Wireless LAN

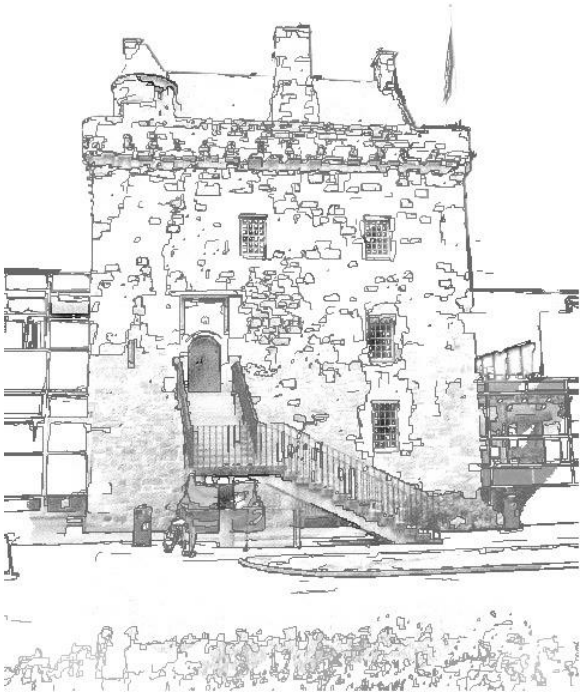
Unit 1: Radio Wave Fundamentals

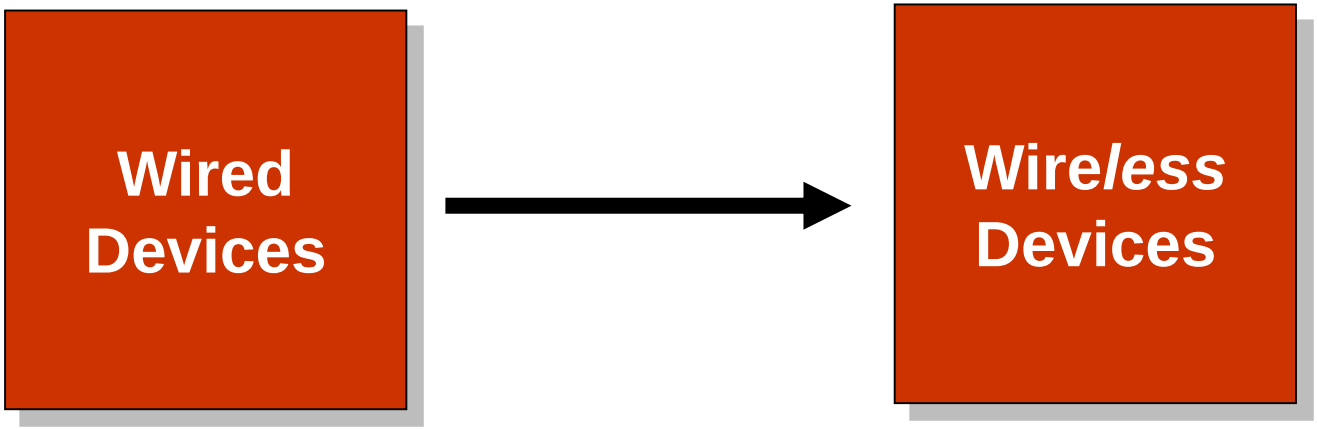
Areas covered:

- **Wireless Communication Types. This area covers the main type of wireless communications.**
- **Radio Wave Fundamentals. This area covers some of the fundamentals of radio waves.**
- **Radio Wave Propagation. This area covers the main type of propagation of radio waves.**
- **Wireless Bandwidth. This area outlines how bandwidth relates to wireless systems.**

Author: Bill Buchanan

The Issues?





Security ...

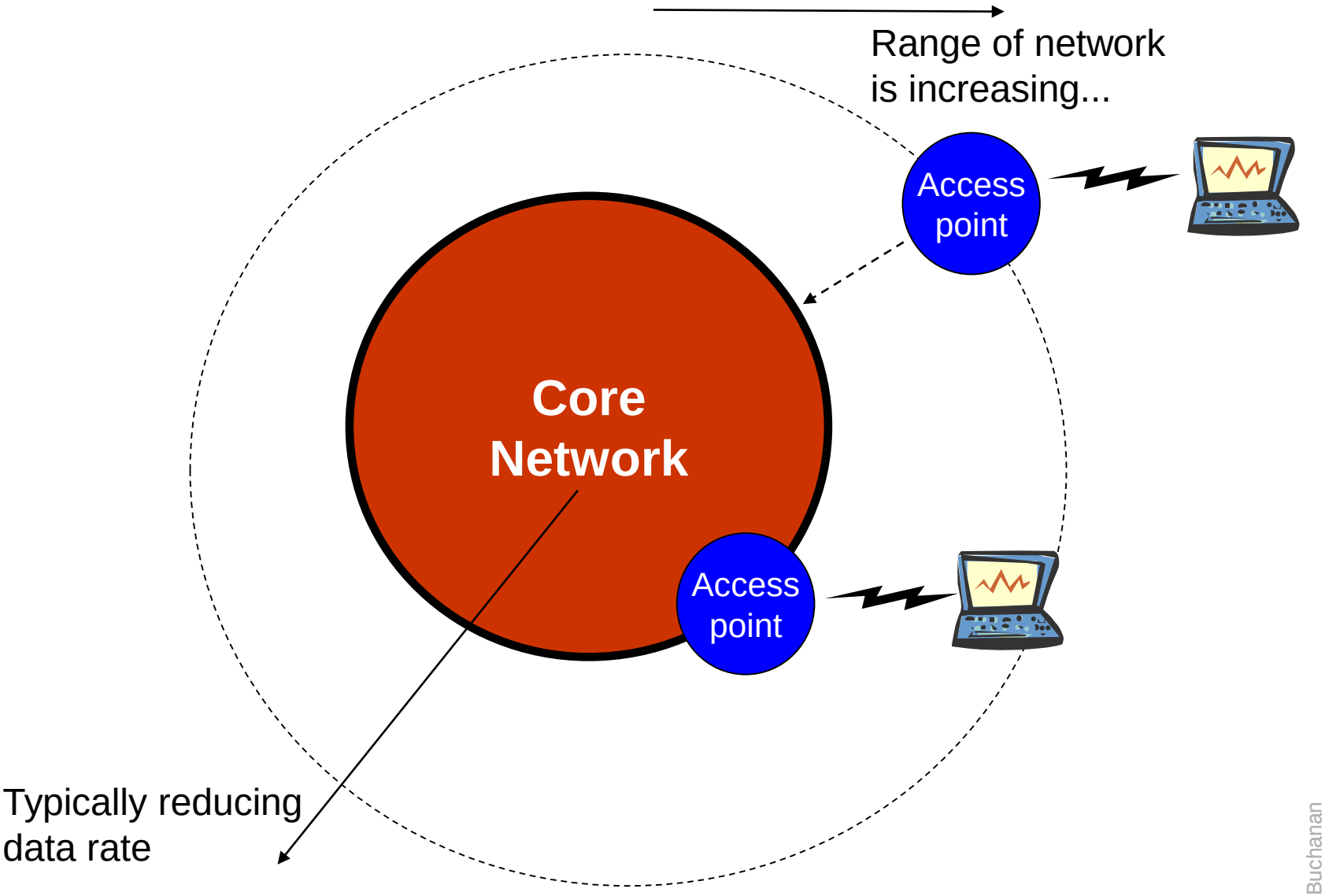
-Privacy.
-Authentication.

Robustness ...

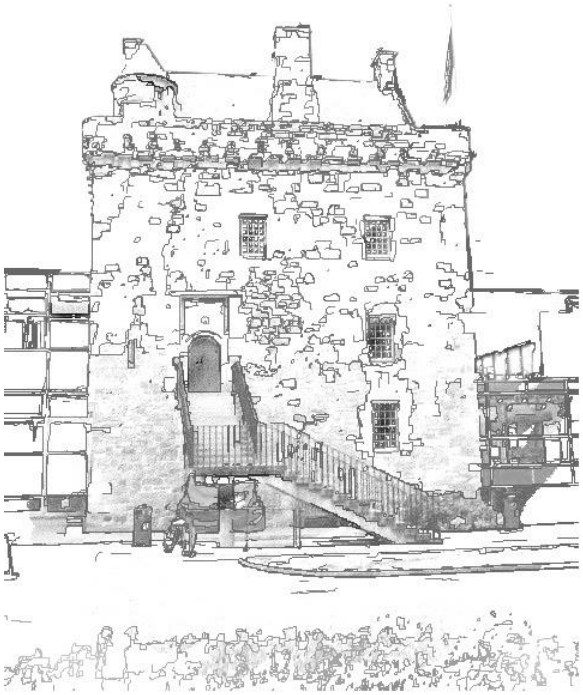
-Denial of service.
-Interference.
-Crowded radio spectrum.

Bandwidth ...

-Capability to support real-time traffic.
-Limited bandwidth.
-Scalability.

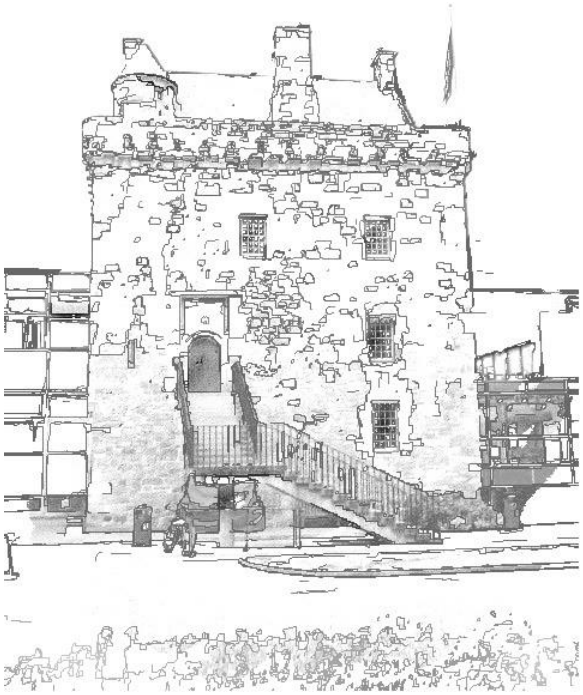

Range of network
is increasing...
Access
point
Core
Network
Access
point
Typically reducing
data rate

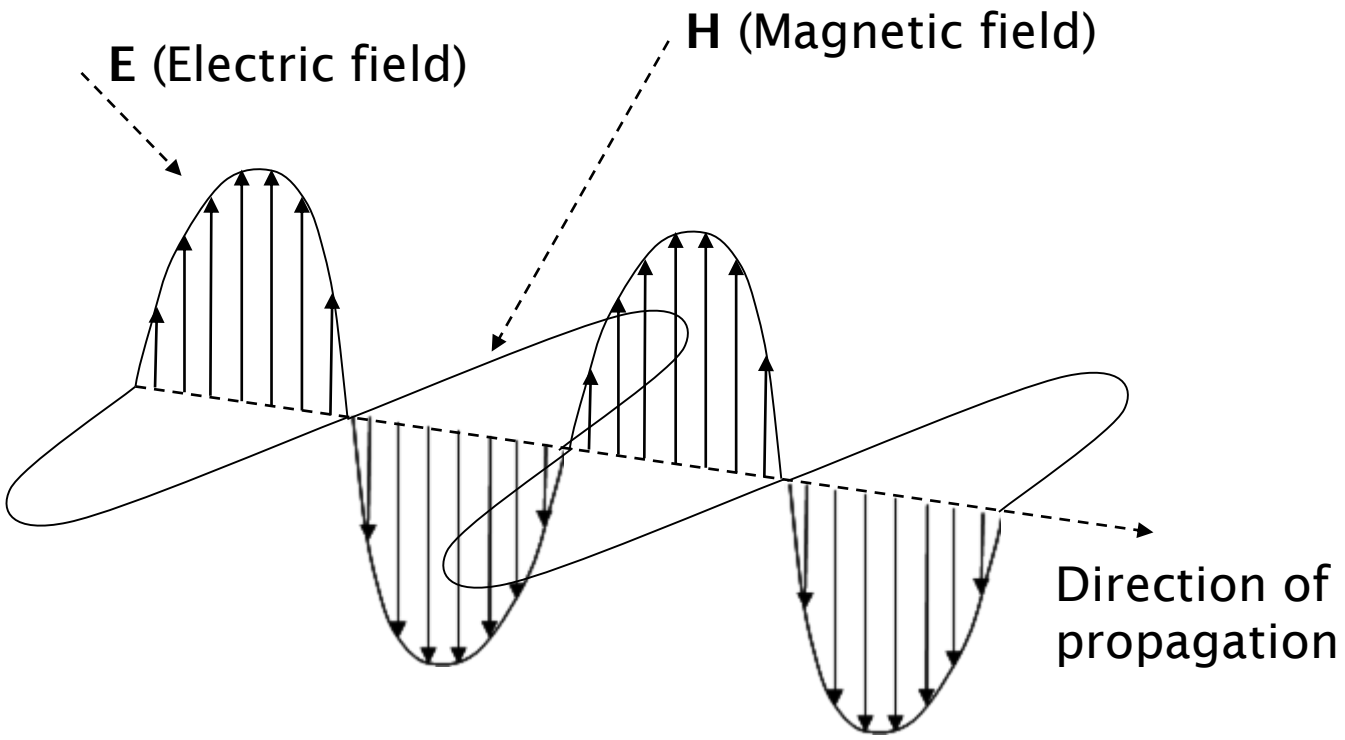
Wireless LAN Types



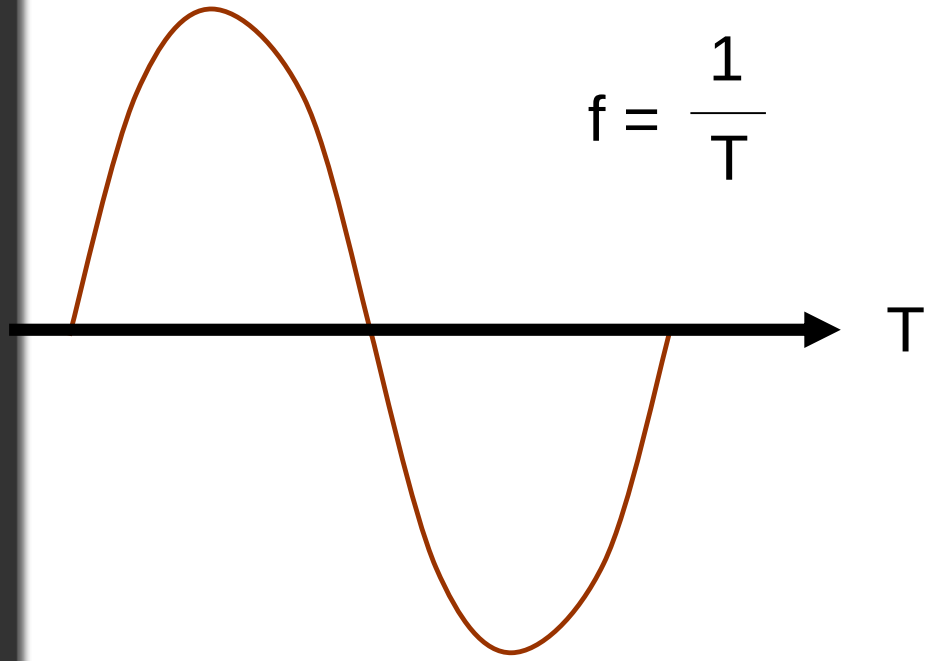
- **Mobile phone technology**. This integrates with the GSM network.
- **Wireless** (IEEE 802.11). This normally integrated with a fixed network.
- **Bluetooth**. This normally allows networking between non-computer-type devices, such as mobile phones, hi-fi's, and so on.
- **Infra-red**. This technology is too slow and has a limited range for most applications.
- **Line-of-sight optics**. This allows for easy connections between buildings, and involves a laser directing it beam to a receiver. It is typically used around cities and gives speeds of several Gbps.
- **UWB** (Ultra-wide Bandwidth). This is a technique which spreads its radio power over a wide range of frequencies, with an extremely low power (so as not to affect other communications.
- **WiMax**.

Radio Wave Fundamentals





Conforms to right-hand rule:
E – Middle finger
H – Thumb
Propagation – Index finger



$$f = \frac{1}{T}$$

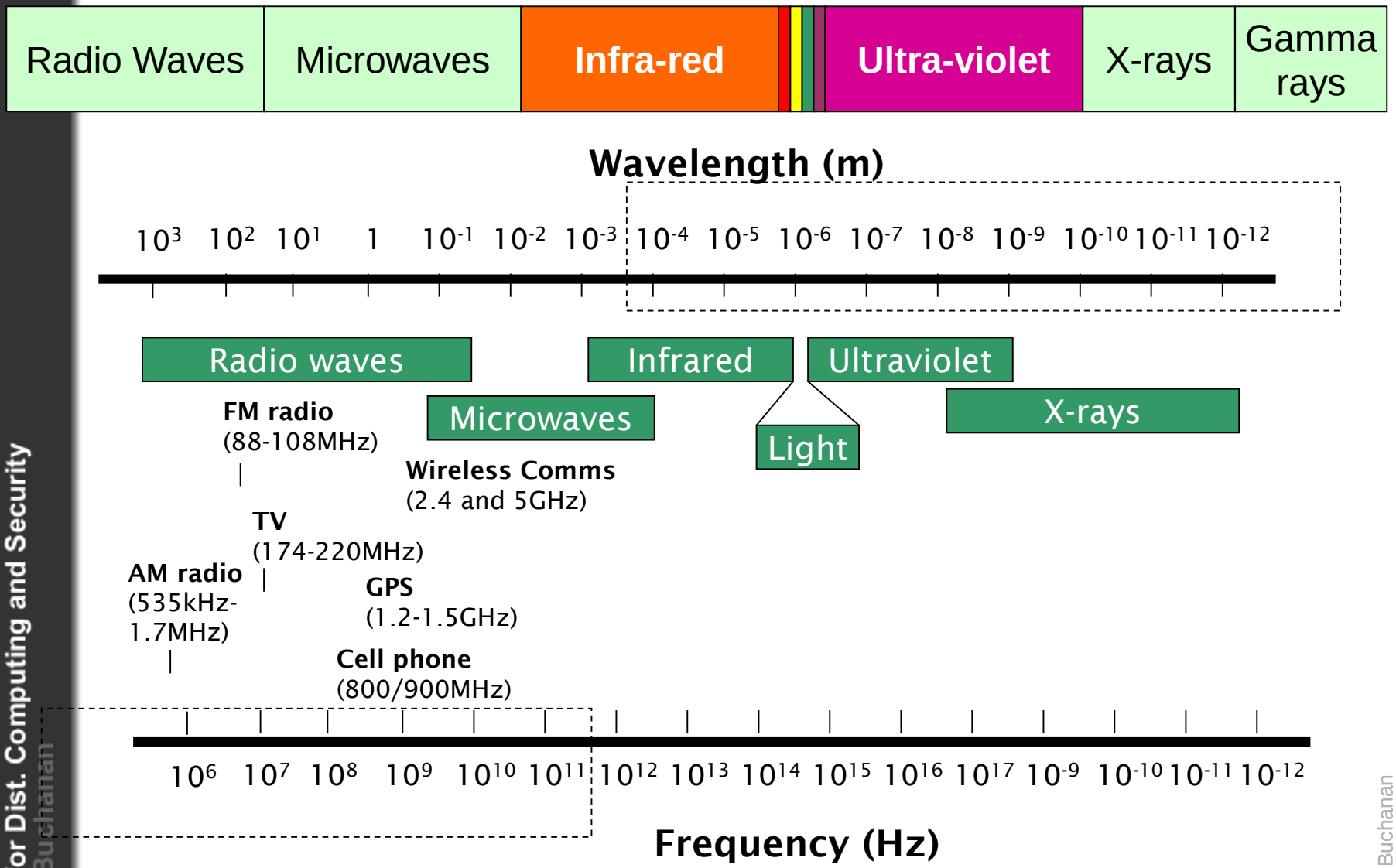
Frequency (Hz)

Wavelength (m)

$$c = f \lambda$$

$$c = 3 \times 10^8 \text{ m/s}$$

$$\lambda = \frac{c}{f} \qquad f = \frac{c}{\lambda}$$

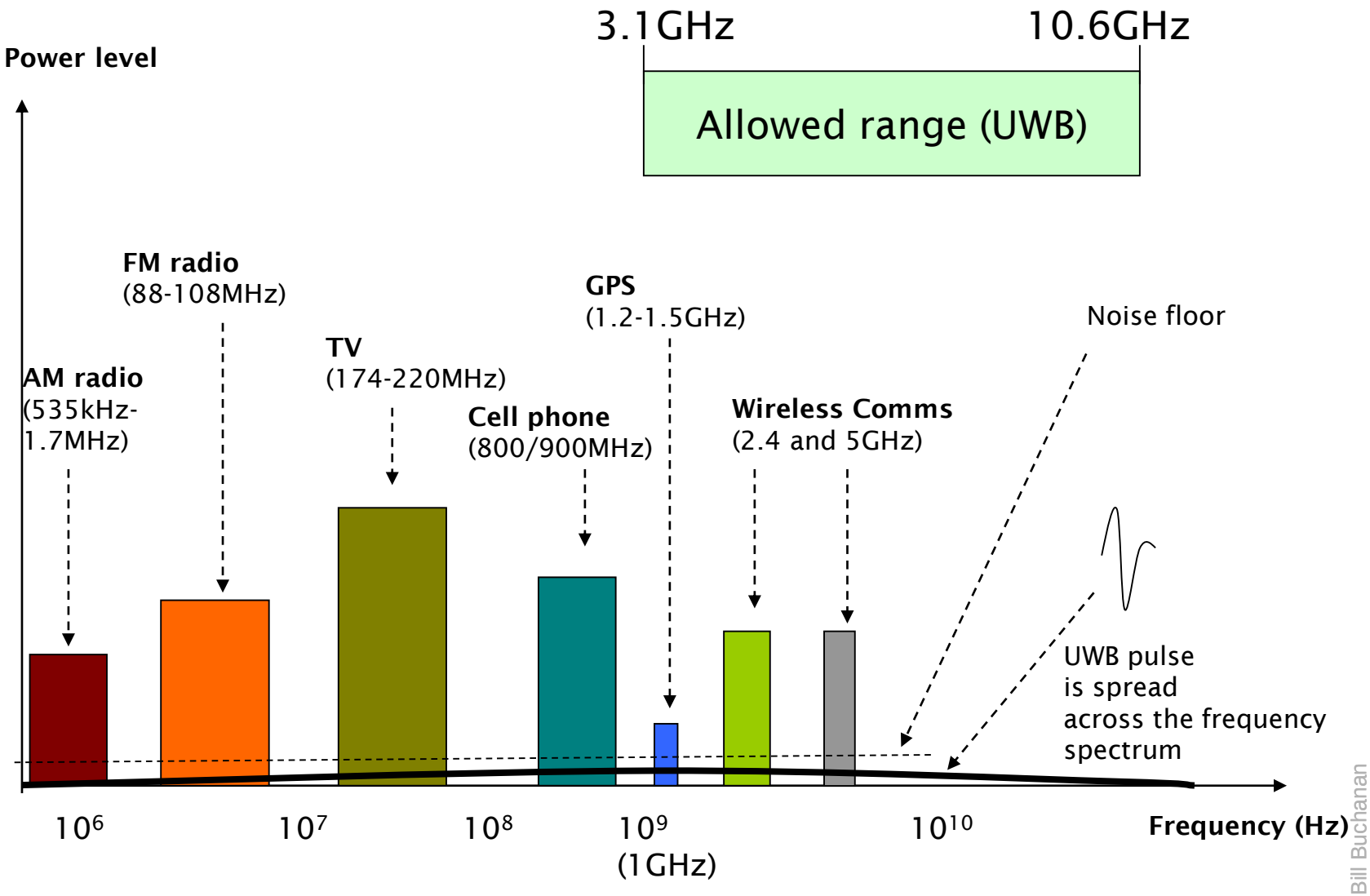

Radio Waves
Microwaves
Infra-red
Ultra-violet
X-rays
Gamma rays
Wavelength (m)
10^3 10^2 10^1 1 10^-1 10^-2 10^-3 10^-4 10^-5 10^-6 10^-7 10^-8 10^-9 10^-10 10^-11 10^-12
Radio waves
Infrared
Ultraviolet
Microwaves
X-rays
Light
FM radio
(88-108MHz)
Wireless Comms
(2.4 and 5GHz)
TV
(174-220MHz)
AM radio
(535kHz-
1.7MHz)
GPS
(1.2-1.5GHz)
Cell phone
(800/900MHz)
10^6 10^7 10^8 10^9 10^10 10^11 10^12 10^13 10^14 10^15 10^16 10^17 10^-9 10^-10 10^-11 10^-12
Frequency (Hz)

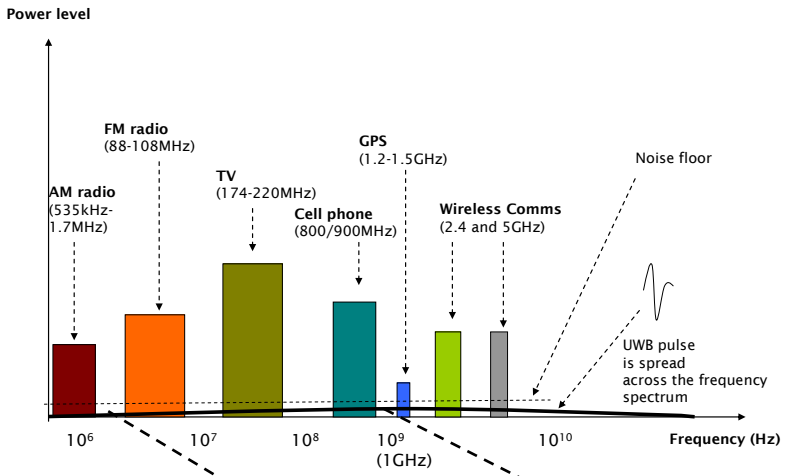
$$B_{av} = \frac{f}{10} bps$$

Available **bandwidth** typically depends on the carrier frequency, and as an estimate it is around one-tenth of the carrier frequency (bps)

Radio Wave (AM)	f=1.7MHz, B_{av}=170kbps.
Radio Wave (TV)	f=200MHz, B_{av} =20Mbps.
Radio Wave (Mobile phone)	f=900MHz, B_{av} =90Mbps.
Microwave (IEEE 802.11b)	f=2.4GHz, B_{av} =240Mbps.
Infra-red	f=10^{13}Hz, B_{av} =1Tbps.

Radio Spectrum





Radio wave propagation
From 50kHz to 2.5GHz

LF	MF	HF	VHF	UHF	Microwave

LF radio — **135kHz**

AM radio — **13.56MHz** **(globally defined standard)**

FM radio — **860-930MHz**

TV signals

Radar/ Satellite/ Wireless — **2.45GHz**

Propagate well over large distances → Line-of-sight communications

Low range (<0.5m) | Med range (1m) | High range (5m) | Med range (1m)

Low read rate → High read rate

Large antenna → Small antenna

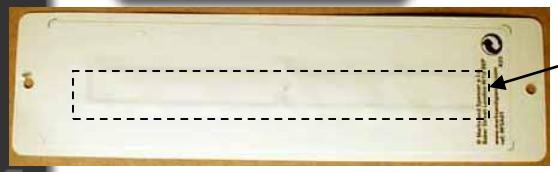
Relatively large → Relatively small

Detachable Tags at M&S

Many organisations feel that RFID is a suspect technology which will allow organisations to track human movement.

M&S have detachable tabs, so the users never have any issues on their usage.

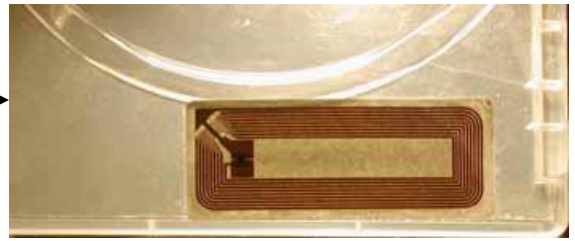
Please retain this label for refund and exchange



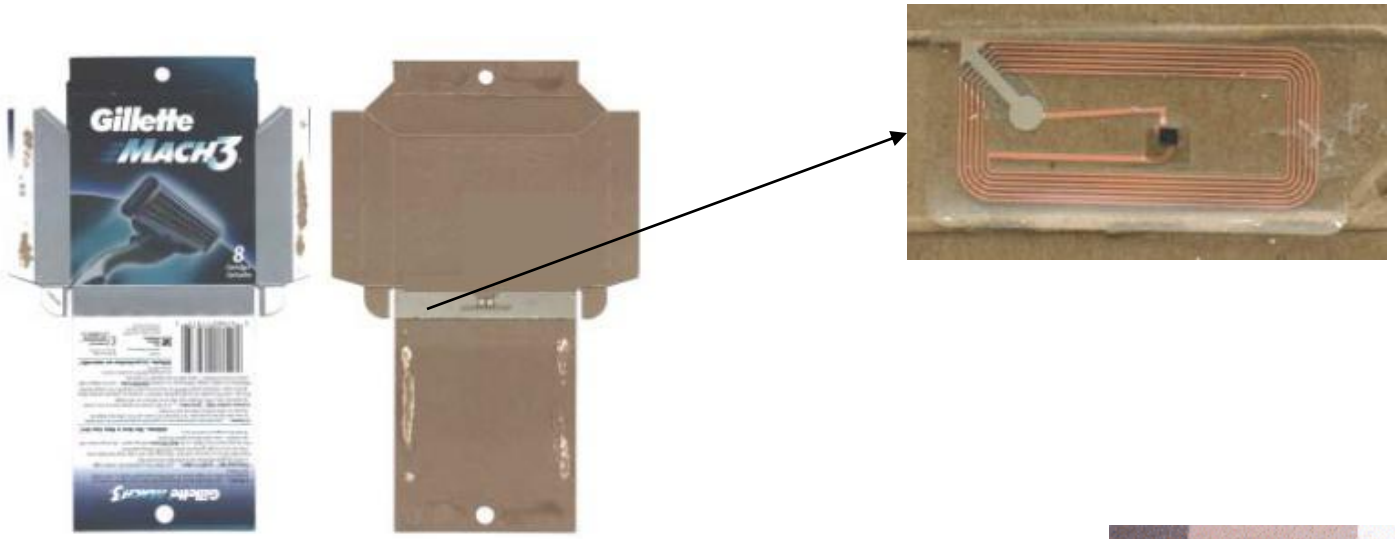
Antenna

At present, the RFID tag is thrown-away after sale.

Tesco's are also trailing the usage of RFID tags, such as this one on a DVD box.

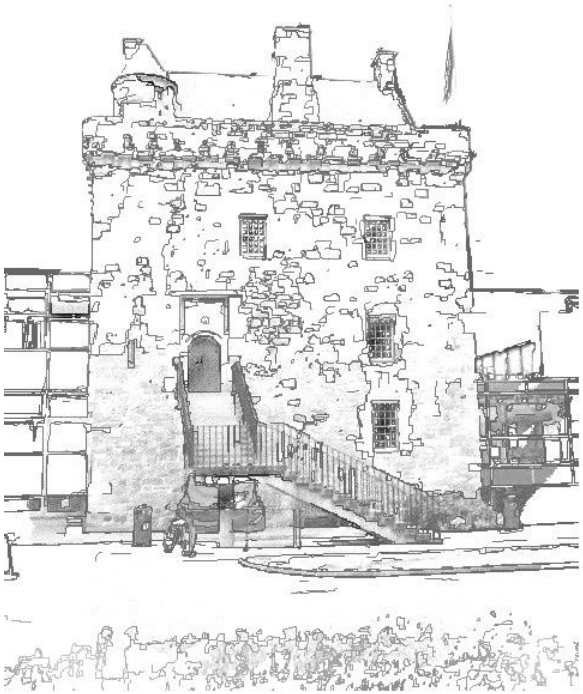


Gillette Wireless Tags

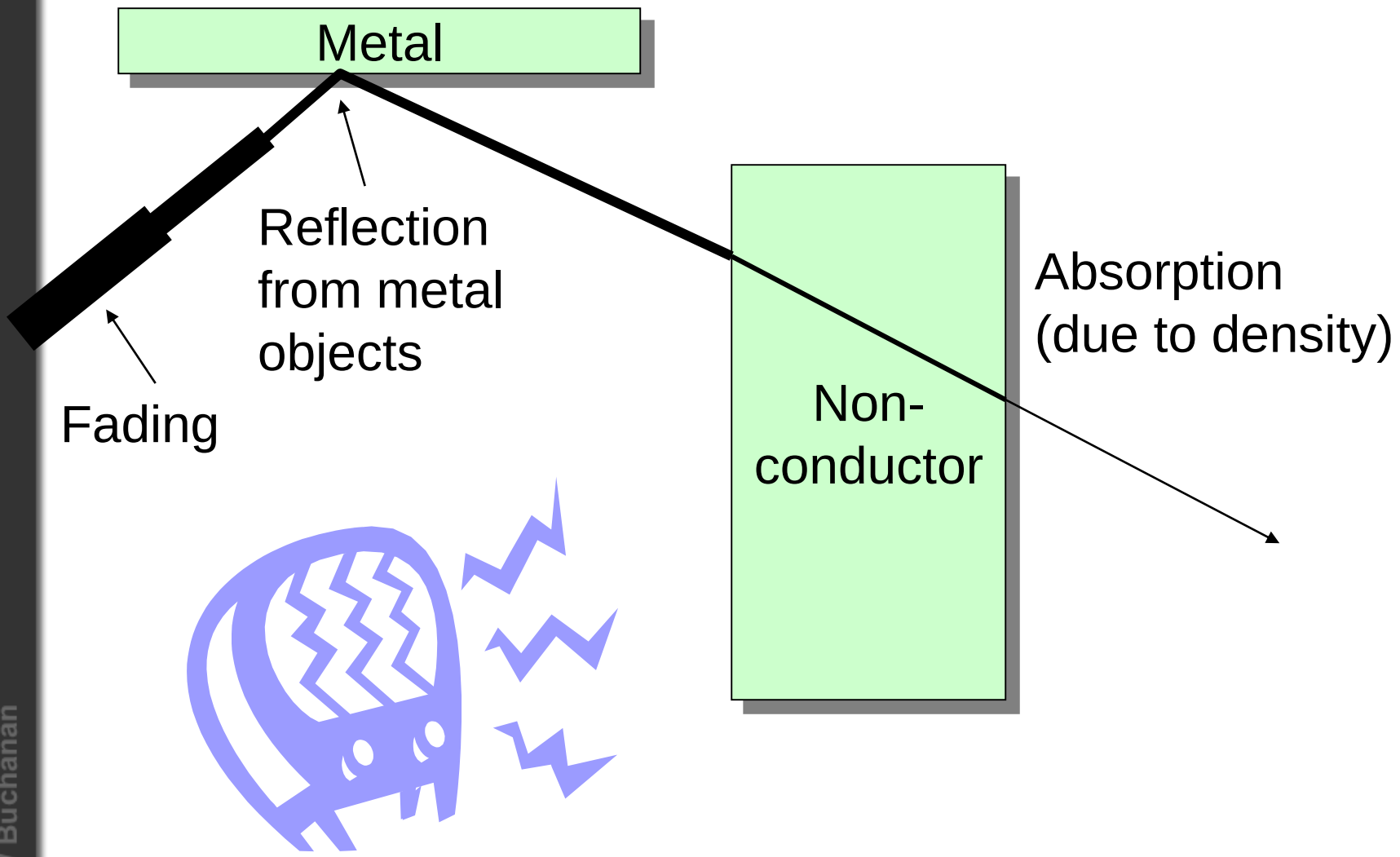


Gillette have bought over 500 million tags for their products, as razors are seen as ‘high shrinkage’ goods, where their products are stolen throughout the supply chain.

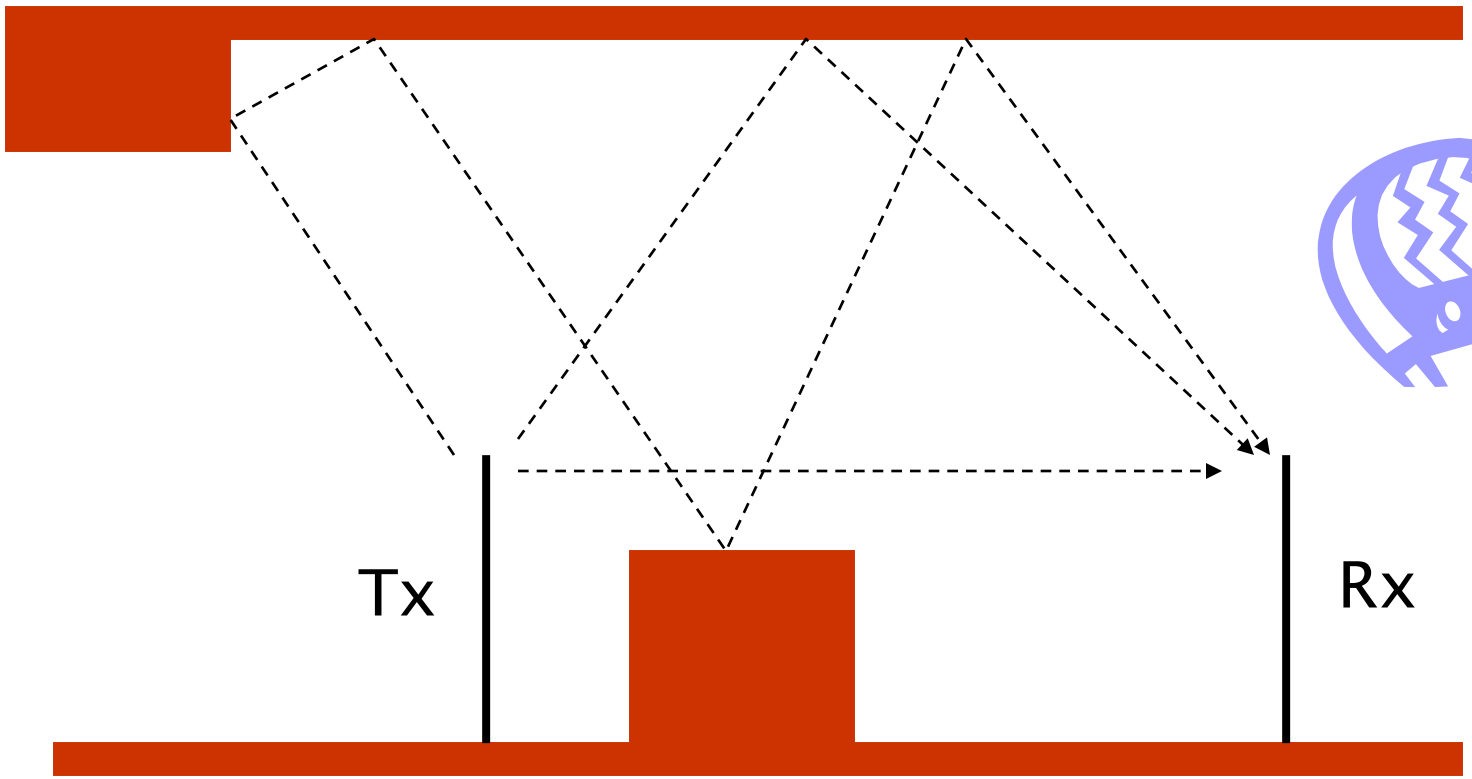
Radio Wave Problems



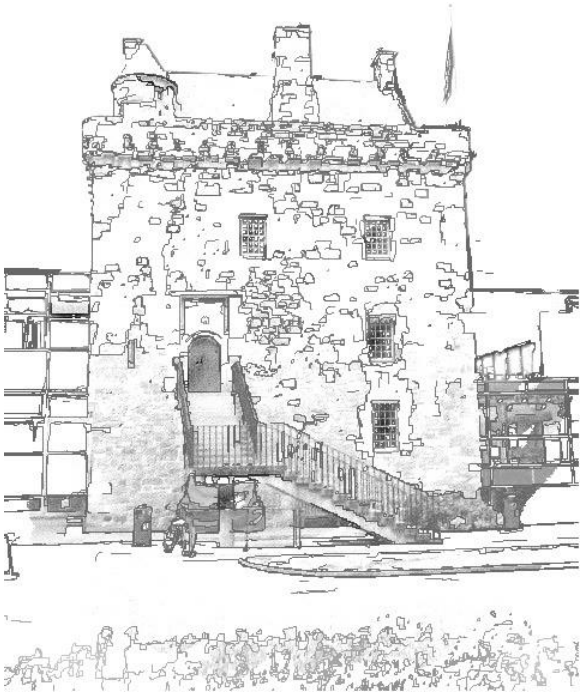
Reflection and absorption



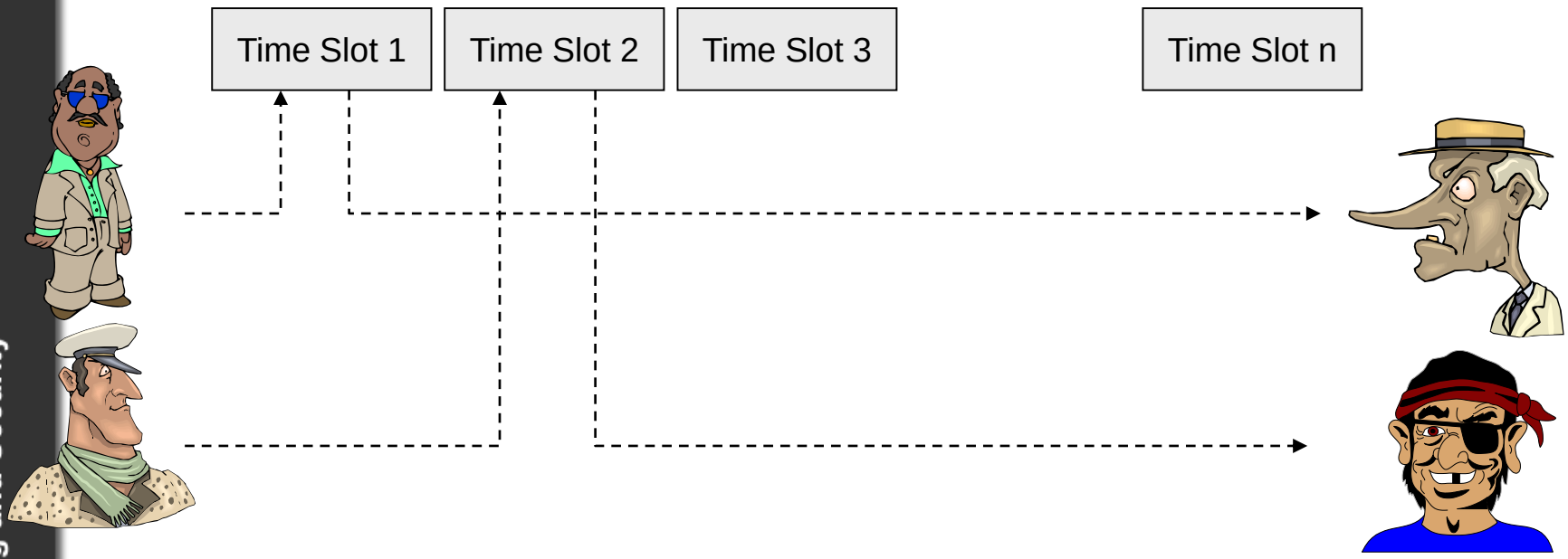
Multipath Problems



Cellular Technology

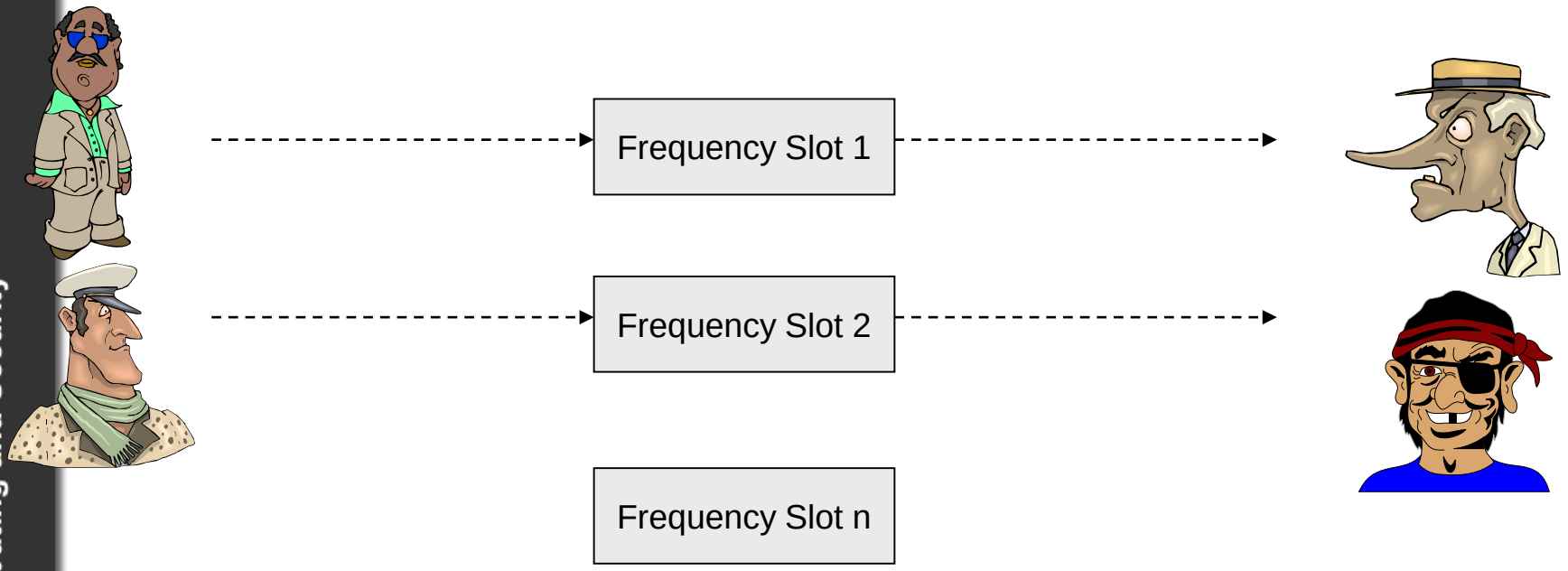


Time Domain Multiplexing (TDM)



TDM is used in the telephone network, GSM/3G, and also in network switching.

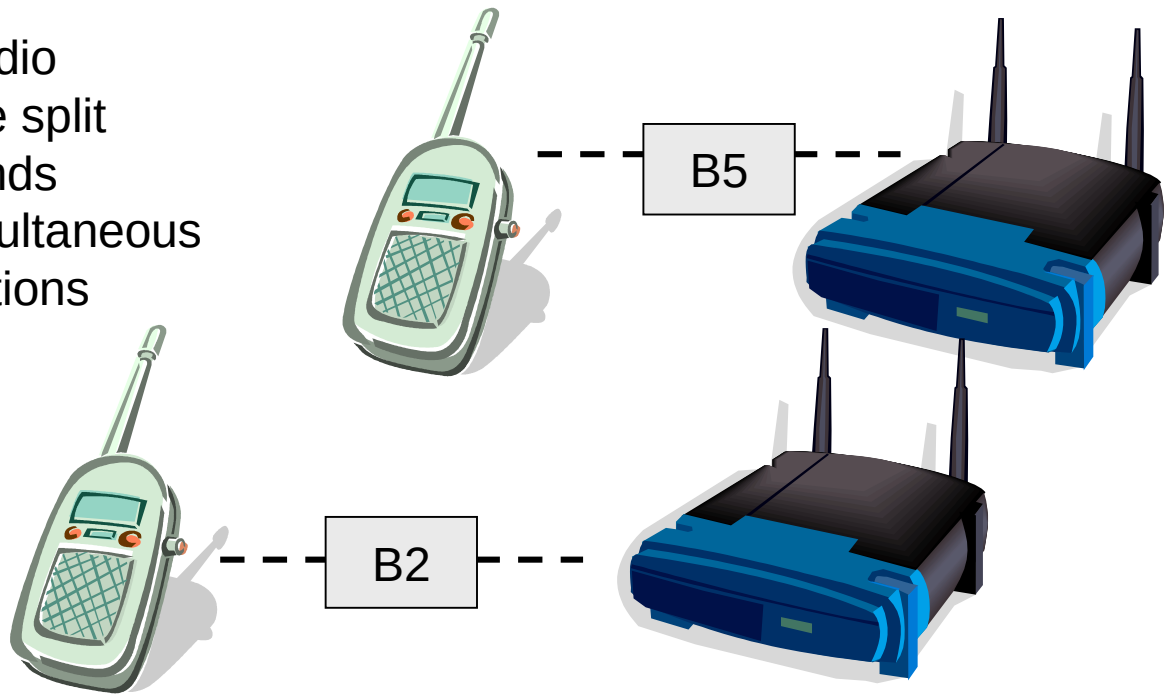
Frequency Domain Multiplexing (FDM)



FDM is used by Radio Stations and most Wireless Networks.

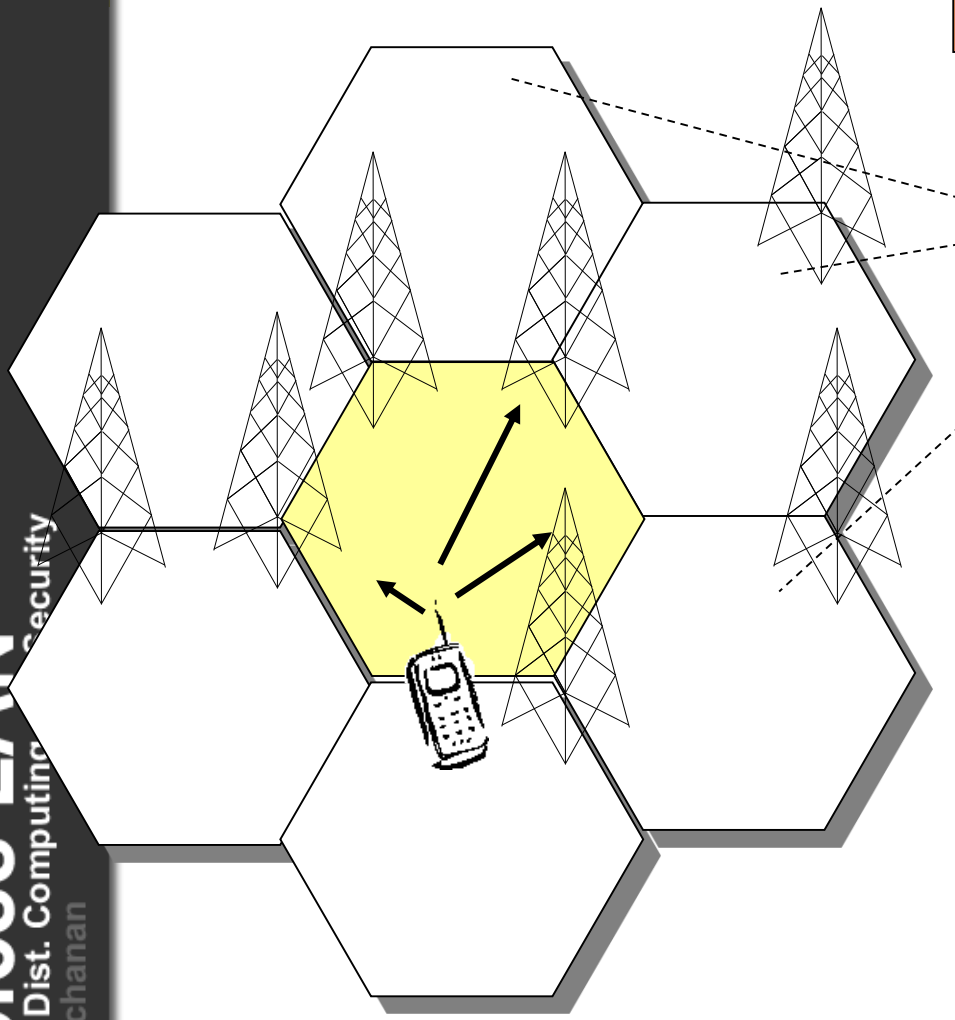
Available Radio Band

Available radio band can be split into sub-bands to allow simultaneous communications



- **First generation** (1G). First generation mobile phones (1G) had very low transmission rates (typically just a few KB/s),
- **Second generation** (2G and 2.5G). These are devices improved this to give several hundred KB/s.
- **Third generation** (3G). These devices give almost workstation network bandwidths (several MBps), which allows for full multimedia transmissions.

Mobile phone technology



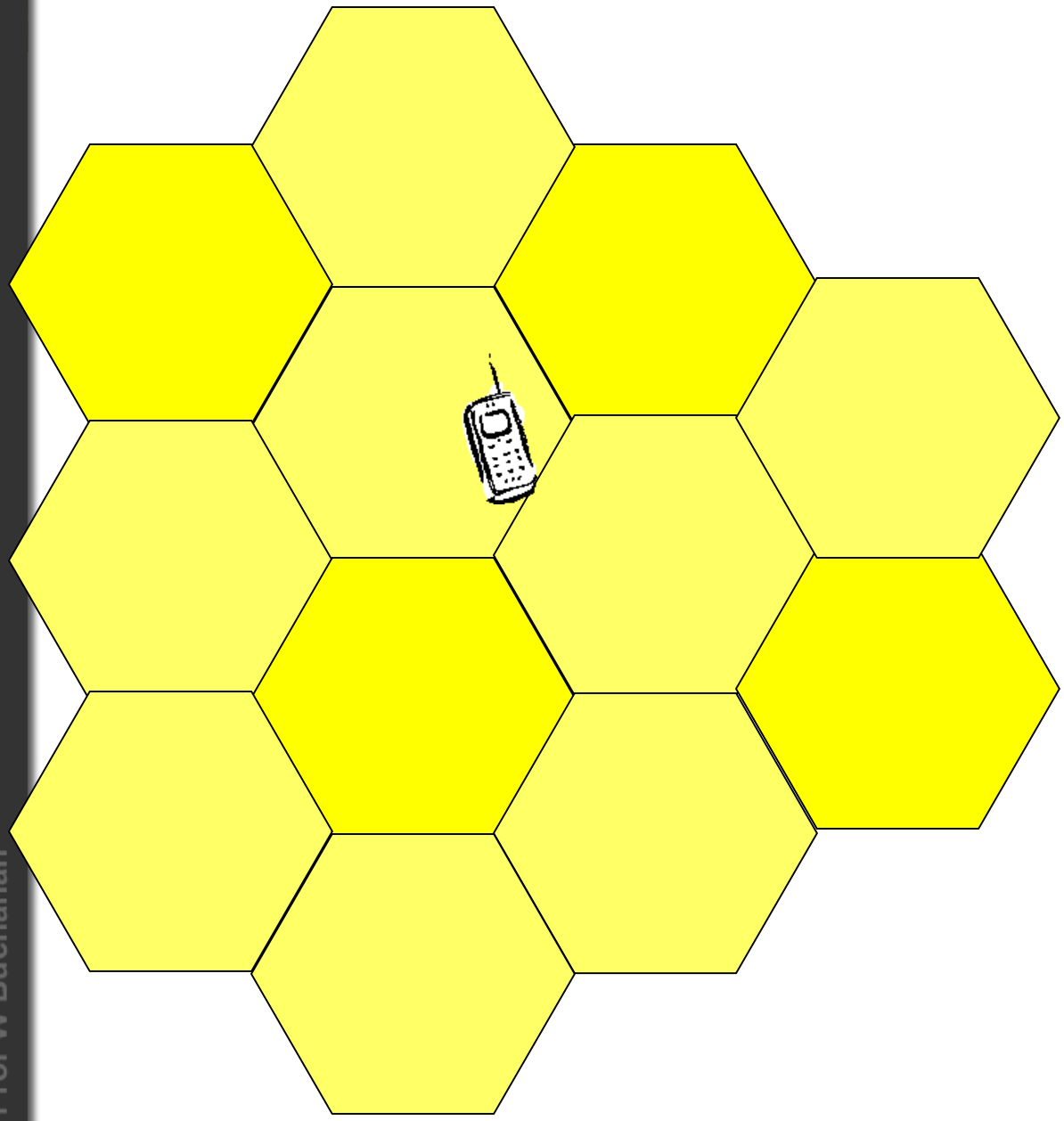
(Plain Old Telephone System)

GSM network

GSM gateway

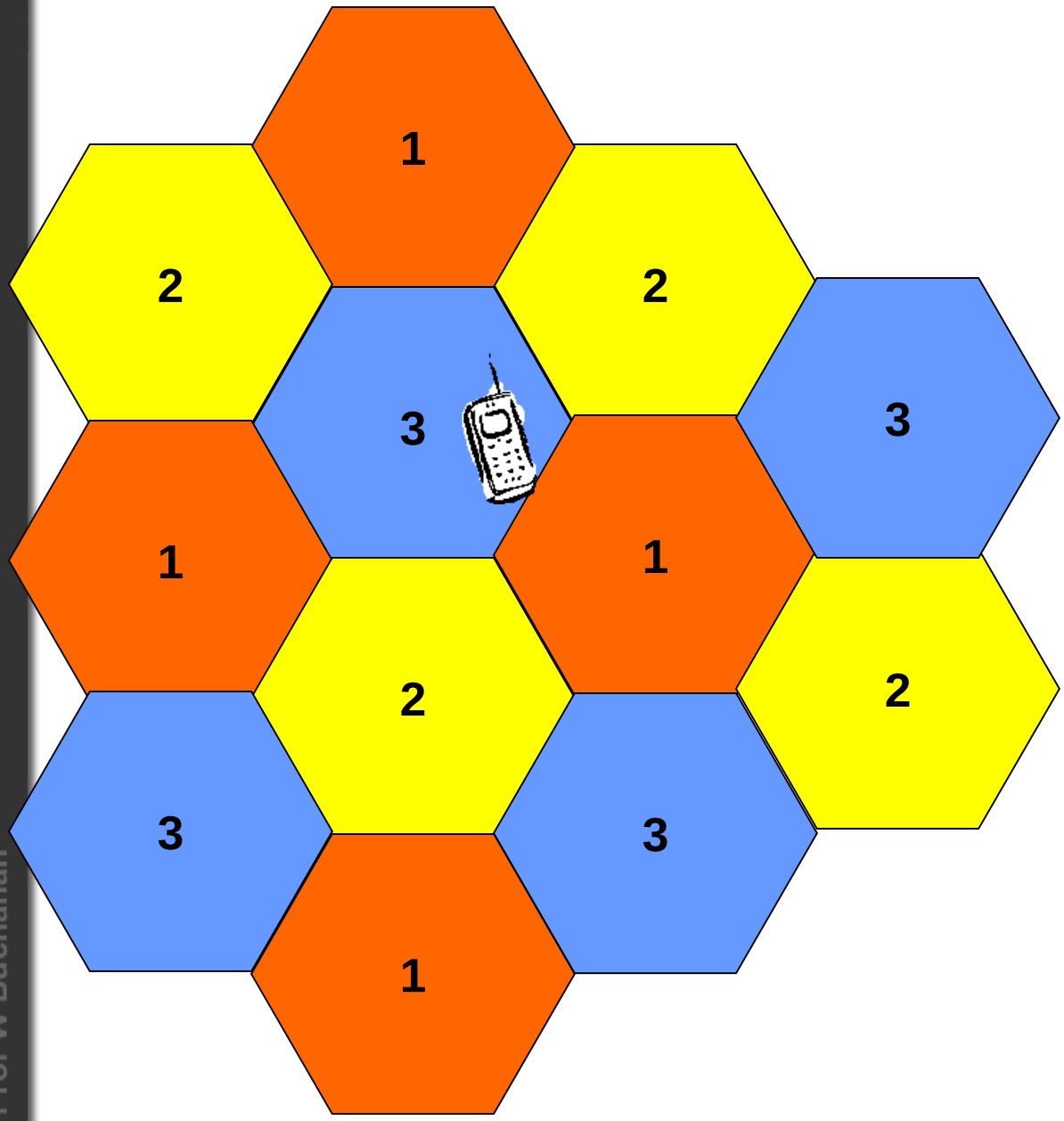
Internet

Cellular networks



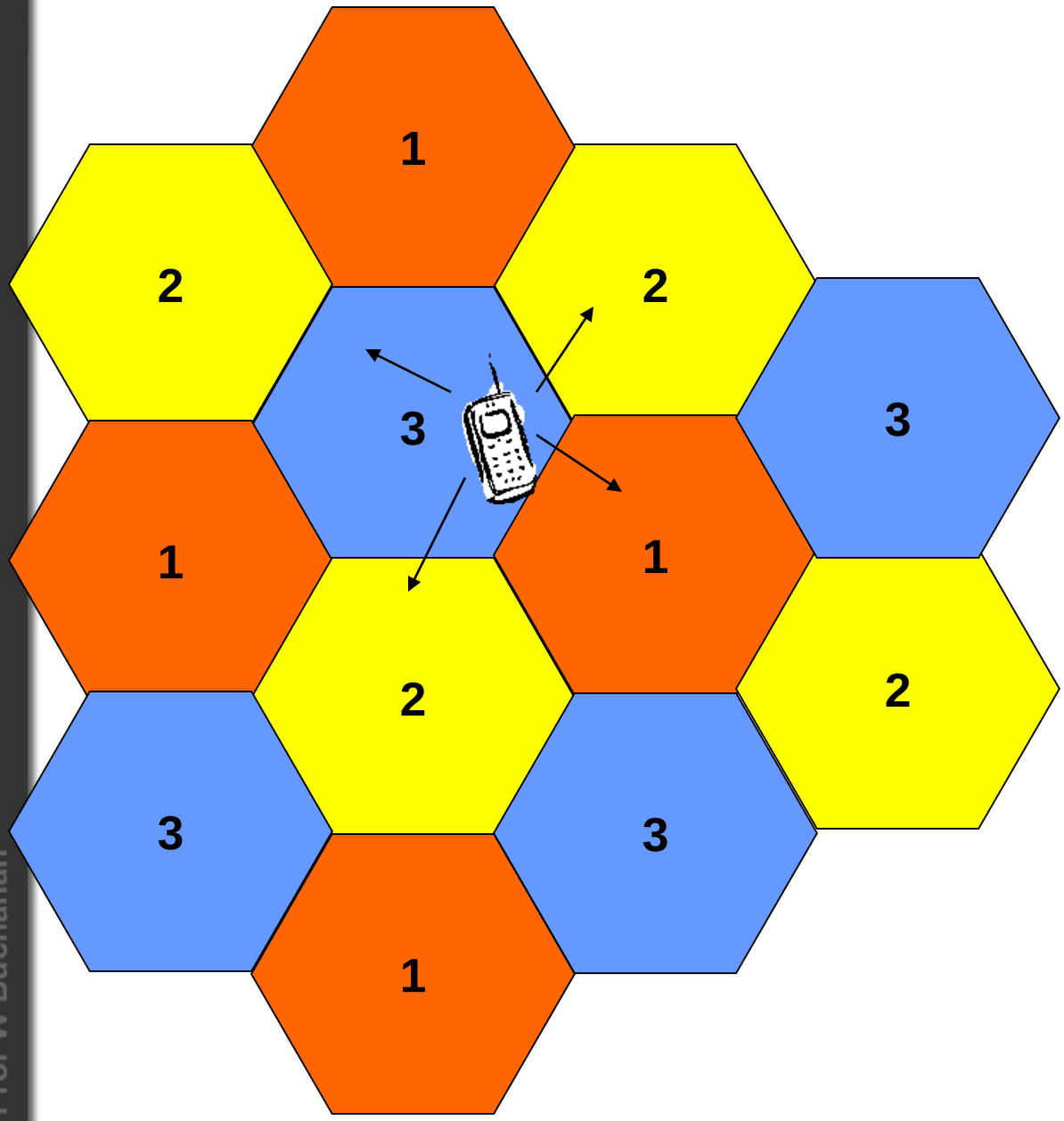
If we wish to setup radio transmitters how many different radio frequencies do we need?

Cellular networks



If we wish to setup radio transmitters how many different radio frequencies do we need?

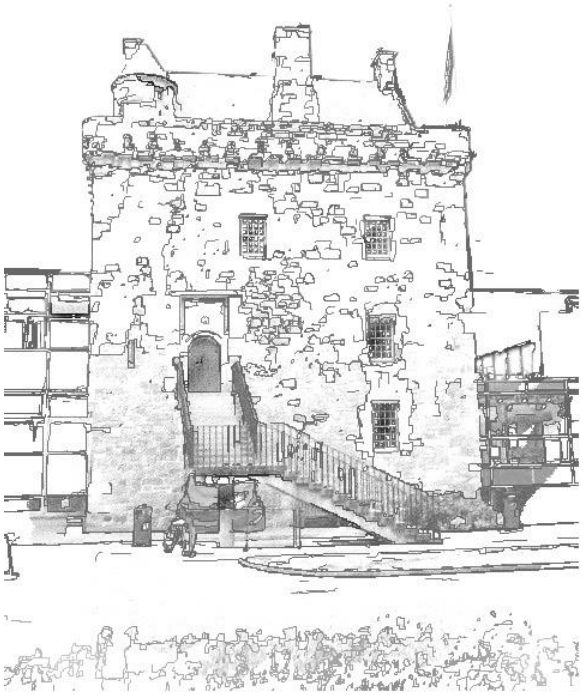
Cellular networks



Mobile device will continually scan for other frequencies, even when it connects to one (in this case, frequency 3).

Sometimes there must be a handover between two cells, if a user moves from one to another, and is still in a call.

Spread Spectrum



Spread Spectrum and Frequency Hopping

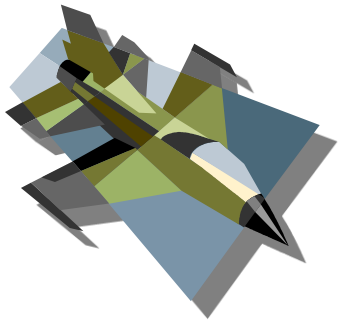
To avoid interference in the band, radio LANs (RLANs) use either **Frequency Hopping** or **Direct Sequence Spread Spectrum** techniques (FHSS & DSSS). These two methods avoid or lower the potential for interference within the band as shown in the next slide. Spread spectrum technologies work by spreading the actual signal over a wider bandwidth for transmission. Using these methods provides resilience from narrow band interference and also reduces interference to other sources using the ISM (Industrial, Scientific and Medical) band.

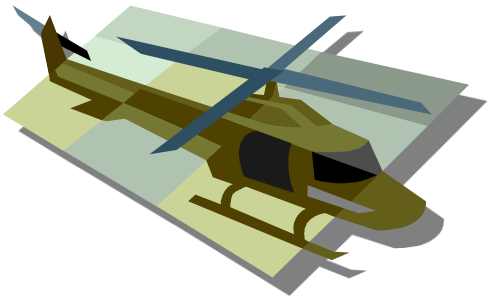
Frequency Hopping Spread Spectrum technology works by splitting the ISM band into 79 1MHz channels. Data is transmitted in a sequence over the available channels, spreading the signal across the band according to a hopping pattern, which has been determined between the wireless devices. Each channel can only be occupied for a limited period of time before the system has to hop.

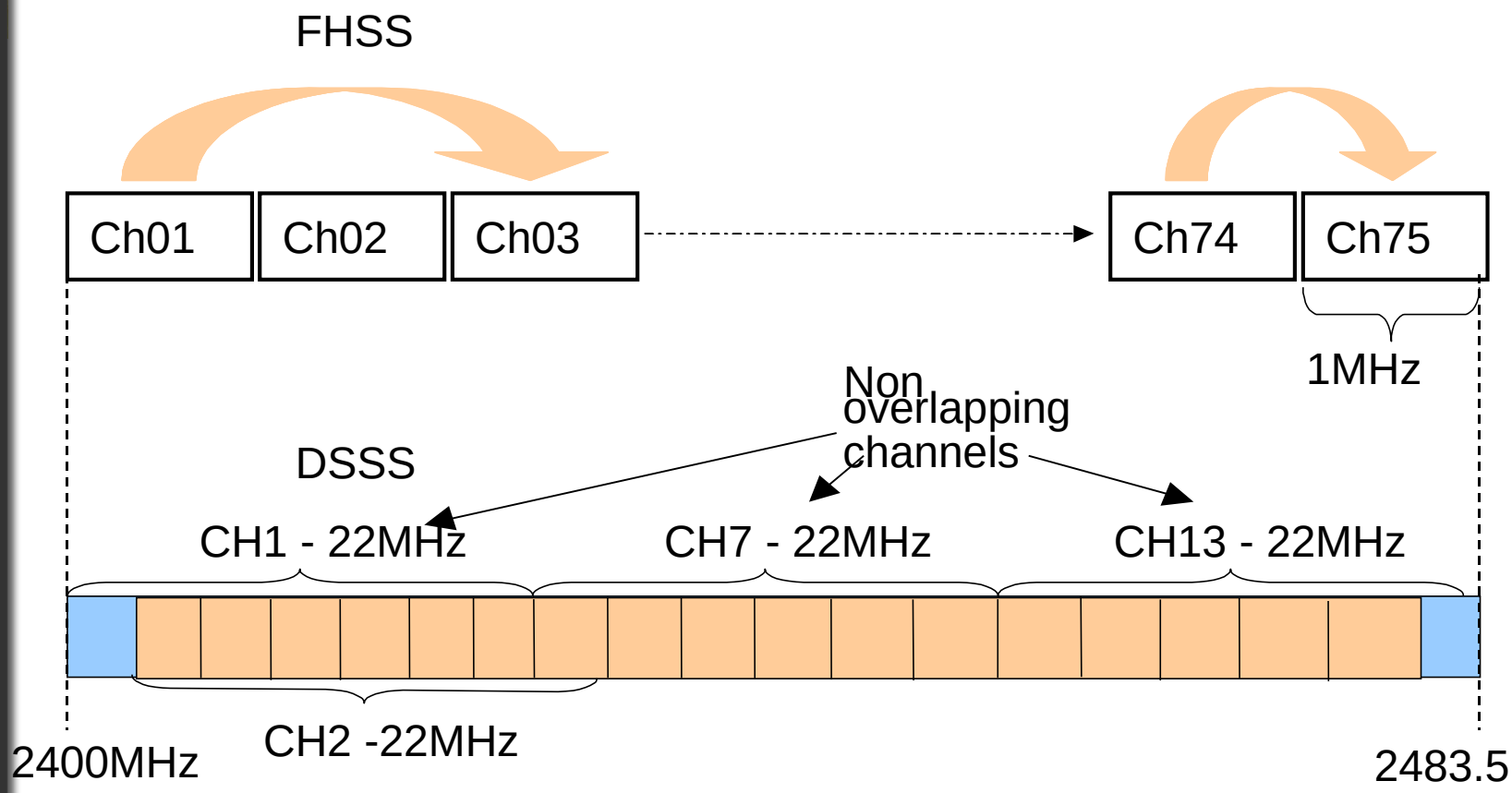
Spread Spectrum and Frequency Hopping

Military systems have been using Spread Spectrum and Frequency Hopping for many years. This is to:

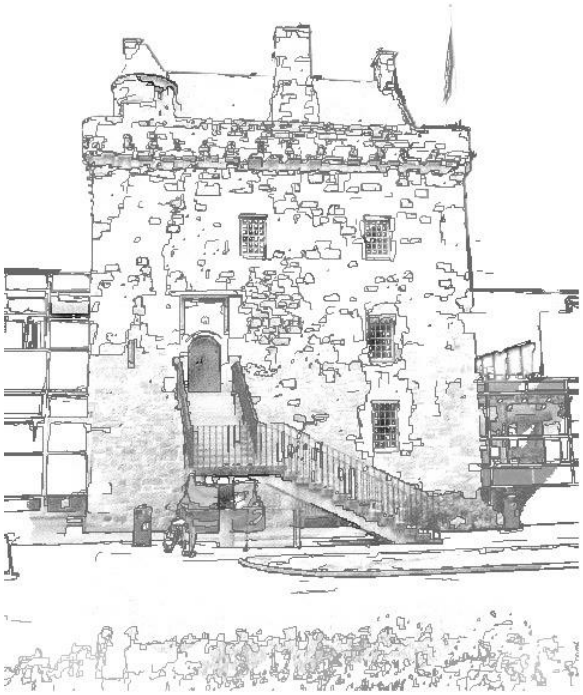
- Avoid jamming on a certain channel.
- Avoid noise on a certain channel.
- Confuse the enemy as the transmitting frequency moves in a way that only the sender and receiver known. Imagine having to move the dial of your radio receiver, each minute to a certain frequency in a give way. Such as Radio 1 is broadcast on 909MHz from 12:00, then 915MHz until 12:01, then 900MHz unit 12:02, and so on.






FHSS
Ch01
Ch02
Ch03
Ch74
Ch75
1MHz
Non overlapping channels
DSSS
CH1 - 22MHz
CH7 - 22MHz
CH13 - 22MHz
CH2 -22MHz
2400MHz
2483.5MHz

IEEE 802.11 Networks



IEEE 802.11 - Wireless

- **IEEE 802.11a.** 802.11a deals with communications available in the **5GHz** frequency, and has a maximum data rate of 54 Mbps.
- **IEEE 802.11b.** 802.11b, or Wi-Fi, is the standard that is most commonly used in wireless LAN communications. It has a maximum bandwidth of 11Mbps, at a frequency of 2.4GHz.
- **IEEE 802.11g.** 802.11g is a proposed standard that hopes to provide **54Mbps** maximum bandwidth over a **2.4GHz** connection, the same frequency as the popular 802.11b standard.
- **IEEE 802.11c.** 802.11c is a group set up to deal with bridging operations when developing access points.
- **IEEE 802.11f.** 802.11f is concerned with standardising access point roaming which is involved in making sure that interoperability between access points is guaranteed

2.4GHz

802.11b (11Mbps)

802.11g (54Mbps)

5GHz

802.11a (54Mbps)

Author: Bill Buchanan

IEEE 802.11b

Operating Channels:

11 for N. America, 14 Japan, 13 Europe (ETSI), 2 Spain, 4 France

Operating Frequency:

2.412-2.462 GHz (North America), 2.412-2.484 GHz (Japan), 2.412-2.472 GHz (Europe ETSI), 2.457-2.462 GHz (Spain), 2.457-2.472 GHz (France)

Data Rate:

1, 2, 5.5 or 11Mbps

Media Access Protocol:

CSMA/CA, 802.11 Compliant

Range:

11Mbps: 140m (460 feet)
5.5Mbps: 200m (656 feet)
2Mbps: 270m (885 feet)
1Mbps: 400m (1311 feet)

RF Technology:

Direct Sequence Spread Spectrum

Modulation:

CCK (11Mps, 5.5Mbps), DQPSK (2Mbps), DBPSK (1Mbps)

Network settings

- **Authentication algorithm**. This sets whether the adapter uses an open system (where other nodes can listen to the communications), or uses encryption (using either a WEP key, or a shared key).
- **Channel**. If an ad-hoc network is used, then the nodes which communicate must use the same channel.
- **Fragmentation threshold**. This can be used to split large data frames into smaller fragments. The value can range from 64 to 1500 bytes. This is used to improve the efficiency when there is a high amount of traffic on the wireless network, as smaller frames make more efficient usage of the network.
- **Network type**. This can either be set to an infrastructure network (which use access points, or wireless hubs) or Ad-hoc, which allows nodes to interconnect without the need for an access point.

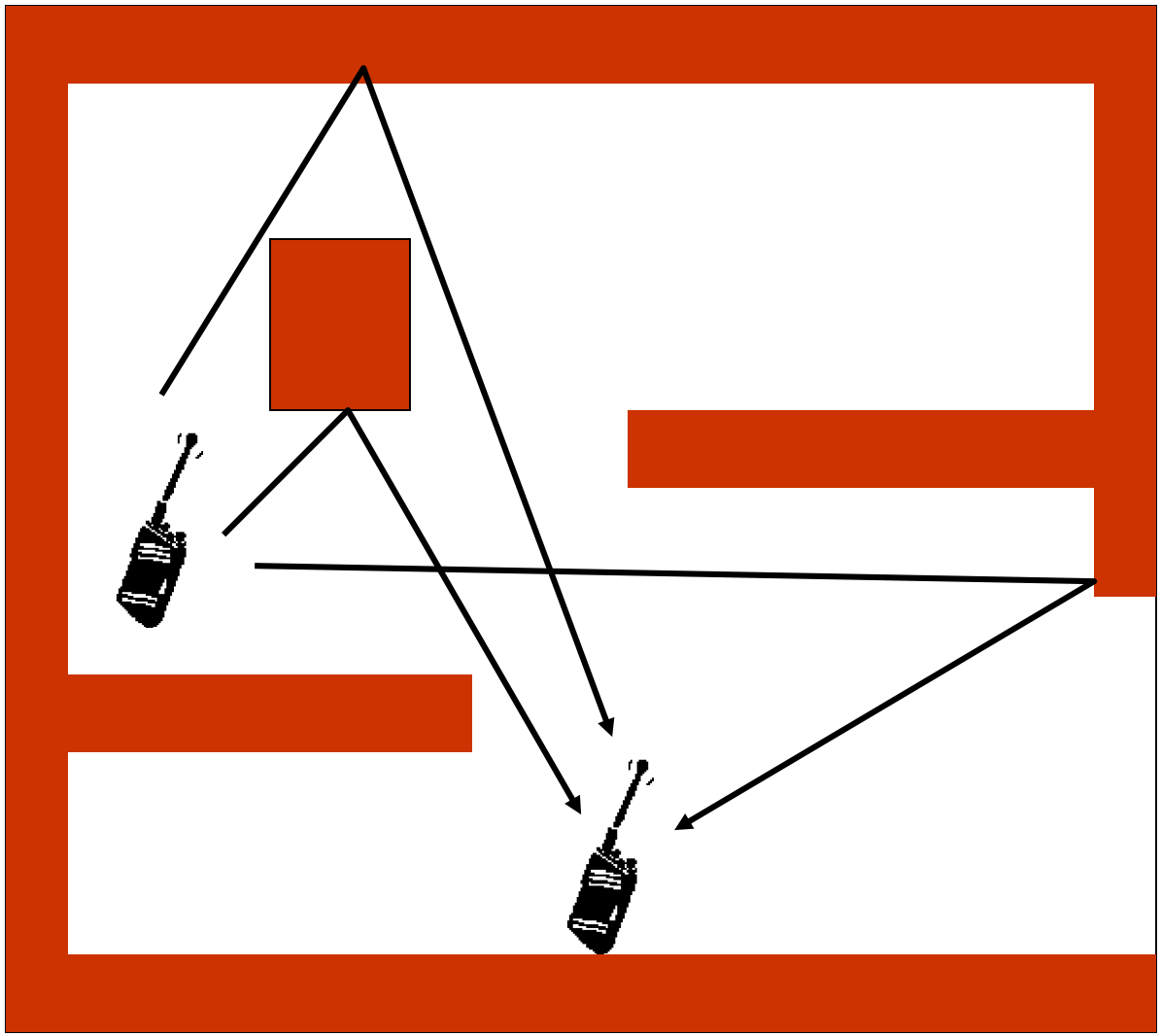
Network settings (cont.)

- **Preamble mode**. This can either be set to Long (which is the default) or short. A long preamble allows for interoperatively with 1Mbps and 2Mbps DSSS specifications. The shorter allows for faster operations (as the preamble is kept to a minimum) and can be used where the transmission parameters must be maximized, and that there are no interoperatablity problems.
- **RTS/CTS threshold**. The RTS Threshold prevents the *Hidden Node* problem, where two wireless nodes are within range of the same access point, but are not within range of each other. As they do not know that they both exist on the network, they may try to communicate with the access point at the same time. When they do, their data frames may collide when arriving simultaneously at the Access Point, which causes a loss of data frames from the nodes. The RTS threshold tries to overcome this by enabling the handshaking signals of Ready To Send (RTS) and Clear To Send (CTS). When a node wishes to communicate with the access point it sends a RTS signal to the access point. Once the access point defines that it can then communicate, the access point sends a CTS message. The node can then send its data.

Problems with wireless environments

- **Multipath radio wave propagation**. Radio wave propagate outwards in all directions, and will thus hit obstacles, which causes multiple paths for the radio wave. These waves thus add/subtract to signal, and can cause distortion on the wave.
- **Radio data frames collide**. Two or more radio devices can be transmitting a data frame at the same time using the same radio frequency. The data frames may thus collide and cause errors in the data frames.
- **Out-of-range threshold**. Wireless devices which are at the boundary of the wireless domain can suffer from problems with signal strength as the data frames is being transmitted. This will typically occur when a device is moving around the threshold of the domain, as weak signal strengths are more affected by noise than strong ones.
- **Noisy environment**. Many types of electrical equipment can generate high-frequency radio waves, which might interfere with the transmitted data frame.

Multiple paths for the wireless signal

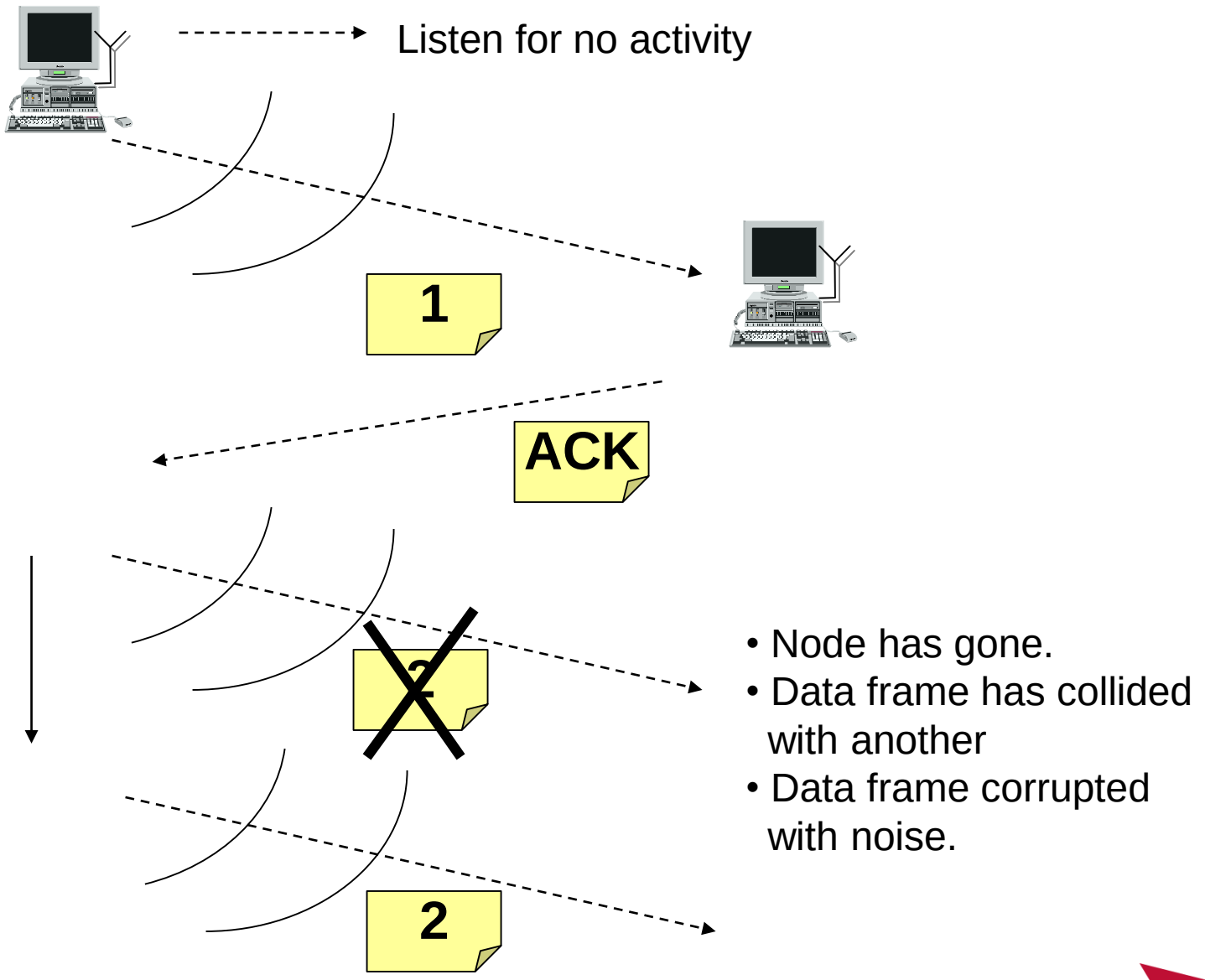


CSMA/CA and PCF

IEEE 802.11 can use two mechanisms for shared access:

- **CSMA/CA**. CSMA/CA is, like standard Ethernet (IEEE 802.3) a contention-based protocol, but uses **collision avoidance** rather than collision detection. It would be impossible to use collision detection as a radio wave is always either sending or receiving and can never do both at the same time. The nodes will thus not be able to listen on the channel while they are transmitting.
- **Point Coordination Function** (PCF). This is an optional priority-based protocol, which provides contention-free frame transfer for transmission of time-critical data, such as real-time video or audio. With this, the point coordinator (PC) operates in the wireless access point and identifies the devices which are allowed to transmit at any given time. Each PC then, with the contention-free (CF) period, the PC polls each of the enabled PCF to determine if they wish to transmit data frames. No other device is allowed to transmit while a another node is being polled. Thus, PCF will be contention-free and enables devices to transmit data frames synchronously, with defined time delays between data frame transmissions.

CSMA/CD



- Node has gone.
- Data frame has collided with another
- Data frame corrupted with noise.

IEEE 802.11 data frame

Frame control	Duration/ ID	Address 1	Address 2	Address 3	Sequence control	Address 4	Frame body	FCS
2 Bytes	**2**	**6**	**6**	**6**	**2**	**6**	**0-2312**	**4**

Frame control. This contains control information.
Duration/ID. This contains information on how long the data frame will last.
Address fields. This contains different types of address, such as an individual address of group addresses. The two main types of group addresses are broadcast and multicast.
Sequence control. This identifies the sequence number of the data frames, and allows the recipient to check for missing or duplicate data frames.
Frame body. This part contains the actual data. The maximum amount is 2312 bytes, but most implementations use up to 1500 bytes.
FCS (Frame Check Sequence). This is a strong error detection code.