7. WIFI FAMILY

1. IEEE 802: What is it, and why should I care?

The early days of networking only saw wireline networks (if you don't count the old AT&T Long lines microwave backbone that at one time crossed the United States) Now many networks are built using both wireline and wireless solutions. Typically networks based on wires or more usually these days, fibres have greater capacity than wireless.
But laying fibre is much more expensive and takes time. So often networks begin as wireless networks and as they grow in use, fibre based networks start to be deployed. In access networks (those near the consumers) or in dense urban environments, often wireless is more practical too. So very importantly as you begin to think about deploying wireless networks in your local area or community, your network could form the basis of the future growth of networking in your region.

An aspect of wired and wireless networks important to understand is the various standards that exist today as well as those new standards that are being developed. Wireless standards are the basis for many wireless products, ensuring interoperability and useability by those who design, deploy and manage wireless networks. We touched on this subject already in the chapter called **Radio Spectrum**. The Standards used in the vast majority of the networks come from the IEEE Standard Association's IEEE 802 Working Group. **IEEE 802** refers to a family of IEEE standards dealing with local area networks and metropolitan area networks.

More specifically, the IEEE 802 standards are restricted to networks carrying variable-size packets. (By contrast, in cell relay networks data is transmitted in short, uniformly sized units called cells). The number 802 was simply the next free number IEEE could assign, though “802” is sometimes associated with the date the first meeting was held — February 1980. The services and protocols specified in IEEE 802 map to the lower two layers (Data Link and Physical) of the seven-layer OSI networking reference model. In fact, IEEE 802 splits the OSI Data Link Layer into two sub-layers named Logical Link Control (LLC) and Media Access Control (MAC).

The IEEE 802 family of standards is maintained by the IEEE 802 LAN/MAN Standards Committee (LMSC).
The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs.

An individual Working group provides the focus for each area and they are listed in the table below.

Name	Description
IEEE 802.1	Bridging and Network Management
IEEE 802.3	Ethernet
IEEE 802.11 a/b/g/n	Wireless LAN (WLAN)
IEEE 802.15	Wireless PAN
IEEE 802.15.1	Bluetooth certification
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence
IEEE 802.15.3	High-Rate wireless PAN
IEEE 802.15.4	Low-Rate wireless PAN eg. Zigbee
IEEE 802.15.5	Mesh networking for WPAN
IEEE 802.15.6	Body Area Network
IEEE 802.16	Broadband Wireless Access (basis of WiMAX)
IEEE 802.16.1	Local Multipoint Distribution Service
IEEE 802.18	Radio Regulatory TAG
IEEE 802.19	Coexistence TAG
IEEE 802.20	Mobile Broadband Wireless Access
IEEE 802.21	Media Independent Handoff
IEEE 802.22	Wireless Regional Area Network
IEEE 802.23	Emergency Services Working Group
IEEE 802.24	Smart Grid TAG
IEEE 802.25	Omni-Range Area Network

2. The 802.11 standard

The standard we are most interested in is 802.11 as it defines the protocol for Wireless LAN.
The 802.11 Amendments are so numerous they have in the last few years started using 2 letters instead of 1. (802.11z - the DLS amendment - gave way to 802.11aa, ab, ac..., etc)

Below is a table of the variants of 802.11, their frequencies and approximate ranges.

802.11 protocol	Release	Freq.	Bandwidth	Data Rate per stream	Approximate indoor range		Approximate outdoor range	
		(GHz)	(MHz)	(Mbit/s)	(m)	(ft)	(m)	(ft)
-	Jun 1997	2.4	20	1, 2	20	66	100	330
a	Sep 1999	5	20	6,9,12, 18, 24, 36, 48, 54	35	115	120	390
b	Sep 1999	2.4	20	1, 2, 5.5, 11	35	115	140	460
g	Jun 2003	2.4	20	6,9,12, 18, 24, 36, 48, 54	38	125	140	460
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	70	230	250	820
			40	15, 30, 45, 60 , 90, 120, 135, 150				
ac	Nov.2011	5	20	Up to 87.6				
			40	Up to 200				
			80	Up to 433.3				
			160	Up to 866.7				

In 2012 IEEE issued the 802.11-2012 Standard that consolidates all the previous amendments.

The document is freely downloadable from:
http://standards.ieee.org/findstds/standard/802.11-2012.html

3. Deployment planning for 802.11 wireless networks

Before packets can be forwarded and routed to the Internet, layers one (the physical) and two (the data link) need to be connected. Without link local connectivity, network nodes cannot talk to each other and route packets.
To provide physical connectivity, wireless network devices must operate in the same part of the radio spectrum.
This means that 802.11a radios will talk to 802.11a radios at around 5 GHz, and 802.11b/g radios will talk to other 802.11b/g radios at around 2.4 GHz.
But an 802.11a device cannot interoperate with an 802.11b/g device, since they use completely different parts of the electromagnetic spectrum.
More specifically, wireless interfaces must agree on a common channel. If one 802.11b radio card is set to channel 2 while another is set to channel 11, then the radios cannot communicate with each other.
The centre frequencies of each channel for 802.11a and 802b/g are given in **Appendix B: Channel Allocations.**
When two wireless interfaces are configured to use the same protocol on the same radio channel, then they are ready to negotiate data link layer connectivity. Each 802.11a/b/g device can operate in one of four possible modes:

1. Master mode (also called AP or infrastructure mode) is used to create a service that looks like a traditional access point. The wireless interface creates a network with a specified name (called the SSID) and channel, and offers network services on it. While in master mode, wireless interfaces manage all communications related to the network (authenticating wireless clients, handling channel contention, repeating packets, etc.) Wireless interfaces in master mode can only communicate with interfaces that are associated with them in managed mode.
2. Managed mode is sometimes also referred to as client mode. Wireless interfaces in managed mode will join a network created by a master, and will automatically change their channel to match it. They then present any necessary credentials to the master, and if those credentials are accepted, they are said to be associated with the master. Managed mode interfaces do not communicate with each

other directly, and will only communicate with an associated master.

3. Ad-hoc mode creates a multipoint-to-multipoint network where there is no single master node or AP. In ad-hoc mode, each wireless interface communicates directly with its neighbours.
   Nodes must be in range of each other to communicate, and must agree on a network name and channel. Ad-hoc mode is often also called Mesh Networking and you can find details of this type of networking in the chapter called **Mesh Networking.**
4. Monitor mode is used by some tools (such as Kismet) to passively listen to all radio traffic on a given channel. When in monitor mode, wireless interfaces transmit no data. This is useful for analysing problems on a wireless link or observing spectrum usage in the local area. Monitor mode is not used for normal communications.

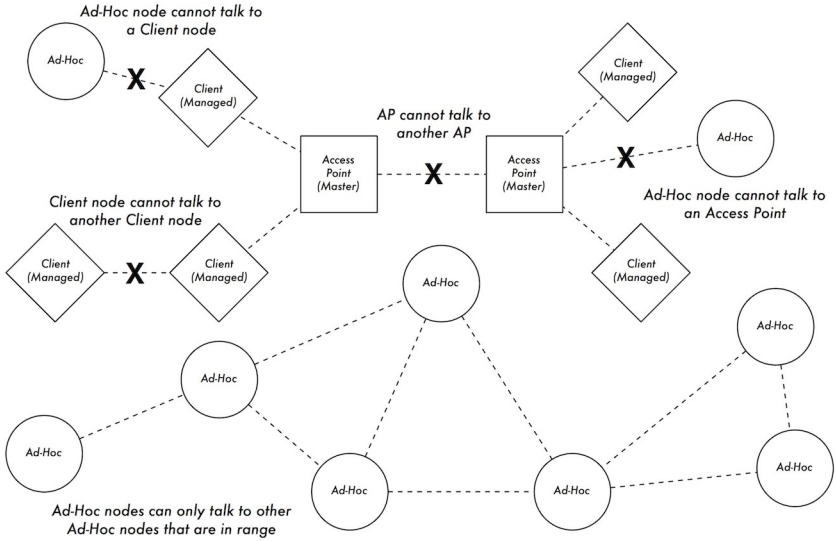

Figure WF 1: APs, Clients, and Ad-Hoc nodes.

When implementing a point-to-point or point-to-multipoint link, one radio will typically operate in master mode, while the other(s) operate in managed mode. In a multipoint-to-multipoint mesh, the radios all operate in ad-hoc mode so that they can communicate with each other directly.

It is important to keep these modes in mind when designing your network layout.

Remember that managed mode clients cannot communicate with each other directly, so it is likely that you will want to run a high repeater site in master or ad-hoc mode.
Ad-hoc is more flexible but has a number of performance issues as compared to using the master / managed modes.

4. The 802.22 Standard

Did you ever wonder why one of the biggest users of wireless spectrum in almost any country on earth, never got into the 2 way communications business? No? Well, you ask, why did the Television Broadcast Industry never want to do two-way communications.
The simple answer is that this was not the business they were in.
What they did instead was get access to and use of the best "beach front" spectrum between DC and day light.. and almost for free to boot.
As analogue TV gets replaced by digital TV, some of that beach front spectrum is being made available for wireless networking. And in parts of the world where TV has been deployed less extensively, these same parts of the radio spectrum are available for wireless networking as well.
The new wireless technology is commonly called TVWS (TV White Spaces) and although relatively new at the time of writing, this technology is in many trials for rural broadband wireless.

From *wikipedia* -
IEEE 802.22, known informally as Super Wi-Fi, is a standard for Wireless Regional Area Networks (WRAN) using white spaces in the TV frequency spectrum.
The development of the IEEE 802.22 WRAN standard is aimed at using cognitive radio (CR) techniques to allow sharing of geographically unused spectrum allocated to the Television Broadcast Service, on a non-interfering basis, to bring broadband access to hard-to-reach, low population density areas, typical of rural environments, and is therefore timely and has the potential for a wide applicability worldwide.
IEEE 802.22 WRANs are designed to operate in the TV broadcast bands while assuring that no harmful interference is caused to the incumbent operation, i.e., digital TV and analog TV broadcasting, and low power licensed devices such as wireless microphones.
The standard was finally published in July 2011.

Technology of 802.22 or TVWS

The initial drafts of the 802.22 standard specify that the network should operate in a point to multipoint topology (p2m). The system will be formed by Base Stations (BS) and Customer Premise Equipment (CPE). The CPEs will be attached to a BS via a wireless link.

One key feature of the 802.22 WRAN Base Stations is that they will be capable of performing sensing of available spectrum.
The Institute of Electrical and Electronic Engineers (IEEE), together with the FCC, in the US, pursued a centralised approach for available spectrum discovery.
Specifically each Base Station (BS) would be armed with a GPS receiver which would allow its position to be reported.
This information would be sent back to centralised servers which would respond with the information about available free TV channels and guard bands in the area of the Base Station.

Other proposals would allow local spectrum sensing only, where the BS would decide by itself which channels are available for communication. This is called *distributed sensing*.

The CPEs will be sensing the spectrum and sending periodic reports to the BS informing it about what they sense. The BS, with the information gathered, will evaluate whether a change is necessary in the channel used, or on the contrary, if it should stay transmitting and receiving in the same one. A combination of these two approaches is also envisioned.

These sensing mechanisms are primarily used to identify if there is an incumbent transmitting, and if there is a need to avoid interfering with it. This means that the physical layer must be able to adapt to different conditions and be flexible in jumping from channel to channel without errors in transmission or losing clients (CPEs).

This flexibility is also required for dynamically adjusting the bandwidth, modulation and coding schemes. OFDMA *(Orthogonal Frequency-Division Multiple Access)* is the modulation scheme for transmission in up and downlinks. With OFDMA it will be possible to achieve this fast adaptation needed for the BSs and CPEs.

By using just one TV channel (a TV channel has a bandwidth of 6 MHz, in some countries they can be 7 or 8 MHz) the approximate maximum bit rate is 19 Mbit/s at a 30 km distance.
The speed and distance achieved is not enough to fulfill the requirements of the standard.
There is a feature called *Channel Bonding* which deals with this problem. Channel Bonding uses more than one channel for transmit/receive. This allows the system to have higher bandwidth which will be reflected in a better system performance.

5. Summary

As we can see the standards for wireline and wireless are mostly incorporated into the IEEE 802 Working Group.
At the moment the 802.11 family of WiFi standards and equipment are by far and away the most widely manufactured and deployed in indoor and outdoor wireless links.
The chapter called **Hardware Selection and Configuration** looks at equipment in much more detail.

The new 802.22 Standard is expected to play an increasing role in many rural (and urban) wireless networks. The free-ing up of unlicensed spectrum currently used by broadcast TV will enable this to happen. As yet the standards and the various groups involved in this standard are in their infancy, as are the bodies around the world involved in spectrum re-allocation.

Available equipment is still very new and deployments are few and far between. In the next 2-3 years it is anticipated that this will change significantly and the next revision of this book may well have case studies and deployment information to share with respect to 802.22 based networks. Meanwhile there is an interesting project underway in Scotland, United Kingdom which is deploying TVWS 802.22 networks.

You can read more about the project here:
http://www.wirelesswhitespace.org/projects.aspx