012	60	7,000	10		Known as WiGig. Short-reach high data rate data transfers.
af	Est. 2016	0.470-0.710	568		6,000	Being called White-Fi because it uses unused TV spectrum.
ah		0.9	40			In development.
ai		45/60	7,000	10		Modification of 802.11ad for 45GHz band for use in China
ax	Est. 2019	2.4/5	450/10,000	35		Revision to 802.11ac to increase efficiency.

802.11 Standards

- Further away from the WAP, the lower the connection speed
- Number of clients attached will also affect performance – try using at an airport – more clients, less bandwidth per client

802.11 Standards

- Further away from the WAP, the lower the connection speed
- Number of clients attached will also affect performance – try using at an airport – more clients, less bandwidth per client

Type	Frequency	Max Throughput	Modulation	Indoor Range	Outdoor Range
-	2.4GHz	2Mbps	FHSS/DSSS	20m	100m
a	5GHz	54Mbps	OFDM	35m	120m
b	2.4GHz	11Mbps	DSSS	40m	140m
g	2.4GHz	54Mbps	DSSS/OFDM	40m	140m
n	5Ghz/2.4GHz	600Mbps	OFDM/DSSS	70m	250m
ac	5GHz	1300Mbps	OFDM	35m	140m

Bluetooth

Version	Data Rate	Maximum Range
1.2	1Mbps	
2.0	3Mbps	
3.0	24Mbps	<60m
4.0	24Mbps	60m
5.0	50Mbps	240m

- PAN
- Sometimes called a piconet
- V5 Designed for privacy, security and low power
  - See difference-between-bluetooth-4-2-and-bluetooth-5-0
  - pcmag.com bluetooth-versions
- 4 Classes

Class	Distance	Power usage
1	100m	100mW
2	10m	2.5mW
3	1m	1mW
4	0.5m	0.5mW

Long-Range Fixed Wireless

- Bluetooth and Wi-Fi are short range technologies

- Long-Range fixed wireless
    - point to point technology
    - Directional antennas
        - Alignment is critical
    - Small satellite dish size

- Unlicensed and licensed frequencies
    - Wi-Fi operates on unlicensed frequencies
        - Free to use
        - Susceptible to interference
    - Licensed Frequencies are managed by government
    - Need to apply for a license to use

Long-Range Fixed Wireless

- Power over Long-Range Fixed Wireless
  - Wireless Power Transfer (WPT)
  - Transmitter generates power and sends using microwave or laser
  - Receiver then converts signal back to power.
  - Efficiency is an issue

Radio Frequency Networking Standards

- RFID – Radio Frequency Identification
- 3 types:
  - Low Frequency (125-134Khz), distance 10cm
  - High Frequency (13.56Mhz), distance 30cm
  - Ultra High Frequency (856-960Mhz), distance 100m
- Tag – attaches to the device to be tracked
  - Passive – no power source, uses power given by the waves of the reader. Max distance 25m
  - Active – own power source, normally a button cell, and own antenna. Max distance 100m
- Reader – have a power source and antenna

Near Field Communication

- Mainly used in contactless payment
  - Apple pay, Android pay
- Initiator and Target
- 3 different modes:
  - NFC Card Emulation Mode – lets device act as smart card. Payments made this way
  - NFC Reader/Writer Mode
  - NFC Peer-to-Peer Mode – allows adhoc data transfer between two NFC enabled devices
- Not encrypted – man in the middle attacks!

Infrared

- Most common TV remote control
- IrDA – Infrared Data Association
- Point to point / Walk up
  - One to one communication
  - Very close proximity
- Approx 1Gbps
- 1 Meter range

Installing and Configuring SOHO networks

- SOHO – Small Office, Home Office

- Internet
  - Dial Up (POTS) and broadband
  - Dial up – max 56Kbps. Cheap and only useful as a backup.
  - DSL – Digital Subscriber Line
    - Requires RJ-45 and DSL Splitter

DSL Standards

- Speeds decrease as the distance to the exchange increases

- Voice 0 to 4KHz

- ADSL 25.875KHz to 138KHz upstream

- ADSL 138KHz to 1104KHz downstream
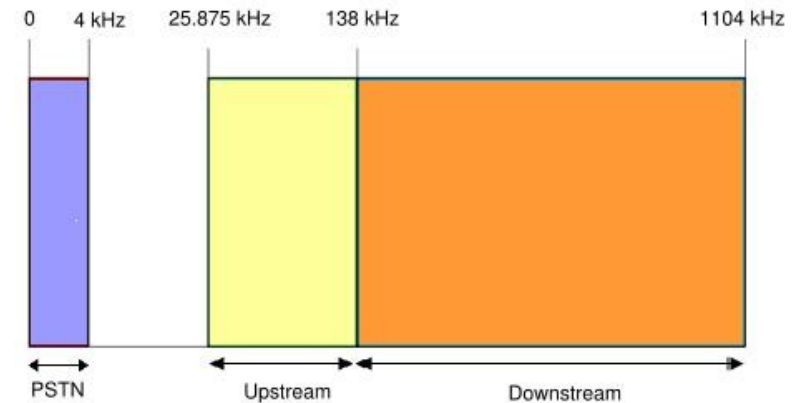
Standard		Download Speed	Upload Speed
ADSL	Asymmetric DSL	Up to 8Mbps	Up to 1Mbps
SDSL	Symmetric DSL	Up to 2.5Mbps	Up to 2.5Mbps
HDSL	High bit rate DSL	Up to 42Mbps	Up to 8Mbps
VDSL	Very high bit rate DSL	Up to 52Mbps	Up to 16Mbps

DSL

- ADSL2+
  - 24Mbps download
  - 3.3Mbps upload

- DSL needs more hardware
- DSL higher cost than dial up

Cable Modem

- DOCSIS – Data Over Cable Service Internet Specification
- Share bandwidth with others – more users slower connection
- Throttled by ISP sometimes
- Do not need landline
- Very reliable
- Needs cable modem
- Higher cost

Fibre-Optic Internet

- High Speed Connections
- Very expensive (not copper – obviously)
- FTTH – Fibre to the home
  - 880Mbps upload and 940Mbps download
- FTTC – Fibre to the curb / FTTN – Fibre to the Node
  - Fibre to box in street the copper to home
  - 25Mbps max speed

Satellite

- Uses Geostationary satellites
- Slower but essential in remote areas
- Download – 125Mbps max
- Upload – 3Mbps max
- Point to multipoint (GPS, Sky TV etc)
- Geo Stationary Satellites are 35786Km up
- Weather affects signal
- Alignment is critical – line of sight critical
- Propagation delay or latency
  - Time to send data to satellite and get a response from the satellite
  - Approx 250 milliseconds (Non Satellite technologies about 10 milliseconds)

Cellular WAN

- GSM – Global System for Mobile Communications
  - 3G – Third Generation
  - 4G – Fourth Generation (2008)
    - Designed to use IP protocol
  - 5G – Fifth Generation (2018)
    - Speed 1Gbps to max of 20Gbps
- Tethering
  - Connecting two devices together
  - Phone and Laptop most common
- Mobile Hotspot
  - Mi-Fi
  - Upto 8 devices

Wireless Internet Service Provider (WISP)

- Allows connection to the internet using wireless technologies.

- Licensed or unlicensed frequencies

- Can also be line of sight
  - Transmitter and Receiver about 10 miles apart
    - Obstructions cause signal loss
    - Weather affects signal
    - Trees growing over time cause issues
  - Costly

Type	Download Speed	Description
Dial Up (POTS)	Up to 56Kbps	Analogue Service
DSL	Up to 50Mbps	Inexpensive, wide availability
Cable	Up to 100Mbps	Inexpensive, wide availability
Fibre	Up to 1Gbps	Very fast but expensive
Cellular	Up to 100Mbps with 5G	Good for rural areas with mobile signals. Maximum 8 devices
Satellite	Up to 25Mbps	Best for rural locations. Expensive
Wireless Internet Service Provider (WISP)	Up to 50Mbps	Fast connection for rural areas without broadband

Internal Network Communications

- Wired Connections
  - Wires still used in backbones of most networks
- Need to know for exam CAT5, CAT5e, and CAT6
- CAT5
  - 100BaseTx – max 100 Mbps and 100m distance
- CAT5e
  - 1000BaseT – max 1 Gbps and 100m distance
- CAT6
  - 10GBaseT – max 10 Gbps and 55m distance (CAT6) or 100m (CAT6a)

Standard	Cables Used	Maximum Speed	Maximum Distance
10BaseT	UTP Cat 3 and above	10Mbps	100 Meters
100BaseTX	UTP Cat 5 and above	100Mbps	100 Meters
100BaseFX	Multi-Mode Fibre	100Mbps	2,000 Meters
1000BaseT	UTP Cat 5e and above	1 Gbps	100 Meters
10GBaseT	UTP Cat 6 and above	10Gbps	55 Meters (Cat 6) 100 Meters (Cat 6a, 7, and 8)
25GBaseT or 40GBaseT	UTP Cat 8	25Gbps or 40Gbps	30 Meters
10GBaseSR	Multi-Mode Fibre	10Gbps	300 Meters
10GBaseLR	Single-Mode Fibre	10Gbps	10K Meters
10GBaseER	Singles-Mode Fibre	10Gbps	40K Meters

- Number corresponds to max speed in Mega bits per second (unless it says G)
- T indicates twisted pair, F is fibre

Internal Network Consideration Questions

- How fast does this network need to be?
- What is the maximum distance any one cable needs to run?
- How important is security?
- Is there a possibility of electrical interference?
- What is the cost?

Keys to planning a Network

- Understand the relevant regulations
- Make a map
  - Include distances. Note power outlets. Mark obstacles.
- Locate the server
- Identify where the client computers will be.
- Locate the network resources
- Determine how users will connect
  - For Wi-Fi 5 (802.11ac) and older, max 30 users per access point
  - No cable runs over 100 Meters
- Designate additional connectivity areas, if needed
  - Switches if extending cable runs

Wireless Setup

- Wi-Fi Alliance (www.wi-fi.org) 5 step router set up
  - Change the routers SSID
  - Change the admin username and password
  - Select AES or WPA2
  - Choose a high security passphrase
  - Configure the clients

Wireless Encryption Methods

- Every wireless has an SSID (Service Set Identifier)
  - Configure not to broadcast – default is to broadcast
- WEP – Wired Equivalent Profile
  - Static key
  - 10,26 or 58 character length hexadecimal key
  - WEP.64 – 64 bit key size – 10 characters
  - WEP.128 – 128 bit key size – 26 Characters
  - WEP.256 – 256 bit key size – 58 Characters
  - Easily cracked so do not use
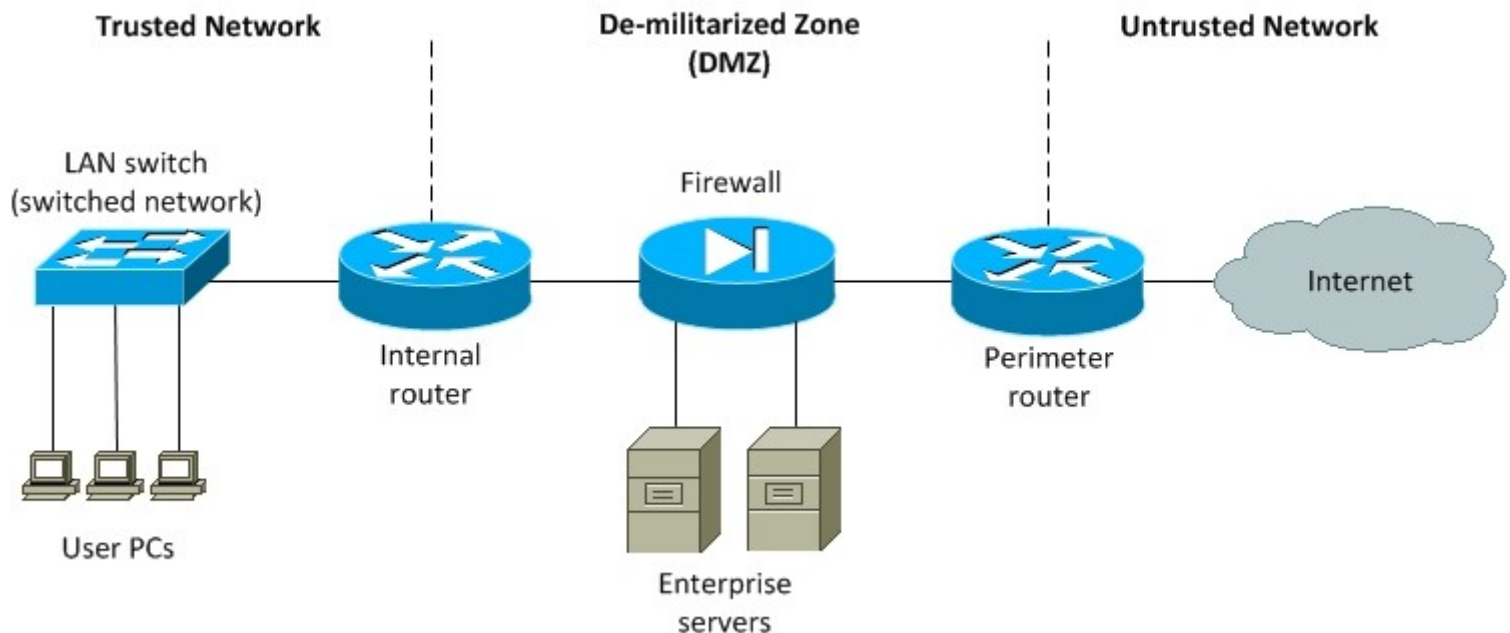
Wireless Encryption Methods

- WPA – Wi-Fi Protected Access
  - TKIP – Temporal Key Integrity Protocol
    - 128bit dynamic per packet key (new key for every packet sent)
- WPA2
  - Implements all of the 802.11i security
  - CCMP – Counter Mode CBC-MAC Protocol – better than TKIP
  - Based on Advanced Encryption Standard (AES)
  - Strongest encryption and data protection

Wireless Channels

- WAP – Wireless Access Point
  - Max 30 people on anyone point
- If need multiple WAPs in one building
  - Set each one to have overlapping ranges, about 20% to allow users to roam and not loose connection.
  - Configure the WAPs with the same SSID
  - Configure WAPs with non-overlapping channels

Additional Wireless Router Services

- Firewall
  - Hardware or software
  - Network Security Guard
  - Filters packets (rules defined by administrator)
  - Public Side (Red)
  - Private Side (Green)
  - DMZ (Amber)

Trusted Network

De-militarized Zone (DMZ)

Untrusted Network

LAN switch
(switched network)

Firewall

Internal
router

Perimeter
router

Internet

User PCs

Enterprise
servers

Firewall Types

- Network Based firewalls
  - Designed to protect entire networks not just one system
  - Normally standalone hardware with specialised software

- Host Based Firewalls
  - On a single machine to protect that machine
  - Normally software
  - All Windows now have this as standard
  - Not as secure as Network Based firewalls
  - Cheap alternative

How Firewalls Work

- Work at a packet level
  - Permit, deny, encrypt, decrypt
- Administrator sets up rules
  - Default Deny (All traffic blocked)
  - Default Allow (No traffic blocked) – what's the point!
- ACL – Access Control List
  - Rules that permit or deny traffic
  - Typically by IP and Port number and Domain name
- Port Triggering
  - Only allows data through to a specific port
  - Port forwarding

Some Essentials

- Change the default SSID
- Change the admin username and password (highly secure)
- Configure the best security protocol, e.g. WPA2 (AES)
- Set a strong passphrase for clients
- Change the passphrase regularly

Configuring Internet of Things

- Home automation is an example
  - Control of devices without being physically present
  - App controlled
  - Thermostats
    - Can create energy reports
    - Voice Activation
    - Integrated with outdoor temperature sensors
    - Geofencing – adjusting to a users individual preferences
- Light Switches, Door Locks

Exam Essentials

- Know the difference between 802.11 standards, specifically a,b,g,n and ac
- Know the three encryption protocols in wireless networks
  - WEP, WPA and WPA2
- Know the various cellular networking standards
- Know basic IoT devices
- Know the two most common IoT standards
- Know the difference between RFID and NFC
- Know the different broadband connections
- Learn the three non-overlapping 2.4Ghz wireless channels
  - 1, 6 and 11