2 Wireless Networks

Ref: http://www.asecuritysite.com/wireless/wireless02

2.1 Introduction

This unit gives an outline of the issues involved in wireless networks, and which must be considered in their design. As the world moves slowly towards a massive wireless network, it is important that many of the limiting factors are thought about at this stage, as they may limit their development. Overall there are many problems, but data security and authentication are two of the major ones, especially from a corporate point-of-view. These areas will be looked in a future module.

A key factor in the adoption of wireless networks is the standardization of them by international standards bodies, as this allows consumers to purchase equipment from different manufacturers without having to worry that they will not interconnect, or that they will be incompatible in any way. The leading standards organisation for Layer 1 and Layer 2 communications are the IEEE who developed the famous IEEE 802 standard for which IEEE 802.3 was used to define the standards for Ethernet. It is the 802 standard that that has provide the foundation for networking, and without it the Internet could not have developed so quickly. For wireless networks they have defined a number of standards such as:

- **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.

2.2 IEEE 802.11b

The IEEE 802.11b standard is seen as the benchmark for most wireless networks, and typically defines the lowest common standard for all wireless nodes. Unfortunately it differs in its operation around the World, as the radio spectrum usage varies across different countries. In the USA, for example, there is 11 available radio channels, 14 in Japan, 13 in Europe (ETSI), 2 in Spain and 4 in France. The frequency range also varies, such as between 2.412GHz and 2.472 GHz for Europe.

IEEE 802.11b provides excellent connectivity and reliability for most communications, and uses different modulation techniques for improved connectivity. For this it detects the best modulation technique, depending of the communication path. At 11Mbps, its maximum bandwidth, it uses CCK modulation, which changes to DQPSK at 2Mbps, and BDPSK at 1Mbps. These techniques automatically change as the signal strength reduces, which is typically related to the distance that the nodes are apart, and/or the characteristics of the communications channel. Typically 11Mbps can be used up to 140m (in an clear area with no obstacles), 5.5Mbps up to 200m, and 1Mbps for up to 400m (Figure 2.1). Thus, although the specification defines that it can reach up to 400m, it is unlikely that it will ever reach this as there is likely to be obstacles in the path, which create multipath problems and attenuation. Also, unfortunately, the available bandwidth is the maximum that is possible. In most cases the actual throughput will be much less than this. Many researchers have found that it is only possible to get up to 50% of the maximum available bandwidth as an actual throughput. It should also be remembered that the bandwidth is also shared between all the users using the given channel, thus it is a shared bandwidth. So, in some cases, this can be a fairly chaotic environment, especially when the data traffic is approaching the limit of the bandwidth. The major problem tends to be the design of the TCP algorithm, on which most communications are based, as it will back-off the TCP acknowledge window as the number of errors in transmissions occur. This can produce the sort of characteristic shown in Figure 2.2, where the actual throughput is fairly linear when the required throughput is much less than the bandwidth. When the required through nears the actual maximum there is more contention for network space, and there is more likely to be more errors and collision of radio waves. When it reaches the actual maximum the network is at saturation, and the nodes may think there are too many retransmissions, and close their TCP acknowledge window, where the nodes will wait for acknowledgements to return from the devices between they transmission new data packets.

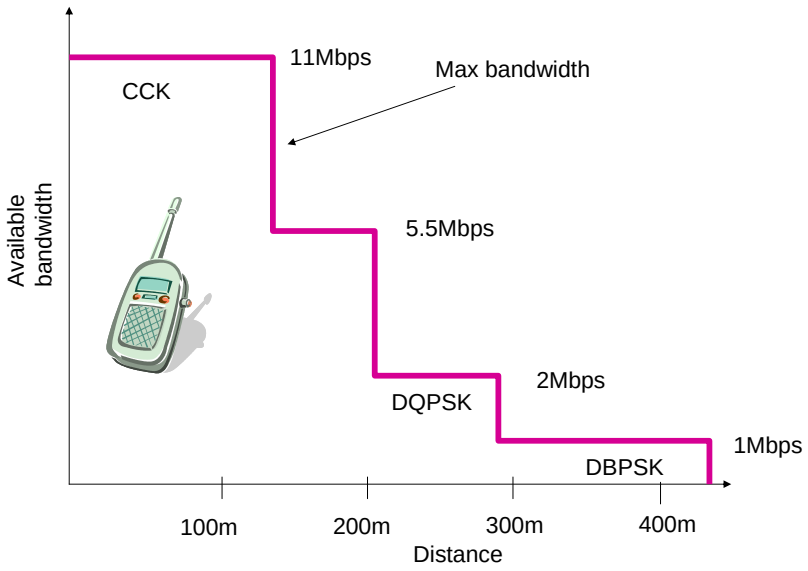

Figure 2.1 Variation of bandwidth over distance

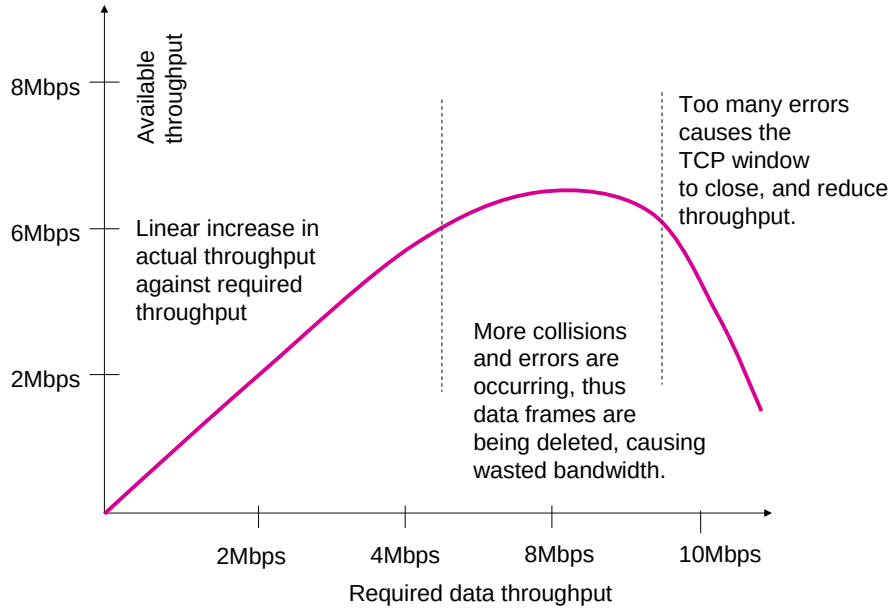

Figure 2.2 Possible variation of available and actual throughput

2.3 Multiple media access

Networking has grown-up through nodes contending for network bandwidth. For example the original version of Ethernet uses a contention algorithm where nodes compete to gain access to the network, and, if two nodes try to gain access to the network, at the same time, they back off for a random period, and one of the nodes thus gains access in favour of the other node. This type of contention is inefficient in the usage of the bandwidth, especially when traffic rates are high, and approaching the capacity of the bandwidth. Luckily network switching has been developed which overcomes this problem when nodes can transmit at any given time, and do not have to contend to gain access to the network. It is thus up to the switch to either send the data at the time that the data is being transmitted, or to buffer it for a future transmission when there is a gap in communications. Unfortunately, with wireless communications, we are almost back in the old days, where nodes again are contending for network access. A network switch, this time, cannot save us, as it would be almost impossible to segment free space up into time slots, and provide buffers which existed in free space (although the GSM/3G network uses a related technique). Thus the major problem is how to allow nodes to gain access to the available media (free-space), in a fair and even way. 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, as illustrated in Figure 2.3.
- **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) oper-

ates 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.

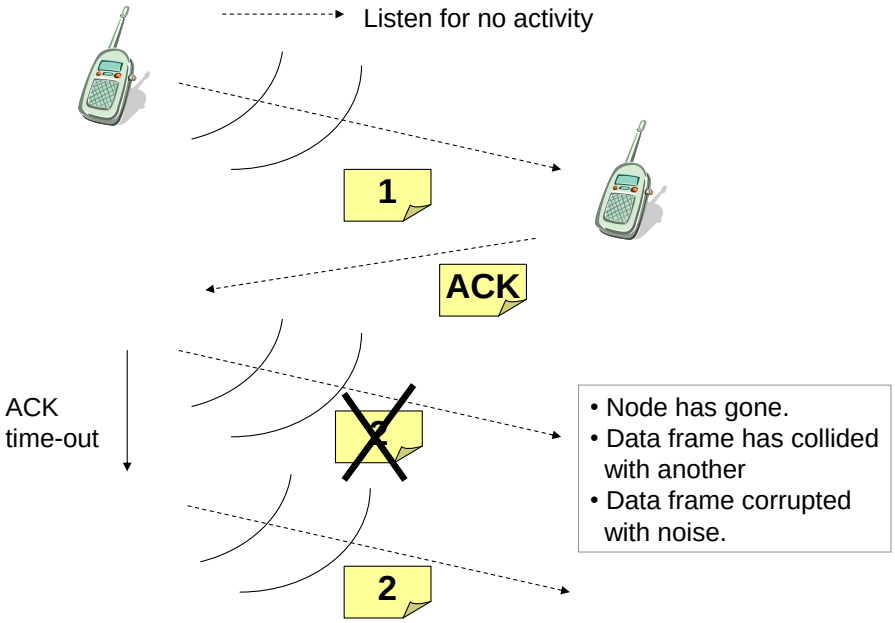

Figure 2.3 CSMA/CA

2.4 Wireless network connections

Wireless networks were originally developed for military operations, where it is important to create networks without any infrastructure, thus the first type of network to be created was an ad-hoc one, where nodes connect to each other and create a network which has no basic infrastructure. This is known as an ad-hoc network, and nodes can add and delete themselves from the network, as they like. Normally, to allow many ad-hoc network to existing at the same time in the same physical location, different frequency channels are used for each ad-hoc network (Figure 2.4). The radio SSID (System Set ID) then defines the unique identifier from the local area (Figure 2.5). In Europe, for example, it would be possible to create up to 14 different ad-hoc networks, within a certain range (between 100 and 400 meters, depending on the environment, and the bit rate).

An infrastructure network uses a central point which is used as a central communication point for all the radio nodes. For range, in an ad-hoc network has a range of L meters, then an infrastructure network will have a diameter range of 2L, as illustrated in Figure 2.6.

In both ad-hoc and infrastructure networks, clients can be setup only to connect to one type or another, or to any of them (although, this is not recommended for security). Ad-hoc networks have advantages in situations when no network infra-

structure currently exists, or is possible. Examples of this might be in emergency situations, where the network infrastructure has been destroyed, or, in mobile situations, where nodes are moving. Unfortunately, there are many issues in ad-hoc networks which make them difficult to control, especially from a security and authentication point-of-view. Thus infrastructure networks have become the most common type, as they are easier to control the access of nodes to the network, and to filter their traffic. Ad-hoc networks, though, should not be dismissed and have their applications, and may also provide a model of the Internet of the future, but, while both modes are supported by wireless clients it gives an alternative design method.

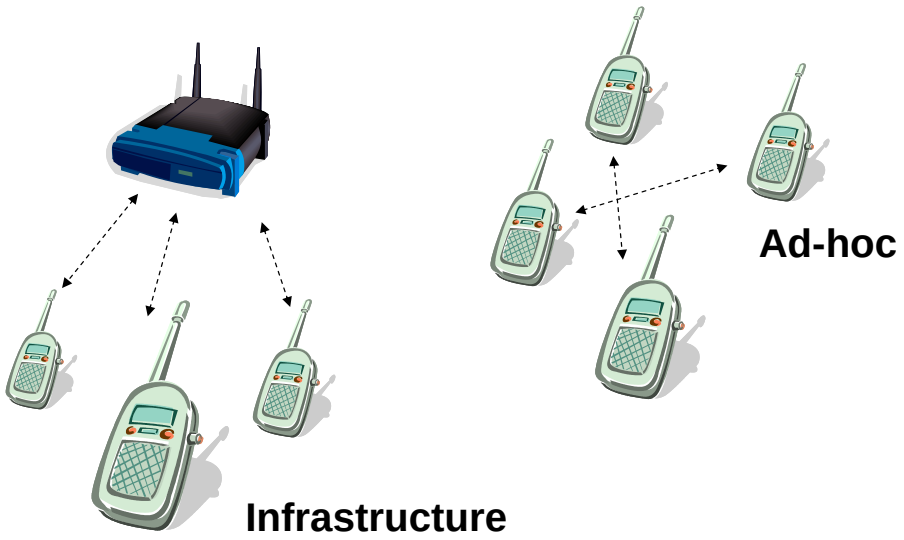

Figure 2.4 Infrastructure network

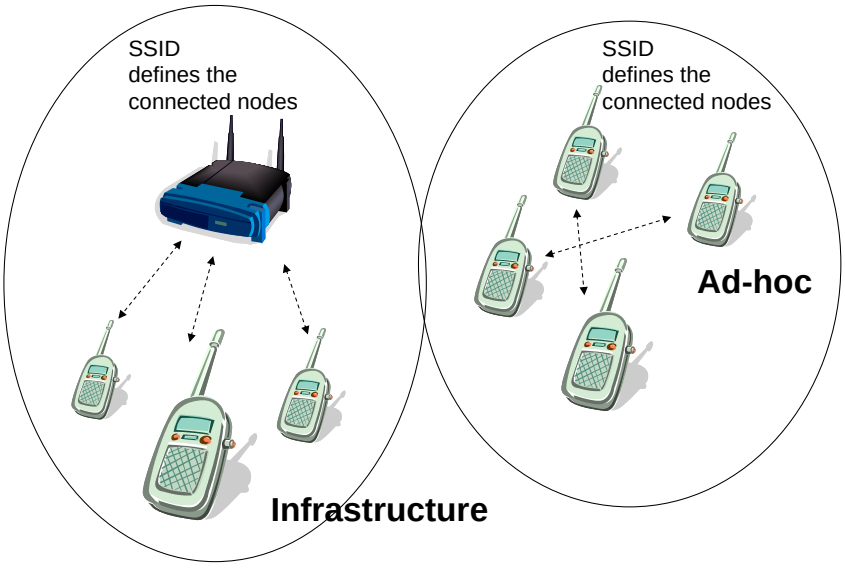

Figure 2.5 SSID for a wireless network

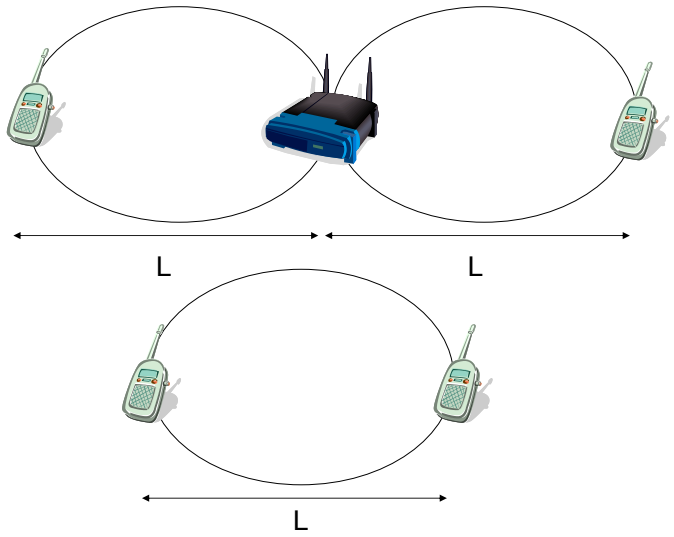

Figure 2.6 Span of networks

2.5 Wireless Configuration

This section outlines some of the main properties which must be configured on an infrastructure network. One of the most popular access points for creating infrastructure networks is the Cisco Aironet 1200 device, which is an industry-standard wireless access point. It has two main networking ports: radio port named Dot11radio0 (**D0**) and an Ethernet one (**E0** or **FA0**). Each of these ports can programmed with an IP address, but a special port named BVI1 is normally used to define the IP address for both ports. Figure 2.7 outlines this, and how the port is programmed.

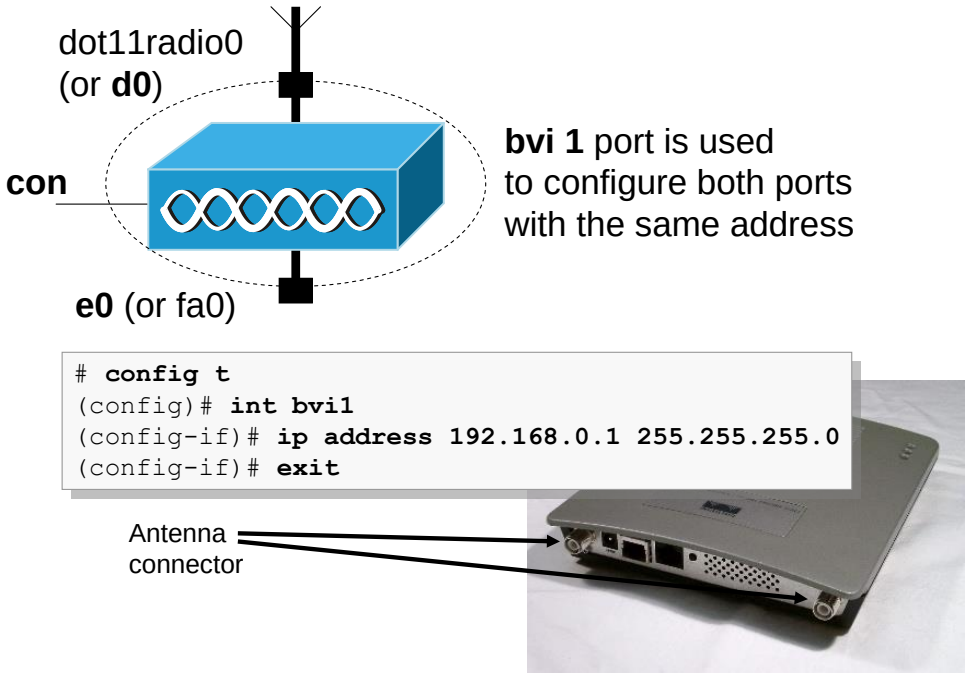

Figure 2.7 Setting the IP address of the wireless access point

2.5.1 Station-role

The wireless access point can either be a root device, where it connects to a fixed network, or a repeater device, which does not connect to the fixed network, as illustrated in Figure 2.8. These are defined from within the D0 port configuration. Another important configuration is the **default-gateway** which is used in order to redirect any data packets which are not destined for the local network. For this the wireless access point will send these data packets which have an unknown destination to the default gateway, which will, hopefully, find a destination for them, or at least know of another router which might be able to help on routing the packets. In most cases the default-gateway is defined as the IP address of the router port which connects to the Ethernet connection of the wireless access point. An example configuration is:

```
# config t
(config)# ip default-gateway 192.168.1.254
(config)# exit
```

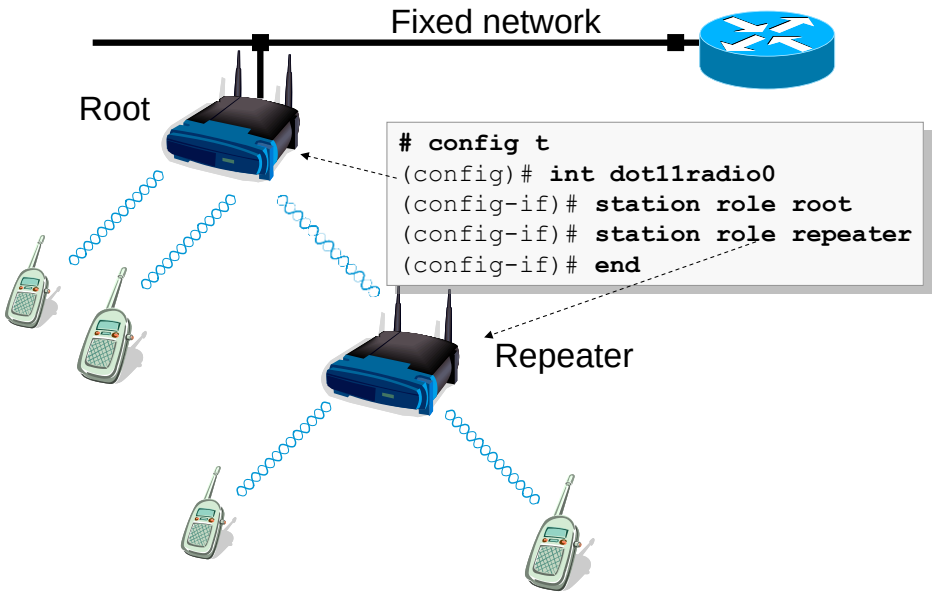

Figure 2.8 Defining the role of the wireless access point

2.5.2 Channel setup

The channel setting is an important one, as it defines the basic identification of the communications channel. In Europe there are 14 channels available which limits the number of simultaneous connections, where each channel is numbered from 1 to 14, each of which has their own transmission/reception frequency, as illustrated in Figure 2.9. Careful planning of these channels is important, especially in creating wireless domains which are overlapping as this allows users to roam around the physical space. The example in Figure 2.9 shows that it is possible to achieve good coverage, without overlapping domains with the same frequency, with just three channels.

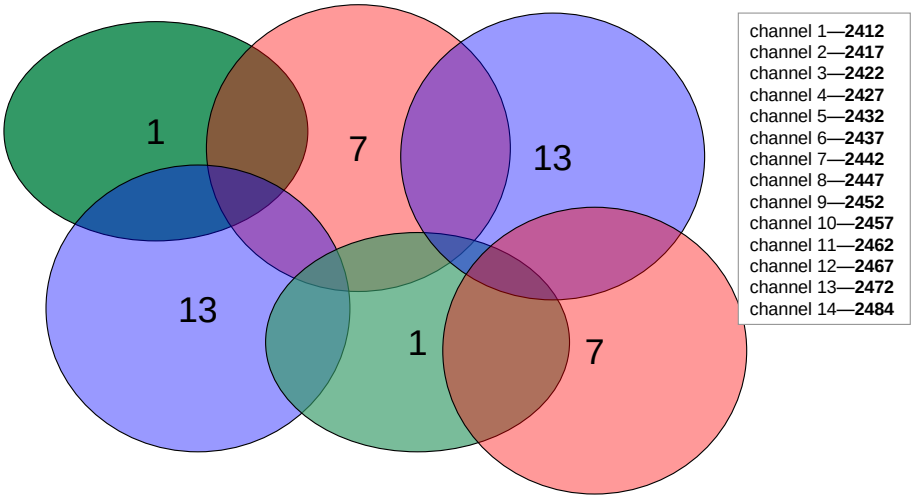

Figure 2.9 Channels in an area

The definition of the channel is defined within the D0 interface:

```
(config)# int dot11radio0
(config-if)# channel ?
  <1-2472>          One of: 1 2 3 4 5 6 7 8 9 10 11 12 13 2412 2417 2422 2427
                    2432 2437 2442 2447 2452 2457 2462 2467 2472
  least-congested   Scan for best frequency
(config-if)# channel 7
(config-if)# no shutdown
```

2.5.3 SSID

The radio SSID (Service Set ID) uniquely identifies a wireless network within a limited physical domain. It is setup within the access point with:

```
# config t
(config)# int dot11radio0
(config-if)# ssid fred
(config-if-ssid)# guest-mode
```

which sets up an SSID of **fred**, and allows guest-mode. Along with the SSID it is also possible to define a beacon time where a beacon signal is sent out at a given time interval, such as:

```
# config t
(config)# int dot11radio0
(config-if)# beacon ?
  dtim-period   dtim period
  period        beacon period
(config-if)# beacon period ?
  <20-4000>  Kusec (or msec)
(config-if)# beacon period 1000
```

which defines the beacon period of 1000 ms (1 seconds).

2.5.4 Fragment threshold

A wireless data frame can have up to 2312 data bytes in the data payload. This large amount could hog the bandwidth too much, and not give an even share to all the

nodes on the network, as illustrated in Figure 2.10. Research has argued that creating smaller data frames, often known as cells, is more efficient in using the available bandwidth, and also for switching data frames. Thus wireless systems provides a fragment threshold, in which the larger data frames are split into smaller parts, as illustrated in Figure 2.11. An example of the configuration is:

```
# config t
(config)# int dot11radio0
(config-if)# fragment-threshold ?
  <256-2346>
(config-if)# fragment-threshold 700
```

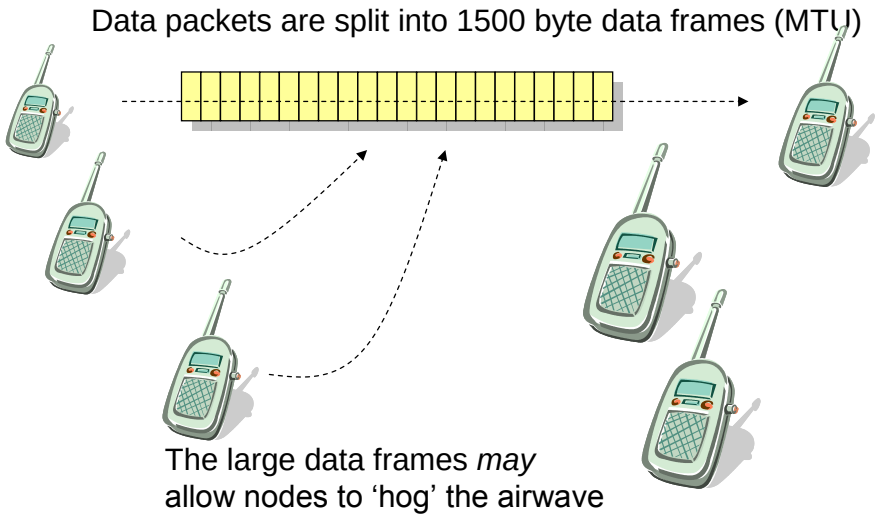

Figure 2.10 Transmission of large data frames

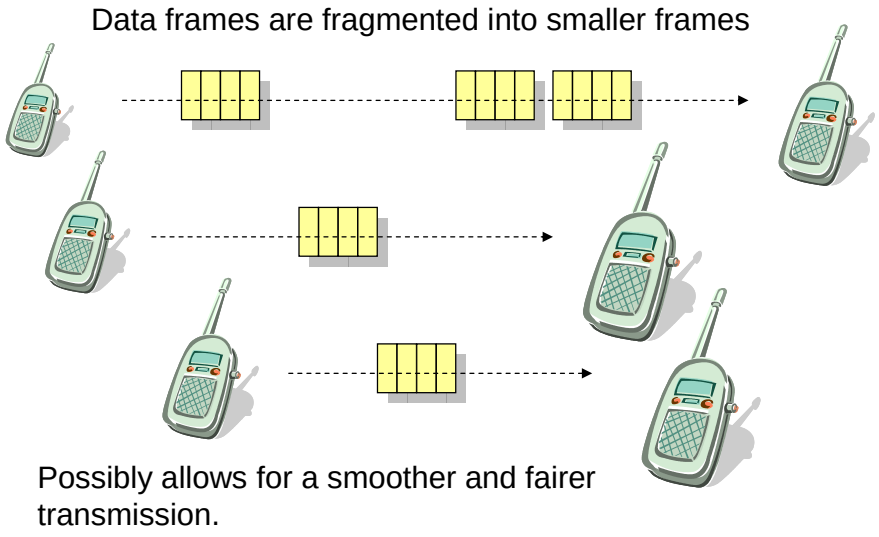

Figure 2.11 Fragmentation of data frames

2.5.5 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 illustrated in Figure 2.12. 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, tit sends a CTS signal. The node can then send its data, as illustrated in Figure 2.13. RTS threshold determines the data frame size that is required, in order for it send an RTS to the WAP. The default value is 4000.

```
# config t
(config)# int dot11radio0
(config-if)# rts ?
  retries    RTS max retries
  threshold  RTS threshold
(config-if)# rts threshold ?
  <0-2347>  threshold in bytes
(config-if)# rts threshold 8000
```

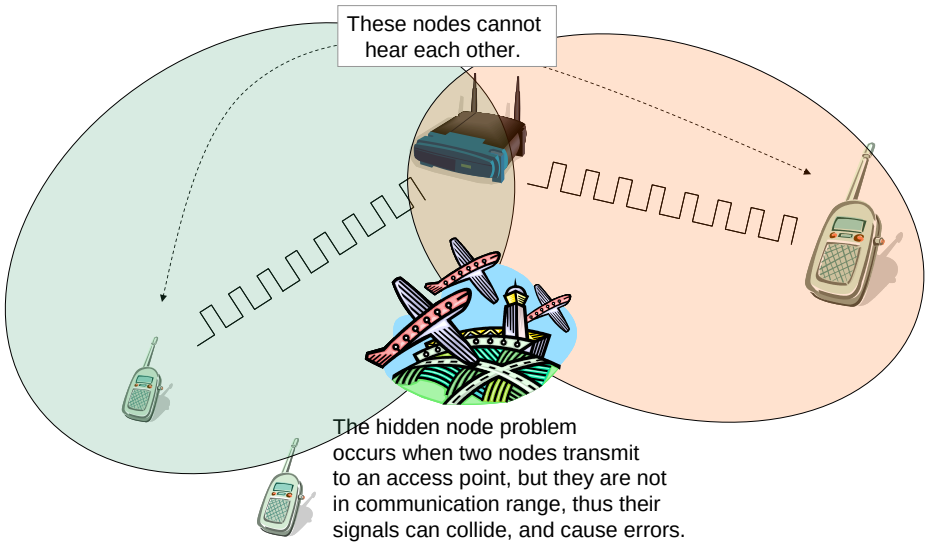

Figure 2.12 Hidden node problem

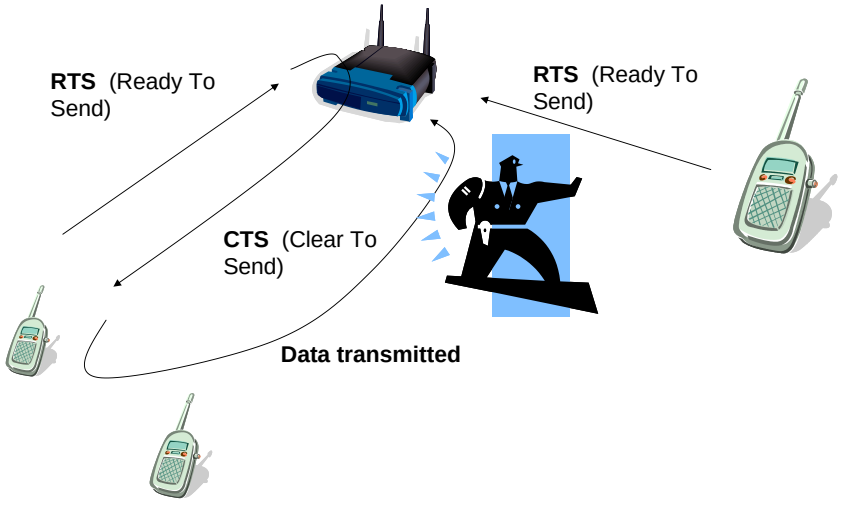

Figure 2.13 RTS/CTS operation

RTS retries defines the number of times that an access point will transmit an RTS signal before it stops sending the data frame. Values range from 1 to 128. For example:

```
# config t
(config)# int dot11radio0
(config-if)# rts retries ?
  <1-128>  max retries
(config-if)# rts retries 10
(config-if)# end
```

2.5.6 Power settings

The power of the access point and also of the clients are important as they will define the coverage of the signal, and must also be within the required safety limits. Thus, the more radio power that is used to transmit the signal, the wider the scope of the wireless network. Unfortunately, the further that the signal goes, the more chance that an intruder can pick up the signal, and, possibly, gain access to its contents, as illustrated in Figure 2.14. To control this power, the access point can set up its own radio power, and also is able to set the power transmission of the client adapter. An example in setting the local power, and the client is shown next:

```
# config t
(config)# int dot11radio0
(config-if)# power ?
(config-if)# power local ?
  <1-50>   One of: 1 5 20 30 50
  maximum  Set local power to allowed maximum
(config-if)# power local 30
(config-if)# power client ?
  <1-50>   One of: 1 5 20 30 50
  maximum  Set client power to allowed maximum
(config-if)# power client 10
```

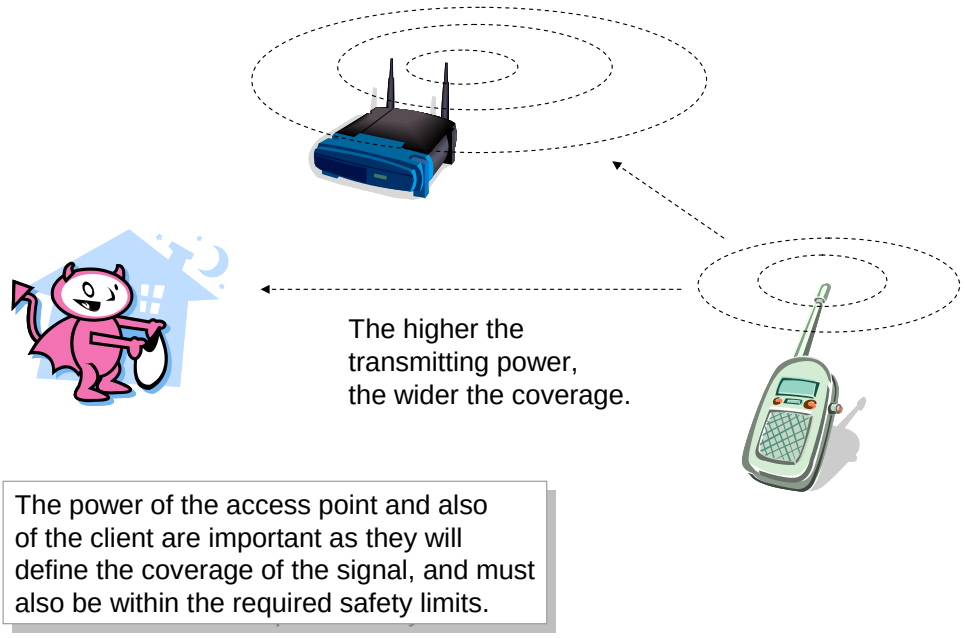

Figure 2.14 Power transmission

One the client, especially with portable devices, the power usage of the radio port is important. Thus there are typically power settings, such as:

- **CAM** (Constant awake mode). Used when power usage is not a problem.
- **PSP** (Power save mode). Power is conserved as much as possible. The card will typically go to sleep, and will only be awoken by the access point, or if there is activity.
- **FastPSP** (Fast power save mode). This uses both CAM and PSP, and is a compromise between the two.

2.5.7 Authentication algorithm

This sets whether the client 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). This area will be covered in a future unit. An example of open authentication is:

```
# config t
(config-if)# ssid fred
(config-if-ssid)# ?
(config-if-ssid)# authentication ?
client          LEAP client information
key-management  key management
network-eap     leap method
open            open method
shared          shared method
(config-if-ssid)# authentication open
(config-if-ssid)# exit
(config-if)# exit
(config)# exit
```

2.5.8 Maximum associations

A particular problem in wireless networks is that the access point may become overburdened with connected clients. This could be due to an attack, such as **DoS** (Denial of Service), or due to **poor planning**. To set the maximum number of associations, the max-associations command is used within the SSID setting:

```
# config t
(config)# int dot11radio0
(config-if)# ssid fred
(config-if-ssid)# max ?
  <1-255>  association limit
(config-if-ssid)# max 100
(config)# exit
```

and to show the associations for the wireless access point:

```
# show dot11 ?
# show dot11 association
# show dot11 statistics client-traffic
```

and for associated access points:

```
# show dot11 adjacent-ap
```

2.5.9 Speed

In some network it is necessary to define the transmission speeds for the nodes, especially to limit their transmission rates. For this the speed command can be used to fix the transmit speed with:

```
(config)# int dot11radio0
(config-if)# speed ?
  1.0          Allow 1 Mb/s rate
  11.0         Allow 11 Mb/s rate
  2.0          Allow 2 Mb/s rate
  5.5          Allow 5.5 Mb/s rate
  basic-1.0    Require 1 Mb/s rate
  basic-11.0   Require 11 Mb/s rate
  basic-2.0    Require 2 Mb/s rate
  basic-5.5    Require 5.5 Mb/s rate
  range        Set rates for best range
  throughput   Set rates for best throughput
  <cr>
(config-if)# speed 1.0
```

2.5.10 Preamble

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. To set short preamble:

```
# config t
(config)# int dot11radio0
(config-if)#  preamble-short
(config-if)# end
```

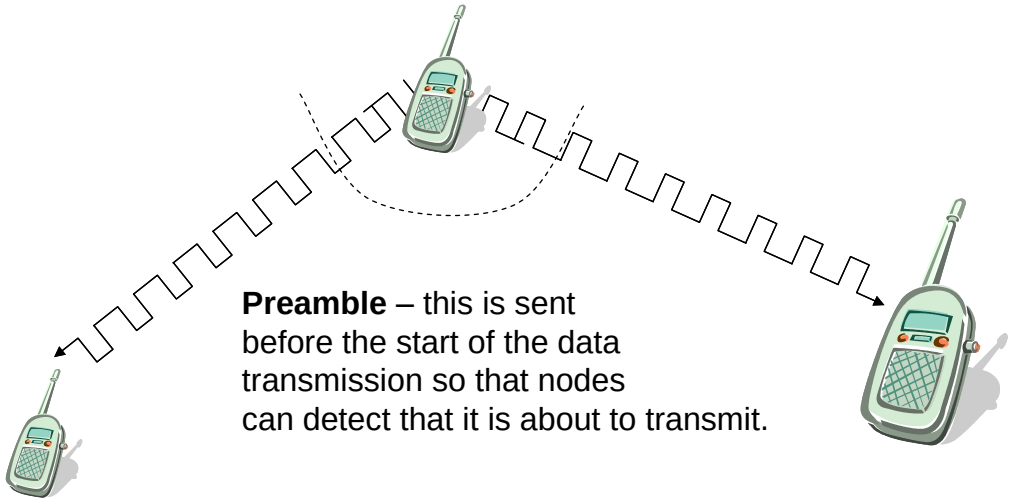

Figure 2.15 Preamble

2.6 Reference

D0 commands:

```
  access-expression       Build a bridge boolean access expression
  antenna                 dot11 radio antenna setting
  arp                     Set arp type (arpa, probe, snap) or timeout
  bandwidth               Set bandwidth informational parameter
  beacon                  dot11 radio beacon
  bridge-group            Transparent bridging interface parameters
  broadcast-key           Configure broadcast key rotation period
  carrier-delay           Specify delay for interface transitions
  cdp                     CDP interface subcommands
  channel                 Set the radio frequency
  countermeasure          countermeasure
  crypto                  Encryption/Decryption commands
  custom-queue-list       Assign a custom queue list to an interface
  default                 Set a command to its defaults
  delay                   Specify interface throughput delay
  description             Interface specific description
  dot11                   IEEE 802.11 config interface commands
  dot1x                   IEEE 802.1X subsystem
  encryption              Configure dot11 encryption parameters
  exit                    Exit from interface configuration mode
  fair-queue              Enable Fair Queuing on an Interface
  fragment-threshold      IEEE 802.11 packet fragment threshold
  help                    Description of the interactive help system
  hold-queue              Set hold queue depth
  infrastructure-client   Reserve a dot11 virtual interface for a WGB client
  ip                      Interface Internet Protocol config commands
  keepalive               Enable keepalive
  l2-filter               Set Layer2 ACL for packet received by upper layer
                          protocols
  load-interval           Specify interval for load calculation for an
                          interface
  logging                 Configure logging for interface
  loopback                Configure internal loopback on an interface
  mac-address             Manually set interface MAC address
  max-reserved-bandwidth  Maximum Reservable Bandwidth on an Interface
  mtu                     Set the interface Maximum Transmission Unit (MTU)
  no                      Negate a command or set its defaults
  ntp                     Configure NTP
  packet                  max packet retries
  parent                  Specify parents with which to associate
  payload-encapsulation   IEEE 802.11 packet encapsulation
  power                   Set radio transmitter power levels
  preamble-short          Use 802.11 short radio preamble
  priority-group          Assign a priority group to an interface
  random-detect           Enable Weighted Random Early Detection (WRED) on an
                          Interface
  rts                     dot11 Request To Send
  service-policy          Configure QoS Service Policy
  shutdown                Shutdown the selected interface
  snmp                    Modify SNMP interface parameters
  speed                   Set allowed radio bit rates
  ssid                    Configure radio service set parameters
  station-role            role of the radio
  timeout                 Define timeout values for this interface
  traffic-class           802.1D traffic class
  transmit-interface      Assign a transmit interface to a receive-only interface
  tx-ring-limit           Configure PA level transmit ring limit
  world-mode              Dot11 radio world mode
```

SSID commands:

```
  accounting           radius accounting
  authentication       authentication method
  exit                 Exit from ssid sub mode
  guest-mode           guest ssid
  infrastructure-ssid  ssid used to associate to other infrastructure devices
  ip                   IP options
  max-associations     set maximum associations for ssid
  no                   Negate a command or set its defaults
  vlan                 bind ssid to vlan
  wpa-psk              Configure Wi-Fi Protected Access pre-shared key
```