

**BSc in Computer Engineering
CMP4204
Wireless Technologies**

**Lecture 6
Wireless LANs**

Eng Diarmuid O'Briain, CEng, CISSP



Department of Electrical and Computer Engineering,
College of Engineering, Design, Art and Technology,
Makerere University

Copyright © 2018 Diarmuid Ó Briain

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Table of Contents

1. WIRELESS LANS.....	5
1.1 ORGANISATIONS IMPACTING WI-FI IMPLEMENTATION.....	6
2. SETUP AN AD-HOC NETWORK.....	7
2.1 CONFIGURING AN AD-HOC NETWORK.....	7
2.2 MICROSOFT WINDOWS WORKSTATION.....	8
2.3 UNIX / LINUX WORKSTATION.....	11
3. LAB EXERCISE – BUILDING A AD-HOC WIRELESS LAN.....	12
3.1 OBJECTIVE.....	12
3.2 BACKGROUND.....	12
3.3 LAB STEPS.....	12
4. WIFI ORGANISATIONS.....	13
4.1 WI-FI ALLIANCE.....	13
4.2 INTERNATIONAL TELECOMMUNICATION UNION (ITU).....	14
4.3 FEDERAL COMMUNICATIONS COMMISSION (FCC).....	14
5. WIRELESS LAN (WIFI) TECHNOLOGY.....	15
5.1 SPREAD SPECTRUM.....	15
5.2 POWER.....	16
5.3 RAKE RECEIVERS.....	16
5.4 IMPLEMENTING SPREAD SPECTRUM.....	16
5.5 FREQUENCY HOPPING SPREAD SPECTRUM (FHSS).....	17
5.6 DIRECT SEQUENCE SPREAD SPECTRUM (DSSS).....	17
5.7 ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING (OFDM).....	19
5.8 802.11B/G/N.....	21
5.9 802.11A/N – 5 GHz.....	22
5.10 IEEE 802.11 FAMILY SUMMARY.....	23
6. IEEE 802.11 WIRELESS LAN (WI-FI).....	24
6.1 802.11 MAC (MEDIA ACCESS CONTROL).....	24
6.2 ACKING.....	25
6.3 MAC LEVEL RETRANSMISSION.....	25
6.4 FRAGMENTATION.....	25
6.5 WI-FI ELEMENTS.....	25
7. WI-FI SECURITY.....	27
7.1 TYPES OF WI-FI SECURITY BREACHES.....	27
7.2 METHODS OF COUNTERACTING SECURITY RISKS.....	29
7.3 WIRELESS ENCRYPTION PROTOCOL (WEP).....	30
7.4 WI-FI PROTECTED ACCESS (WPA).....	31
7.5 802.11i WPA2.....	33
8. NON WI-FI SOLUTIONS IN UNLICENSED SPECTRUM.....	34
8.1 MIKROTIK - NSTREME / NV2.....	34
8.2 NSTREME.....	34
8.3 NSTREME 2.....	34
8.4 NV2 (NSTREME VERSION 2).....	34
9. MODULATION AND CODING SCHEMES.....	35
9.1 MODULATION ON POOR QUALITY LINKS.....	36
10. WIRELESS SETUP.....	37
10.1 RB10 CONFIGURATION.....	37
10.2 RB20 CONFIGURATION.....	38
10.3 TESTING.....	40
11. LAB EXERCISE – BUILD WIRELES NETWORK.....	45
12. SELF-TEST QUIZ.....	46

Illustration Index

Illustration 1: MikroTik Wireless Devices.....	5
Illustration 2: Ad-hoc network.....	7
Illustration 3: Microsoft Windows Ad-hoc network.....	8
Illustration 4: Microsoft Windows Ad-hoc network #2.....	9
Illustration 5: Microsoft Windows - set IP address.....	9
Illustration 6: Microsoft Windows IP Address.....	10
Illustration 7: Ad-hoc network lab.....	12
Illustration 8: Wireless governing bodies.....	13
Illustration 9: Spread spectrum.....	15
Illustration 10: Spread Spectrum Spreader/Correlator.....	16
Illustration 11: Spread spectrum techniques.....	17
Illustration 12: Operation of Direct Sequence Spread Spectrum.....	18
Illustration 13: OFDM Technique.....	19
Illustration 14: 2.4 GHz Wi-Fi channels.....	21
Illustration 15: 5 GHz classes and frequencies.....	22
Illustration 16: IEEE 802.1 Family Summary.....	23
Illustration 17: WLAN in the OSI Physical & Data Link Layers.....	24
Illustration 18: Wireless Encryption Standard.....	30
Illustration 19: IEEE 802.1X.....	32
Illustration 20: 802.11i WPA2.....	33
Illustration 21: Modulation and coding scheme.....	35
Illustration 22: Modulation levels dropped in 16 QAM.....	36
Illustration 23: Addition of wireless site to lab from lecture 4.....	37
Illustration 24: Winbox scanning tool.....	40
Illustration 25: Radio Spectrogram.....	42
Illustration 26: Wireless snoopers.....	43
Illustration 27: Wireless lab.....	45

1. Wireless LANs

IEEE 802.11 is a set of standards for Wireless Local Area Network (WLAN) computer communication, developed by the IEEE LAN/MAN Standards Committee (IEEE 802) in the 5 GHz and 2.4 GHz public spectrum bands.

The 802.11 family includes over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, and are amendments to the original standard. 802.11a was the first wireless networking standard, but 802.11b was the first widely accepted one, followed by g and n. Security was originally purposefully weak due to export requirements of some governments, and was later enhanced via the 802.11i amendment after US governmental and legislative changes. 802.11n is a new multi-streaming modulation technique that is still under draft development, but products based on its proprietary pre-draft versions are being sold. Other standards in the family (c-f, h, j) are service amendments and extensions or corrections to previous specifications.



Illustration 1: MikroTik Wireless Devices

The segment of the radio frequency spectrum used varies between countries. In the US, 802.11a and g devices may be operated without a license, as explained in Part 15 of the Federal Communications Commission (FCC) Rules and Regulations. Frequencies used by channels one through six (802.11b) fall within the 2.4 GHz amateur radio band. Licensed amateur radio operators may operate 802.11b/g devices under Part 97 of the FCC Rules and Regulations, allowing increased power output but not commercial content or encryption.

1.1 Organisations impacting Wi-Fi implementation

1.1.1 Institute of Electrical and Electronics Engineers

The IEEE has long been at the forefront of LAN standards and Wi-Fi standards come under the umbrella of the IEEE 802.11 standards. *802.11* refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

There are several specifications in the 802.11 family:

- 1 **802.11** - applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS).
- 2 **802.11a** - an extension to 802.11 that applies to wireless LANs and provides typically 25 Mbps to a maximum of 54 Mbps in the 5GHz band. 802.11a uses an Orthogonal Frequency Division Multiplexing (OFDM) encoding scheme rather than FHSS or DSSS. Max range is 30 M.
- 3 **802.11b** - (also referred to as *802.11 High Rate* or *Wi-Fi*) -- an extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet. Max range is 30 M.
- 4 **802.11g** - applies to wireless LANs and provides typically 24 Mbps to a maximum of 54 Mbps in the 2.4 GHz band. It also uses OFDM. Max range is 30 M.
- 5 **802.11n** - 200 Mbps standard to a maximum of 540 Mbps out to 50 M in either the 2.4 or 5 GHz bands. It uses Multiple In, Multiple Out (MIMO) antennas.
- 6 **802.11ac** - The latest standard which gives multi-station WLAN throughput of at least 1 Gb/s and a single link throughput of at least 500 Mb/s. This is achieved by extending the air interface concepts embraced by 802.11n, using wider RF bandwidth of up to 160 MHz, up to 8 MIMO spatial streams, up to 4 downlink multi-user MIMO clients, and 256 QAM high-density modulation. Space-division multiple access (SDMA) is employed where streams not separated by frequency, but instead resolved spatially, analogous to 11n-style MIMO.

2. Setup an Ad-hoc network

An ad hoc network is a temporary connection between computers and devices used for a specific purpose, such as sharing documents during a meeting or playing multiple-player computer games. You can also use an ad hoc network to temporarily share an Internet connection. Ad hoc networks can only be wireless, so you must have a wireless network adapter installed in your computer to set up or join an ad hoc network.

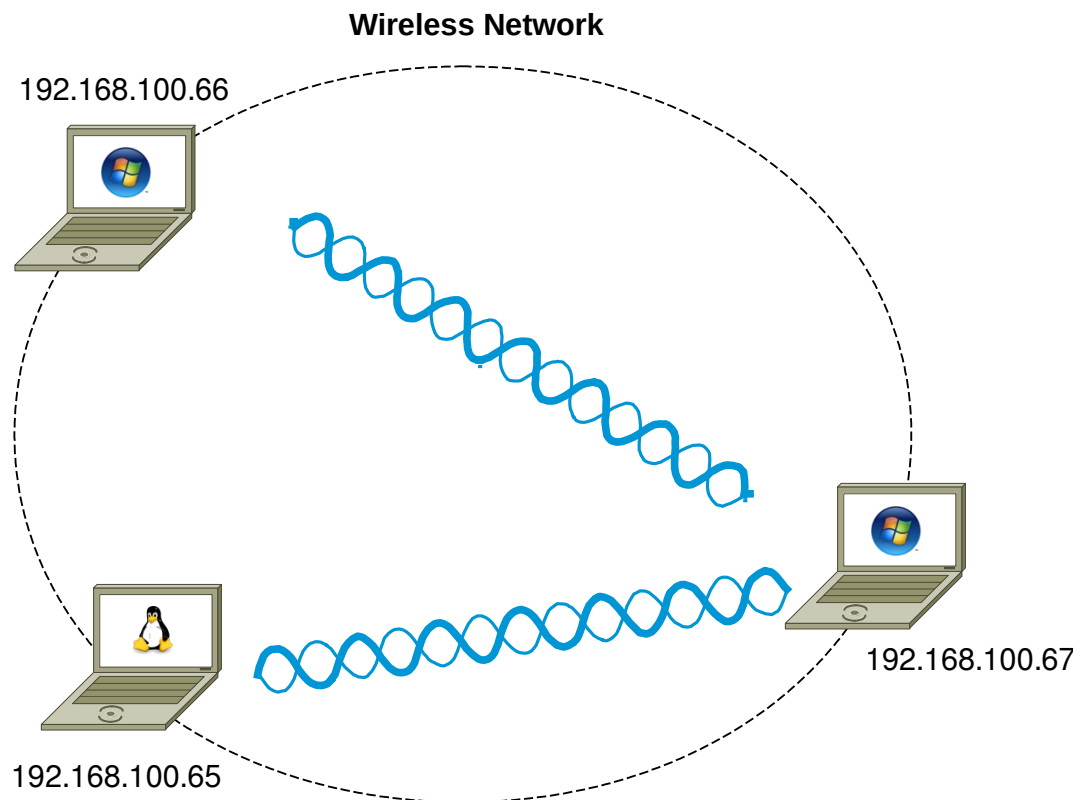


Illustration 2: Ad-hoc network

2.1 Configuring an ad-hoc network

To do this you will need the following information.

- SSID to share on ad-hoc network
- Key IP Address of workstation.
- Subnetmask for the network the workstation is participating.
- IP Address of the router interface on the network (Default Gateway)
- Domain Name Server IP Address. This is the server that will convert domain names to IP Address for the workstation on request.

2.2 Microsoft Windows Workstation

On Windows XP follow the following procedure.

- Start → Settings → Network Connections
- Right click on the Wireless LAN icon and select **Connect / Disconnect**.
- In the next screen highlight “Setup Wireless ad hoc network” and click **Next**.
- On the next informational screen click **Next**.

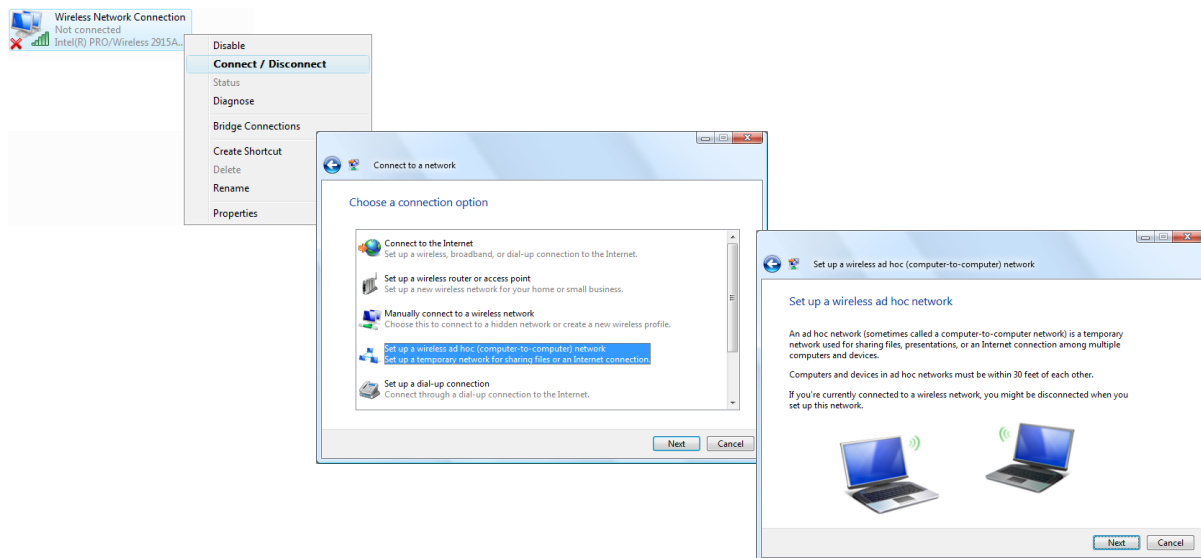


Illustration 3: Microsoft Windows Ad-hoc network

- In the next screen enter the following information and click Next.
 - Network name : **ad-hoc_net**
 - Security type : **WEP**
 - Security key/Passphrase : **ad-hocpassword**
- On the next informational screen click **Close**.

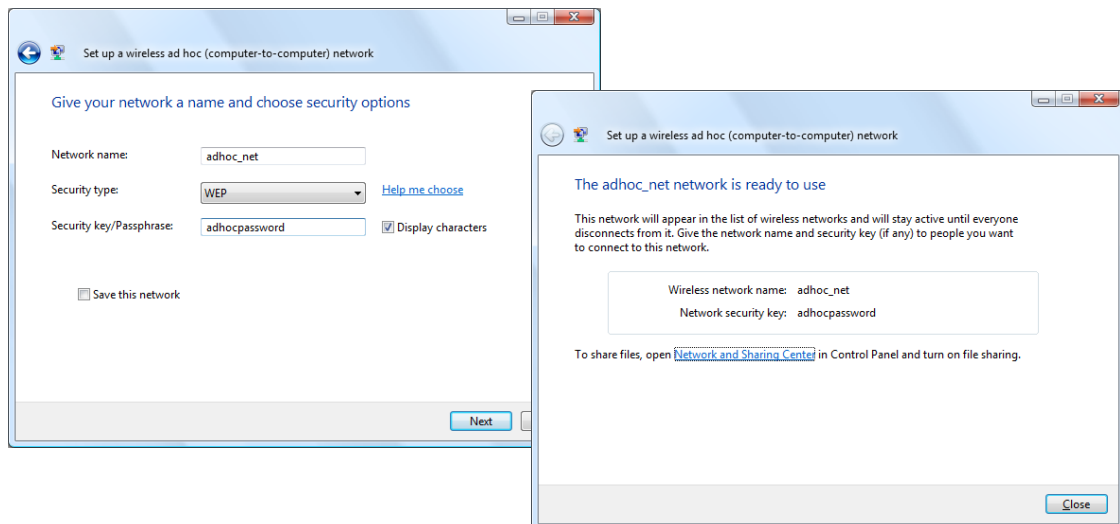


Illustration 4: Microsoft Windows Ad-hoc network #2

- Start → Settings → Network Connections
- Right click on the LAN icon and select **Properties**.
- In the next screen highlight Internet Protocol Version 4 (TCP/IPv4) and click **Properties**.

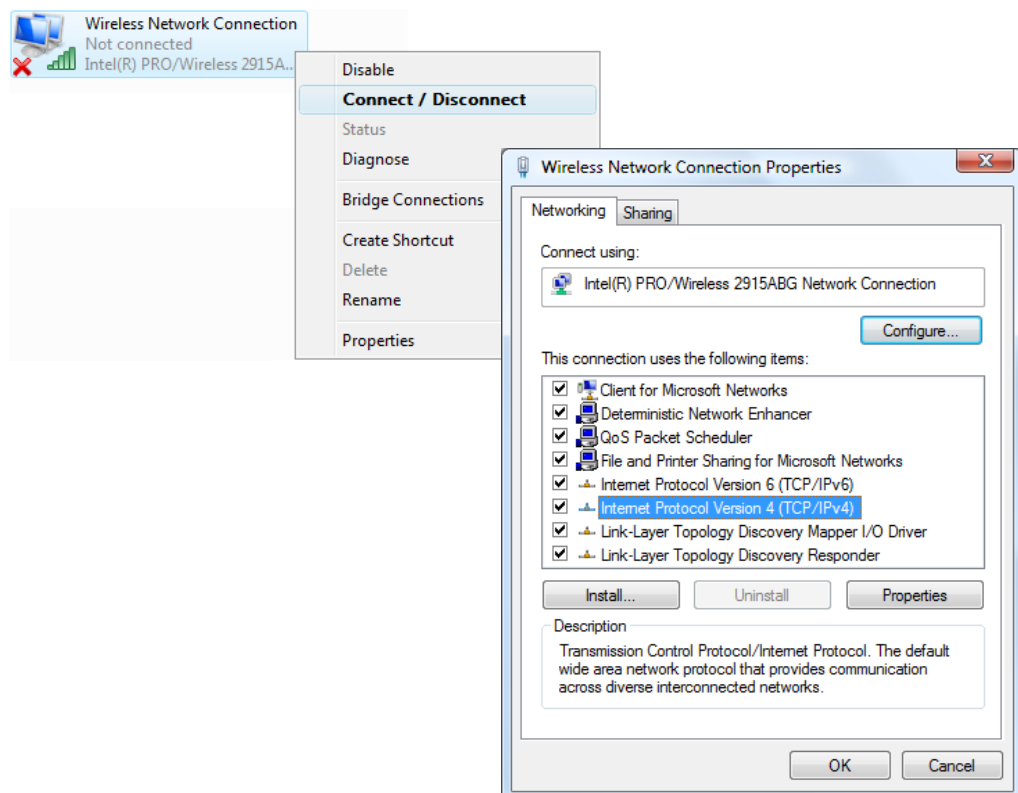


Illustration 5: Microsoft Windows - set IP address

- In the next screen highlight Internet Protocol Version 4 (TCP/IPv4) and click **Properties**.

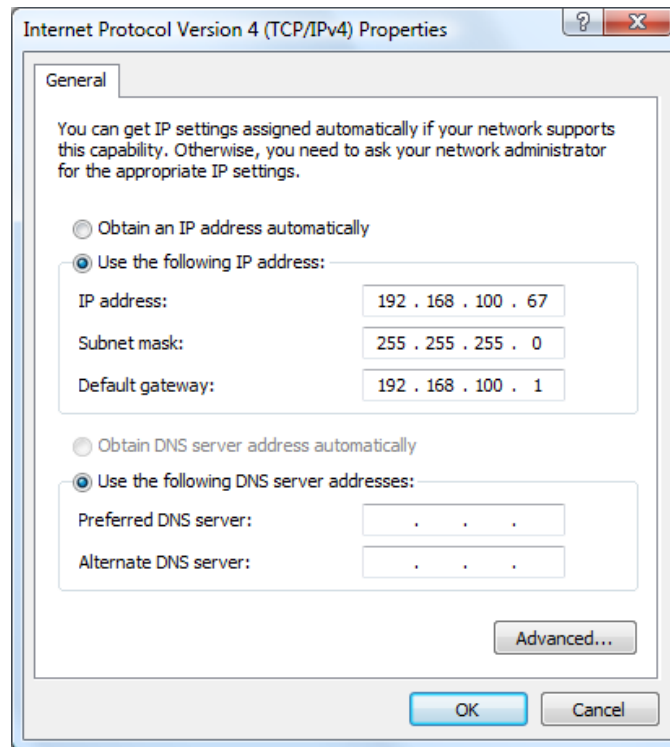


Illustration 6: Microsoft Windows IP Address

- Filling the IP Address, Subnetmask, Default Gateway such that it will match that on the other side of the ad-hoc connection and click **OK**.

Notes:

An ad hoc network is automatically deleted after all users disconnect from the network or when the person who set up the network disconnects and goes out of range of the other users of the network, unless you choose to make it a permanent network when you create it.

If you do not configure IP Address on Windows, a 169. Address will be automatically assigned by the Operating System.

2.3 UNIX / Linux Workstation

On UNIX and Linux you can use the graphical tools on the system you use or you can use the commands in the shell. You must be logged in as the “root” user to have permissions to make these changes.

2.3.1 Gnome Desktop

The UNIX or Linux Gnome Desktop does not have a method of configuring an ad-hoc network, however it is configurable using the *iwconfig* command.

2.3.1.1 UNIX/Linux Shell

Here are the steps to go through to setup on Linux.

1. Switch the card into ad-hoc mode.
2. Set the channel/frequency that you want to use.
3. Add the name (ssid) for the network you want to create/join. Use single quotes if there is a space in the name.
4. Add a WEP encryption key.
5. Give the interface an IP Address.

```
GNU/Linux# su
```

```
Password: <password>
```

```
GNU/Linux# iw phy phy0 interface add eth1 mode ibss
```

```
GNU/Linux# iw dev eth1 connect -w AP_ITC keys 0: abcdef0123
```

```
GNU/Linux# ip addr add 192.168.1.60/24 dev eth1
```

3. Lab Exercise – Building a ad-hoc Wireless LAN

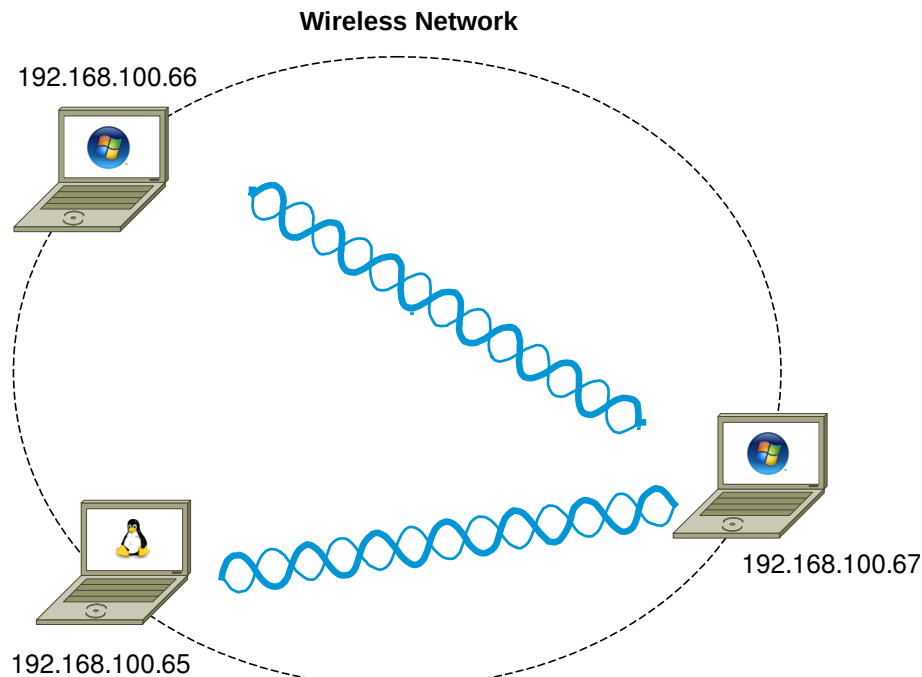


Illustration 7: Ad-hoc network lab

3.1 Objective

- Practice building LANs.
- Practice configuring Workstations for inclusion in a LAN.

3.2 Background

Knowing how to build ad-hoc Wireless LAN is an essential building block to you networking knowledge.

3.3 Lab Steps

3.3.1 Workstation Configuration

Use the notes to configure the workstations.

3.3.2 Test Configuration

Ping from one ad-hoc host to another ad-hoc host.

4. WiFi Organisations

In 1999, several industry leaders came together to form a global, non-profit organisation with the goal of driving the adoption of a single worldwide-accepted standard for high-speed wireless local area networking. We are that organisation. We are known as the Wi-Fi Alliance.

Today, with more than 300 members from more than 20 countries and growing, common goals still bind us together.



Illustration 8: Wireless governing bodies

4.1 Wi-Fi Alliance

As Wi-Fi networks continue to expand through businesses, homes, and now public hotspots that provide wireless access locations for people on the go, compatibility is critical. The Wi-Fi Alliance develops rigorous tests and conducts Wi-Fi certification of wireless devices that implement the universal IEEE 802.11 specifications. The end result leads to the confidence that both home and enterprise users need to continue to get the most out of Wi-Fi.

To date we have certified the interoperability of more than 3,500 products. There is more, however, to Wi-Fi Alliance than interoperability. We work to provide Wi-Fi users with the information they need to make decisions about today's Wi-Fi systems. Whether you are a tech-savvy IT director, a security-minded CIO, or a home user intrigued by Wi-Fi possibilities, our aim is to provide the information you need to proceed with confidence and peace of mind.

As the market continues to evolve, so will our efforts. We will continue to test and certify the compatibility of Wi-Fi devices, we will take the lead in initiatives designed to enhance and simplify the user experience, we will provide thought leadership and up-to-date information, and we will continue to promote the standards that reduce costs - all in hopes of helping what was once a futuristic vision of Wi-Fi become a full-fledged reality.

Although the terms 802.11 and Wi-Fi are often used interchangeably, the Wi-Fi Alliance uses the term "Wi-Fi" to define a slightly different set of overlapping standards. In some cases, market demand has led the Wi-Fi Alliance to begin certifying products before amendments to the 802.11 standard are complete.

4.2 International Telecommunication Union (ITU)

ITU is the leading United Nations agency for information and communication technologies. As the global focal point for governments and the private sector, ITU's role in helping the world communicate spans 3 core sectors: radio-communication, standardisation and development.

4.3 Federal Communications Commission (FCC)

The FCC is an independent United States government agency, directly responsible to the US Congress. The FCC was established by the Communications Act of 1934 and is charged with regulating interstate and international communications by radio, television, wire, satellite and cable. The FCC's jurisdiction covers the 50 states, the District of Columbia, and US possessions.

5. Wireless LAN (WiFi) Technology

In 1985, The Federal Communications Commission (FCC) in the USA authorised the use of non-licensed spread spectrum systems in the 902-928 MHz, 2400-2483.5 MHz, and 5725-5850 MHz bands under Part 15 of the rules at a power level of 1W, which was significantly higher than previously permitted unlicensed use in other bands (FCC, 1985).

An unlicensed device or Intentional radiators are devices that intentionally generate and emit Radio Frequency (RF) energy by radiation or induction. Such devices cannot cause interference to licensed operations nor are they protected from any interference received (Marcus et al., 2002).

5.1 Spread Spectrum

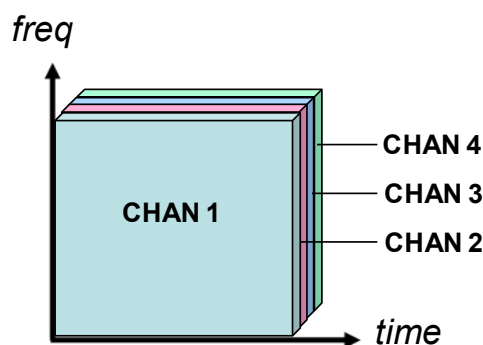


Illustration 9: Spread spectrum

With Time Division Multiple Access (TDMA) individual signals use unique portions of time to separate within the same frequency band. In Frequency Division Multiple Access (FDMA) the frequency is subdivided into narrow channels separated by guard bands to cater for multiple signals. Spread spectrum signals are unique in that they share the same frequency and space in time.

In Illustration 9 we can see this and can wonder at how it is achieved. Spread spectrum modulation was originally developed for military applications where channels would mimic the Gaussian noise that is heard by a radio operator as 'static' and would therefore appear not to exist.

The spread signal mimic the background Gaussian noise when transmitted and a receiver without the same hopset (hopping cycle) or Pseudo Noise (PN) code will be unable to extract the signal from the band.

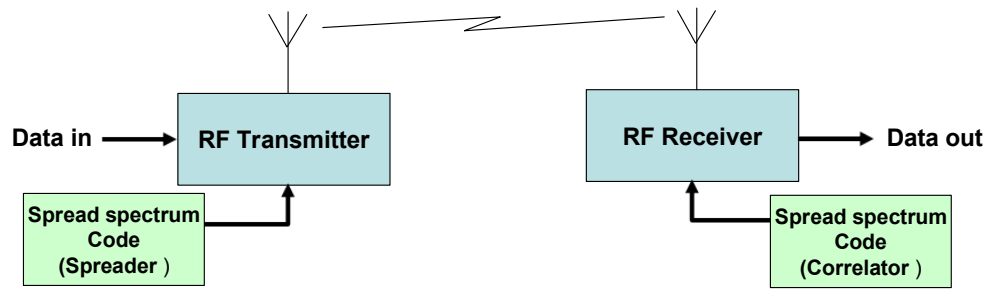


Illustration 10: Spread Spectrum Spreader/Correlator

In Illustration 10 it can be seen that the data for transmission is initially spread by a *Spreader* before being sent to the transmitter. The receiver with the same PN code extracts the signal from the noise and using a circuit called a *Correlator* extracts the original data signal.

5.2 Power

The Spread Spectrum transmitter uses similar transmit power levels to narrow band transmitters, and they are said to be power neutral.

$$\text{Total Power} = \text{Spectral density (W/Hz)} \times \text{Bandwidth}$$

and as the spectral density of spread spectrum signal will be much lower considering the wider frequency band for the same total power. The power at any point in the signal is much lower for a comparable narrow band transmission. This can be seen clearly in Illustration 11(b) where the spread signal appears at the same power level as the background Gaussian noise.

5.3 RAKE Receivers

At the receiver the multipath spread signal is extracted using RAKE receivers. A RAKE receiver consists of multiple correlators (fingers on a rake) where each of the fingers can detect/extract the signal from one of the multipath components created by the spread signal. The outputs of the fingers are then combined to recover the signal.

5.4 Implementing Spread Spectrum

The two primary methods used to spread the baseband data spectrum are:

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)

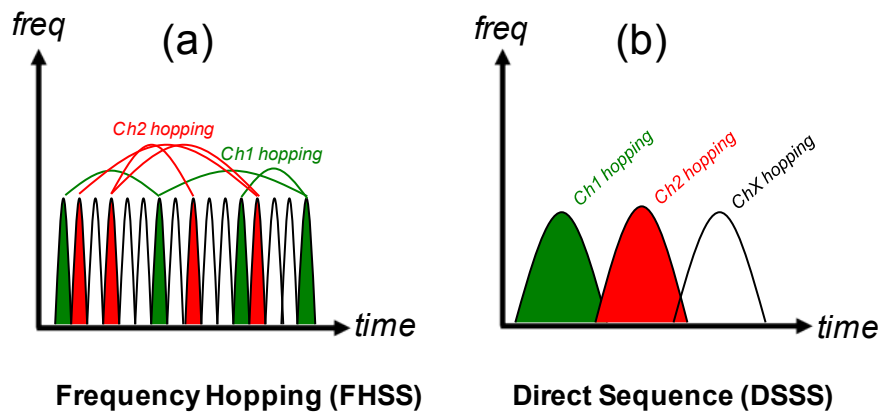


Illustration 11: Spread spectrum techniques

Both direct sequencing and frequency hopping techniques are used to spread data out across a range of spectrum. DSSS essentially spreads out the carrier signal, allowing for a much lower power transmission. FHSS can use the same frequency range but uses a narrow signal over a constantly rotating set of frequencies.

5.5 Frequency Hopping Spread Spectrum (FHSS)

FHSS systems transmit the signal by varying (hopping) the frequency of the carrier in a pseudo-random manner unique to each user. As can be seen in Illustration 11(a) Each channel is rapidly changing the instantaneous carrier frequency following a pseudo random pattern. This makes the signal appear like background noise and resistant to interference from narrowband channels. A narrowband radio signal at a certain frequency would only encounter interference 1/75 of the time in the presence of an FHSS signal. Multiple FHSS systems can easily co-exist as well timed pseudo-random frequency generator protocols can ensure they will never interfere with each other.

5.6 Direct Sequence Spread Spectrum (DSSS)

DSSS transmissions spread the data by multiplication with a channelisation code prior to up-conversion to an intermediate frequency. This signal is spread as shown in Illustration 12(b) The chipping code includes a redundant bit pattern for each transmitted bit, increasing the signal's resistance to interference. That means that even if some bits are lost in the transmission to interference, the original data stream can be rebuilt from other redundant pieces (Reynolds, 2004).

Spread Spectrum techniques proved to be highly immune to interference and a low probability of interception making them ideal for unlicensed spectrum where multiple signals share the same band.

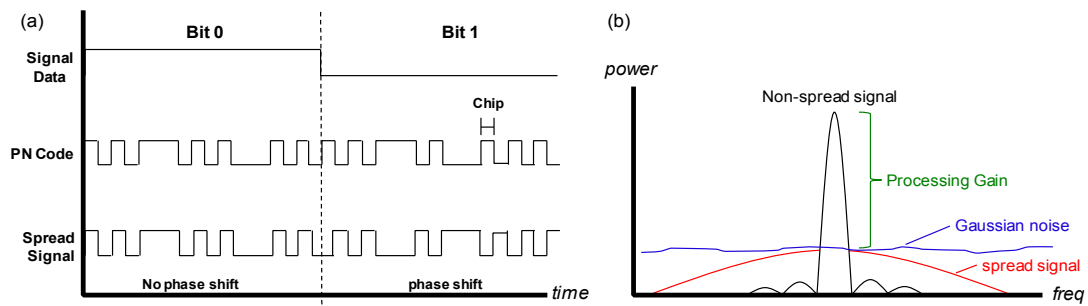


Illustration 12: Operation of Direct Sequence Spread Spectrum

Referring to Illustration 12(a) the spread signal to be transmitted uses phase shift techniques to modulate the signal data to the PN coded signal. In this simple Binary Phase Shift Keying (BPSK) example there are only 2 possible states, a single symbol, however in practice more complex systems can be employed like Quadrature Phase Shift Keying (QPSK) and Quadrature Amplitude Modulation (QAM) where a greater number of states exist thereby increasing the symbol rate and therefore the throughput.

The PN code is constructed from a number of Chips. The chipping rate far exceeds the symbol rate of the signal to be modulated and the ratio of chipping rate to symbol rate is called *Processing Gain* and is demonstrated in Illustration 12(b). The classical definition of processing gain is:

$$10 \log(R_c / R_s) \text{ in decibels (dB)}$$

Where: R_c is chipping frequency and R_s is the symbol rate.

By this definition a system, that has a symbol rate of 15Ksymbol/s and a chipping rate of 4Mchips/s will have a processing gain of 24.25 dB.

5.7 Orthogonal Frequency Division Multiplexing (OFDM)

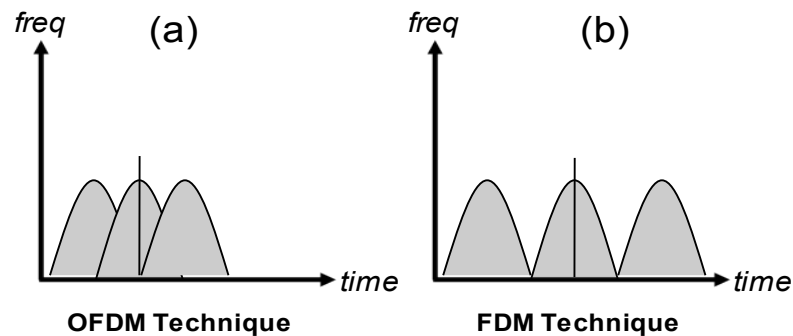


Illustration 13: OFDM Technique

OFDM is a particular form of Frequency Division Multiplex (FDM) where a datastream is transmitted over a number of low rate subcarriers. Unlike FDM instead of having the channels non overlapping as shown in Illustration 13 (b) OFDM makes more efficient use of spectrum by over-lapping the channels. This can only be achieved by reducing crosstalk between the carriers using a precise mathematical relationship between the frequencies, an orthogonal relationship. The sub-carrier frequencies are chosen so that the sub-carriers are orthogonal to each other, meaning that cross-talk between the sub-channels is eliminated and inter-carrier guard bands are not required.

To use OFDM the data to be transmitted is broken down into several streams that are broadcast simultaneously, on different frequencies, to a receiver that collects and reassembles them which makes it less susceptible to multipath and other radio interference.

This greatly simplifies the design of both the transmitter and the receiver; unlike conventional Frequency Division Multiplex (FDM), a separate filter for each sub-channel is not required. Each sub-carrier is modulated with a conventional modulation scheme such as QAM at a low symbol rate, maintaining data rates similar to conventional single-carrier modulation schemes in the same bandwidth.

The primary advantage of OFDM over single-carrier schemes is its ability to cope with severe channel conditions — for example, attenuation of high frequencies at a long copper wire, narrowband interference and frequency-selective fading due to multipath without complex equalisation filters. Channel equalisation is simplified because OFDM may be viewed as using many slowly-modulated narrowband signals rather than one rapidly-modulated wideband signal. Low symbol rate makes the use of a guard interval between symbols affordable, making it possible to handle time-spreading and eliminate Inter Symbol Interference (ISI).

OFDM has developed into a popular scheme for wideband digital communication systems.

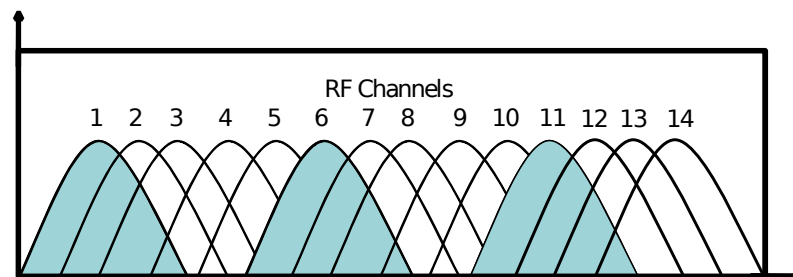
5.7.1 Summary of advantages

- Can easily adapt to severe channel conditions without complex equalisation
- Robust against narrow-band co-channel interference
- Robust against ISI and fading caused by multipath propagation
- High spectral efficiency
- Efficient implementation using Fast Fourier Transform (FFT)
- Low sensitivity to time synchronisation errors
- Tuned sub-channel receiver filters are not required (unlike conventional FDM)
- Facilitates Single Frequency Networks, i.e. transmitter macro-diversity.

5.8 802.11b/g/n

The 802.11b standard defines a total of 14 frequency channels in the 2.4 GHz Wi-Fi signal range. In the Europe the first 13 channels are available for use, while in the United States, only the Wi-Fi channels 1 - 11 can be chosen. In Japan, all 14 channels are licensed for 802.11b.

These channels were incorporated into the 802.11g and 802.11n.



802.11b WiFi Channels

Channel	Lower Frequency (GHz)	Centre Frequency (GHz)	Upper Frequency (GHz)
1	2.401	2.412	2.423
2	2.404	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473
12	2.456	2.467	2.478
13	2.461	2.472	2.483
14	2.473	2.484	2.495

Illustration 14: 2.4 GHz Wi-Fi channels

Many wireless products ship with a default Wi-Fi channel of 6. If encountering interference from other devices within the home, consider changing the channel up or down to avoid it. Note that all Wi-Fi devices on the network must use the same channel.

Some Wi-Fi channel numbers overlap with each other. Channel 1 uses the lowest frequency band and each subsequent channel increases the frequency slightly. Therefore, the further apart two channel numbers are, the less the degree of overlap and likelihood of interference. If encountering interference with a neighbour's WLAN, change to a distant channel. Both channels 1 and 11 do not overlap with the default channel 6; use one of these three channels for best results.

5.9 802.11a/n – 5 GHz

802.11a defines the physical air interface for up to 200 channels in the 5 GHz unlicensed spectrum with a channel size of 20 MHz. Channel centre frequency for each channel can be calculated by the formula $5000 + 5 \times N_{ch}$ (MHz) where $N_{ch} = 0 - 200$.

It is based on an OFDM implementation using 52 subcarriers that are modulated using BPSK, QPSK, 16-QAM, or 64-QAM. 802.11a has data throughput capabilities of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s.

These channels were incorporated into the higher speed 802.11n standard and are the channels used in the newer 802.11ac standard.

Regulatory Class	Channel starting frequency	Channel Spacing (MHz)	Channel set	Frequencies (GHz)
1	5	20	36	5.180
			40	5.200
			44	5.220
			48	5.240
2	5	20	52	5.260
			56	5.280
			60	5.300
			64	5.320
3	5	20	100	5.500
			104	5.520
			108	5.540
			112	5.560
			116	5.580
			120	5.600
			124	5.620
			128	5.640
			132	5.660
			136	5.680
			140	5.700

Illustration 15: 5 GHz classes and frequencies

In some countries wideband data transmission systems for the provision of Fixed Wireless Access Networks/Metropolitan Area Networks (FWA/MAN) is also permitted in the 5.8GHz (5725 – 5875MHz) band up to a maximum radiated power of 2W Effective Isotropic Radiated Power (EIRP) on a licence exempt basis. This gives an additional 7 20 MHz channels. 5.745, 5.765, 5.785, 5.805, 5.825, 5.845, 5.865 GHz.

5.10 IEEE 802.11 Family Summary

IEEE Designation	Modulation	Max Speed	Operating Frequency	Non-overlapping channels	Antenna	Range	
						Indoor	Outdoor
802.11b	DSSS	11 Mbps	2.4 GHz	3		~38 M	~140 M
802.11a	OFDM	54 Mbps	5 GHz	12		~35 M	~120 M
802.11g	OFDM	54 Mbps	2.4 GHz	3		~35 M	~140 M
802.11n	OFDM	248 Mbps	2.4 (5) GHz	3 (12 **)	MIMO	~70 M	~250 M
802.11ac	OFDM	1 Gbps	5 GHz	12 **	MIMO	~35 M	

Illustration 16: IEEE 802.11 Family Summary

** at 20 Mhz channel sizes, technology allows for larger channel sizes which obviously reduces the number of available channels.

6. IEEE 802.11 Wireless LAN (Wi-Fi)

OSI
Layer

2	Data Link	802.2 - Logical Link Control (LLC) Sub-layer		
		Media Access Control (MAC) Sub-layer		
1	Physical	802.3 Wired Ethernet	802.5 Token Ring	802.11 WLAN (WiFi)

Illustration 17: WLAN in the OSI Physical & Data Link Layers

The Institute of Electrical and Electronics Engineers (IEEE) decided to build a standard to use the new unlicensed spectrum made available by the FCC in 1985. In 1990 they formed the 802.11 Working Group for WLAN (IEEE, 1997). This group worked on defining the physical layer (PHY) and the Media Access Control layer (MAC) air interface to link with the existing 802.2 Logical Link Control (LLC). The protocol is based on Carrier Sense Multiple Access (CSMA) with Collision Avoidance (CA). CSMA is also used in 802.3 Ethernet where a station wishing to transmit listens to see if the medium is free before transmitting and if not it backs off for a period of time before trying again. The difference between 802.3 Ethernet and 802.11 WLAN is that with Ethernet it detects a collision if one occurs while in a wireless network it cannot be assumed that all stations hear each other so a CA system is employed. A station wishing to transmit senses the medium and if busy waits, if the medium is free for a specific time called Distributed Inter Frame Space (DIFS) the station transmits, the receiving station checks the Cyclic Redundancy Check (CRC) and transmits an Acknowledgement (ACK). Receipt of the ACK by the transmitter confirms that no collision occurred.

6.1 802.11 MAC (Media Access Control)

The 802.11 family uses a MAC layer known as CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) NOTE: Classic Ethernet uses CSMA/CD - collision detection. CSMA/CA is, like all Ethernet protocols, peer-to-peer (there is no requirement for a master station).

In CSMA/CA a Wireless node that wants to transmit performs the following sequence:

- Listen on the desired channel.
- If channel is idle (no active transmitters) it sends a packet.
- If channel is busy (an active transmitter) node waits until transmission stops then a further CONTENTION period. (The Contention period is a random period after every transmit on every node and statistically allows every node equal access to the media. To allow TX to RX turn around the contention time is slotted 50 micro sec for FH and 20 micro sec for Direct Sequence (DS) systems).
- If the channel is still idle at the end of the CONTENTION period the node transmits its packet otherwise it repeats the process defined in 3 above until it gets a free channel.

6.2 ACKing

At the end of every packet the receiver, if it has successfully received the packet, will return an ACK packet (if not received or received with errors the receiver will NOT respond i.e. there is no NACK). The transmit window allows for the ACK i.e. CONTENTION period starts after the ACK should have been sent.

6.3 MAC level retransmission

If no ACK is received the sender will retry the transmit (using the normal CSMA/CA procedures) until either successful or the operation is abandoned with exhausted retries.

6.4 Fragmentation

Bit error rates on wireless systems (10^{-5} , 10^{-6}) are substantially higher than wire-line systems (10^{-12}). Large blocks may approach the number of bits where the probability of an error occurring is so high that every block could fail including the re-transmission. To reduce the possibility of this happening large blocks may be fragmented by the transmitter and reassembled by the receiver node e.g. a 1500 byte block (12,000 bits) may be fragmented into 5 blocks of 300 bytes (2,400 bits). While there is some overhead in doing this - both the probability of an error occurring is reduced and, in the event of an error, the re-transmission time is also reduced.

6.5 Wi-Fi Elements

802.11 networks are organised in two ways:

1. In infrastructure mode one station acts as a master with all the other stations associating to it; the network is known as a Basic Service Set (BSS) and the master station is termed an AP. In a BSS all communication passes through the AP; even when one station wants to communicate with another wireless station messages must go through the AP.
2. In the second form of network there is no master and stations communicate directly. This form of network is termed an Independent Basic Service Set (IBSS) and is commonly known as an ad-hoc network.

6.5.1 Wireless Access Point (AP)

The Wireless Access Point is the hub of a wireless network. Wireless clients connect to the access point, and traffic between two clients must travel through the access point. Access Points are often abbreviated to AP, and you may also see them referred to as "wireless routers," "wireless gateways," and "base stations."

6.5.2 Service Set Identifier (SSID)

An SSID is a secret key attached to all packets on a wireless network to identify each packet as part of that network. The code consists of a string of 1-32 octets. All wireless devices attempting to communicate with each other must share the same SSID. Apart from identifying each packet, an SSID also serves to uniquely identify a group of wireless network devices used in a given "Service Set".

There are two major variants of the SSID:

- Ad-hoc wireless networks (IBSS) that consist of client machines without an access point use the IBSS ID (Independent Basic Service Set Identifier)
- Infrastructure networks which include an AP (BSS or possibly an ESS) use the BSS ID or ESS ID (E for Extended) instead.

The naming is for convention only as the IEEE 802.11 standard dictates that an IBSS, BSS, and ESS are each defined by an SSID, otherwise known as a "Network Name". A Network Name is commonly set to the name of the network operator, such as a company name. Equipment manufacturers have liberally used all of the above SSID naming conventions to essentially describe the same thing. In some instances, the convention is wrong, as in the case of BSSID.

The SSID on wireless clients can be set either manually, by entering the SSID into the client network settings, or automatically, by leaving the SSID unspecified or blank. A network administrator often uses a public SSID that is set on the access point and broadcast to all wireless devices in range.

Most 802.11 access point vendors allow the use of an SSID of "any" to enable an 802.11 NIC to connect to any 802.11 network.

6.5.3 Disabling SSID Broadcasting

Many Wireless Access Point (WAP) vendors have added a configuration option which lets you disable broadcasting of the SSID. This adds little security because it is only able to prevent the SSID from being broadcast with Probe Request and Beacon frames. The SSID must be broadcast with Probe Response frames. In addition, the wireless access cards will broadcast the SSID in their Association and Re-association frames. Because of this, the SSID cannot be considered a valid security tool.

7. Wi-Fi Security

The ability to enter a network while mobile has great benefits. However, wireless networking has many security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks.

7.1 Types of Wi-Fi Security Breaches

7.1.1 Accidental association

When a user turns on a computer and it latches on to a wireless access point from a neighbouring company's overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other.

7.1.2 Malicious association

"Malicious associations" are when wireless devices can be actively made by crackers to connect to a company network through their cracking laptop instead of a company AP. These types of laptops are known as "soft APs" and are created when a cracker runs some software that makes his/her wireless network card look like a legitimate access point.

7.1.3 Ad-hoc networks

Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-to-peer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.

7.1.4 Non-traditional networks

Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even barcode readers, handheld Personal Digital Assistants (PDA), and wireless printers and copiers should be secured. These non-traditional networks can be easily overlooked by IT personnel who have narrowly focused on laptops and access points.

7.1.5 Identity theft (MAC spoofing)

Identity theft (or MAC spoofing) occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to only allow authorised computers with specific MAC IDs to gain access and utilise the network. However, a number of programs exist that have network “sniffing” capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the cracker desires, and the cracker can easily get around that hurdle.

7.1.6 Man-in-the-middle attacks

A man-in-the-middle attacker entices computers to log into a computer which is set up as a soft AP. Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network.

7.1.7 Denial of service (DoS)

A DoS occurs when an attacker continually bombards a targeted AP or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash.

7.1.8 Network injection

In a network injection attack, a cracker can make use of access points that are exposed to non-filtered network traffic, specifically broadcast network traffic such as “Spanning Tree” (802.1D), OSPF, RIP, Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP). The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.

7.2 Methods of counteracting security risks

There are many technologies available to counteract wireless network intrusion, but currently no method is absolutely secure. The best strategy may be to combine a number of security measures.

There are three steps to take towards securing a wireless network:

- 1) All wireless LAN devices need to be secured.
- 2) All users of the wireless network need to be educated in wireless network security.
- 3) All wireless networks need to be actively monitored for weaknesses and breaches.

7.2.1 Steps in securing a wireless network

The following are some basic steps that are recommended to be taken to secure a wireless network; in order of importance:

- Turn on encryption. Wi-Fi Protected Access version 2 (WPA2) encryption should be used if possible. Wi-Fi Protected Access (WPA) encryption is the next best alternative, and Wired Equivalent Privacy (WEP) is better than nothing.
- Change the default password needed to access a wireless device — Default passwords are set by the manufacturer and are known by crackers. By changing the password you can prevent crackers from accessing and changing your network settings.
- Change the default SSID, or network name — Hackers know the default names of the different brands of equipment, and use of a default name suggests that the network has not been secured. Change it to something that will make it easier for users to find the correct network. You may wish to use a name that will not be associated with the owner in order to avoid being specifically targeted.
- Disable file and print sharing if it is not needed — this can limit a cracker's ability to steal data or commandeer resources in the event that they get past the encryption.
- Access points should be arranged to provide radio coverage only to the desired area if possible. Any wireless signal that spills outside of the desired area could provide an opportunity for a cracker to access the network without entering the premises. Directional antennas should be used, if possible, at the perimeter directing their broadcasting inward. Some access points allow the signal strength to be reduced in order to minimise such signal leakage.
- Divide the wired and wireless portions of the network into different segments, with a firewall in between. This can prevent a hacker from accessing a wired network by breaking into the wireless network.
- Implement an overlay Wireless intrusion prevention system to monitor the wireless spectrum 24x7 against active attacks and unauthorised devices such as Rogue APs. These systems can detect and stop the most subtle or brute force methods of wireless attacks, and provide you with deep visibility into the use and performance of the WLAN.

7.3 Wireless Encryption Protocol (WEP)

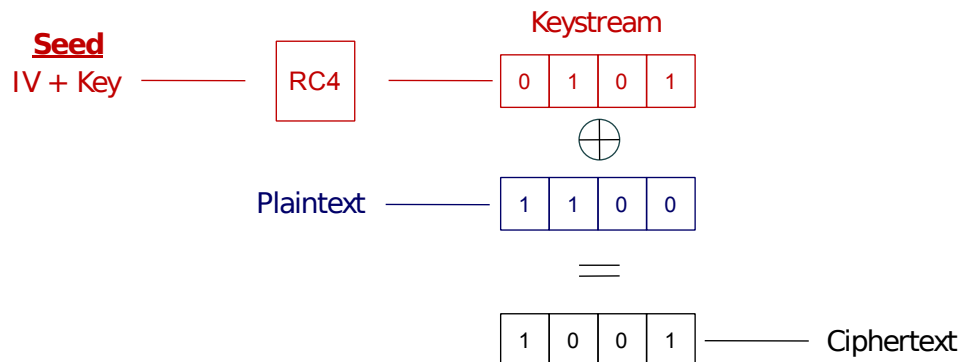


Illustration 18: Wireless Encryption Standard

WEP is part of the IEEE 802.11 wireless networking standard. Because wireless networks broadcast messages using radio, they are susceptible to eavesdropping.

WEP was intended to provide confidentiality comparable to that of a traditional wired network. Several serious weaknesses were identified by cryptanalysts; a WEP connection can be cracked with readily available software within minutes. WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, followed by the full IEEE 802.11i standard in 2004. Despite its weaknesses, WEP provides a level of security that may deter casual snooping.

Standard 64-bit WEP uses a 40 bit key, which is concatenated with a 24-bit Initialisation Vector (IV) to form the 64-bit Rivest Cipher 4 (RC4) traffic key. At the time that the original WEP standard was being drafted, US Government export restrictions on cryptographic technology limited the key size. Once the restrictions were lifted, all of the major manufacturers eventually implemented an extended 128-bit WEP protocol using a 104-bit key size.

A 128-bit WEP key is almost always entered by users as a string of 26 Hexadecimal (Hex) characters (0-9 and A-F). Each character represents 4 bits of the key. $4 \times 26 = 104$ bits; adding the 24-bit initialisation vector brings us what we call a "128-bit WEP key". A 256-bit WEP system is available from some vendors, and as with the above-mentioned system, 24 bits of that is for the I.V., leaving 232 actual bits for protection. This is typically entered as 58 Hexadecimal characters. $(58 \times 4 = 232 \text{ bits}) + 24 \text{ I.V. bits} = 256 \text{ bits of WEP protection}$.

Key size is not the only major security limitation in WEP. Cracking a longer key requires interception of more packets, but there are active attacks that stimulate the necessary traffic. There are other weaknesses in WEP, including the possibility of IV collisions and altered packets that are not helped at all by a longer key.

7.4 Wi-Fi Protected Access (WPA)

WPA is a class of systems to secure wireless (Wi-Fi) computer networks. It was created in response to several serious weaknesses researchers had found in the previous system, WEP. WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 (also called 802.11i) implements the full standard, but will not work with some older network cards. Both provide good security, with two significant issues:

- Either WPA or WPA2 must be enabled and chosen in preference to WEP. WEP is usually presented as the first security choice in most installation instructions.
- In the "Personal" mode, the most likely choice for homes and small offices, a passphrase is required that, for full security, must be longer than the typical 6 to 8 character passwords users are taught to employ.

WPA resolves the issue of weak WEP headers, which are called initialisation vectors (IV), and insures the integrity of the messages passed through (Message Integrity Check (MIC) using Temporal Key Integrity Protocol (TKIP) to enhance data encryption.

WPA-PSK is a special mode of WPA for home users without an enterprise authentication server and provides the same strong encryption protection.

7.4.1 Security in pre-shared key mode

Pre Shared Key (PSK) mode is designed for home and small office networks that cannot afford the cost and complexity of an 802.1X authentication server. Each user must enter a passphrase to access the network. The passphrase may be from 8 to 63 printable American Standard Code for Information Interchange (ASCII) characters or 64 hexadecimal digits (256 bits). If you choose to use the ASCII characters, a hash function reduces it from 504 bits (63 characters * 8 bits/character) to 256 bits (using also the SSID). The passphrase may be stored on the user's computer at their discretion under most operating systems to avoid re-entry. The passphrase must remain stored in the Wi-Fi access point.

Security is strengthened by employing a Password-Based Key Derivation Function version 2 (PBKDF2). However, the weak passphrases users typically employ are vulnerable to password cracking attacks.

Some consumer chip manufacturers have attempted to bypass weak passphrase choice by adding a method of automatically generating and distributing strong keys through a software or hardware interface that uses an external method of adding a new Wi-Fi adapter or appliance to a network.

7.4.2 Security with an Authentication Server

With WPA the use of 802.1x is supported for operation with databases of users stored in Remote Access Dialin User Service (RADIUS) and this is accessed using Extensible Authentication Protocol (EAP).

7.4.3 IEEE 802.1X

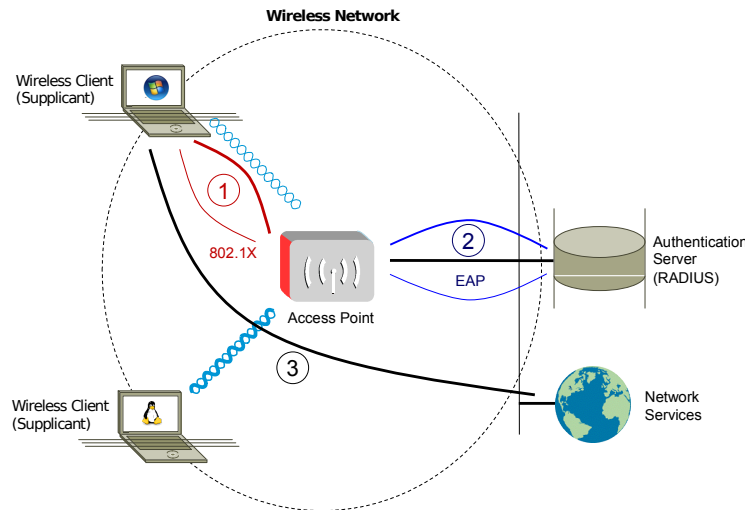


Illustration 19: IEEE 802.1X

802.1X is an IEEE standard for port-based network access control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. It is used for certain closed wireless APs, and is based on the EAP.

Some vendors are implementing 802.1X for wireless APs, to be used in certain situations where an access point needs to be operated as a closed AP, addressing the security vulnerabilities of WEP. The authentication is usually done by a third-party entity, such as a RADIUS server. This provides for client-only authentication, or more appropriately, strong mutual authentication using protocols such as EAP-Transport Layer Security (EAP-TLS).

Upon detection of the new client or the supplicant, the port on the switch (authenticator) will be enabled and set to the "unauthorised" state. In this state, only 802.1X traffic will be allowed; other traffic, such as DHCP and Hypertext Transfer Protocol (HTTP), will be blocked at the data link layer. The authenticator will send out the EAP-Request identity to the supplicant, the supplicant will then send out the EAP-response packet that the authenticator will forward to the authenticating server. The authenticating server can accept or reject the EAP-Request; if it accepts the request, the authenticator will set the port to the "authorised" mode and normal traffic will be allowed. When the supplicant logs off, he will send an EAP-logoff message to the authenticator. The authenticator will then set the port to the "unauthorised" state, once again blocking all non-EAP traffic.

7.5 802.11i WPA2

The Wi-Fi Alliance approved full 802.11i as WPA2, also called Robust Security Network (RSN). WPA2 implements the mandatory elements of 802.11i. It introduces Advanced Encryption Standard (AES) algorithm based algorithm, Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) that is considered fully secure.

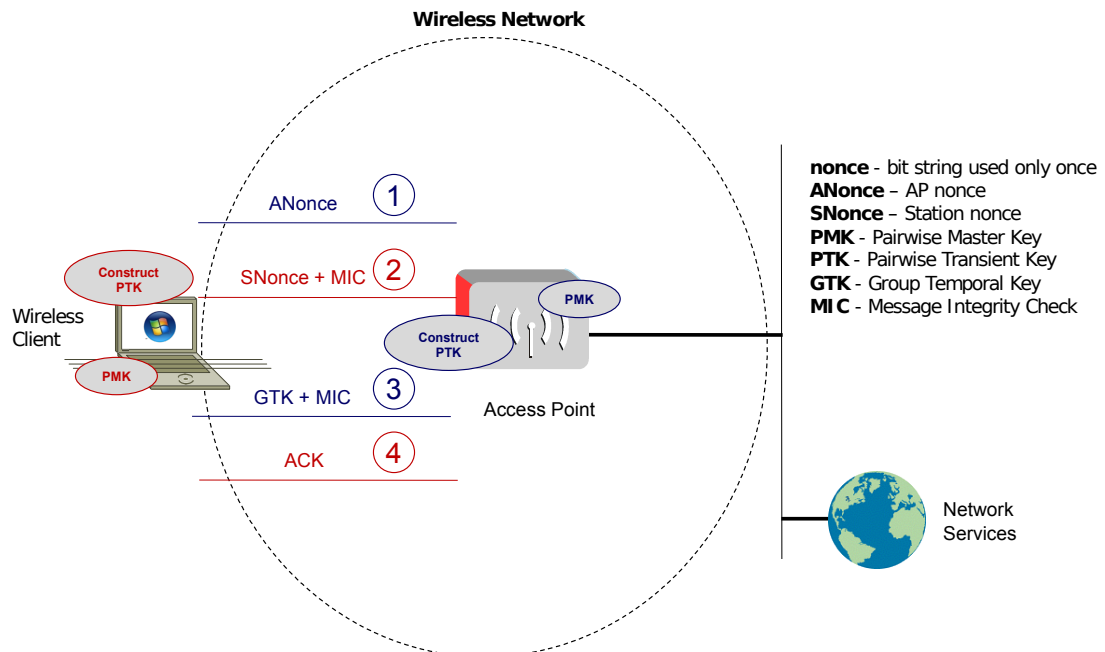


Illustration 20: 802.11i WPA2

The authentication process leaves two considerations: the AP still needs to authenticate itself to the client station, and keys to encrypt the traffic need to be derived. An EAP exchange provides the shared secret key Pairwise Master Key (PMK). This key is however designed to last the entire session and should be exposed as little as possible. Therefore the four-way handshake is used to establish another key called the Pairwise Transient Key (PTK). The PTK is generated by concatenating the following attributes: PMK, AP Nonce (ANonce), Station Nonce (SNonce), AP MAC address and Station MAC address. In cryptography, a Nonce is a random, arbitrary number that is generated for security purposes and is used one time only. The product is then put through a cryptographic hash function.

The handshake also yields the Group Temporal Key (GTK), used to decrypt multicast and broadcast traffic. The actual messages exchanged during the handshake are depicted in the diagram.

Note that from March 13, 2006, WPA2 certification is mandatory for all new devices wishing to be Wi-Fi certified.

8. Non Wi-Fi Solutions in Unlicensed Spectrum

A number of manufacturers have developed solutions for unlicensed spectrum to provide both PTP and Point to Multi Point (PTMP) connectivity. Such systems are targeted at WISPs who typically started out as a small local broadband scheme plugging a hole in the area where broadband was not being supplied by the traditional carriers. As WISPs expand their channel capacity with growth, interference becomes an issue. The proprietary solutions generally claim to suffer less from interference than standard WLAN. Motorola Canopy and Alvarion BreezeACCESS are examples. MikroTik and Ubiquiti offer 802.11 based solutions with proprietary enhancements in an attempt to achieve the same outcome. Both of these companies are now also offering TDMA based solutions to overcome the problems 802.11 has in the outdoors.

8.1 MikroTik - Nstreme / Nv2

MikroTik implement a software router operating system called RouterOS which can run on i386 based hardware. They also have a hardware arm called RouterBOARD who develop hardware for specific needs like P2P and PTMP for the RouterOS. MikroTik wireless devices are based on 802.11 protocols with the addition of some proprietary additions.

8.2 Nstreme

Nstreme and Nstreme2 are MikroTik proprietary wireless protocols developed by MikroTik for use with Atheros wireless chips to achieve higher performance on a very long range links. Regular 802.11 wireless links will have large time delays for data travelling over long distances, nstreme overcomes this problem.

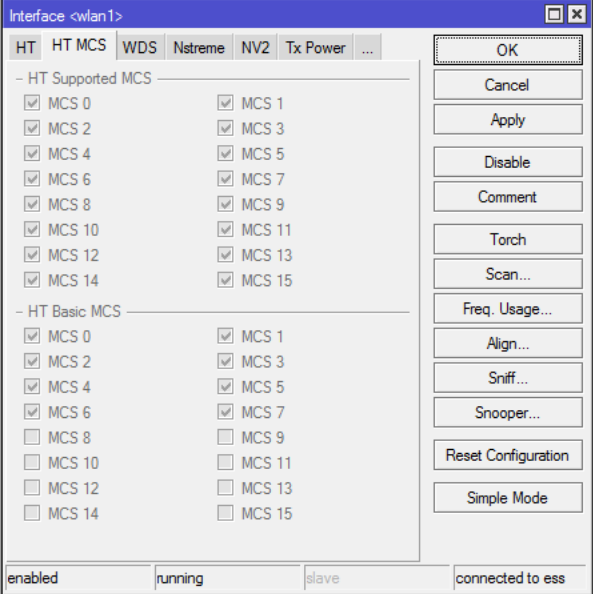
8.3 Nstreme 2

Nstreme 2 gives further range by using two Atheros based wireless cards in each end - one for transmit and one for receive.

8.4 Nv2 (Nstreme version 2)

Nv2 protocol is proprietary wireless protocol developed by MikroTik for use with Atheros 802.11 wireless chips. Nv2 is based on Time Division Multiple Access (TDMA) media access technology instead of using CSMA as used in IEEE 802.11.

9. Modulation and Coding Schemes



MCS Index	Number of spatial streams	Modulation (Stream 1 2 3 4)	Data Rate (in Mbps)	
			(GI = 400ns)	
			20MHz	40MHz
0	1	BPSK	7.2	15
1	1	QPSK	14.4	30
2	1	QPSK	21.7	45
3	1	16-QAM	28.9	60
4	1	16-QAM	43.3	90
5	1	64-QAM	57.8	120
6	1	64-QAM	65	135
7	1	64-QAM	72.2	150
8	2	BPSK	14.4	30
9	2	QPSK	28.9	60
10	2	QPSK	43.3	90
11	2	16-QAM	57.8	120
12	2	16-QAM	86.7	180
13	2	64-QAM	115.6	240
14	2	64-QAM	130.3	270
15	2	64-QAM	144.4	300

Illustration 21: Modulation and coding scheme

Modulation and Coding Scheme (MCS) in 802.11n wireless LAN describes the combination of the radio carrier Modulation scheme, such as BPSK through to 64QAM; and the Coding Scheme, such as rate 1/2 through 5/6, that are used when transmitting data. Each MCS has an associated data rate. For example MCS 0 equates to 7.2Mbps, MCS 15 to 300Mbps and MCS 31 up to 600Mbps using the short 400ns guard interval.

With 802.11n, the factors that affect the data rate include (in each case with an increasing data rate):

- The modulation scheme: BPSK, QPSK, 16-QAM, 64-QAM
- Coding rate: 1/2, 2/3, 3/4, 5/6
- The number of spatial streams: 1, 2, 4
- The number of Forward Error Correction (FEC) coders: 1, 2
- The RF channel bandwidth: 20MHz, 40 MHz
- The OFDM Guard Interval: 800ns, 400ns

9.1 Modulation on poor quality links

It may happen that on poor quality links the modulation is dropping to a lower level from time to time and then moving back up to the higher modulation level when it can. Such modulation fluctuations can have an impact on OSPF and real time traffic. It may be that a steady connection is preferable to high speeds and it would therefore make sense to drop the modulation permanently. Here we will drop the 64 QAM such that 16 QAM will be the top modulation level and should remain steady on the link.

```
[admin@MikroTik] > interface wireless set 0 rate-set=configured
                        ht-basic-mcs=mcs-0,mcs-1,mcs-2,mcs-3,mcs-4,mcs-8,
                        mcs-9,mcs-10,mcs-11,mcs-12 ht-rxchains=0,1 ht-supported-mcs=mcs-0,mcs-1,mcs-
                        2,mcs-3,mcs-4,mcs-8, mcs-9,mcs-10,mcs-11,mcs-12
```

MCS levels MCS-5, MCS-6, MCS-7, MCS-13, MCS-14 and MCS-15 are associated with 64 QAM as shown in Illustration 22 and are turned off to maintain the radio at the lower modulation level.

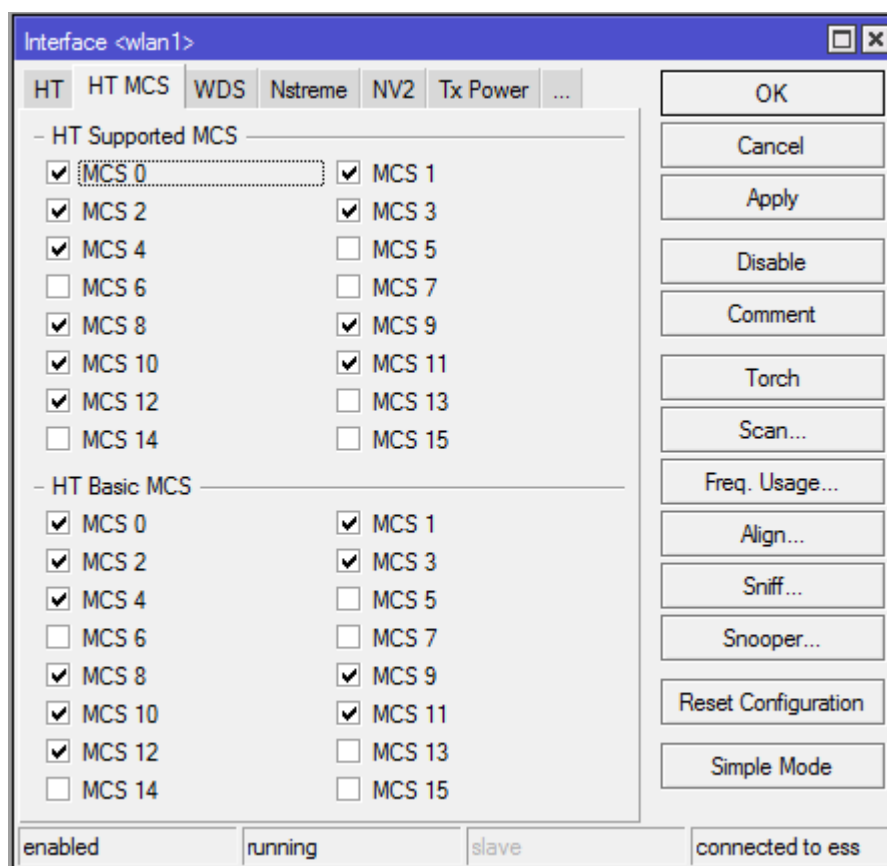


Illustration 22: Modulation levels dropped in 16 QAM

10. Wireless Setup

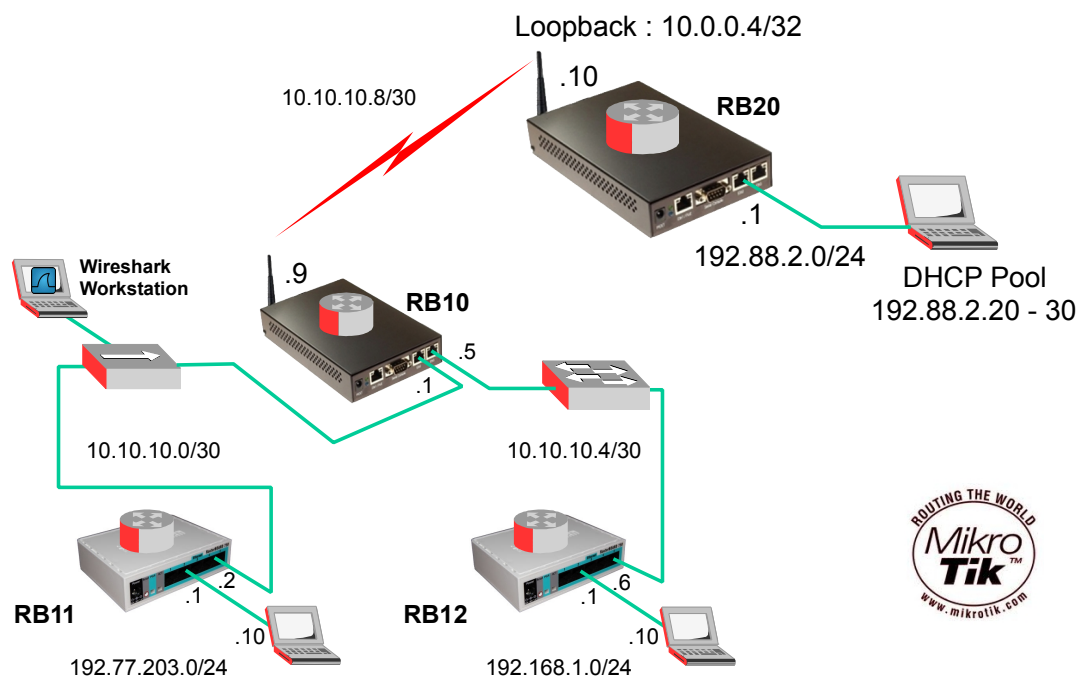


Illustration 23: Addition of wireless site to lab from lecture 4

10.1 RB10 Configuration

10.1.1 Wireless Interface

Configure the Wireless LAN interface. Establish the SSID.

```
[admin@RB10] > interface wireless set wlan1 ssid=OB_MK
```

Configure the frequency for use. 802.11b 2.4 GHz.

```
[admin@RB10] > interface wireless set wlan1 band=2ghz-b
```

Configure the unit as an Access Point bridge.

```
[admin@RB10] > interface wireless set wlan1 mode=ap-bridge
```

Configure a WPA2 dynamic PSK which will be matched at the other side. Set to advertise support for Advanced Encryption Standard (AES) AES in Counter with CBC-MAC (CCM) {Cipher Block Chaining Message Authentication Code (CBC-MAC)} mode ciphers for unicast broadcast and multicast frames. Also require that associations are only made with remote devices that support management protection.

```
[admin@RB10] > interface wireless security-profiles add
                  name=OB_Sec_Profile
                  mode=dynamic-keys
                  authentication-types=wpa2-psk
                  unicast-ciphers=aes-ccm
                  group-ciphers=aes-ccm
                  wpa2-pre-shared-key=OB_MK_Key
                  management-protection=required

[admin@RB10] > interface wireless set wlan1
                  security-profile=OB_Sec_Profile
```

Enable the Wireless interface.

```
[admin@RB10] > interface wireless set wlan1 disabled=no
```

Assign the Wireless interface with an IP Address.

```
[admin@RB10] > ip address add address=10.10.10.9/30 interface=wlan1
```

10.1.2 OSPF

Add the Wireless network to the OSPF list of networks.

```
[admin@RB10] > routing ospf network add area=backbone
                  network=10.10.10.8/30
```

10.2 RB20 Configuration

10.2.1 Configuration

```
[admin@MikroTik] > system identity set name RB20

[admin@RB20] > ip address add address=192.88.2.1/24 interface=ether2

[admin@RB20] > ip pool add name=dhcp-pool1
                  ranges=192.88.2.20-192.88.2.30

[admin@RB20] > ip dhcp-server add address-pool=dhcp-pool1 disabled=no
                  interface=ether2 lease-time=3d
                  name=dhcp-server-ether2

[admin@RB20] > ip dhcp-server network add netmask=24
                  gateway=192.88.2.1

[admin@RB20] > interface bridge add name=loopback1 protocol-mode=none
                  arp=disabled

[admin@RB20] > ip address add address=10.0.0.4/32 interface=loopback1
```

10.2.2 Wireless interface

```
[admin@RB20] > interface wireless set wlan1 ssid=OB_MK
```

```
[admin@RB20] > interface wireless set wlan1 band=2ghz-b
```

Configure the is unit as a station.

```
[admin@RB20] > interface wireless set wlan1 mode=station
```

```
[admin@RB20] > interface wireless security-profiles add
                    name=OB_Sec_Profile
                    mode=dynamic-keys
                    authentication-types=wpa2-psk
                    unicast-ciphers=aes-ccm
                    group-ciphers=aes-ccm
                    wpa2-pre-shared-key=OB_MK_Key
                    management-protection=required
```

```
[admin@RB20] > interface wireless set wlan1 disabled=no
```

```
[admin@RB20] > ip address add address=10.10.10.10/30 interface=wlan1
```

10.2.3 OSPF

```
[admin@RB20] > routing ospf instance set default router-id=10.0.0.4
                    redistribute-connected=as-type-1
```

Add the two networks and loopback to the OSPF list of networks.

```
[admin@RB20] > routing ospf network add area=backbone
                    network=10.10.10.8/30
```

```
[admin@RB20] > routing ospf network add area=backbone
                    network=192.88.2.0/24
```

```
[admin@RB20] > routing ospf network add area=backbone
                    network=10.0.0.4/32
```

10.3 Testing

- Ping, Traceroute from workstation to workstation.
- Use Wireshark to sniff traffic on the hub, observe the OSPF messages.
- Use MikroTik Packet Sniffer to review packets in and out of each router.

10.3.1 Scanning Tool

MikroTik has a wireless scanning tool that will show the Wireless LANs available.

```
[admin@RB20] > interface wireless scan wlan1
```

Flags: A - active, B - bss, P - privacy, R - RouterOS-network, N - nstreme

	ADDRESS	SSID	BAND	FREQ	SIG	NF	SNR	RADIO-NAME
ABP	00:23:F8:D7:29:40	eircom8...	2.4ghz-b	2412	-80	-101	21	
AB R	00:0C:42:3A:CD:E8	OB_MK	2.4ghz-b	2412	-56	-101	45	000C423ACDE8
ABP	00:1E:C1:09:38:C2		2.4ghz-b	2412	-92	-101	9	
ABP	00:0F:CC:D9:AD:8C	SSLAIR	2.4ghz-b	2442	-82	-100	18	
ABP	00:22:3F:0A:B1:B8	Ripplec...	2.4ghz-b	2462	-47	-101	54	
ABP	00:1B:2F:AE:40:7E	AML	2.4ghz-b	2462	-66	-101	35	
ABP	00:90:4B:19:A6:1F	SSLAIR	2.4ghz-b	2457	-94	-101	7	
ABP	C4:7D:4F:C7:25:A0	SSLAIR	2.4ghz-b	2422	-94	-101	7	

```
-- [Q quit|D dump|C-z pause]
```

Using the scanning tool from WinBox.

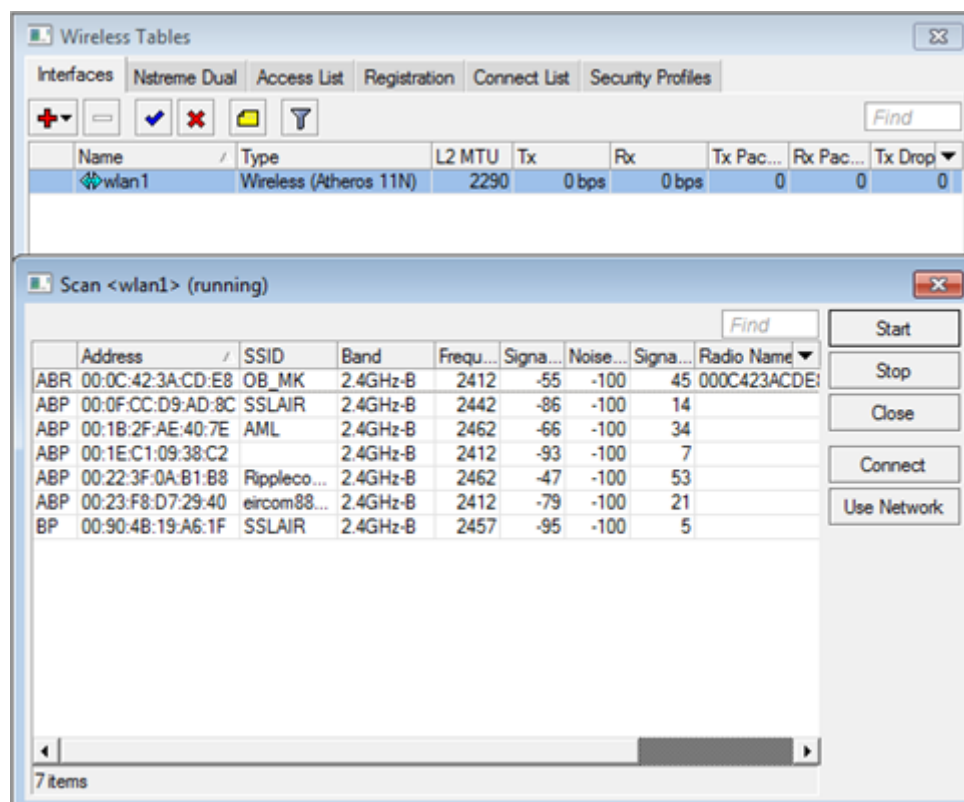


Illustration 24: Winbox scanning tool

It may be necessary to reduce the scan-list to the area of interest. In the 5 GHz band the default steps are 20 MHz but you may want 5 GHz steps when troubleshooting.

```
[admin@RB20] > interface wireless set 0 scan-list=2412-2422
```

```
[admin@RB20] > interface wireless scan 0
```

Flags: A - active, P - privacy, R - RouterOS-network, N - nstreme, T - tdma,
W - wds, B - bridge

	ADDRESS	SSID	BAND	CHANNEL-WIDTH	FREQ	SIG	NF	SNR	RADIO-NAME
A	00:27:0D:38:9B:08	Hotel30	2ghz-n	20mhz	2412	-80	-110	30	
APR B	D4:CA:6D:21:17:0F	MikroTik	2ghz-n	20mhz	2412	-43	-110	67	
APR B	00:0C:42:66:69:91	M	2ghz-n	20mhz	2412	-87	-110	23	
AP	D8:5D:4C:A0:2F:EA	SZ	2ghz-n	20mhz	2417	-90	-110	20	
A	00:27:0D:38:90:D8	Hotel15	2ghz-n	20mhz	2422	-91	-110	19	
AP	00:22:15:E3:BB:80	FLORDENT	2ghz-n	20mhz	2412	-90	-110	20	
A	00:1E:8C:4B:FE:A2	WebSTAR	2ghz-n	20mhz	2412	-89	-110	21	

```
-- [Q quit|D dump|C-z pause]
```

10.3.2 Frequency Monitor

The frequency monitor tool gives a view of each channel in the scan-list, its usage and its noise floor.

```
[admin@RB20] > interface wireless frequency-monitor 0
```

FREQ	USE	NF
2412MHz	4.6%	-107
2417MHz	2.8%	-109
2422MHz	0.8%	-110
2427MHz	4.8%	-110
2432MHz	12.9%	-110
2437MHz	14.6%	-110
2442MHz	1.8%	-109
2447MHz	0.3%	-109
2452MHz	0%	-110
2457MHz	0%	-109
2462MHz	0%	-109

10.3.3 Spectral Scan

The spectral scan is a fantastic tool that was introduced with Atheros Merlin chips (AR9220, AR9280, AR9223). It can scan the frequency band of the wireless card and plot them on the terminal.

The scan is carried out at 10 MHz frequency increments which is half the typical channel spacing. This means the sample coverage is doubled at each specific frequency.

```
[admin@RB20] > interface wireless spectral-scan 0
```

```
FREQ  DBM  GRAPH
2385  -91  .....
2391  -67  .....
2397  -66  .....
2403  -51  .....
2409  -45  .....
2416  -46  .....
2422  -75  .....
2428  -83  .....
2434  -85  .....
2441  -86  .....
2447  -83  .....
2453  -86  .....
2459  -87  .....
2465  -86  .....
2472  -77  .....
2478  -78  .....
2484  -75  .....
2490  -75  .....
2497  -75  .....
2503  -76  .....
2509  -76  .....
2515  -80  .....
-- [Q quit|D dump|C-z pause|down]
```

10.3.4 Spectral History

```
[admin@RB20] > interface wireless spectral-history 0
```

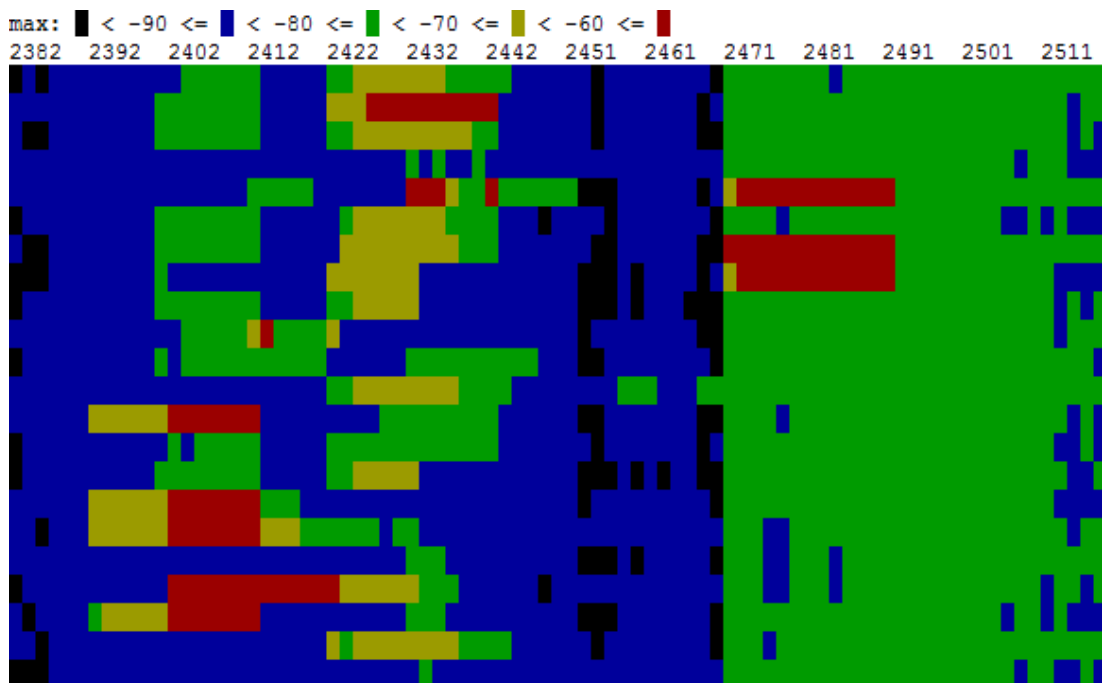


Illustration 25: Radio Spectrogram

The spectral history command plots a spectrogram. It is a plot of the frequency spectrum as a power values represented with colours as shown on the legend. The spectral history and spectral scan use the same data source, it is just different ways to display the same data.

10.3.5 Wireless Snooper

The wireless snoop tool monitors the surrounding frequency usage, and displays the devices that occupy each frequency.

```
[admin@RB20] > interface wireless snoop snoop wlan1
```

```

BAND      FREQ      USE      BW NET-COUNT  NOISE-FLOOR  STA-COUNT
2ghz-n    2412MHz  14.9%    101.2kbps      2             -108          5
2ghz-n    2417MHz   6.7%     36.7kbps       0             -109          0
2ghz-n    2422MHz   5.7%     29.2kbps       1             -109          2
2ghz-n    2427MHz   8.5%     68.6kbps       0             -110          1
2ghz-n    2432MHz   9.6%    234.8kbps      2             -110          4
2ghz-n    2437MHz   8.3%     61.9kbps       5             -110          5
2ghz-n    2442MHz   1.3%     10.3kbps       0             -109          0
2ghz-n    2447MHz   1.4%      3.1kbps        2             -110          4
2ghz-n    2452MHz   0%        0bps           0             -109          0
2ghz-n    2457MHz   0%        0bps           0             -109          0
2ghz-n    2462MHz   1.1%     4.6kbps        0             -110          2
-- [Q quit|D dump|C-z pause|n networks|s stations]

```

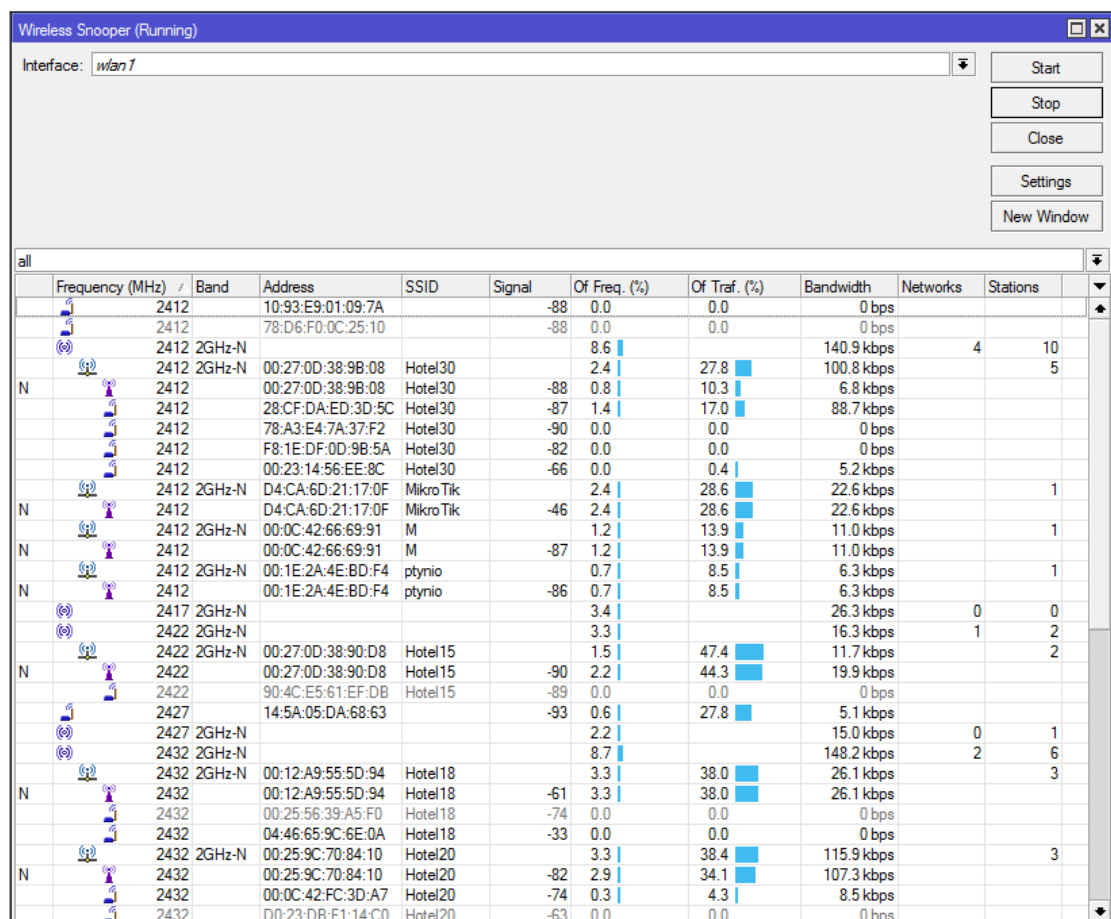


Illustration 26: Wireless snoop

10.3.6 Wireless Debugging

To log wireless information that may be of use when debugging, add the logging topics wireless and debug. The debugs can be sent to many places like file, syslog etc.. but in this case they are sent to memory. Using the log print command the log in memory is printed to the terminal.

```
[admin@RB20] > system logging add topics=wireless,debug
                        action=memory disabled=no

[admin@RB20] > log print

00:38:43 wireless,debug 00:0C:42:66:69:91: on 2412 AP: yes SSID M caps 0x431 rates 0xff0f basic 0xf MT: yes
00:38:43 wireless,debug D4:CA:6D:21:17:0F: on 2412 AP: yes SSID MikroTik caps 0x431 rates 0xff0f basic 0xf MT: yes
00:38:43 wireless,debug 00:27:0D:38:90:D8: on 2422 AP: yes SSID Hotel15 caps 0x401 rates 0xff0f basic 0xf MT: no
00:38:43 wireless,debug 00:25:9C:70:84:10: on 2432 AP: yes SSID Hotel20 caps 0x1 rates 0xff0f basic 0xf MT: no
00:38:43 wireless,debug 00:12:A9:55:5D:94: on 2432 AP: yes SSID Hotel18 caps 0x421 rates 0xff0f basic 0xf MT: no
00:38:43 wireless,debug 94:0C:6D:BC:5A:DA: on 2437 AP: yes SSID truskawki caps 0x431 rates 0xff0f basic 0xf MT: no
00:38:43 wireless,debug 00:27:19:1D:46:C6: on 2437 AP: yes SSID deo76 caps 0x431 rates 0xff0f basic 0xf MT: no
00:38:43 wireless,debug 00:27:19:C5:F9:F0: on 2437 AP: yes SSID caps 0x31 rates 0xff0f basic 0xf MT: no
00:38:43 wireless,debug 00:0D:65:D8:FE:93: on 2437 AP: yes SSID t-mobile.pl caps 0x21 rates 0xf basic 0xf MT: no
00:38:43 wireless,debug 00:12:A9:55:87:97: on 2447 AP: yes SSID Hotel7 caps 0x421 rates 0xff0f basic 0xf MT: no
00:38:43 wireless,debug 00:27:0D:38:9B:08: on 2412 AP: yes SSID Hotel30 caps 0x401 rates 0xff0f basic 0xf MT: no
00:38:43 wireless,debug 00:1E:2A:4E:BD:F4: on 2462 AP: yes SSID ptynio caps 0x411 rates 0xff0f basic 0xf MT: no
00:38:43 wireless,debug 00:19:CB:4E:03:FC: on 2437 AP: yes SSID ZyXEL caps 0x421 rates 0xff0f basic 0xf MT: no
00:38:43 wireless,debug wlan1: no network that satisfies connect-list, by default choose with strongest signal
```

The log tool has a number of different formats to present the log data depending on individual choice.

```
[admin@RB20] > log print detail
```

```
[admin@RB20] > log print brief
```

```
[admin@RB20] > log print terse
```

If the log has lots of entries from different “topics” it is possible to extract the ones required as follows.

```
[admin@RB20] > log print follow where topics~"wireless"
```

11. Lab Exercise – Build Wireless network

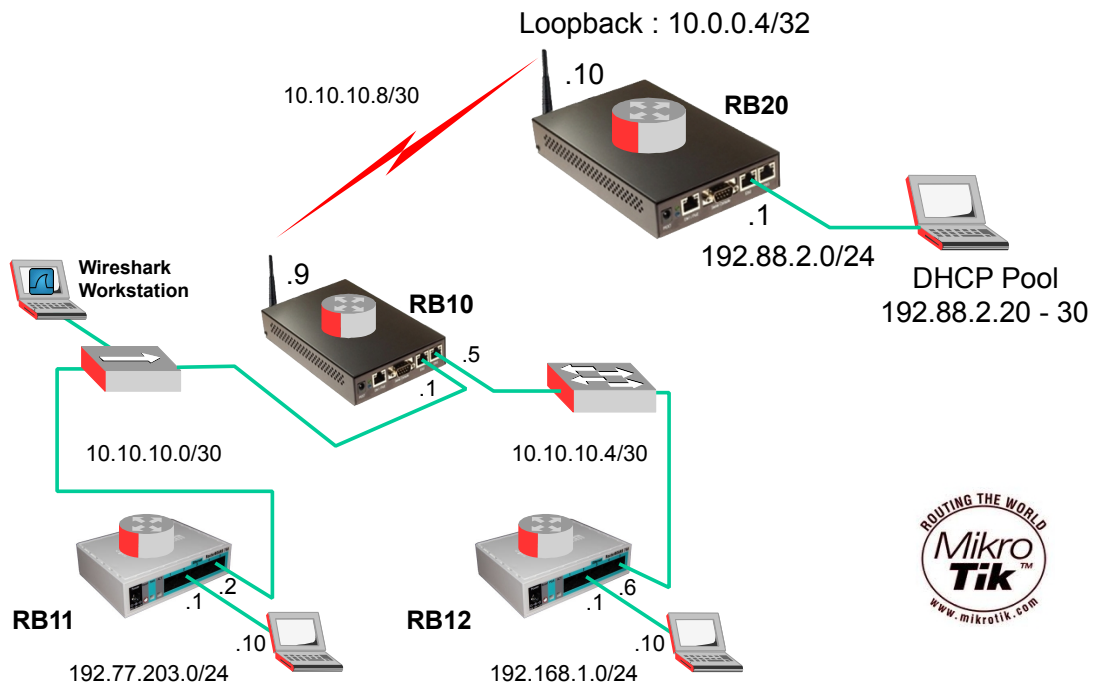


Illustration 27: Wireless lab

Extend the network built in lecture 4 with the wireless client as shown.

12. Self-test Quiz

1. List the IEEE standards that use the 5 GHz Short Range Devices band.
2. Define the difference between:
 - Independent Basic Service Set
 - Basic Service Set
3. What are the key differences between WEP and WPA2?