CMP3214
Computer Communication Networks

Lecture 8

Wireless LAN (WLAN)

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Wireless LANs

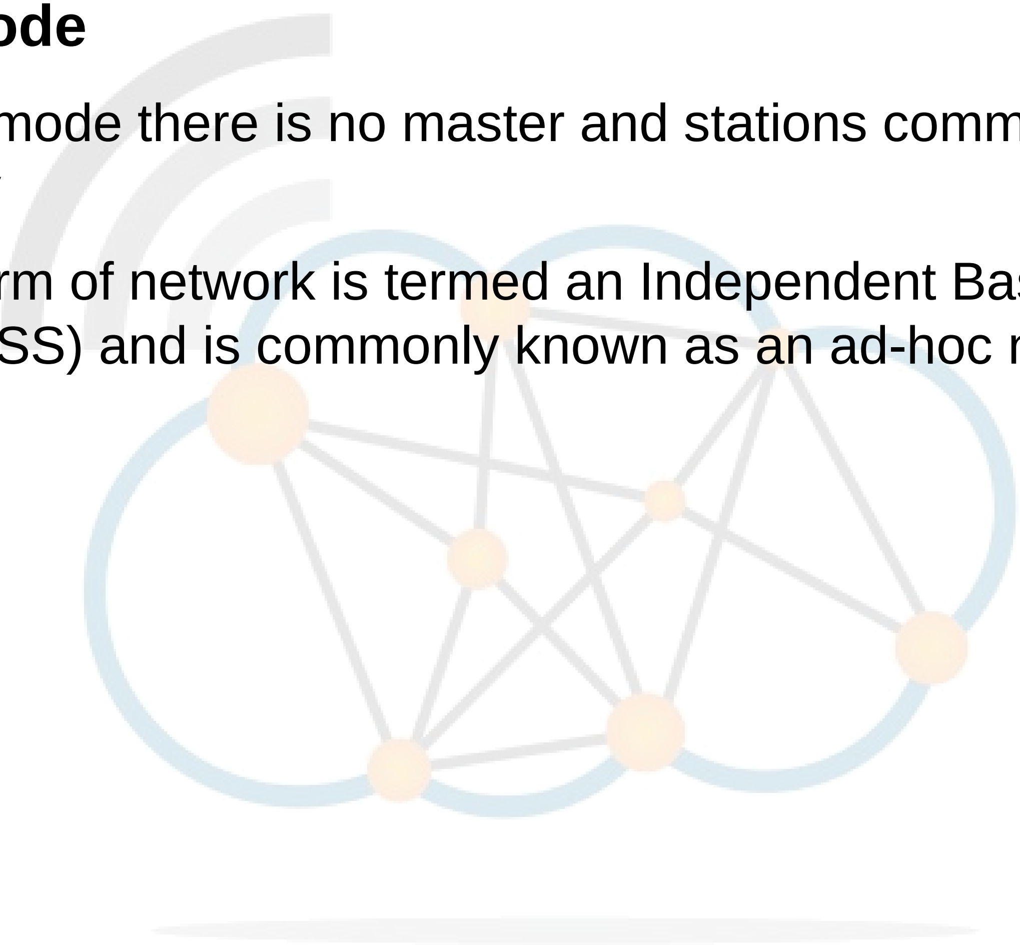
- Wireless LANs are over-the-air modulation techniques that use the same basic protocol to create a wireless LAN.
- The most popular are those defined by the 802.11b and 802.11g protocols.
- 802.11n is a new multi-streaming modulation technique that is still under draft development, but products based on its proprietary pre-draft versions are being sold.
- 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

- **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.
  - An Extended Service Set (ESS) is one or more interconnected BSSs and their associated LANs. To the logical link control layer the ESS appears as a solitary BSS at any one of the STAs.

Wi-Fi Structure

- **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
  - 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).
- 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.

802.11 Variants

- 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.
- 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.

802.11 Variants

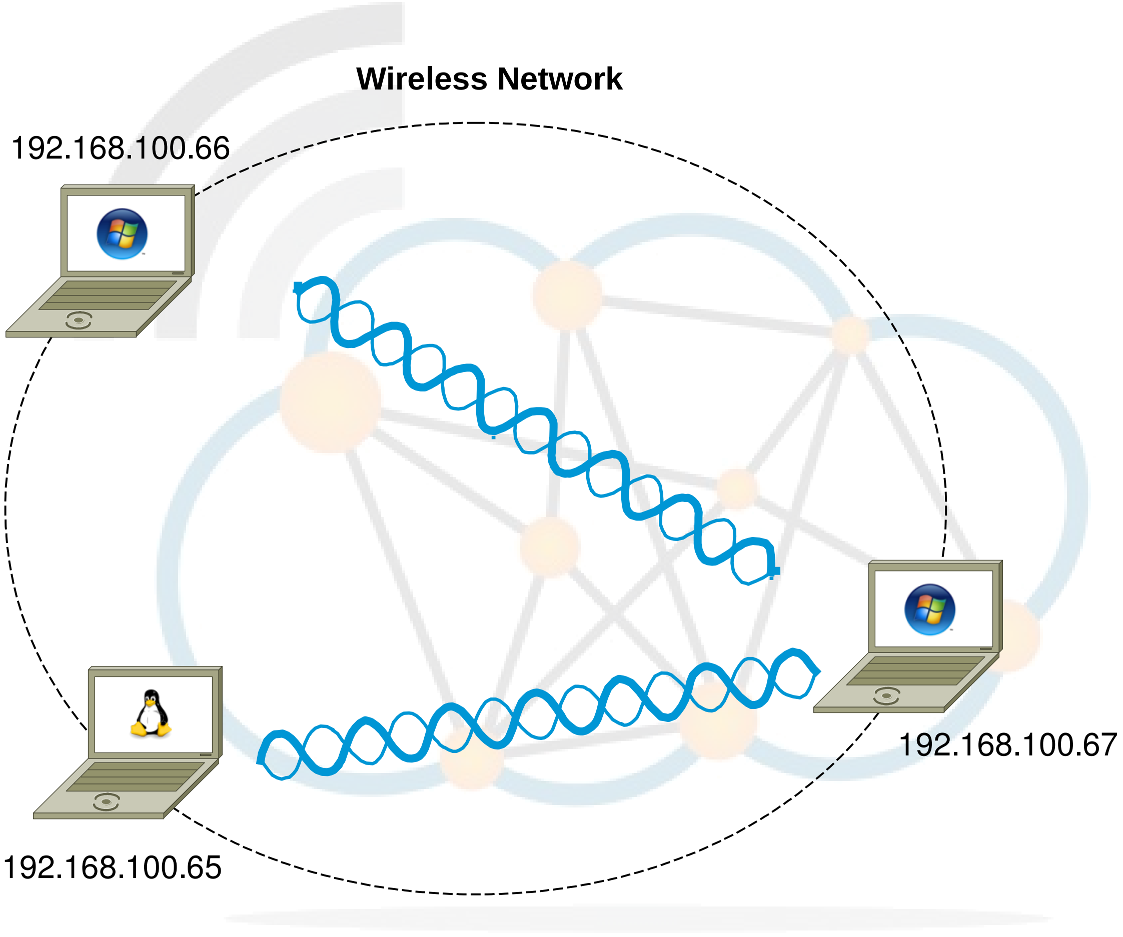
- 802.11n
  - New standard to give typically 200 Mbps to a maximum of 540 Mbps out to 50 M in either the 2.4 or 5 GHz bands. It uses Multiple In, Multiple Out (MiMo) antennas.
- 802.11ac
  - The latest standard which gives multi-station WLAN throughput of at least 1 Gb/s and a single link throughput 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.

Establish an Ad-hoc network

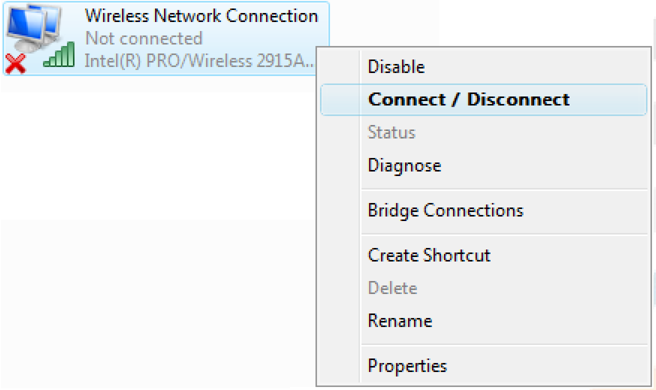
Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

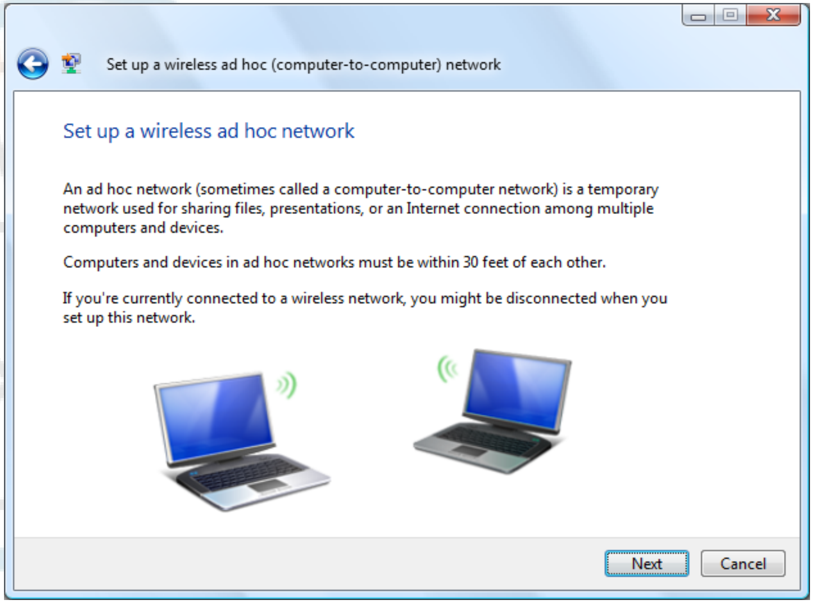
Ad-hoc network



Setting up the Wireless ad hoc network



Start → Settings → Network Connections

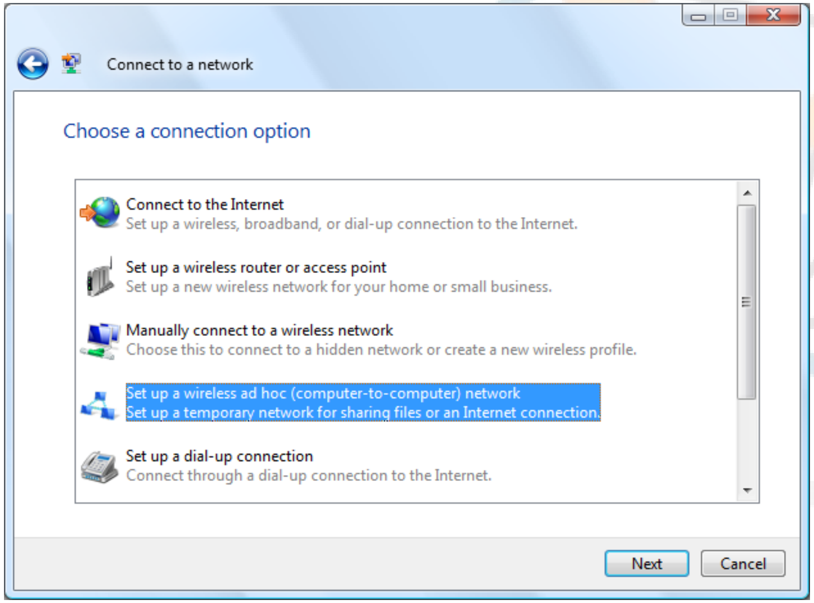

Set up a wireless ad hoc (computer-to-computer) network

Set up a wireless ad hoc network

An ad hoc network (sometimes called a computer-to-computer network) is a temporary network used for sharing files, presentations, or an Internet connection among multiple computers and devices.

Computers and devices in ad hoc networks must be within 30 feet of each other.

If you're currently connected to a wireless network, you might be disconnected when you set up this network.


Connect to a network

Choose a connection option

Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

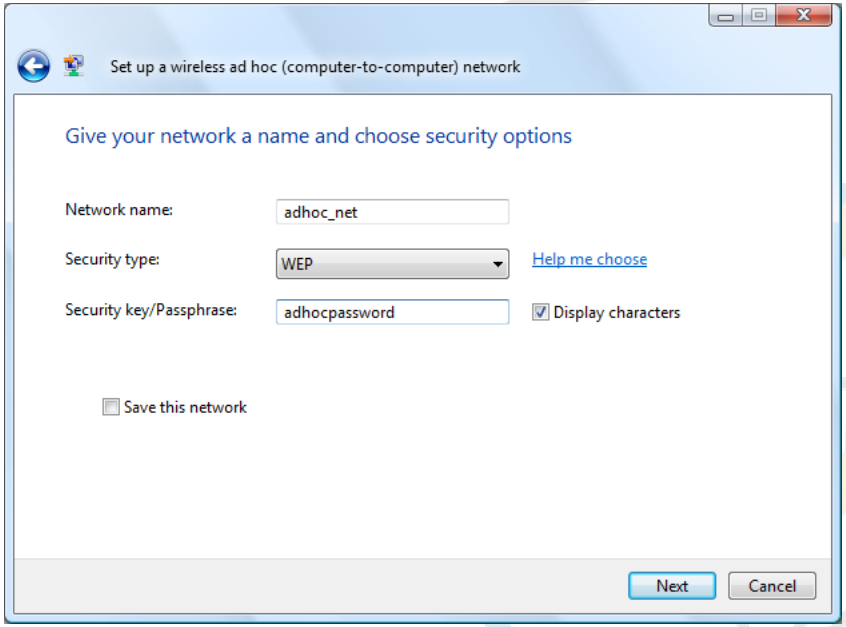
Set up a wireless router or access point
Set up a new wireless network for your home or small business.

Manually connect to a wireless network
Choose this to connect to a hidden network or create a new wireless profile.

Set up a wireless ad hoc (computer-to-computer) network
Set up a temporary network for sharing files or an Internet connection.

Set up a dial-up connection
Connect through a dial-up connection to the Internet.

Setting up the Wireless ad hoc network



Set up a wireless ad hoc (computer-to-computer) network

Give your network a name and choose security options

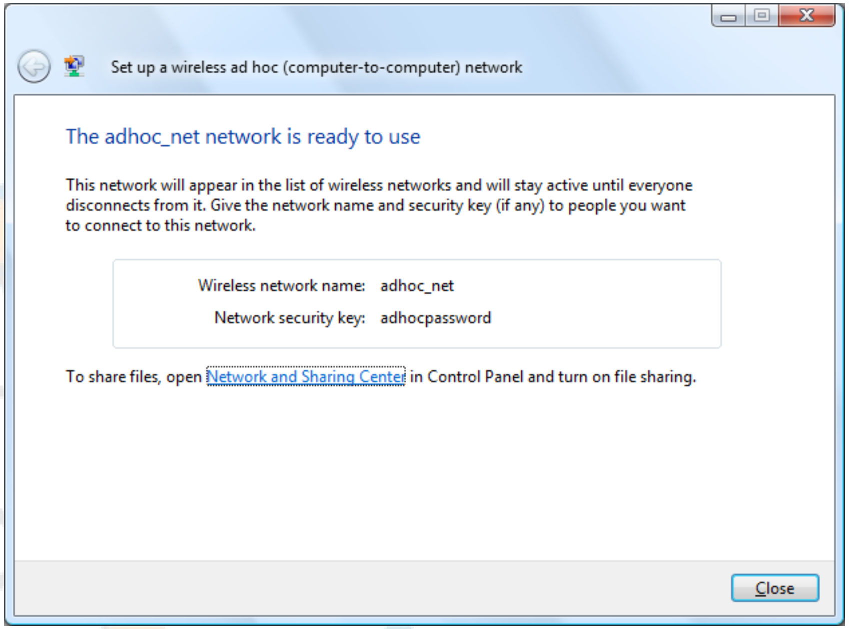
Network name: adhoc_net

Security type: WEP

Security key/Passphrase: adhocpassword

☑ Display characters

□ Save this network



Set up a wireless ad hoc (computer-to-computer) network

The adhoc_net network is ready to use

This network will appear in the list of wireless networks and will stay active until everyone disconnects from it. Give the network name and security key (if any) to people you want to connect to this network.

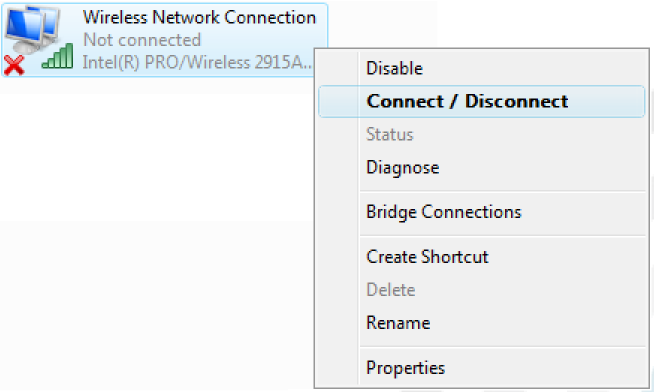
Wireless network name: adhoc_net

Network security key: adhocpassword

To share files, open Network and Sharing Center in Control Panel and turn on file sharing.

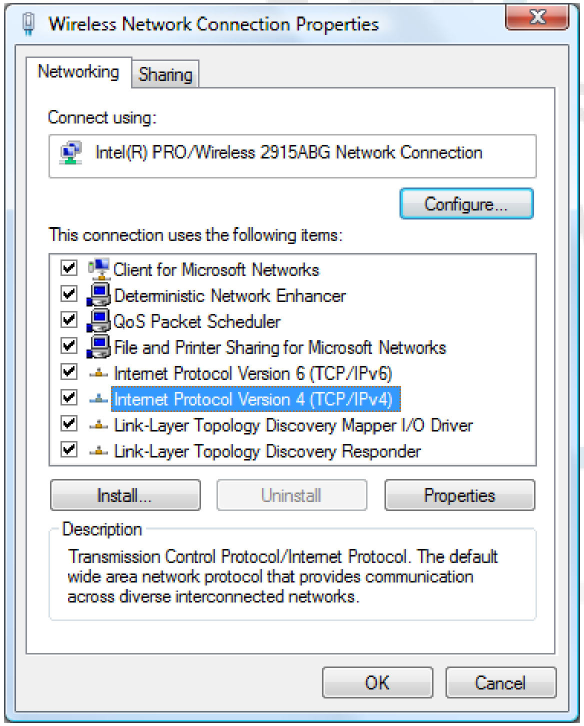
Network Name: **adhoc_net**
Security key/Passphrase: **adhocpassword**

Setting up the Wireless ad hoc network



Wireless Network Connection
Not connected
Intel(R) PRO/Wireless 2915A...

Start → Settings → Network Connections



Wireless Network Connection Properties

Connect using:

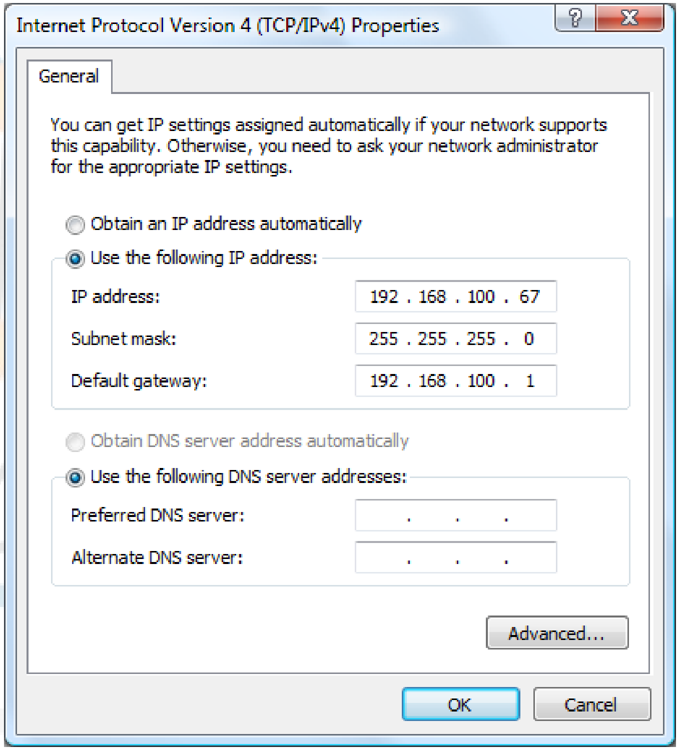
Intel(R) PRO/Wireless 2915ABG Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Deterministic Network Enhancer
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

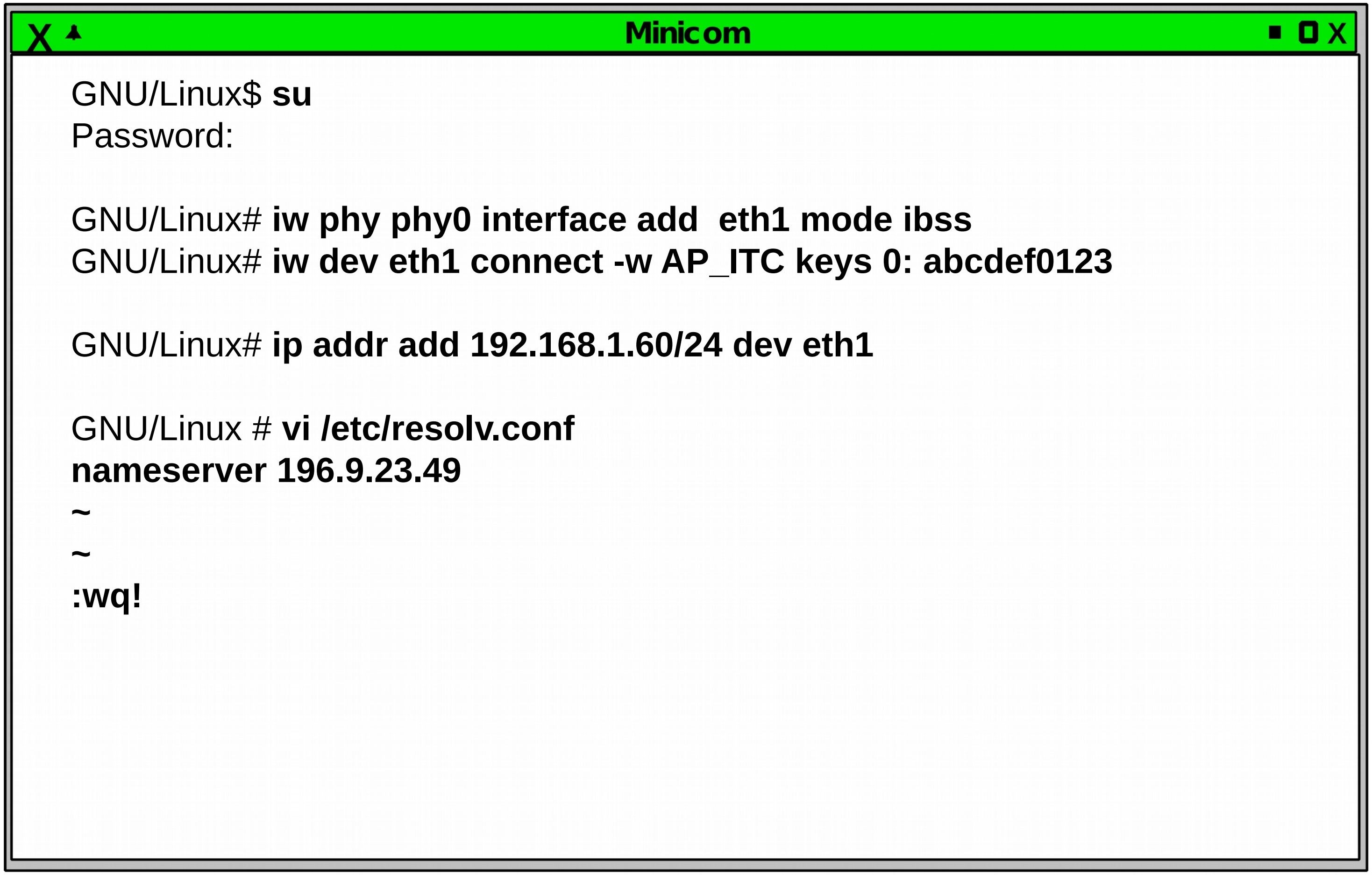
IP address:	192 . 168 . 100 . 67
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 100 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

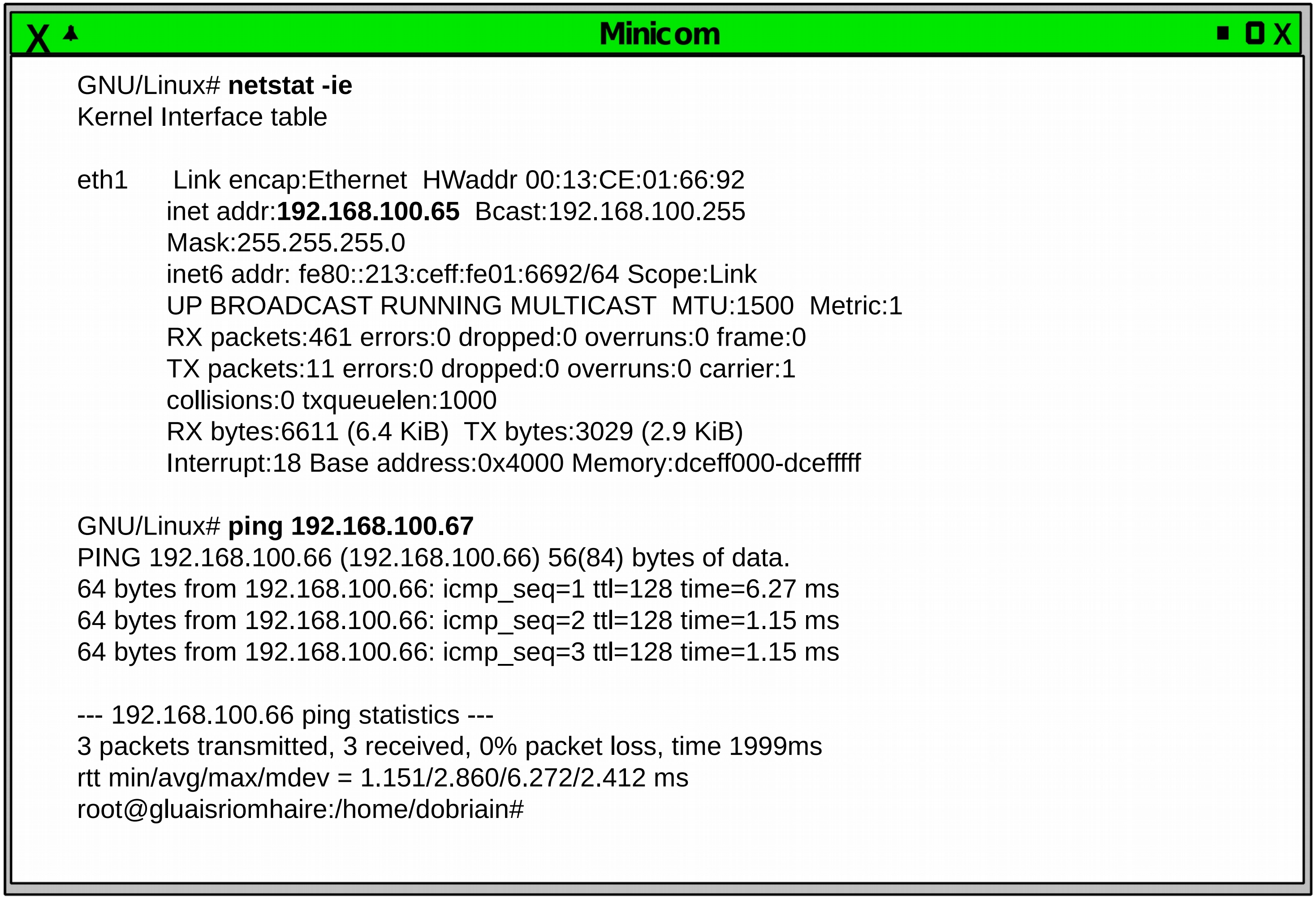
Preferred DNS server:	. . .
Alternate DNS server:	. . .

Setting up the Wireless ad hoc network



```
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

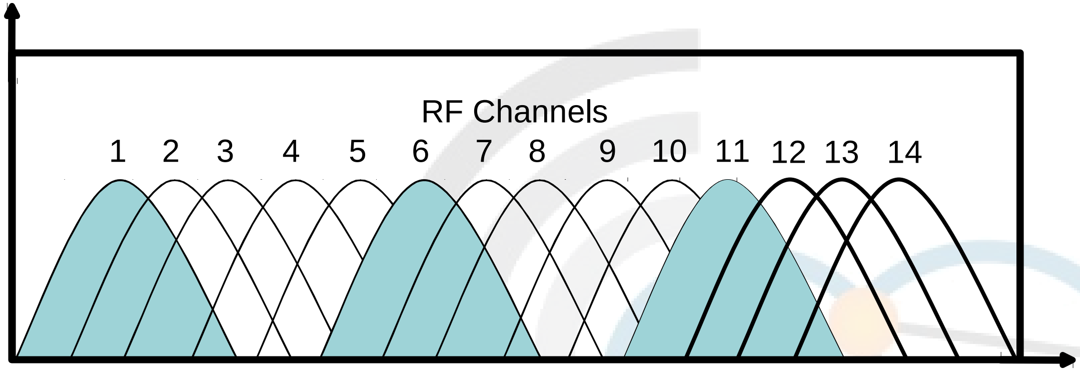


```
GNU/Linux# netstat -ie
Kernel Interface table

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

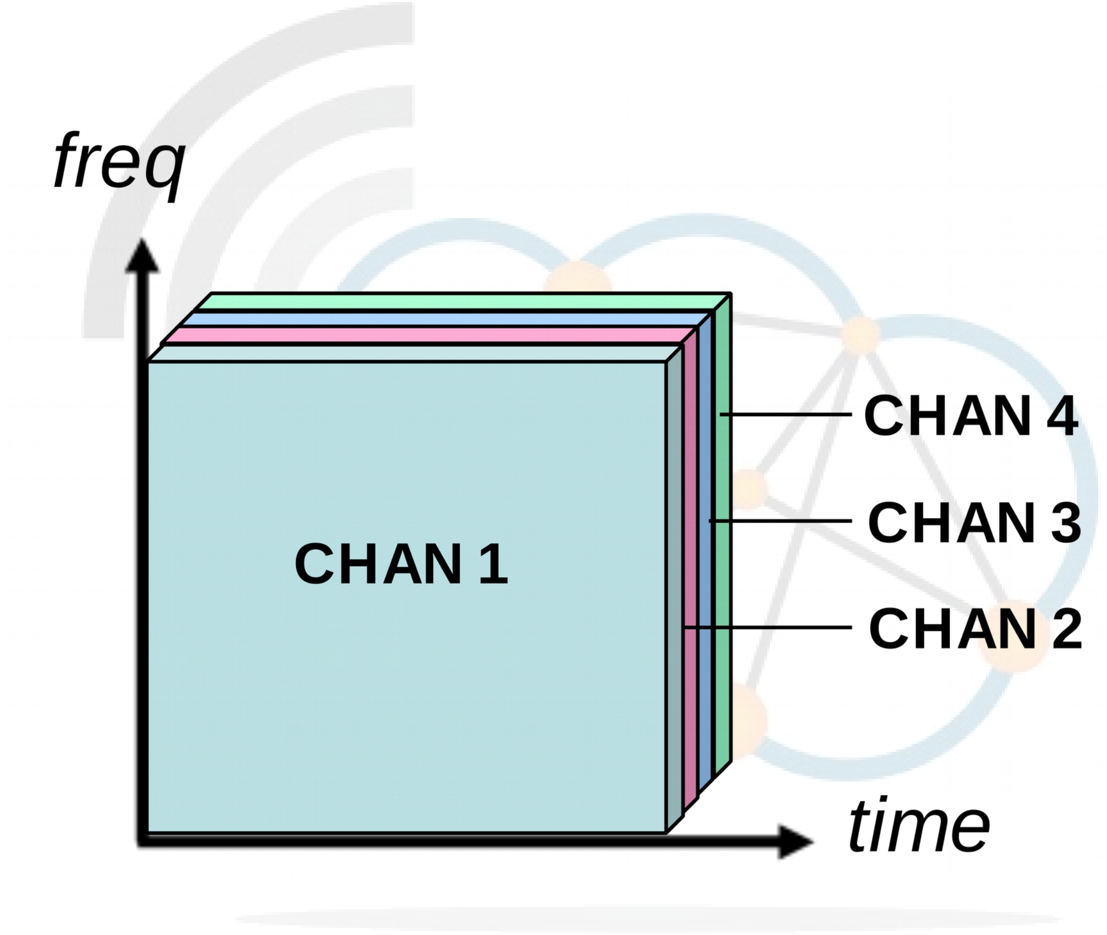


802.11b WiFi Channels

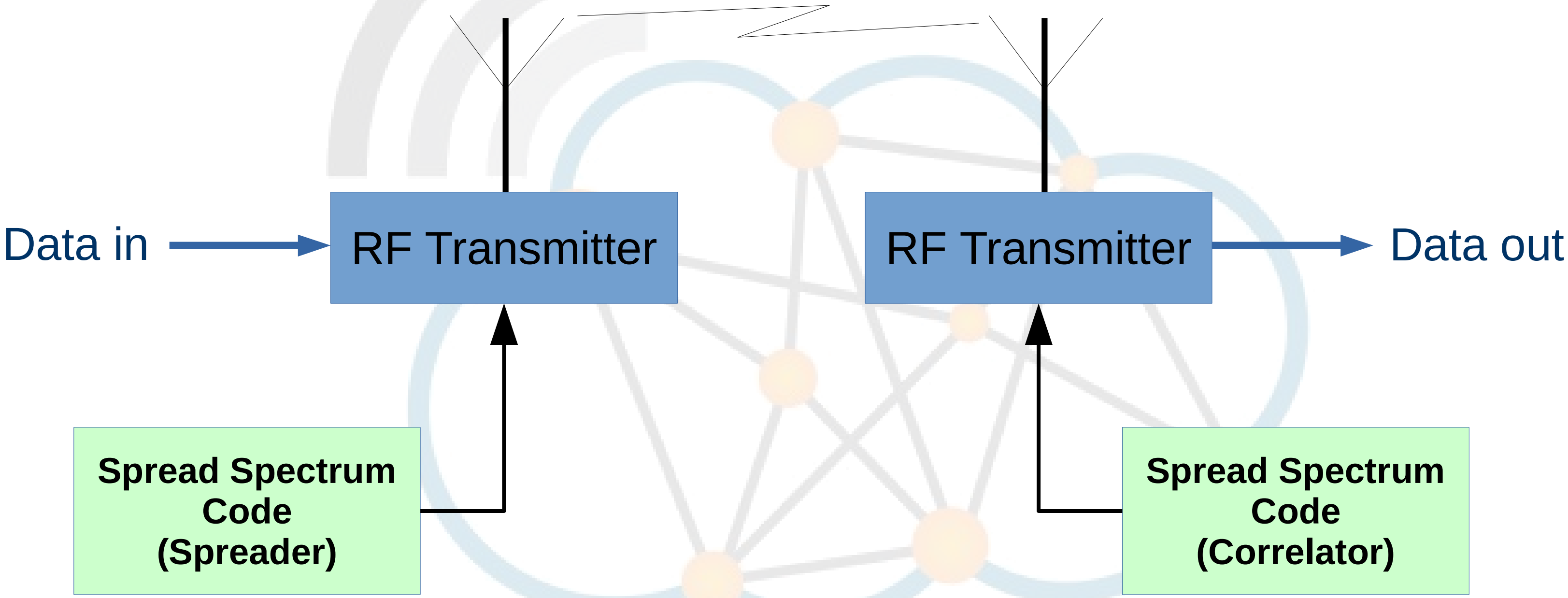
Channel	Lower Frequency (GHz)	Centre Frequency (GHz)	Upper Frequency (GHz)
1	2.401	2.412	2.423
2	2.404	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473
12	2.456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

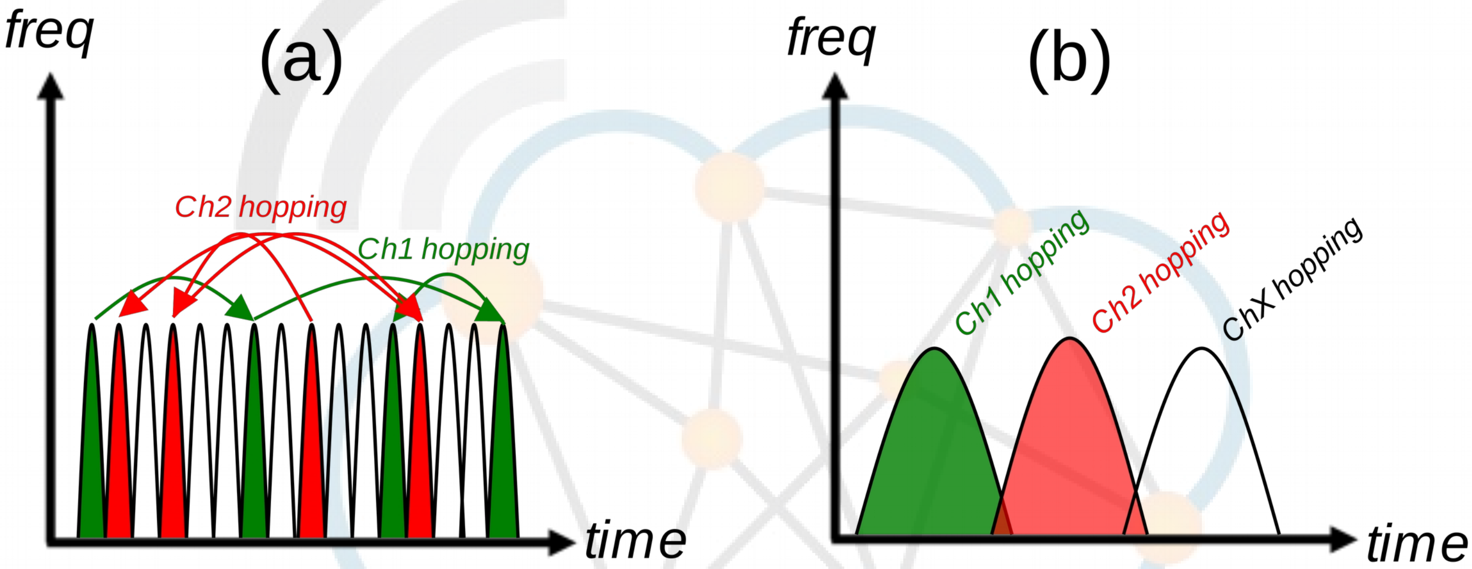
Spread spectrum



Spread spectrum

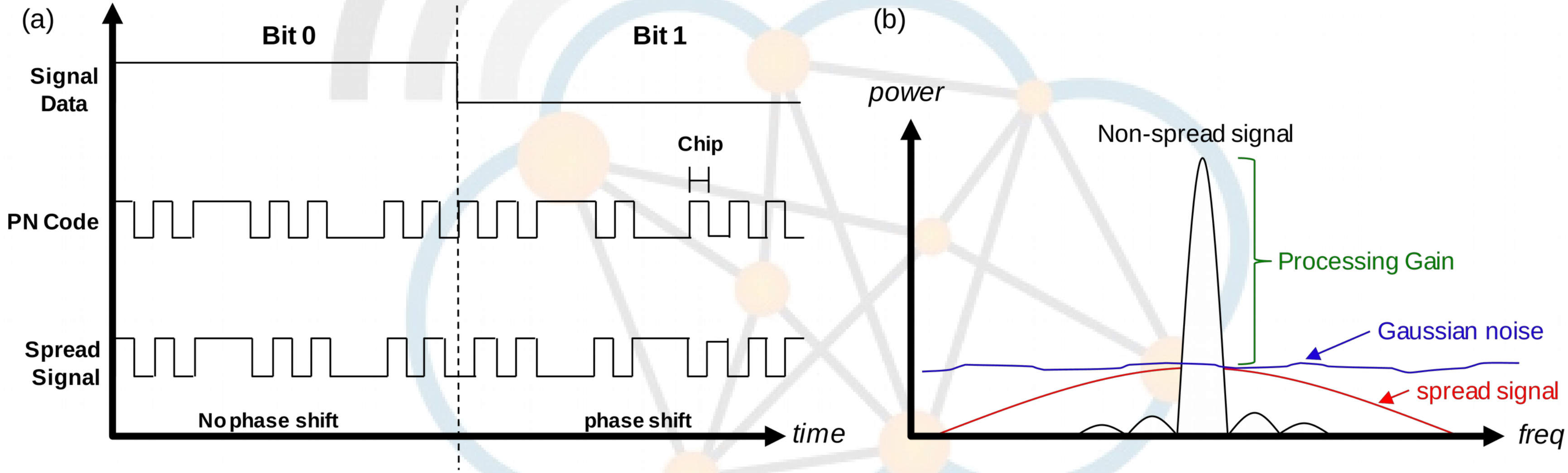

Data in
RF Transmitter
RF Transmitter
Data out
Spread Spectrum Code (Spreader)
Spread Spectrum Code (Correlator)

Spread spectrum



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

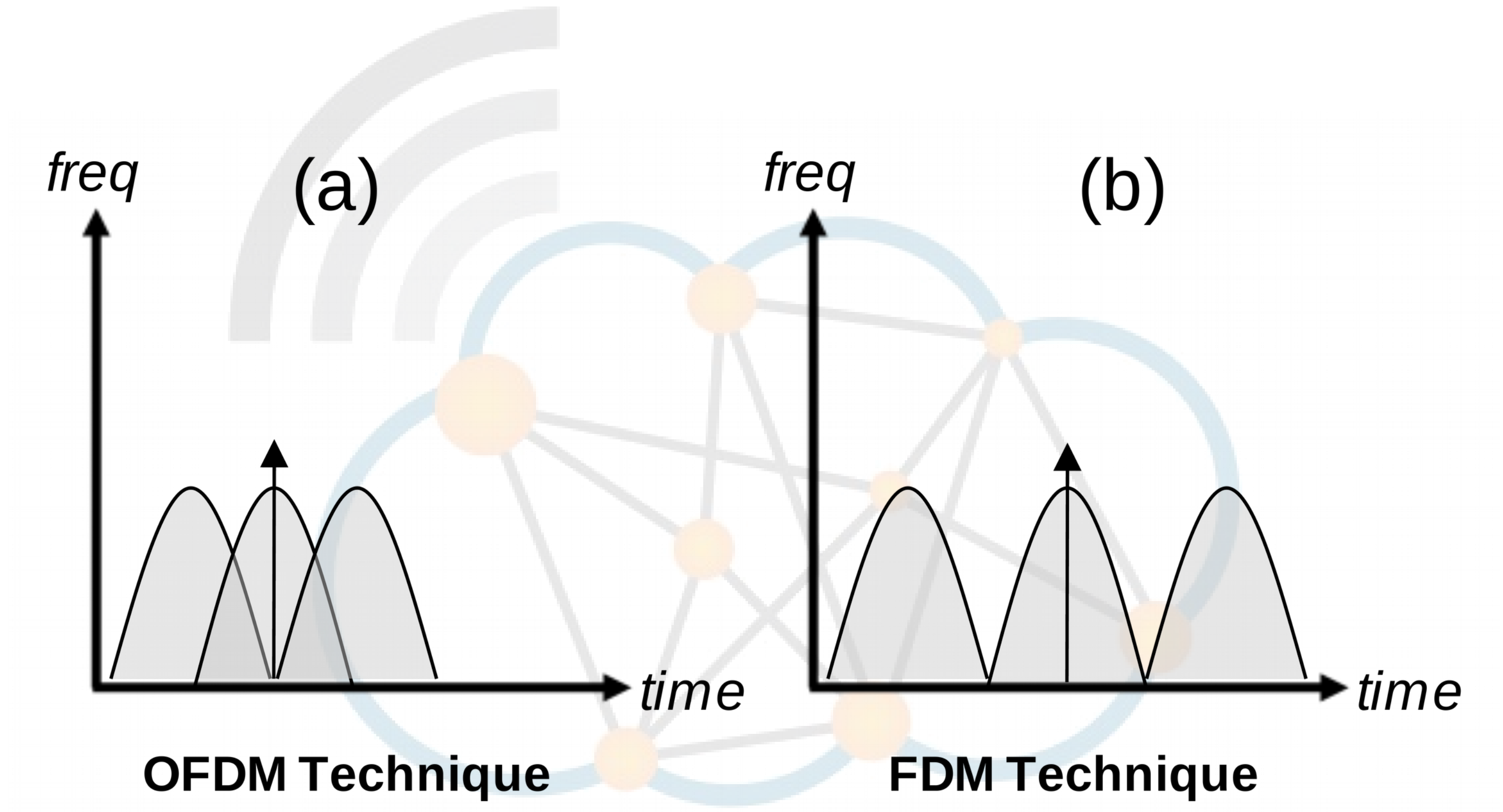
Spread spectrum



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 and inter-carrier guard bands are not required
  - BPSK, QPSK, 16-QAM, 64-QAM in each channel
  - 6, 9, 12, 18, 24, 36, 48, 54 Mb/s.

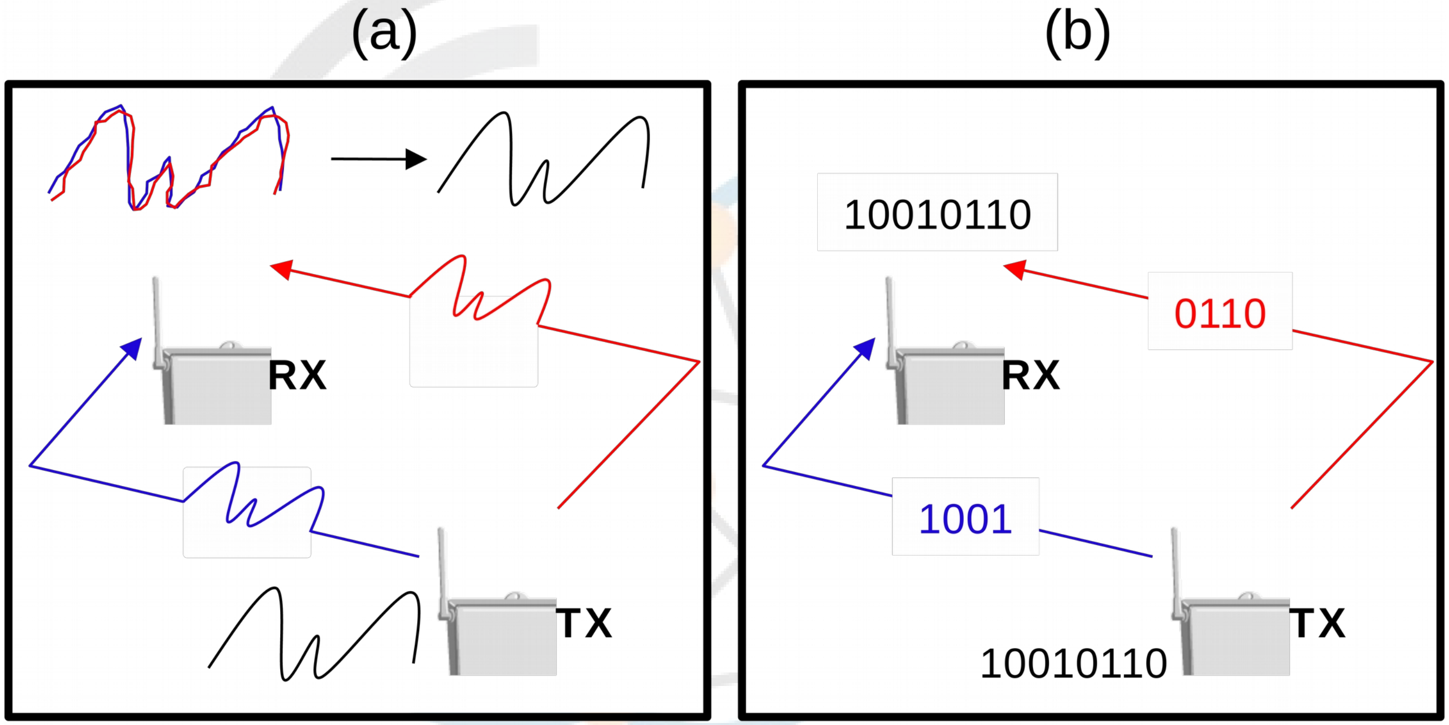
Orthogonal Frequency Division Multiplexing



OFDM Technique

FDM Technique

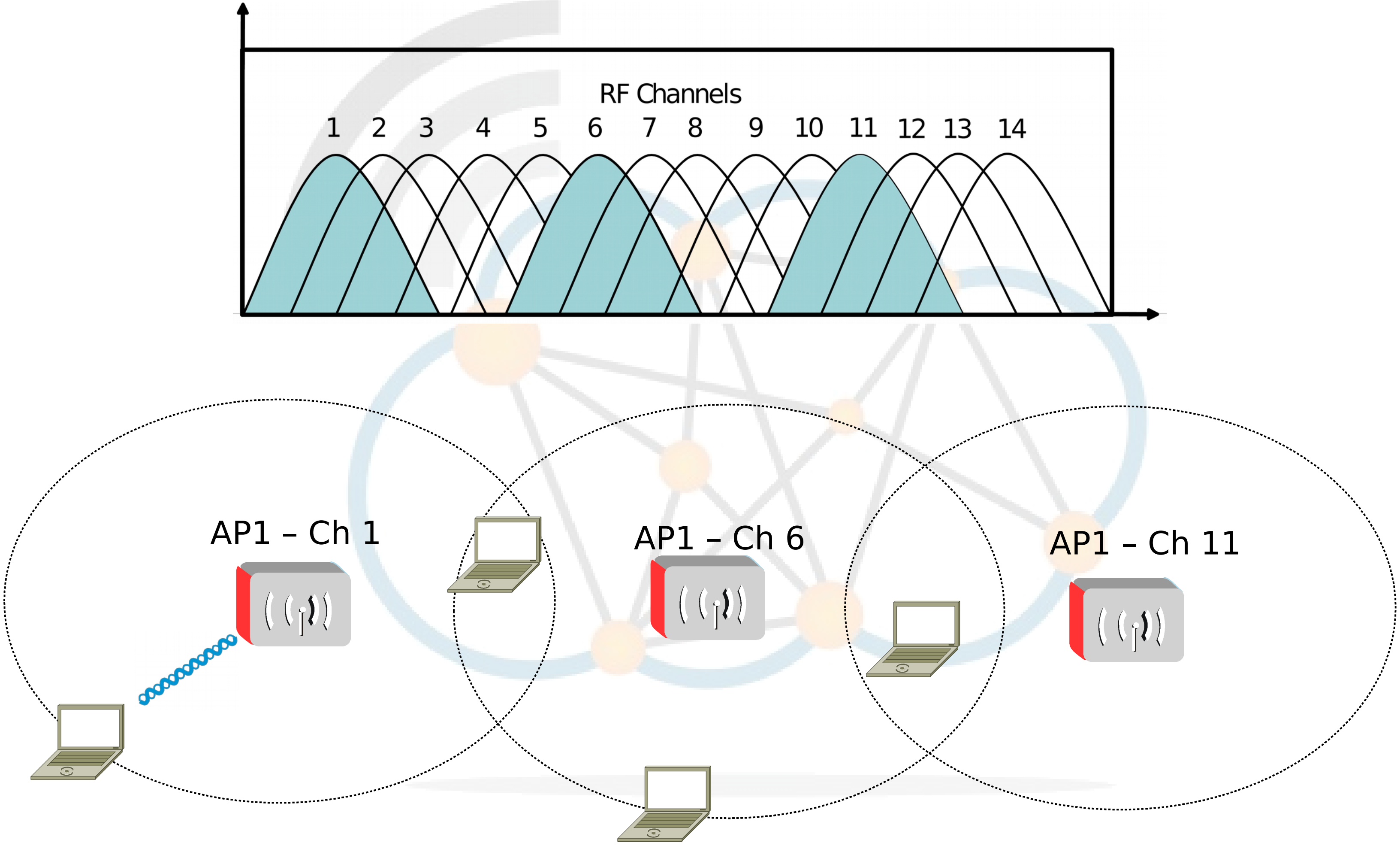
Multiple In, Multiple Out



Transmit-Receive Diversity

Spatial 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

- Fixed wireless access networks are typically 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.

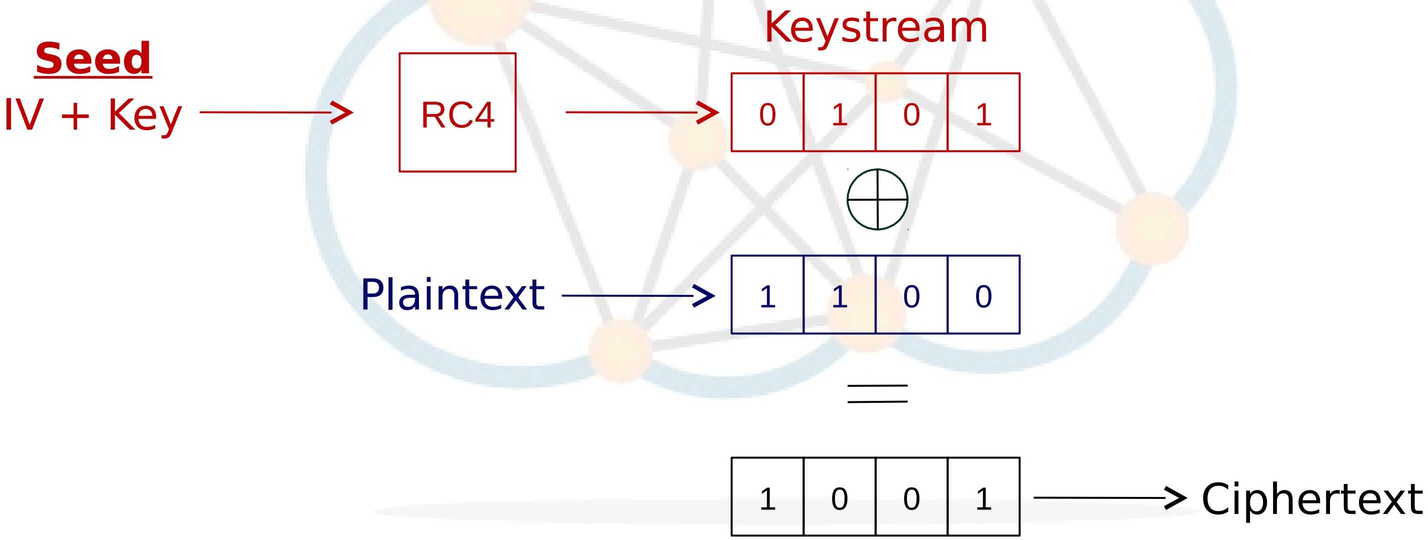
Steps in securing a wireless network

- 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.



Seed

IV + Key → RC4 → Keystream

0	1	0	1

$\oplus$

Plaintext →

1	1	0	0

=

1	0	0	1

→ Ciphertext

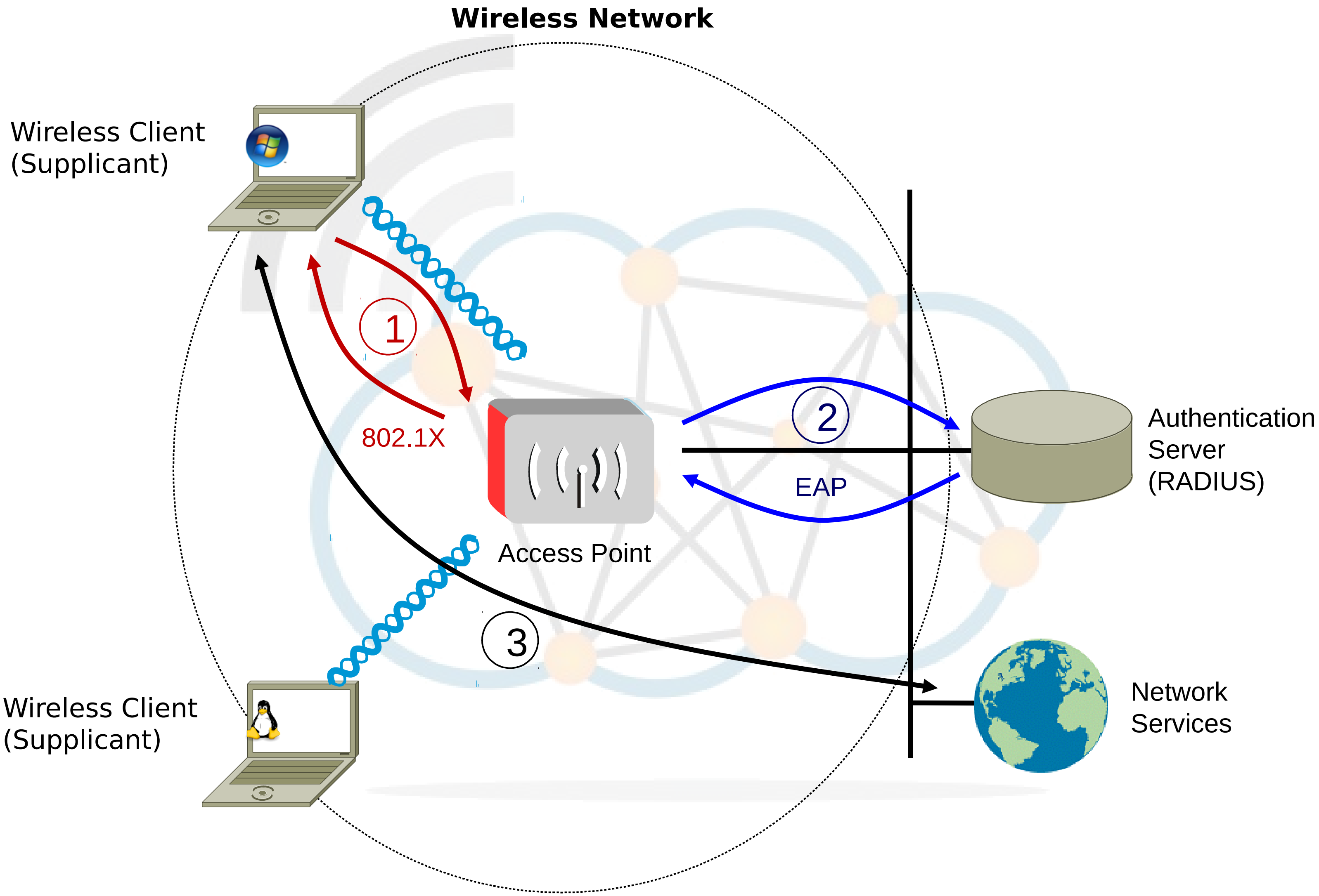
Wi-Fi Protected Access (WPA)

- 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).

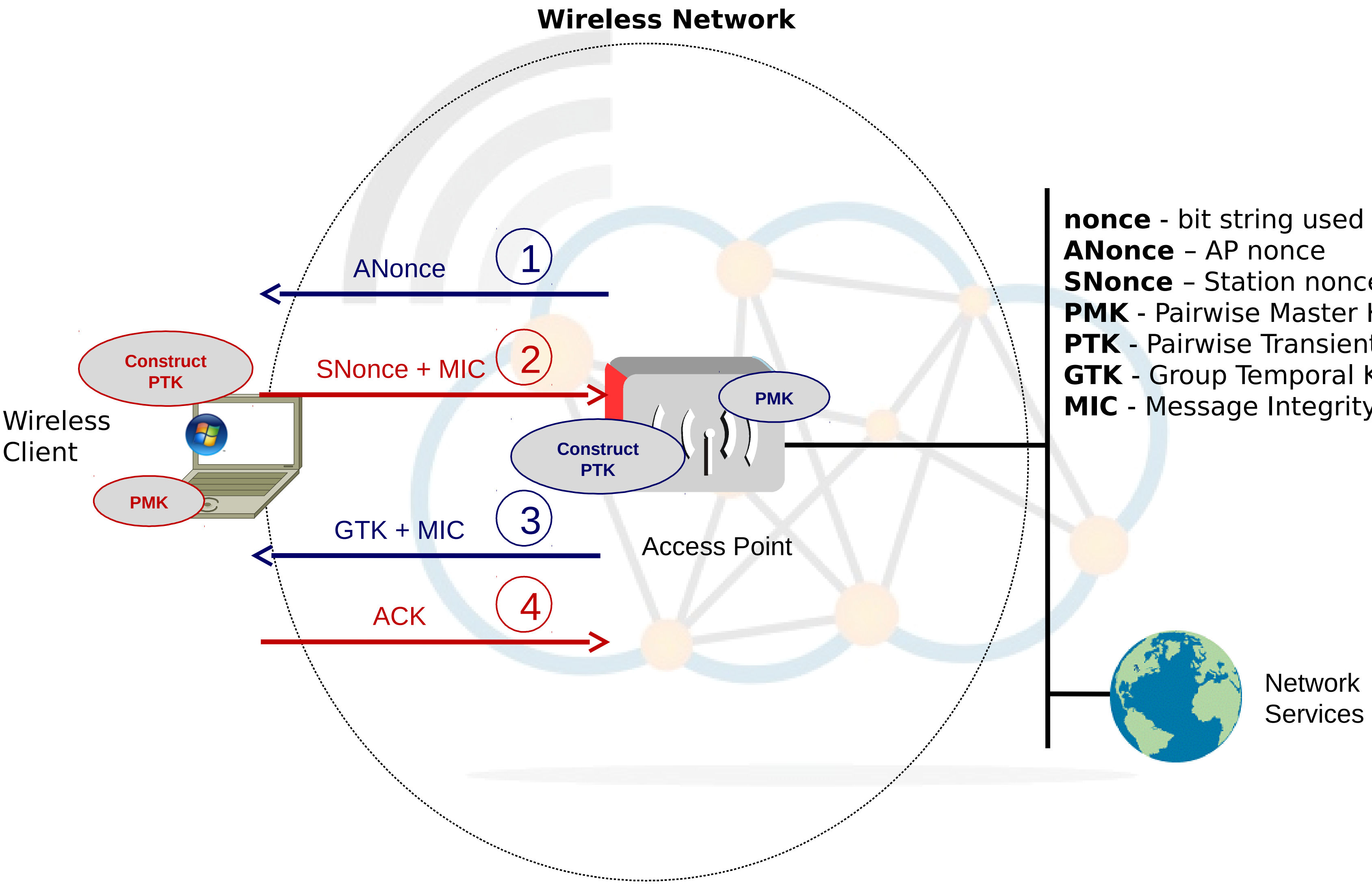
802.11i WPA2

- 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
Access Point
Authentication
Server
(RADIUS)
3
Wireless Client
(Supplicant)
Network
Services

802.11i WPA2



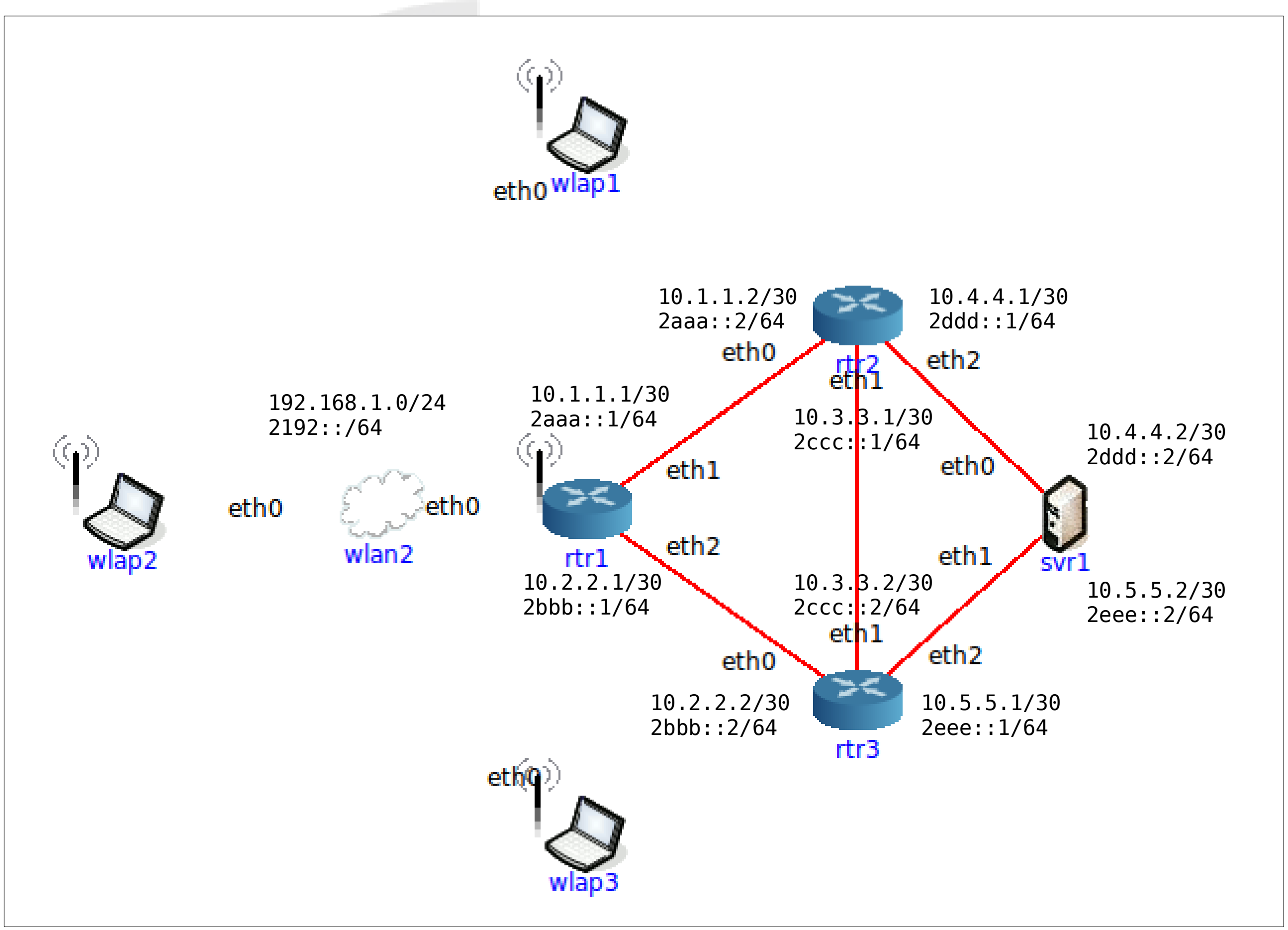
nonce - bit string used only once
ANonce – AP nonce
SNonce – Station nonce
PMK - Pairwise Master Key
PTK - Pairwise Transient Key
GTK - Group Temporal Key
MIC - Message Integrity Check

WLAN Configuration

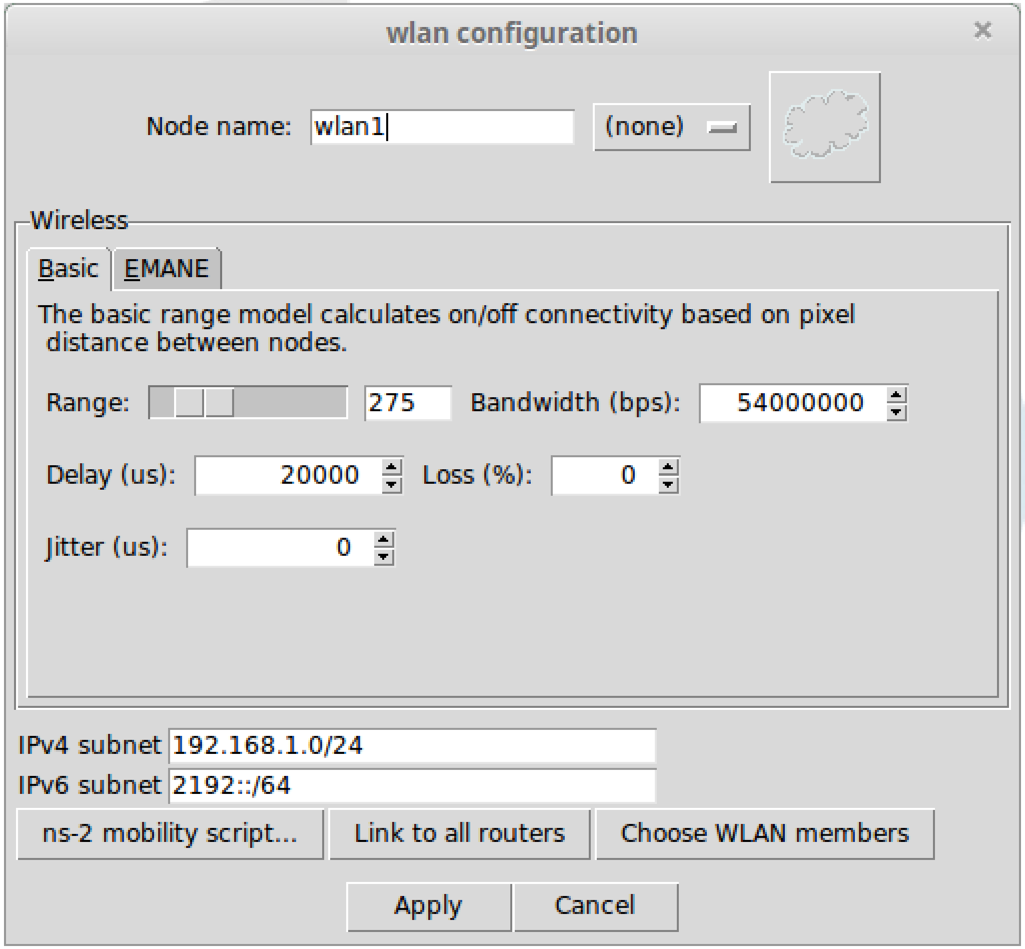
Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Wireless LAN example



Configuration of wlan1



wlan configuration

Node name: wlan1 (none)

Wireless

The basic range model calculates on/off connectivity based on pixel distance between nodes.

Range: 275 Bandwidth (bps): 54000000

Delay (us): 20000 Loss (%): 0

Jitter (us): 0

IPv4 subnet 192.168.1.0/24

IPv6 subnet 2192::/64

Configuration of svr1

- Add IP addresses for interfaces.
- Add an IPv4 default gateway.
- Add an IPv6 default gateway.

```
root@svr1:/tmp/pycore.41960/svr1.conf# ip addr add 10.4.4.2/30 dev eth0
root@svr1:/tmp/pycore.41960/svr1.conf# ip -6 addr add 2ddd::2/64 dev eth0

root@svr1:/tmp/pycore.41960/svr1.conf# ip addr add 10.5.5.2/30 dev eth1
root@svr1:/tmp/pycore.41960/svr1.conf# ip -6 addr add 2eee::2/64 dev eth1

root@svr1:/tmp/pycore.41960/svr1.conf# ip route add default via 10.4.4.1
root@svr1:/tmp/pycore.41960/svr1.conf# ip -6 route add default via 2ddd::1
```

Configuration of Routers

- The routers are configured in much the same manner as previous routing examples except:
  - **lo** interface address are also routed
  - For OSPFv2 the network 10.0.0.0/8 adds all subnetworks to OSPF.

Thank You

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com