CMP4204
Wireless Technologies

Lecture 06

Wireless LAN (WLAN)

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Wireless LANs

- Wireless LANs are over-the-air modulation techniques that use the same basic protocol to create a wireless LAN.
- The most popular are those defined by the 802.11b and 802.11g and 802.11n protocols.
- 802.11ac is a new multi-streaming modulation technique that can offer up to 1 Gb/s of throughput.
- The segment of the radio frequency spectrum used varies between countries. Typically Wi-Fi falls within the 2.4 GHz radio band, though 5 GHz is also popular in some countries.

Wi-Fi Structure

- 802.11 networks are organised in two ways:
  - **Infrastructure mode**
    - In this 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 access point (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.
  - **adhoc mode**
    - In this mode 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.

802.11 Variants

- 802.11
  - provides 1 or 2 Mbps transmission in the 2.4 GHz band using either FHSS or DSSS.
- 802.11a
  - An extension to 802.11
  - provides typically 25 Mbps to a maximum of 54 Mbps in the 5GHz band.
  - 802.11a uses OFDM encoding scheme
  - Max range is 30m.

802.11 Variants

- 802.11b (also referred to as 802.11 High Rate or Wi-Fi)
  - An extension to 802.11
  - 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 30m.
- 802.11g
  - provides typically 24 Mbps to a maximum of 54 Mbps in the 2.4 GHz band.
  - It uses OFDM. Max range is 30m.

802.11 Variants

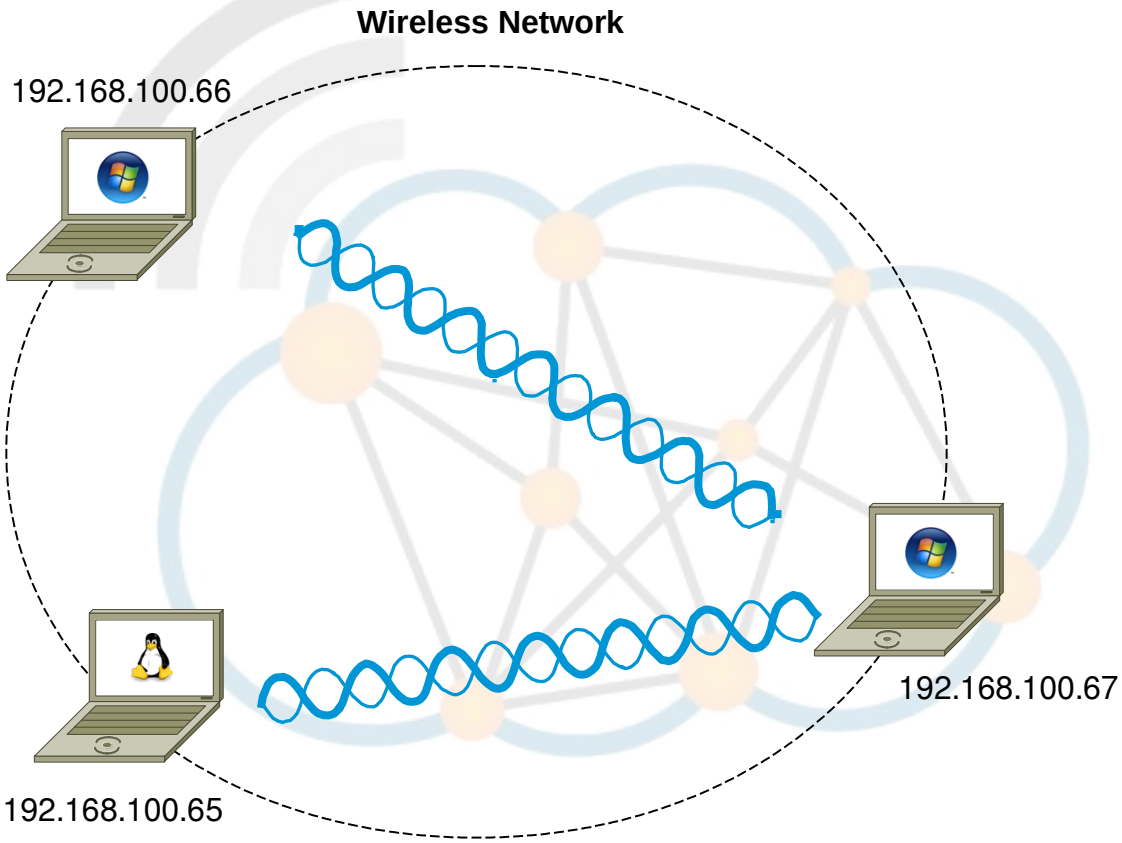
- 802.11n
  - 200 Mbps to a maximum of 540 Mbps out to 50m in either the 2.4 or 5 GHz bands. MIMO Antennas.
- 802.11ac
  - Multi-station WLAN throughput of at least 1 Gb/s and a single link throughput of at least 500 Mb/s.
  - Extended air interface concepts embraced by 802.11n,
    - wider RF bandwidth of up to 160 MHz
    - up to 8 MIMO spatial streams
    - up to 4 downlink multi-user MIMO clients
    - 256 QAM high-density modulation.
    - Space-division multiple access (SDMA).

Establish an Ad-hoc network

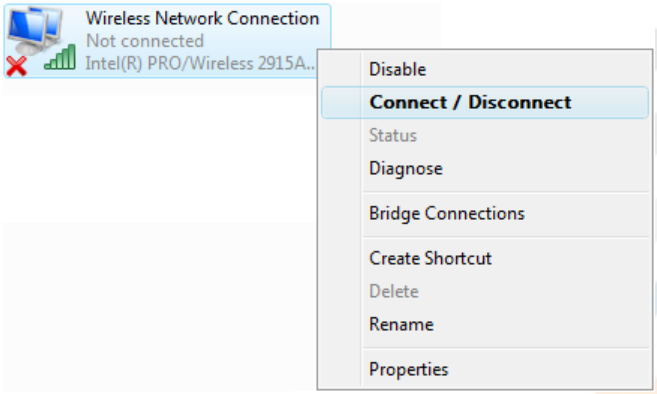
Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

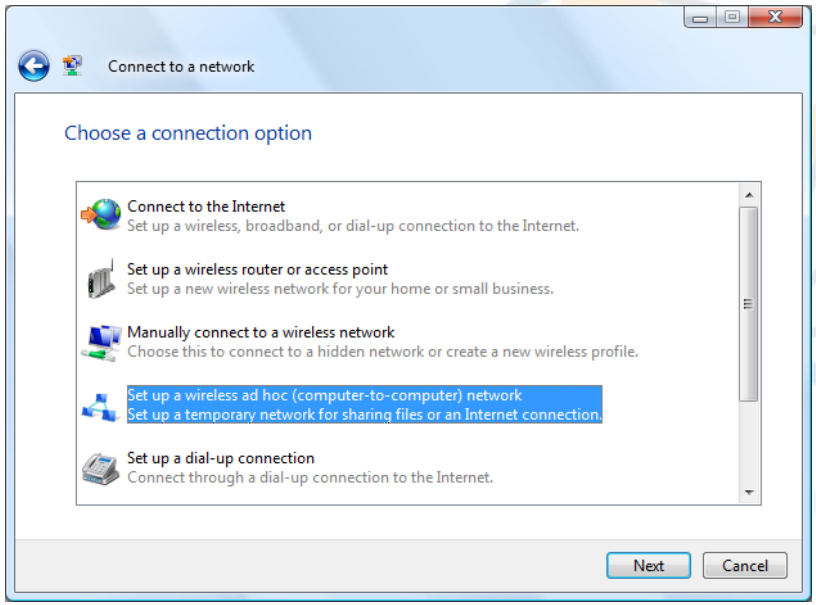
Ad-hoc network

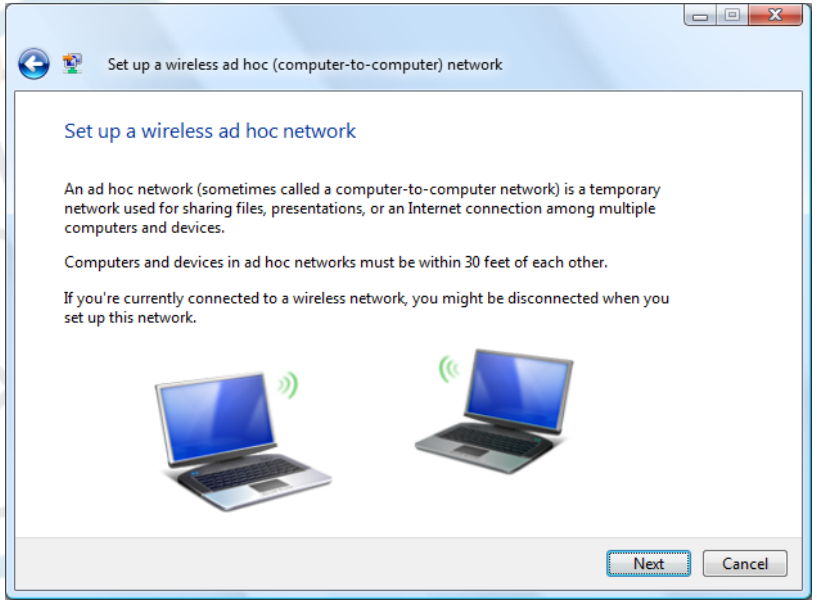


Setting up the Wireless ad hoc network

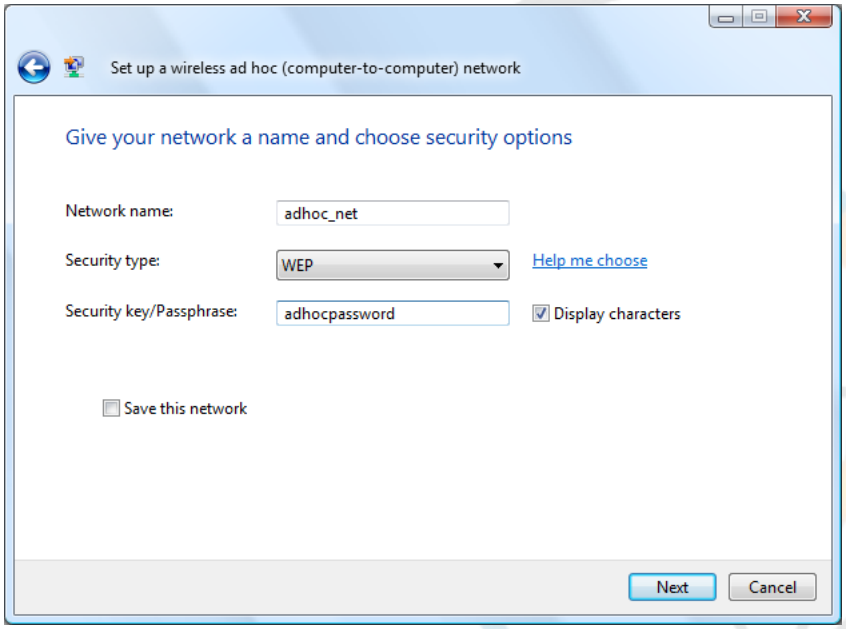


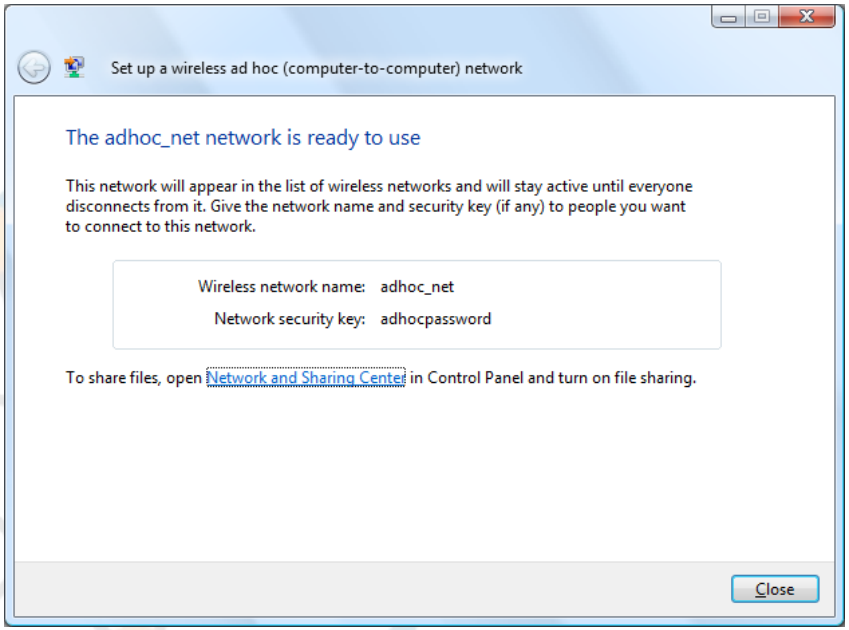
Start → Settings → Network Connections





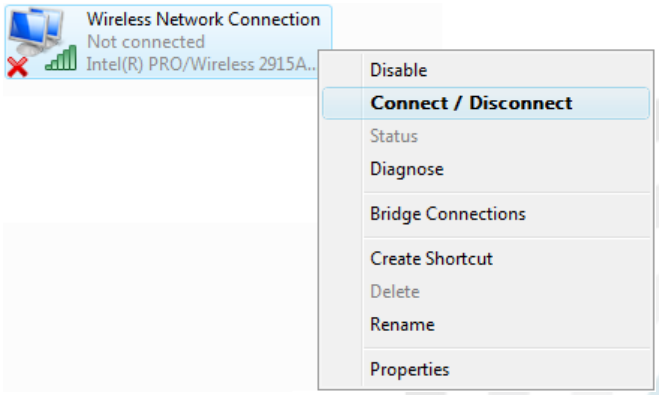
Setting up the Wireless ad hoc network



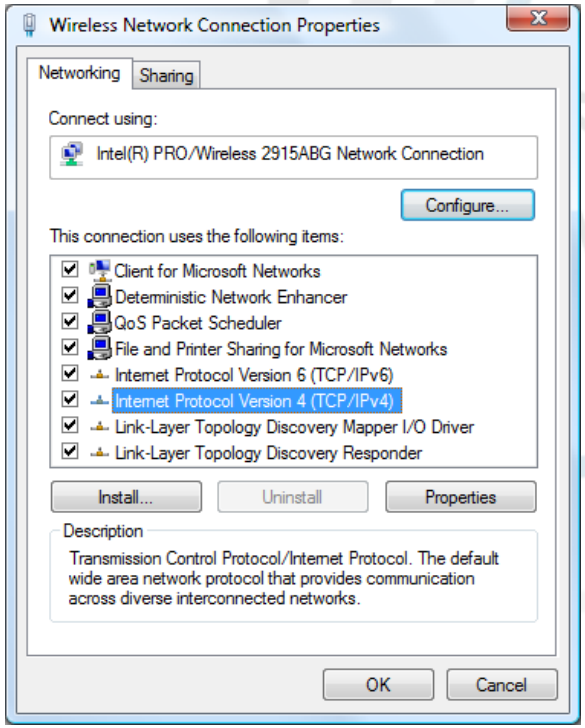


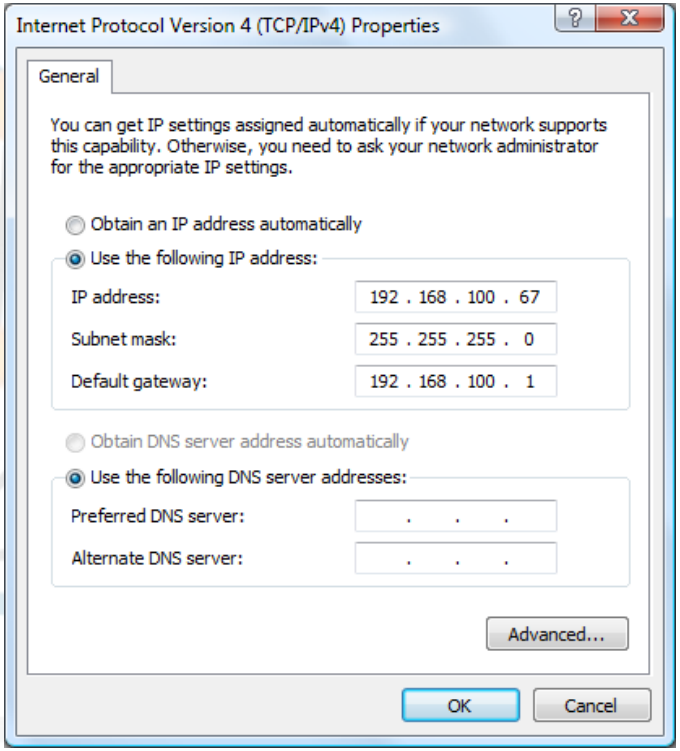
Network Name: **adhoc_net**
Security key/Passphrase: **adhocpassword**

Setting up the Wireless ad hoc network



Start → Settings → Network Connections





Setting up the Wireless ad hoc network

Minicom

GNU/Linux$ **su**
Password:

GNU/Linux# **iw phy phy0 interface add eth1 mode ibss**
GNU/Linux# **iw dev eth1 connect -w AP_ITC keys 0: abcdef0123**

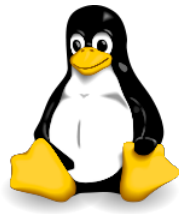
GNU/Linux# **ip addr add 192.168.1.60/24 dev eth1**

GNU/Linux # **vi /etc/resolv.conf**
nameserver 196.9.23.49
~
~
:wq!

Setting up the Wireless ad hoc network

Minicom

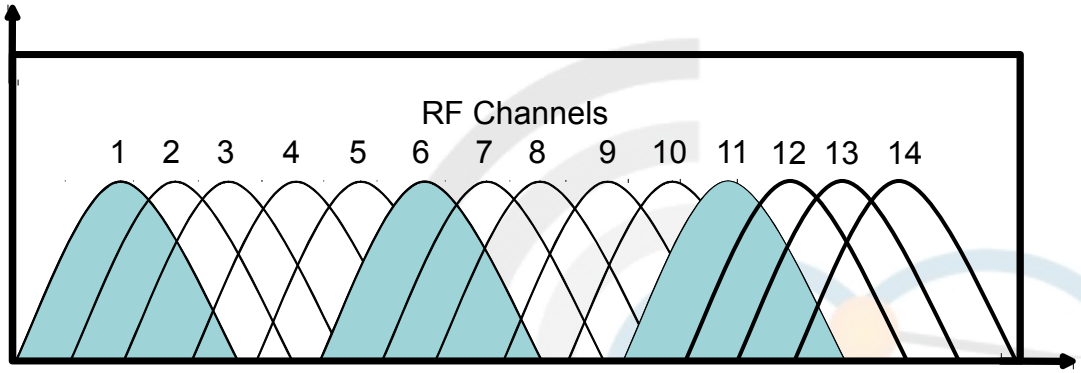
```
GNU/Linux# netstat -ie
Kernel Interface table

eth1      Link encap:Ethernet  HWaddr 00:13:CE:01:66:92
          inet addr:192.168.100.65  Bcast:192.168.100.255
          Mask:255.255.255.0
          inet6 addr: fe80::213:ceff:fe01:6692/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:461 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:1000
          RX bytes:6611 (6.4 KiB)  TX bytes:3029 (2.9 KiB)
          Interrupt:18 Base address:0x4000 Memory:dceff000-dcefffff

GNU/Linux# ping 192.168.100.67
PING 192.168.100.66 (192.168.100.66) 56(84) bytes of data.
64 bytes from 192.168.100.66: icmp_seq=1 ttl=128 time=6.27 ms
64 bytes from 192.168.100.66: icmp_seq=2 ttl=128 time=1.15 ms
64 bytes from 192.168.100.66: icmp_seq=3 ttl=128 time=1.15 ms

--- 192.168.100.66 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 1.151/2.860/6.272/2.412 ms
root@gluaisriomhaire:/home/dobriain#
```



Wireless Organisations

- IEEE
  - 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.
- Wi-Fi Alliance
  - The Wi-Fi Alliance develops rigorous tests and conducts Wi-Fi certification of wireless devices that implement the universal IEEE 802.11 specifications.
- ITU
  - ITU is the leading United Nations agency for information and communication technologies.
- FCC
  - The FCC is an independent United States government agency, directly responsible to the US Congress.

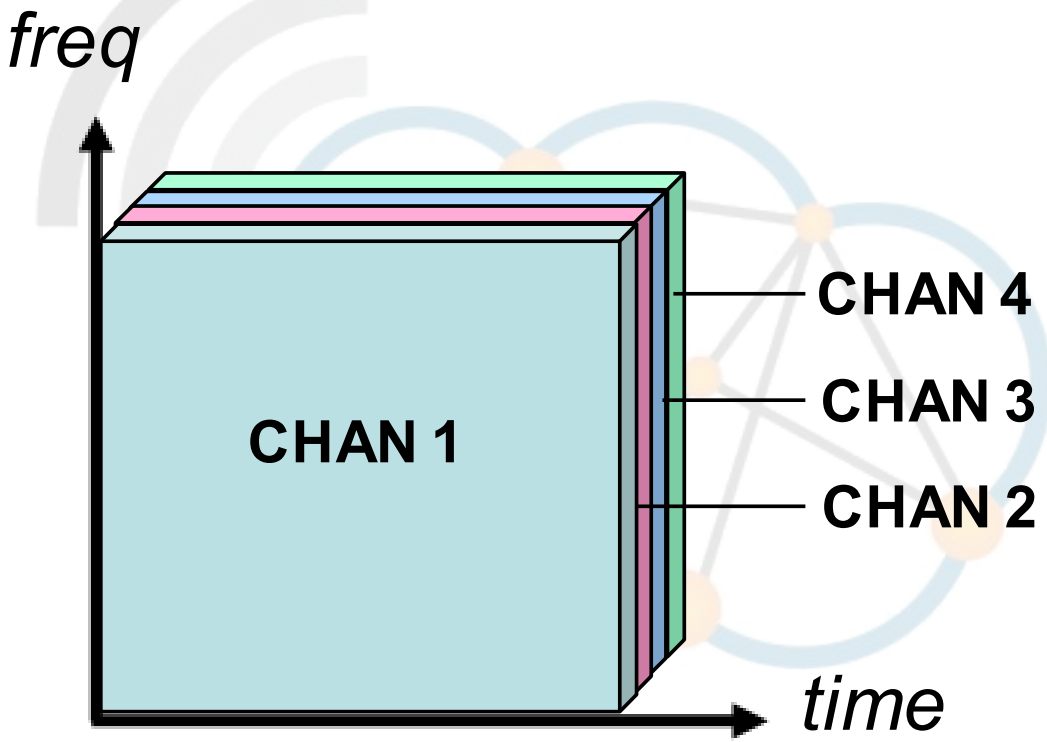
DSSS



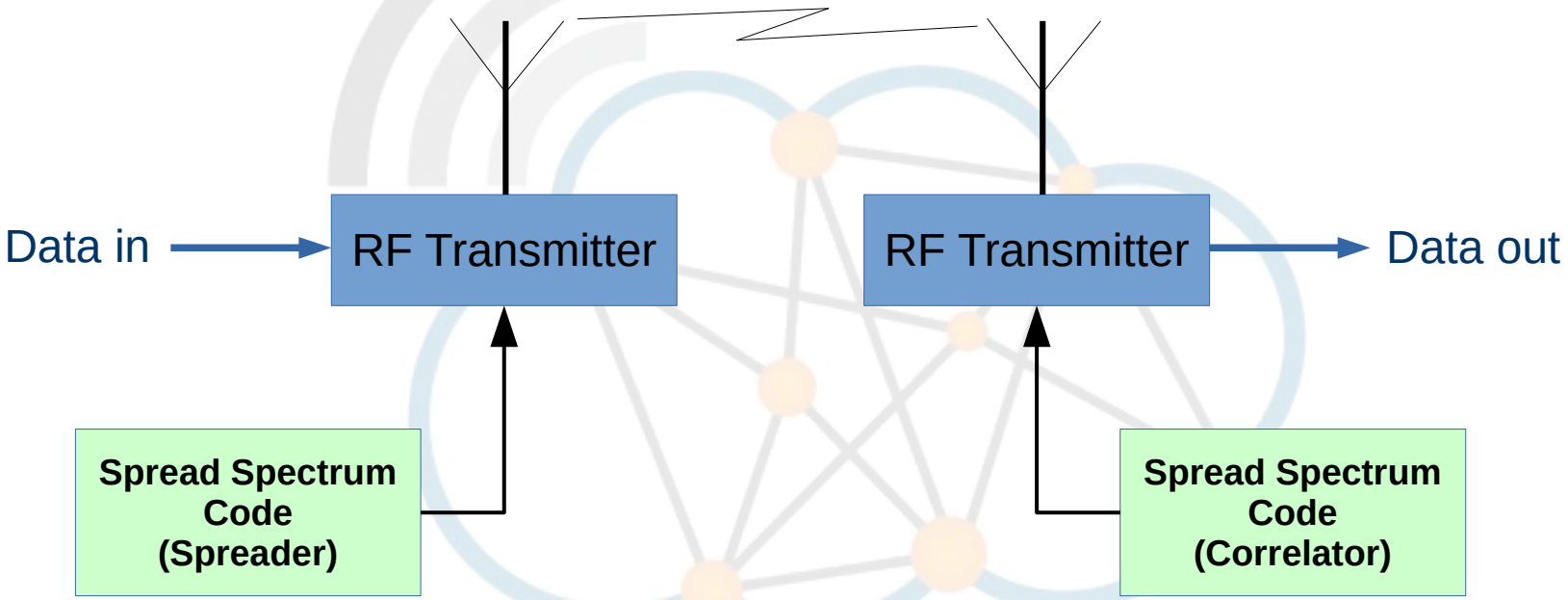
802.11b WiFi Channels			
Channel	Lower Frequency (GHz)	Centre Frequency (GHz)	Upper Frequency (GHz)
1	2.401	2.412	2.423
2	2.404	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
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

- 802.11b - 11 overlapping DSSS Channels at 2.4 GHz

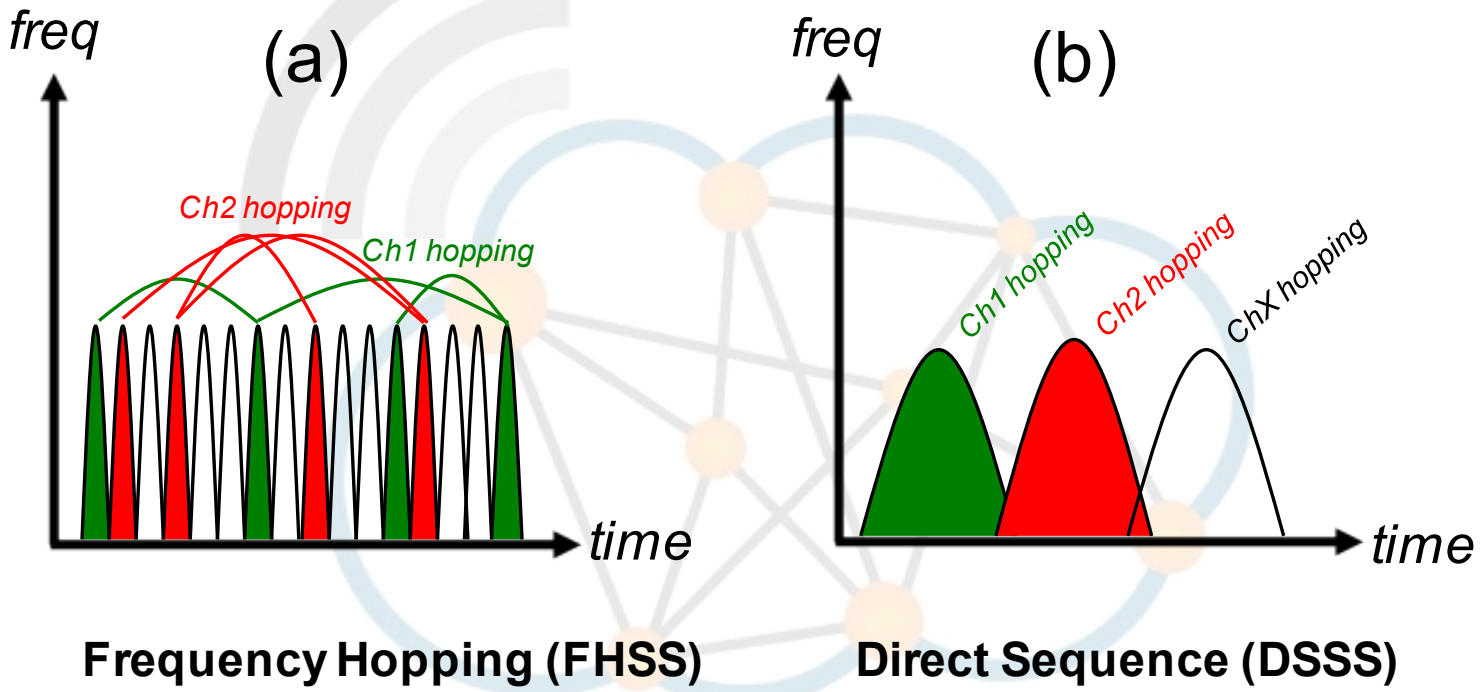
Spread spectrum



Spread spectrum

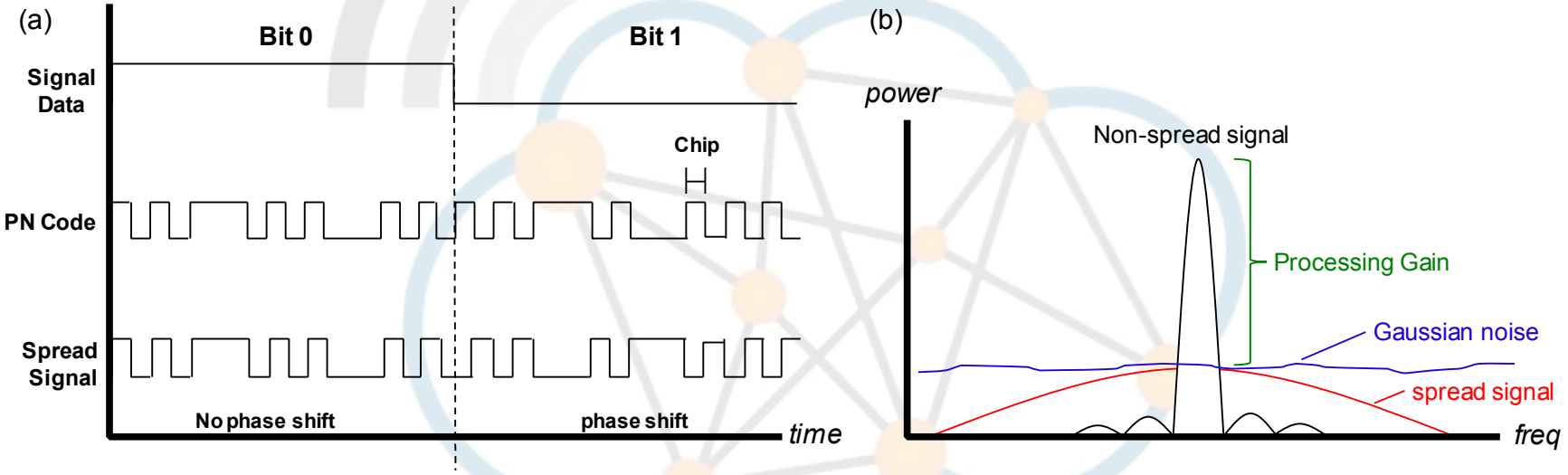


Spread spectrum



Frequency Hopping (FHSS) **Direct Sequence (DSSS)**

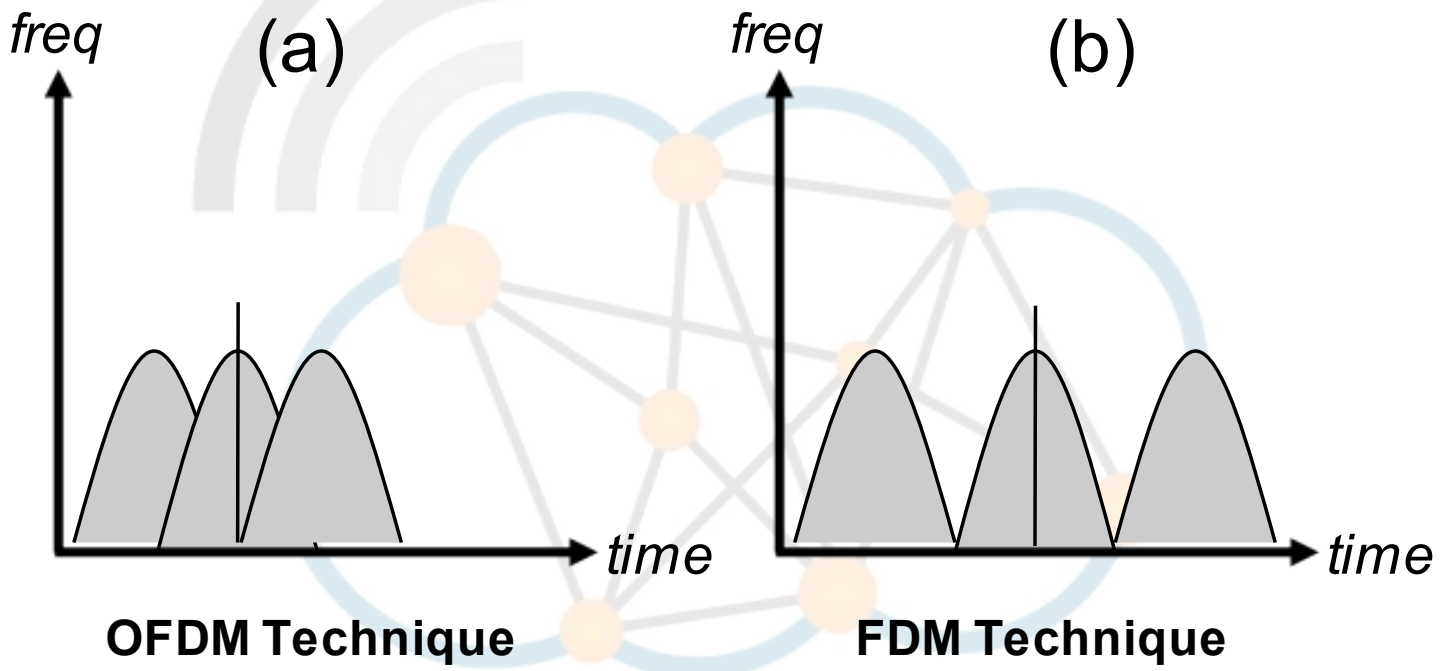
Spread spectrum



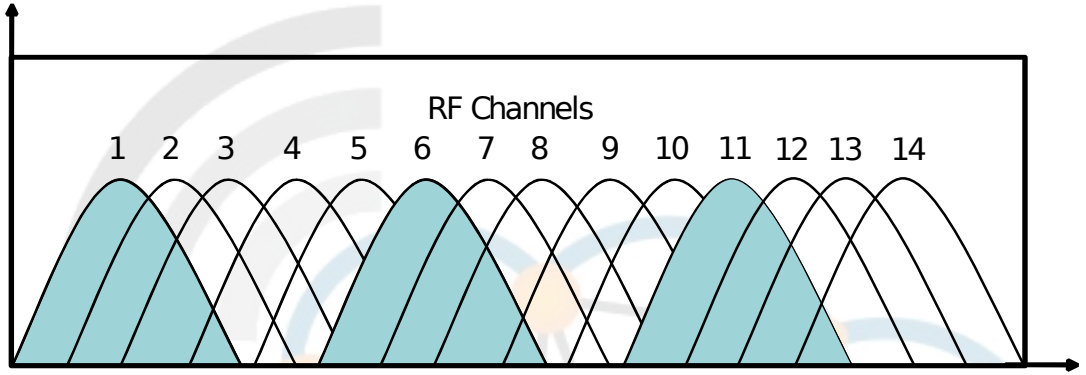
Orthogonal Frequency Division Multiplexing

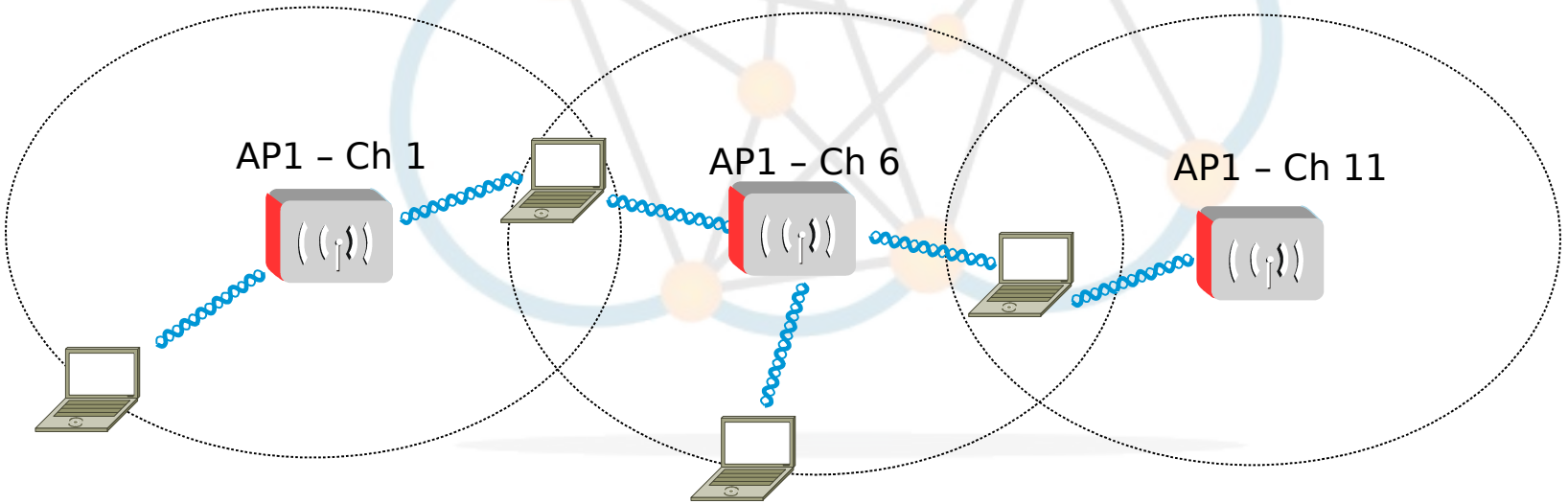
- Digital multi-carrier modulation scheme, which uses 52 orthogonal sub-carriers.
- Sub-carrier frequency are orthogonal to each other
  - Cross-talk between the sub-channels is eliminated so no inter-carrier guard bands
  - BPSK, QPSK, 16-QAM, 64-QAM in each channel
  - 6, 9, 12, 18, 24, 36, 48, 54 Mb/s.

Orthogonal Frequency Division Multiplexing



Non-overlapping Channels





5 GHz Channels – 802.11A/N/AC

5000 + 5 × Nch (MHz)

where Nch = 0 – 200

5.8 GHz FWA/MAN Band

Operation in the 5.8GHz band is subject to meeting the following conditions:

- Operating Freq Band: 5725 – 5875MHz;
- Maximum power: 100mW/MHz EIRP (to a maximum of 2W EIRP);
- Registration of operational base stations.

Effective Isotropic Radiated Power (EIRP) - is the amount of power that a theoretical isotropic antenna (which evenly distributes power in all directions) would emit to produce the peak power density observed in the direction of maximum antenna gain

Regulatory Class	Channel start freq	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

5.8 GHz band

- In some countries fixed wireless access networks are permitted in the 5.8GHz (5725 – 5875MHz) band up to a maximum radiated power of 2W EIRP on a licence exempt basis.
- This gives an additional 7 x 20 MHz channels.
- 5.745, 5.765, 5.785, 5.805, 5.825, 5.845, 5.865 GHz.

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	

802.11 MAC (Media Access Control)

- The 802.11 family uses a MAC layer known as CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) .
- CSMA/CA is, like all Ethernet protocols, peer-to-peer (there is no requirement for a master station).
- A Wireless node transmitter 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 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.

Wi-Fi Elements

- 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."
- 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".

Wi-Fi Security

- Crackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks.
- Types of Wi-Fi Security Breaches:
  - Accidental association
  - Malicious association
  - Ad-hoc networks
  - Non-traditional networks (Bluetooth, PDAs, barcode readers)
  - Identity theft (MAC spoofing)
  - Man-in-the-middle attacks
  - Denial of service (DOS)
  - Network injection.

Methods of counteracting security risks

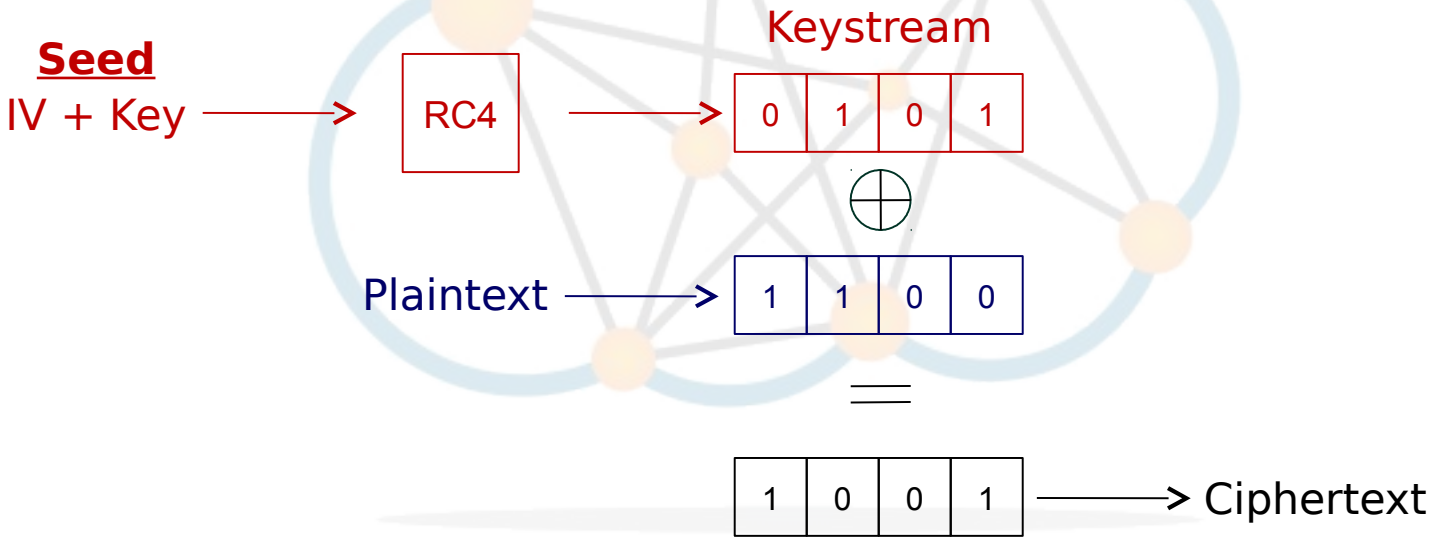
- There are many technologies available to counteract wireless network intrusion, but currently no method is absolutely secure.
- The best strategy may be to combine a number of security measures.
- There are three steps to take towards securing a wireless network:
  - All wireless LAN devices need to be secured
  - All users of the wireless network need to be educated in wireless network security
  - All wireless networks need to be actively monitored for weaknesses and breaches.

Steps in securing a wireless network

- Turn on encryption - WPA2 , WPA, WEP.
- Change the default password needed to access a wireless device.
- Change the default SSID, or network name.
- Disable file and print sharing if it is not needed.
- Access points should be arranged to provide radio coverage only to the desired area if possible.
- Divide the wired and wireless portions of the network into different segments, with a firewall in between.
- Implement an overlay Wireless intrusion prevention system to monitor the wireless spectrum 24x7 against active attacks and unauthorised devices such as Rogue Access Points.

Wireless Encryption Protocol (WEP)

- WEP is part of the WPA2.
- IEEE 802.11 wireless networking standard.
- 64-bit WEP uses a 40 bit key plus a 24 bit IV
  - 10 Hex characters
- 128-bit WEP uses 26 hex characters
- 356-bit WEP uses 58 hex characters
- Superseded by WPA & WPA2.



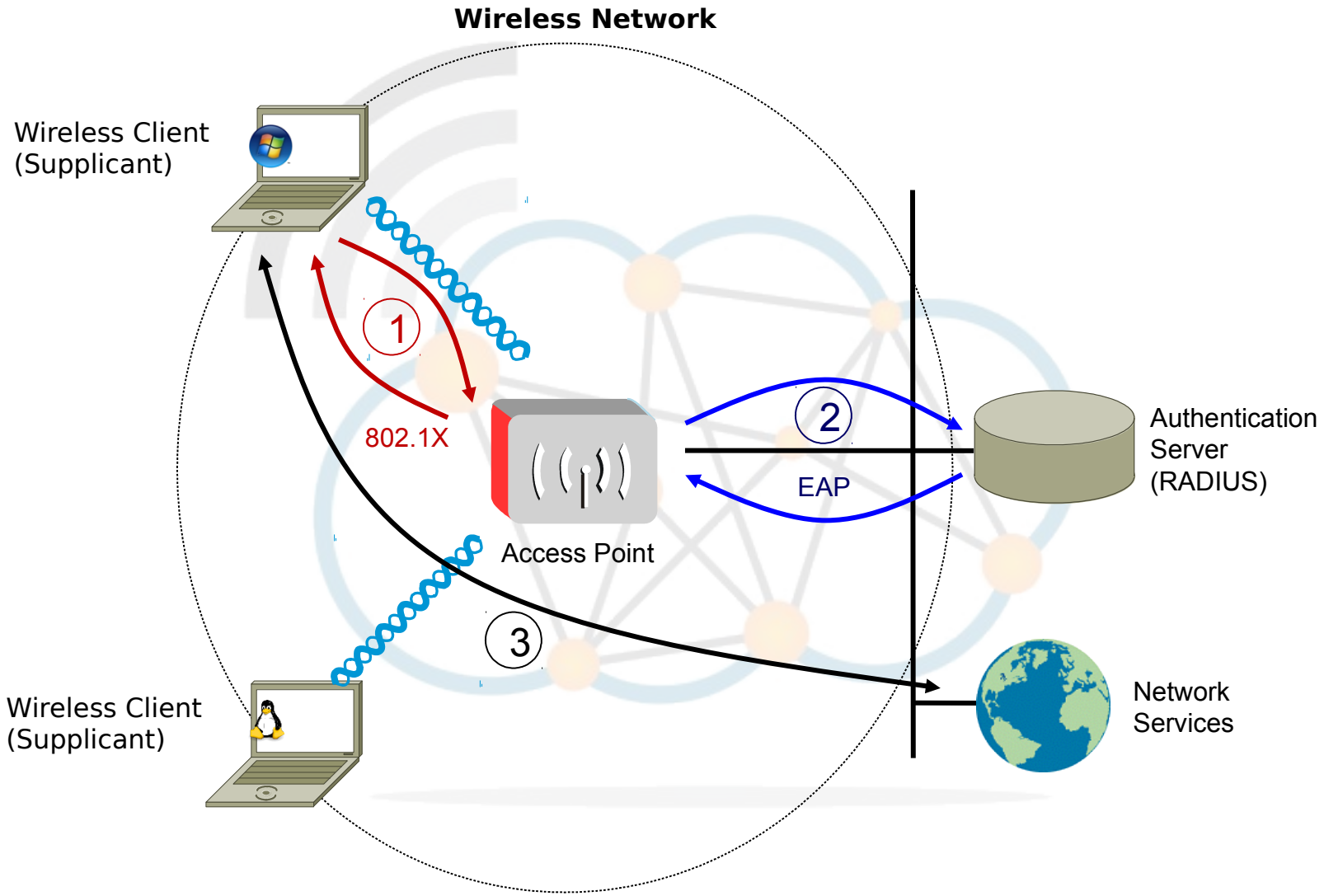
Wi-Fi Protected Access (WPA)

- WPA resolves the issue of weak WEP headers, which are called initialisation vectors (IV), and insures the integrity of the messages passed through MIC (Message Integrity Check) using TKIP (Temporal Key Integrity Protocol) to enhance data encryption.
- WPA-Pre-Shared Key (WPA-PSK)
  - WPA-PSK is a special mode of WPA for home users without an enterprise authentication server and provides the same strong encryption protection.
- 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).

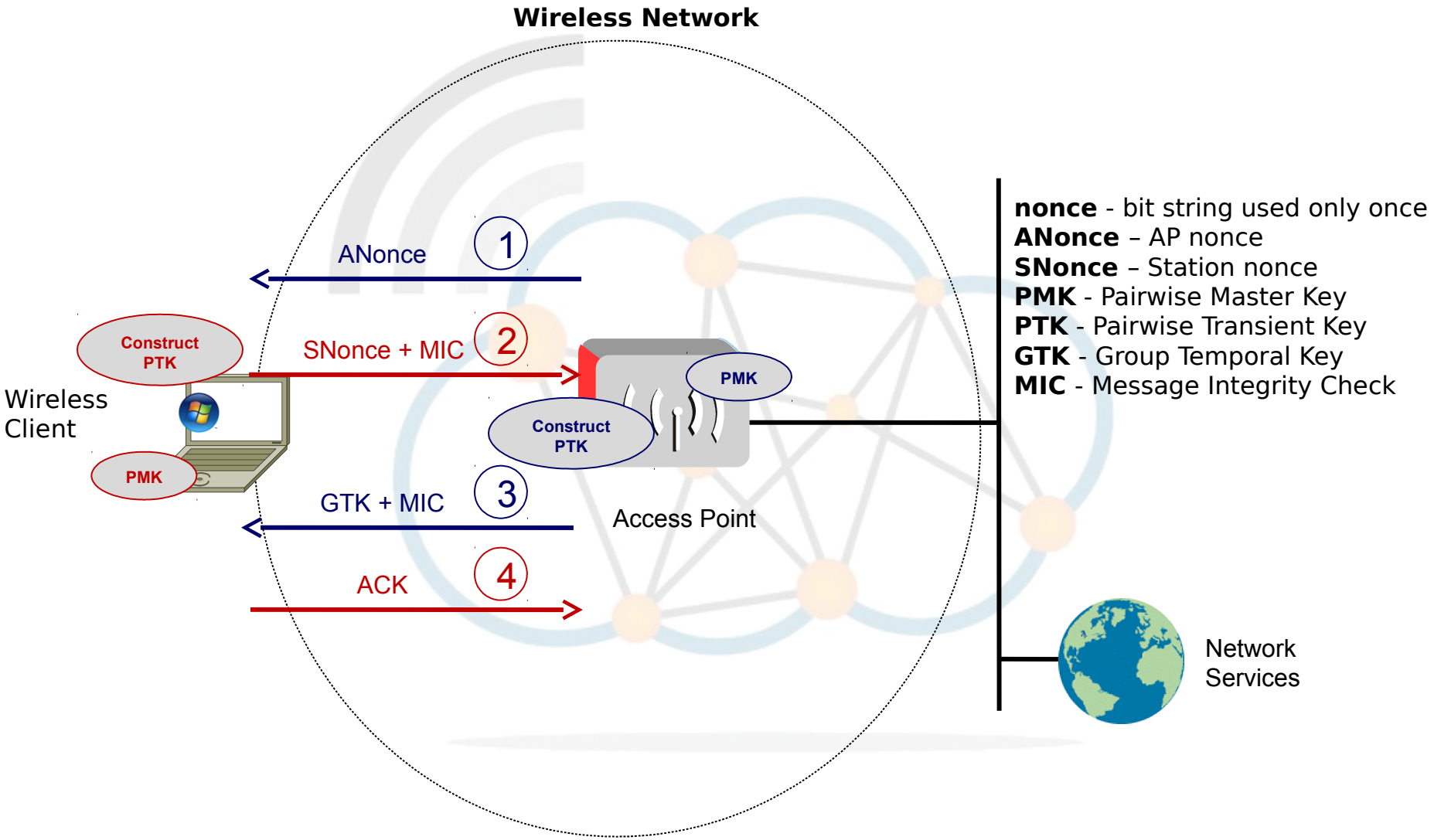
802.11i WPA2

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

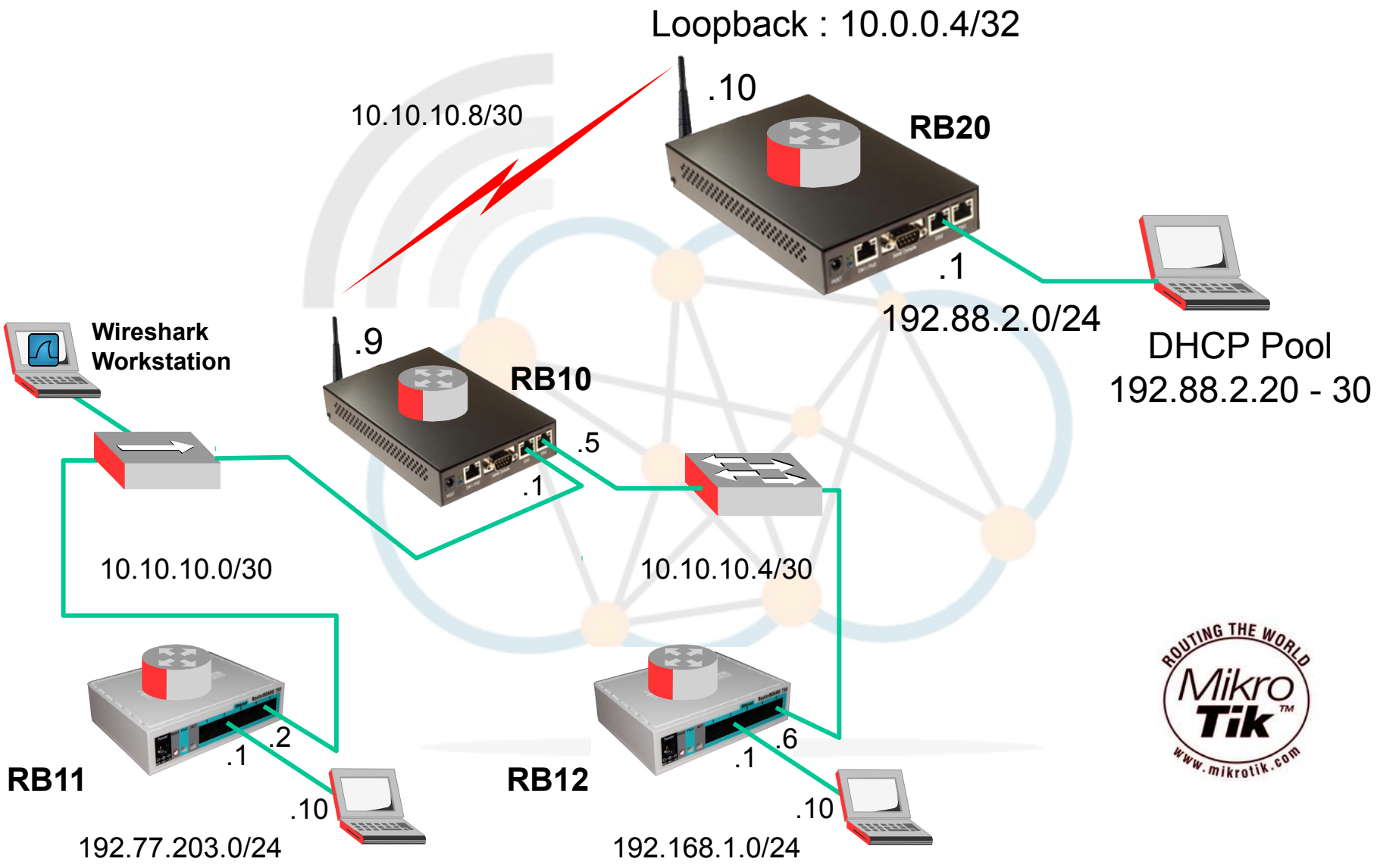
802.1x


Wireless Network
Wireless Client
(Supplicant)
1
802.1X
2
EAP
Authentication
Server
(RADIUS)
Access Point
3
Wireless Client
(Supplicant)
Network
Services

802.11i WPA2


Wireless Network
ANonce
1
SNonce + MIC
2
GTK + MIC
3
ACK
4
Construct PTK
PMK
Wireless Client
Construct PTK
PMK
Access Point
nonce - bit string used only once
ANonce – AP nonce
SNonce – Station nonce
PMK - Pairwise Master Key
PTK - Pairwise Transient Key
GTK - Group Temporal Key
MIC - Message Integrity Check
Network Services

Wireless Network Diagram



Configure RB10 Wireless interface

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

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

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

[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**

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

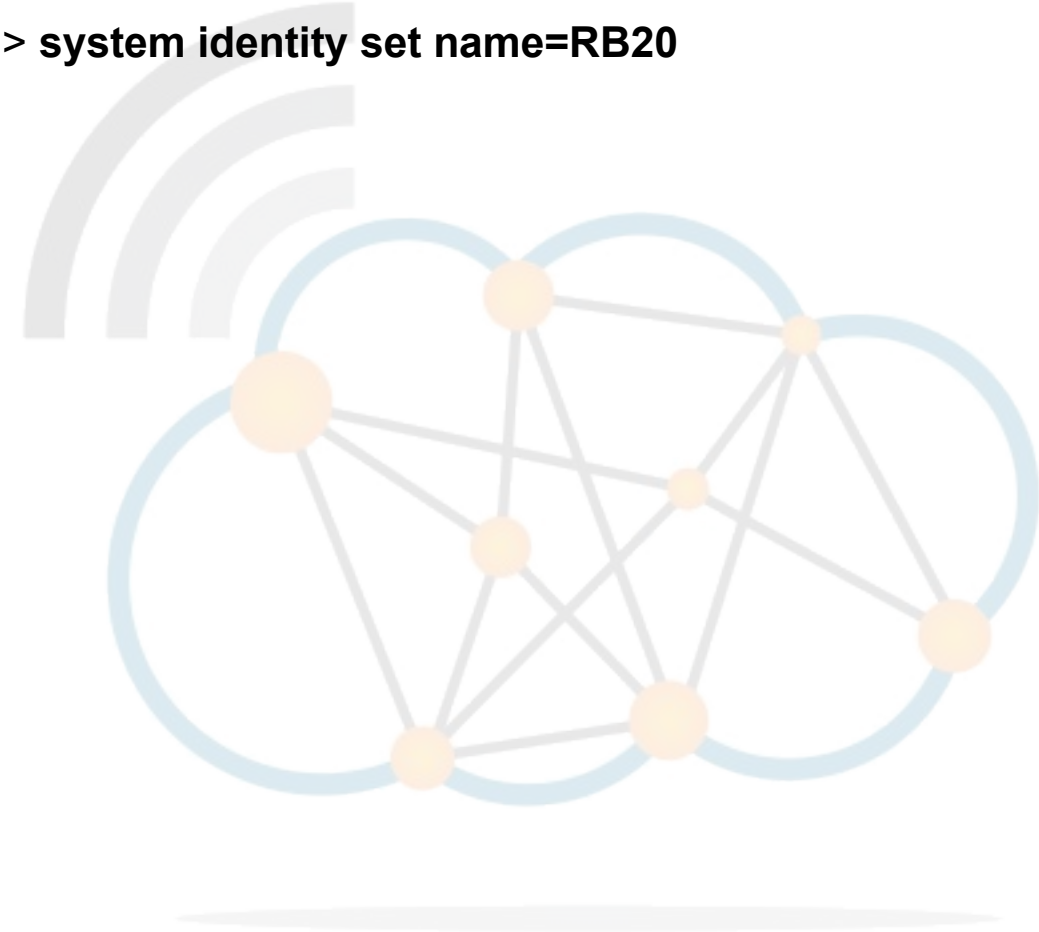
[admin@RB10] > **ip address add address=10.10.10.9/30 interface=wlan1**

Configure RB10 OSPF additional network

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

Configure RB20 Identity

[admin@MikroTik] > **system identity set name=RB20**



Configure RB20 LAN Interface

[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**

Configure RB20 Loopback interface

[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**

Configure RB20 Wireless interface

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

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

[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 security-profile=OB_Sec_Profile**

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

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

Configure RB20 OSPF

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

[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**

Testing

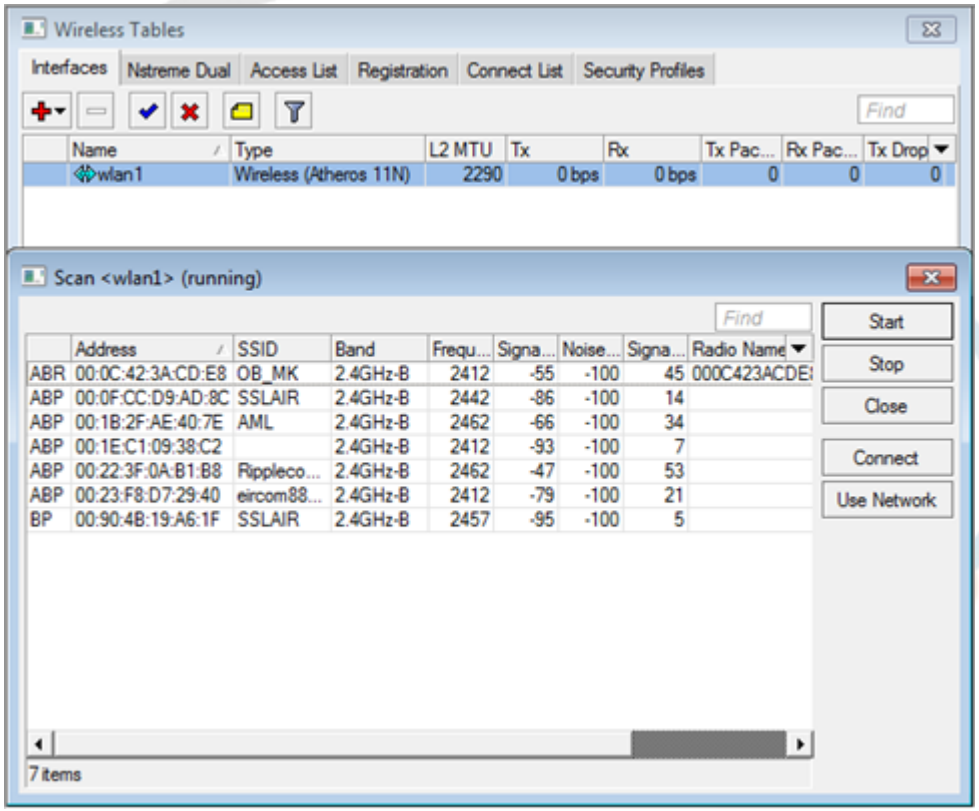
- Ping, Traceroute from workstation to workstation.
- Use wireshark to sniff traffic on the hub, observe the OSPF messages.
- Use MikroTik Packet Sniffer to review packets in and out of each router.

Scanning Wireless networks

```
[admin@RB20] > interface wireless scan 0
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
 BP   C4:7D:4F:C7:25:A0 SSLAIR           2.4ghz-b   2422 -94 -101 7
-- [Q quit|D dump|C-z pause]
```

5200-5245

Scanning Wireless networks



Scanning Wireless networks

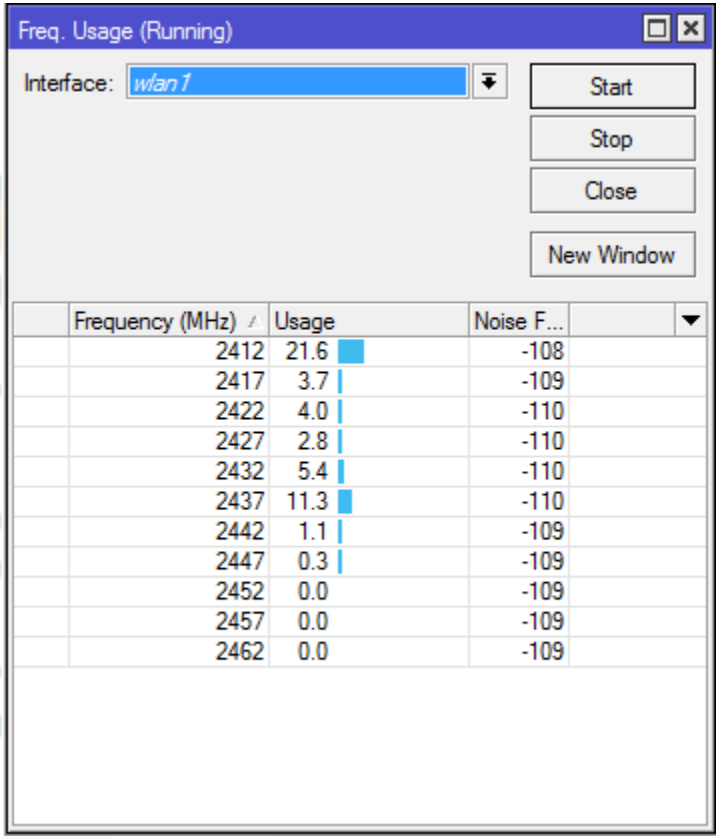
- It may be necessary to reduce the scan-list to the area of interest.
- In the 5 GHz band the default steps are 20 MHz but you may want 5 GHz steps when troubleshooting.

```
[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]
```

Frequency Monitor

[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



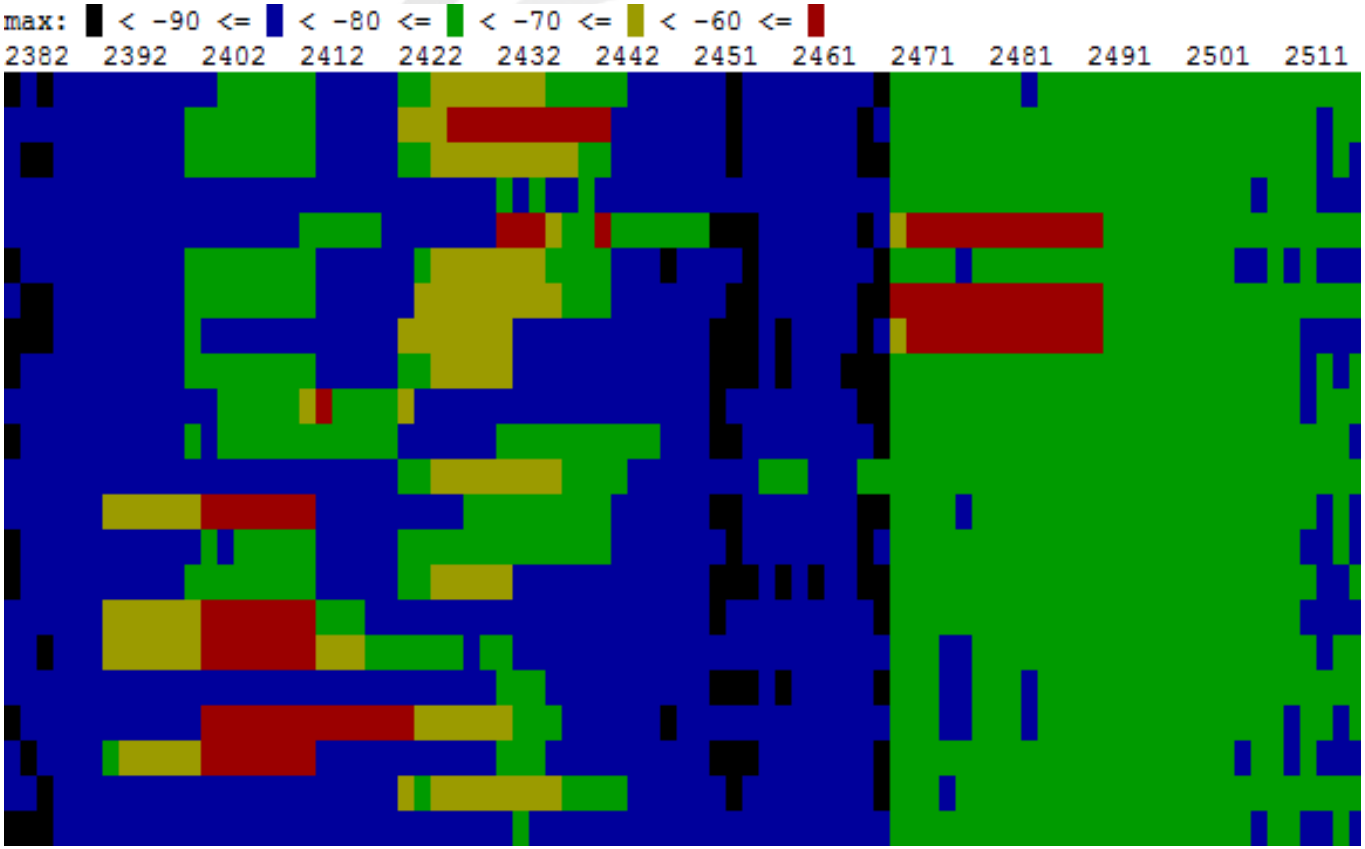
Spectral Scan

[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]
```

Spectral History

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



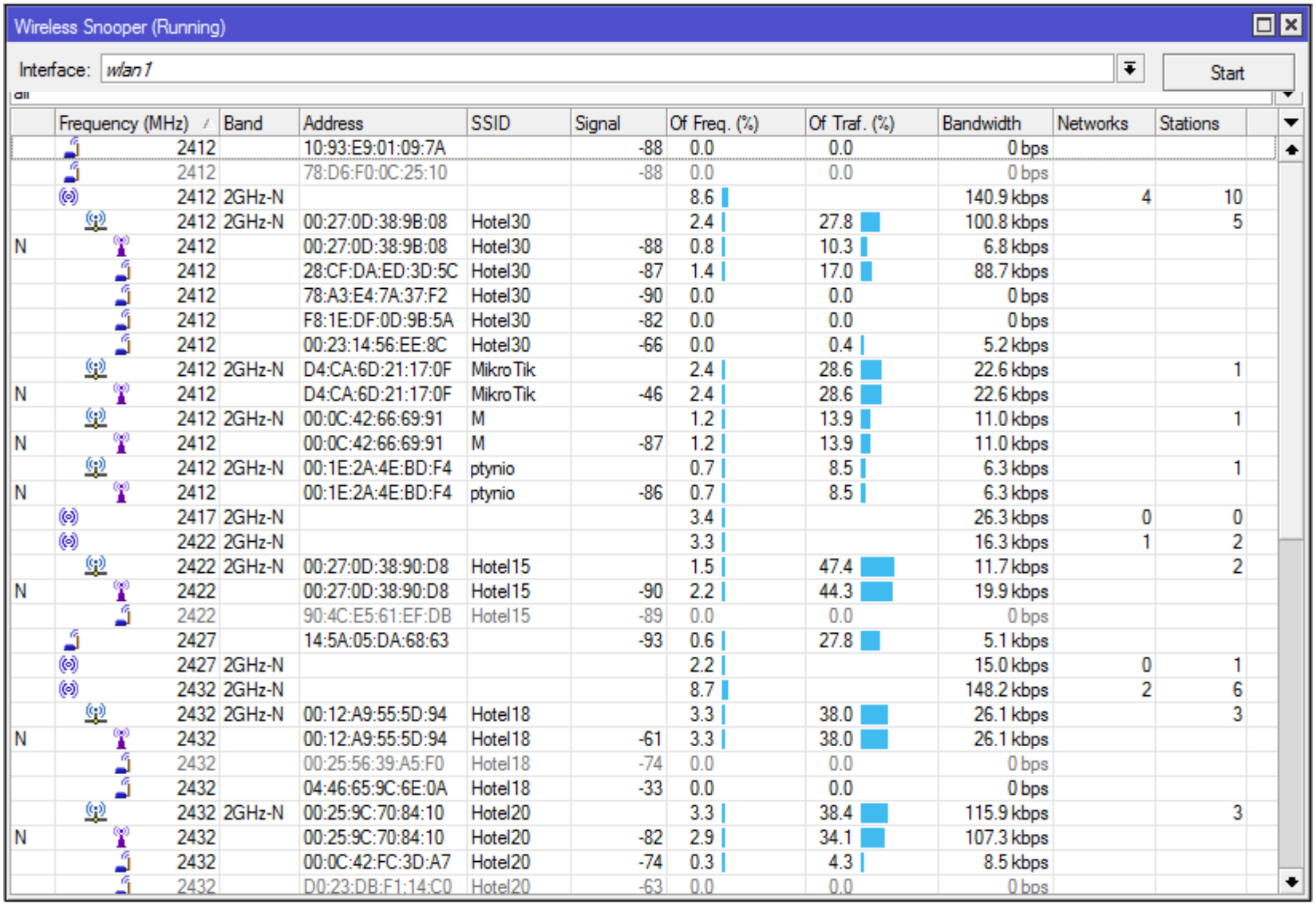
Wireless Snooper

[admin@RB20] > **interface wireless snooper 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]

Wireless Snooper



	Frequency (MHz)	Band	Address	SSID	Signal	Of Freq. (%)	Of Traf. (%)	Bandwidth	Networks	Stations
	2412		10:93:E9:01:09:7A		-88	0.0	0.0	0 bps		
	2412		78:D6:F0:0C:25:10		-88	0.0	0.0	0 bps		
	2412	2GHz-N				8.6		140.9 kbps	4	10
	2412	2GHz-N	00:27:0D:38:9B:08	Hotel30		2.4	27.8	100.8 kbps		5
N	2412		00:27:0D:38:9B:08	Hotel30	-88	0.8	10.3	6.8 kbps		
	2412		28:CF:DA:ED:3D:5C	Hotel30	-87	1.4	17.0	88.7 kbps		
	2412		78:A3:E4:7A:37:F2	Hotel30	-90	0.0	0.0	0 bps		
	2412		F8:1E:DF:0D:9B:5A	Hotel30	-82	0.0	0.0	0 bps		
	2412		00:23:14:56:EE:8C	Hotel30	-66	0.0	0.4	5.2 kbps		
	2412	2GHz-N	D4:CA:6D:21:17:0F	MikroTik		2.4	28.6	22.6 kbps		1
N	2412		D4:CA:6D:21:17:0F	MikroTik	-46	2.4	28.6	22.6 kbps		
	2412	2GHz-N	00:0C:42:66:69:91	M		1.2	13.9	11.0 kbps		1
N	2412		00:0C:42:66:69:91	M	-87	1.2	13.9	11.0 kbps		
	2412	2GHz-N	00:1E:2A:4E:BD:F4	ptynio		0.7	8.5	6.3 kbps		1
N	2412		00:1E:2A:4E:BD:F4	ptynio	-86	0.7	8.5	6.3 kbps		
	2417	2GHz-N				3.4		26.3 kbps	0	0
	2422	2GHz-N				3.3		16.3 kbps	1	2
	2422	2GHz-N	00:27:0D:38:90:D8	Hotel15		1.5	47.4	11.7 kbps		2
N	2422		00:27:0D:38:90:D8	Hotel15	-90	2.2	44.3	19.9 kbps		
	2422		90:4C:E5:61:EF:DB	Hotel15	-89	0.0	0.0	0 bps		
	2427		14:5A:05:DA:68:63		-93	0.6	27.8	5.1 kbps		
	2427	2GHz-N				2.2		15.0 kbps	0	1
	2432	2GHz-N				8.7		148.2 kbps	2	6
	2432	2GHz-N	00:12:A9:55:5D:94	Hotel18		3.3	38.0	26.1 kbps		3
N	2432		00:12:A9:55:5D:94	Hotel18	-61	3.3	38.0	26.1 kbps		
	2432		00:25:56:39:A5:F0	Hotel18	-74	0.0	0.0	0 bps		
	2432		04:46:65:9C:6E:0A	Hotel18	-33	0.0	0.0	0 bps		
	2432	2GHz-N	00:25:9C:70:84:10	Hotel20		3.3	38.4	115.9 kbps		3
N	2432		00:25:9C:70:84:10	Hotel20	-82	2.9	34.1	107.3 kbps		
	2432		00:0C:42:FC:3D:A7	Hotel20	-74	0.3	4.3	8.5 kbps		
	2432		D0:23:DB:F1:14:C0	Hotel20	-63	0.0	0.0	0 bps		

Wireless Debugging

[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
```

[admin@RB20] > **log print detail**
[admin@RB20] > **log print brief**
[admin@RB20] > **log print terse**
[admin@RB20] > **log print follow where topics~"wireless"**

Thank You

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com