Building Wireless Community Networks

Kennedy Ronoh

Objectives

- At the end this module, learners will be able to:
  - Explain wireless network options and standards for community networks
  - Explain how to conduct a viability study for a wireless community network
  - Calculate a link budget
  - Distinguish between various components of a network
  - Explain the different network topologies applicable to a wireless network

Outline

- Wireless Networking
  - Why Wireless for CNs
  - Why WiFi for CNs
  - Last mile, middle mile and first mile
  - IEEE 802.11 Standards
- Radio Physics
- Viability Study
- Radio Link Design

Outline

- Network Infrastructure Components
  - OSI Model
  - Components: Router, Switch, Firewall, Access Point, Wireless Router
- Network Topologies
  - Star
  - Mesh

Wireless Networking

Why Wireless for CNs

- CNs are often deployed using wireless technologies because it is cheaper to roll out a wireless network.
- Wireless network options for CNs:
  - Wimax
  - WiFi
  - Cellular Networks (LTE)
  - TV White Spaces

Why WiFi for CNs

- WiFi is the preferred wireless technology for wireless community networks because it is cheaper that other wireless technologies.
- WiFi is cheaper because of the following reasons:
  - Lower hardware cost
  - Uses unlicensed spectrum – the ISM band (2.4GHz and 5GHz) – no need to pay spectrum fees.

WiFi (IEEE 802.11) Generations

1997	802.11b
1999	802.11b
|	802.11a
2003	802.11g802.
2009	802.11n (Wi-Fi 4)
2014	802.11ac (Wi-Fi 5)
2019	802.11ax (Wi-Fi 6)
|	802.11ax (Wi-Fi 6E)
Future	802.11be (Wi-Fi 7) ?

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

WiFi 5 vs WiFi 6 vs WiFi 6E

	Wi-Fi 5	Wi-Fi 6	Wi-Fi 6E
Availability	Now	Now	2020/2021
Spectrum (GHz)	2.4, 5	2.4, 5	6 (7x 160Mhz channels, no DFS)
Channel Bandwidth (MHz)	20, 40, 80, 80+80, 160	20, 40, 80, 80+80, 160	20, 40, 80, 80+80, 160
MU-MIMO	Downlink (4x4 DL, 1x1 UL)	Downlink and Uplink (8x8 DL and UL)	Downlink and Uplink (8x8 DL and UL)
Modulation	16/64/256QAM	16/64/256/1024QAM	16/64/256/1024QAM
Clients per Channel	OFDM – 1 client (20MHz channel)	OFDMA – up to 74 clients (160MHz channel)	OFDMA – up to 74 clients (160MHz channel)
Max Data Rate	3.5Gb/s	9.6Gb/s (1.5Gb/s per device)	9.6Gb/s (2.3Gb/s per device)

Last Mile, Middle Mile and First Mile

FIRST MILE

The greater Internet. Big "pipes" transmitting data between large servers.

MIDDLE MILE

The network connection between the last mile and greater Internet.

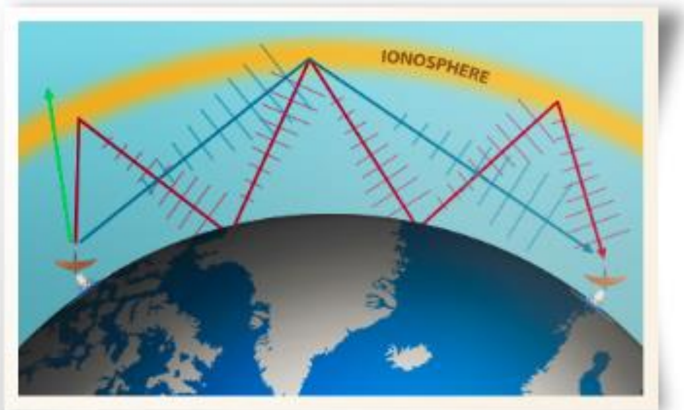
LAST MILE

The final leg of a connection between a service provider and the customer, i.e. into your home.

Connects: Small offices, home

Radio Physics

Radio Propagation



Radio propagation is the behavior of radio waves when they are transmitted, or propagated from one point to another.

As a form of electromagnetic radiation (like light waves), radio waves are affected by the phenomena of:

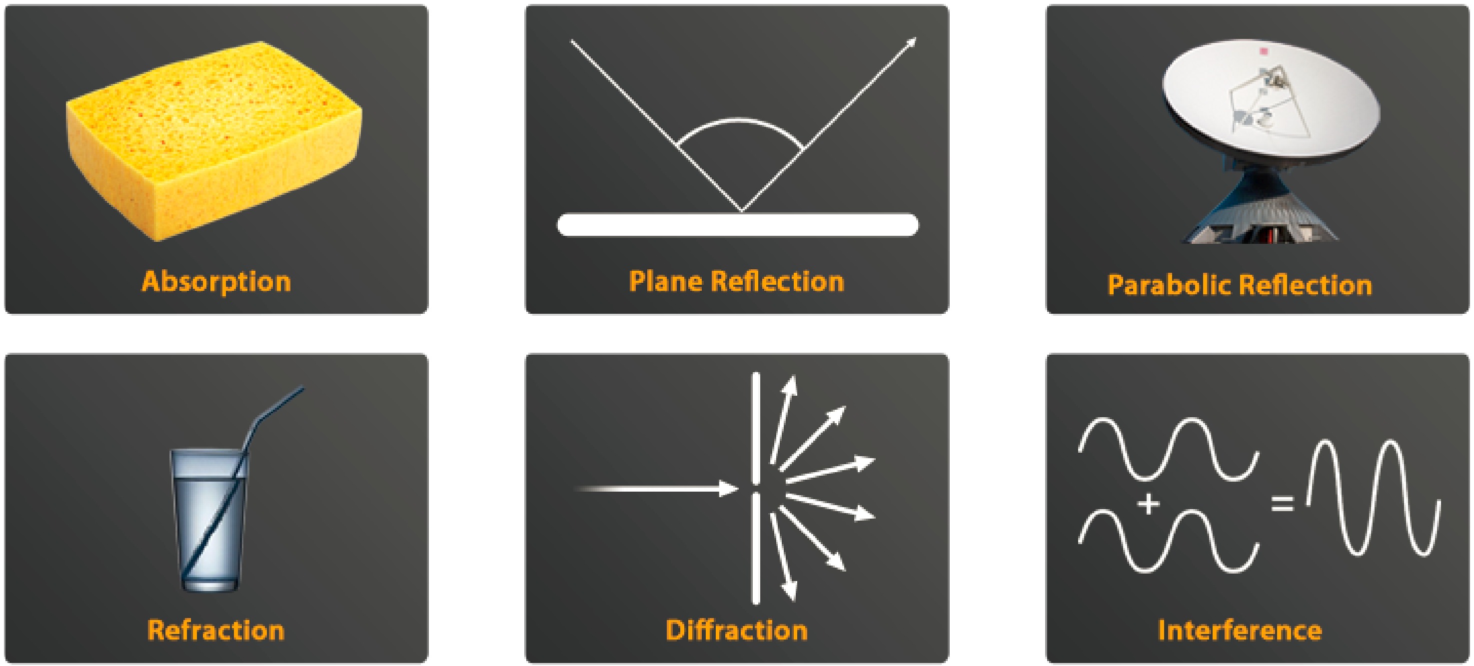
- absorption;
- reflection;
- refraction;
- diffraction; and
- interference.

Radio propagation is affected by the daily changes of water vapor and ionization in the atmosphere due to the sun.

In order to design, build, or maintain reliable wireless systems, you should understand the effects of varying conditions on radio propagation.

Radio Propagation

Electromagnetic waves propagate in the same way as visible light waves do.



Propagation in Free Space

Radio waves are subject to many effects while propagating through free space.

Some of the main effects that need to be taken into consideration are:

Free Space Loss (FSL)

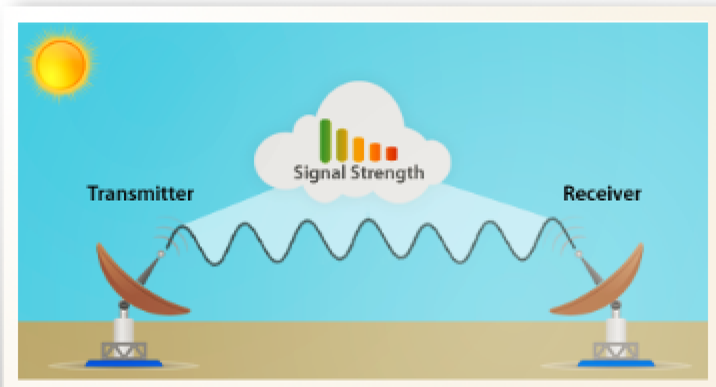
Line of Sight (LOS) and Multipath Effects

Fresnel Zones

Propagation in Free Space

Free Space Loss

The majority of the power of a radio signal will be lost in free space.



The **Free Space Loss (FSL)** measures the power loss in a free space without any kind of obstacles.

Radio signals spreading is the principal contributor to signal loss. As a signal radiates, it spreads or expands.

Case Study

The power loss of electromagnetic waves in free space is:

- proportional to the square of the distance; and
- proportional to the square of the radio frequency.

In the relative unit decibel (dB), that results in:

$$FSL(dB) = 20 \log_{10}(d) + 20 \log_{10}(f) + K$$

In this equation, **d** is the distance from the transmitter, **f** is the frequency of the wave, and **K** is a constant that depends on the units of d and f.

Click here to learn more.

Propagation in Free Space

Line of Sight and Multipath Effects

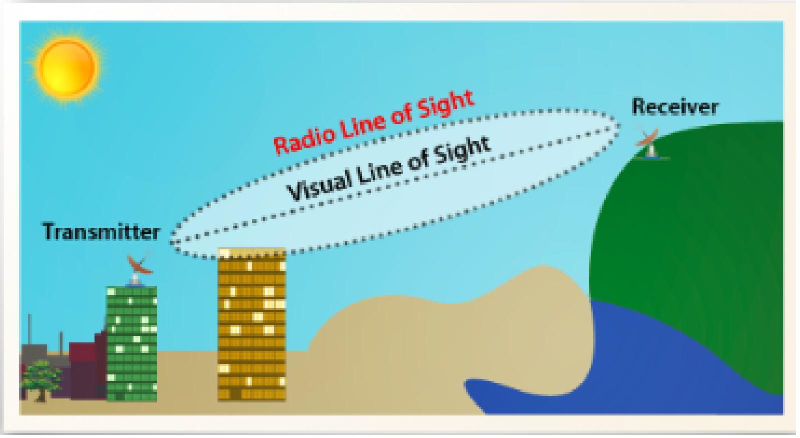
Radio transmission requires a clear path between antennas known as radio line-of-sight.

The visual line-of-sight is easy to understand and verify. For example, using binoculars on a clear day, it is easy to determine if visual line-of-sight exists between two points that are miles apart.

To have a clear line-of-sight there must be no obstructions between the two locations.

However, things are a bit more complicated for radio links as they are not visible for our eyes.

In general an optical line-of-sight is still needed, but there's also the **Fresnel Zones** to take into consideration - this means that space around the optical line of sight also needs to be free.



Propagation in Free Space

Line of Sight and Multipath Effects

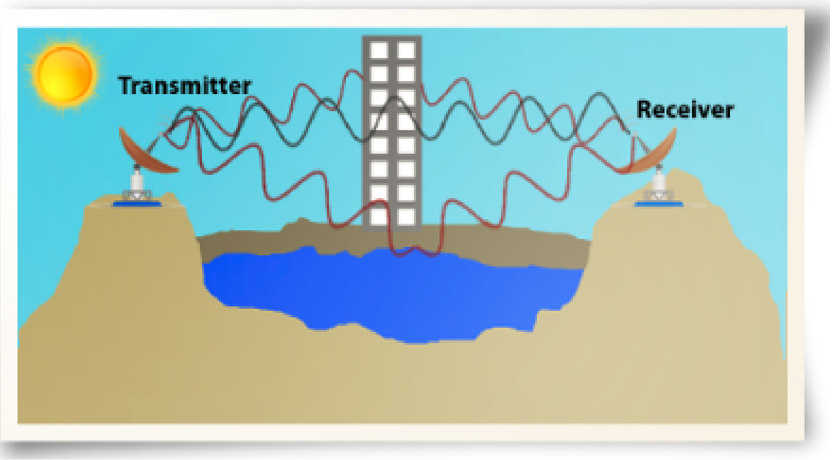
Radio waves will take different paths towards the transmitter, and causes **Multipath Effects**.

The different paths are caused by reflecting off obstacles, so this is especially prevalent when the radio line-of-sight isn't fully clear.

Waves taking different paths can cause delays, interference and partial modification of signals, and can cause big problems when receiving the signal and trying to make sense of it.

Non-Line-of-Sight (NLOS) Link
However, multipath effects aren't all bad. If the technology can handle it, then multipath effects can be exploited to get around the line of sight restriction.

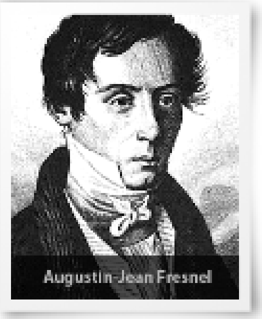
A **NLOS link** can become possible with wireless technologies that are robust enough against multipath effects to let them contribute to the transmission of signals.



Propagation in Free Space

Fresnel Zones

As you now know, radio waves take different paths towards the receiver (because of reflection, diffraction, absorption etc.), and spread out into a certain area around the visual line-of-sight once they leave the transmitter.



This area is called the **Fresnel Zone** and named after **Augustin-Jean Fresnel**.

Although there is more than one Fresnel zone, we are only interested in the first Fresnel zone in this module.

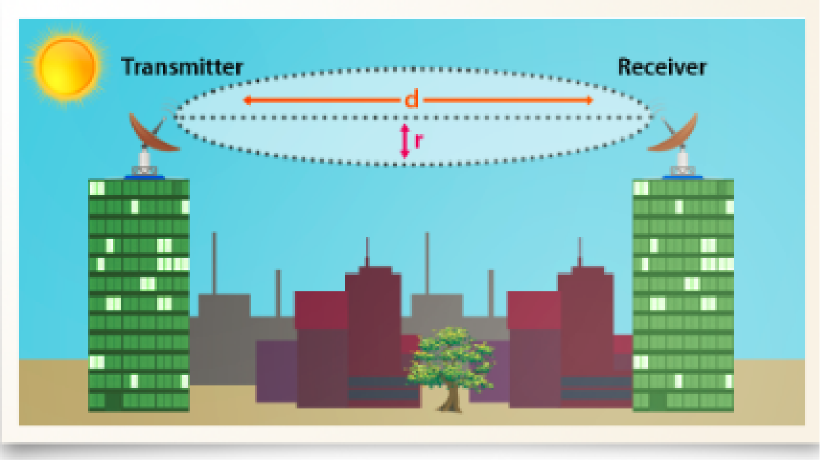
It is essential to know how to calculate the radius of the first Fresnel zone because **the first Fresnel zone must be kept free of obstacles**.

If there are obstacles inside of the Fresnel zone, the reflections of the waves in those obstacles can provoke higher attenuations of the signal in the receiver.

The formula for the first Fresnel zone is:

$$r = 8.657\sqrt{\frac{D}{f}}$$

In this equation, **r** is the radius of the first Fresnel zone in meters, **D** is the distance between transmitter and receiver in kilometers, and **f** is the frequency in hertz.



Propagation in Free Space
Fresnel Zones

Case Study

In a 2.4GHz wireless network at a distance of 100m (0.1km) between the transmitter and receiver, the first Fresnel zone would work out to be:

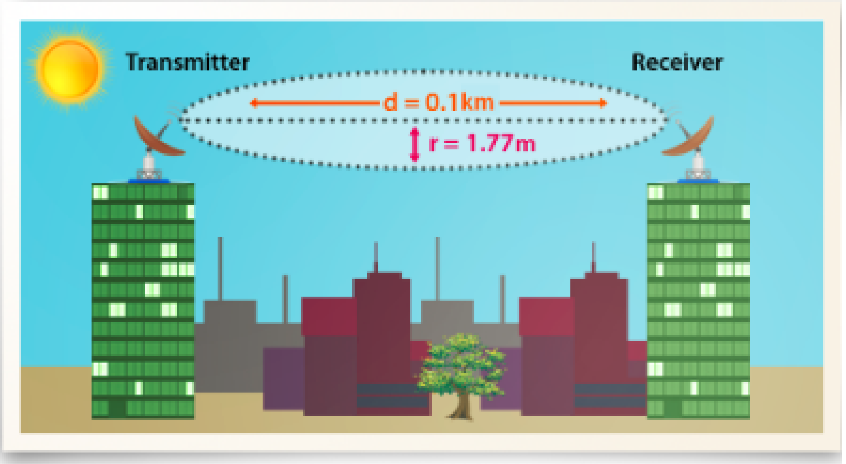
$$r = 8.657\sqrt{\frac{0.1}{2.4}}$$

$$r = 1.77m$$

The first Fresnel zone in this case is 1.77m.

This value is relatively small, but can be considerably larger when the distance is increased or frequency decreased.

The Fresnel zone is definitely something that needs to be considered, especially when the radius is large.



Viability Study

Viability Study

A viability study should answer the following four questions:

Viability Study

1. **What physical infrastructure is available?**
2. **What technical infrastructure is already in use?**
3. **Where is the closest source of power/energy?**
4. **Where is the closest source of Internet connection or communication on site?**

These four questions can have a great impact on the final price of the wireless implementation.

Additional facts that are of importance are:

- Weather conditions (temperature, rain, thunder, humidity);
- Type of terrain (sand, soil, stones);
- Population (sparsely or dense populated);
- Access to road for transportation;
- Radio/tower Legislation;
- Conditions for importing equipment; and
- Communication factors.

Make sure that the viability study is always presented to you (or your organization) face-to-face.

Furthermore, it is a good idea that you have at least one week to go through the written report in advance.

- Details the implementation plan once all the above questions are answered

Viability Study

Existing Physical Infrastructure

In order to be able to evaluate your options for the exact location of the implementation, start by studying existing suitable physical infrastructure on site in terms of existing masts, towers or high buildings.

Ask for available and up-to-date maps of the area to make a theoretical study before making the on-site visit.

The more information you possess in advance, the better chances you will do something useful when you move to the site.

Viability Study

Existing Technical Infrastructure

If any kind of technical infrastructure exists on the site where you want to implement the wireless link, start by contacting your neighbors to get the necessary information regarding their equipment.

This is so you can plan your project without interference.

You can also discuss possibilities for co-location with them.

Viability Study
Access to Power/Energy

When building a wireless link, **access to electricity on the site is of course vital**.

If the equipment is going to be placed on a roof top, powering the equipment with electricity might not be so complicated.

But, if your tower needs to be far away from the closest power grid, you might have to work a bit harder.

If the distance to the closest power grid is reasonable, you should ask the power company for permission to hook on to the network by digging down an extension cable to the grid. Most probably, the connection to the grid has to be performed by the power company themselves.

If the distance is too long, or digging is not feasible for other reasons, another source of energy should be considered, for example wind turbines, or solar panels.

Power Grid

Wind Turbines

Solar Panels

Viability Study

Access to Power/Energy

To ensure reliability of your service, the source of electricity also needs to be reliable. In countries with frequent power cuts and frequency fluctuations, a uninterruptible power supply (UPS) is essential.

Furthermore, when you budget for energy, you should not only budget for the equipment (solar panels, batteries, wind mills, diesel) but for a fixed cost of installation, transport, and yearly maintenance cost.

Viability Study

Communication Factors

In most cases, you will need to procure a source of Internet access at the exact location where your wireless equipment will be located.

This implies that you must extend the Internet connection to the physical location of your wireless equipment.

If possible, **avoid using another wireless link** as this can have serious implications on the overall performance of your main wireless backbone link.

Instead, wire the Internet connectivity (using a fibre, or copper connection) to your wireless backbone. Whether the cable is dug down or placed over ground, the cable needs to be protected from external elements in terms of weather, animals and thieves.

The first enemy of cables are rats and without proper PVC protection the cable will soon be damaged. PVC pipes can be dug down or left on the ground.

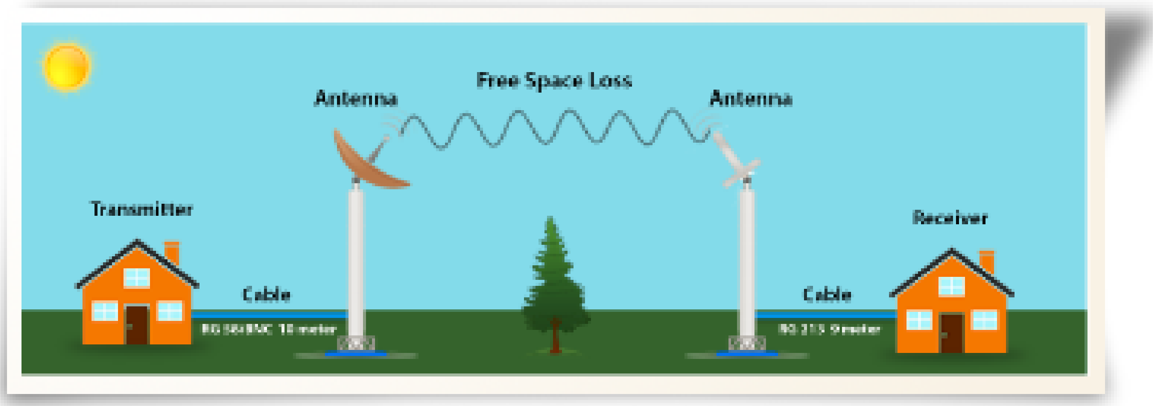
Radio Link Design

- Link budget
- Receiver sensitivity

Establishing a Link Budget

After your viability study for your wireless implementation has been accepted by your stakeholders you will need to move on to the next stage. This involves you making decisions about the equipment you need to buy to ensure that you will achieve a good wireless signal.

This stage is called **Establishing a Link Budget** - but take note that this is not primarily to do with the funds you will need. Its objective is to ensure that your choice of equipment will result in a good functioning link.



Establishing a Link Budget

Having a **good link budget is essential**, as it is the basic requirement of a functioning link.

A link budget is like the foundation of a building; it does not matter how well the floors, walls and roofs are built, if the foundation is weak the whole building will collapse eventually.

A link budget is the sum of all losses and gains across the full link. This includes accounting for all gains and losses from the radio transmitter (source of the radio signal), through cables, connectors and free air to the receiver.

A simple link budget equation looks like this:

Received Power (dbm) = Transmitted Power (dbm) + Gains (dB) – Losses (dB)

Estimating the value of 'power' in different parts of the radio link is necessary to be able to make the best design and the most adequate choice of radio equipment.

Establishing a Link Budget

A link budget is the accounting of all of the gains and losses in a wireless link, and ensuring the receiver can handle the transmitting power . The equation to work out the budget is:

Transmitter Power [dBm] - Cable TX Loss [dB] + Antenna TX Gain [dBi] - Free Space Loss [dB] + Antenna RX Gain - Cable RX Loss [dB] = Margin - Receiver Sensitivity

One aspect that might be surprising is that the equation is adding **dBm**, **dB**, and **dBi** units like they were of the same dimension.

How is it possible to simply add and subtract dBm, dB and dBi?

The answer lies in the fact that the decibel (dB) is a measure of the 'ratio' between two quantities and it is a dimensionless unit like percent (%).

Unit	Description
dB	A dB is a **decibel** and is used for measuring losses in cables and connectors.
dBm	A dBm is a **decibel milli** and is used to express transmitting power.
dBi	A dBi is a **decibel isotropic** and is used for expressing the antenna gain.

Establishing a Link Budget

Transmitting Side - Transmit Power

Transmitter

Transmit power (Tp)
The transmit power is the power output of the radio card.

The upper limit depends on regulatory limits on country/region and point in time. The transmit power of your card can normally be found in the vendor's technical specification.

Keep in mind that the technical specifications will give values tested in a laboratory, real life values may vary with factors like temperature and voltage.

Typical transmission power in IEEE 802.11b and IEEE 802.11a

Protocol	Power
IEEE 802.11b	+18 dBm
IEEE 802.11a	+20 dBm

Information

In our example, we are using the IEEE 802.11b protocol. The typical transmission power is **+18 dBm**.

Establishing a Link Budget

Transmitting Side - Cable Loss

Cable

Cable Loss (CL_{TX})
Losses in the radio signal will take place in the cables that connect the transmitter and the receiver to the antennas.

You will also need to take into account the loss that occurs in the cable connectors.

Click on the images above for further information.

Cables

The amount of loss in cables depend on:

- the type of cable used; and
- the frequency the wireless link is operating at.

Cable loss is usually measured in dB/m, or dB/foot.

Typical loss in cables is around 0.1 dB/m - 1 dB/m.

When calculating the loss of your cable, it is important to make sure we use the right values for the frequency range used in your wireless link.

Check the distributor's data sheets and if possible, verify the losses by taking your own measurements.

As a rule of thumb, we can count double the amount of cable loss [dB] for 5 GHz compared with 2.4 GHz.

For example, if you had cable loss of 1 dB in a 2.4 GHz link, there would be a cable loss of 2 dB in a 5 GHz link.

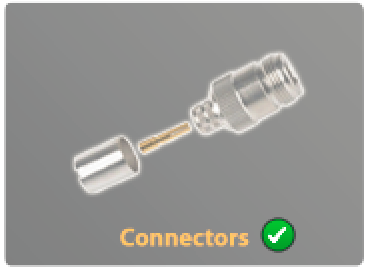
Establishing a Link Budget

Transmitting Side - Cable Loss

Cable

Cable Loss (CL_{TX})
Losses in the radio signal will take place in the cables that connect the transmitter and the receiver to the antennas.

You will also need to take into account the loss that occurs in the cable connectors.



Connectors

Typically each connector may potentially lose 0.25 dB.

This value applies to properly made connectors while badly soldered DIY connectors will imply higher loss. Check data sheets for losses at your frequency range versus the available connector type.

If long cables are used, the accounting of the connector losses is normally included in the "cable loss" part of the equation.

But to be on the safe side, **always assume an average of 0.3 to 0.5 dB** loss per connector as a rule of thumb.

Additionally, **lightning arrestors** that are typically used between antennas and the radio gear behind them **should be budgeted to typically incur a 1 dB loss**.

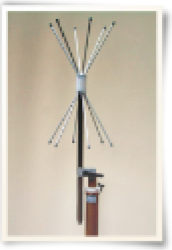
Establishing a Link Budget

Transmitting Side - Antenna Gain

Antenna Gain (G_{TX})

A typical antenna gain ranges from 2 dBi for a simple integrated antenna, to 5 dBi for a standard omni-directional antenna, and even up to 25-30 dBi for a parabolic antenna.

Integrated
2 dBi



Omni-directional
5 dBi

Parabolic
25-30 dBi

Click on the button to the right for more information about industrial antennas, antenna functions, and antenna capabilities

Amplifiers
Amplifiers can be used to compensate for cable loss or for signal boosting. In general, the use of amplifiers should be seen as a last option. Intelligently optimized antennas and high sensitivity in the receiver are better than brute force amplification.

Quality amplifiers depend on frequency characteristics (broadening) and add extra noise to the signal.

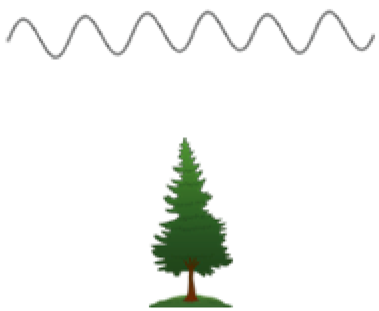
We must consider the legal limits in your target location while adding amplifiers.

Information

In our example, for the transmitting side, we are using a parabolic antenna. We will take the highest possible gain which is **+30 dBi**.

Establishing a Link Budget
Propagation Losses

Free Space Loss



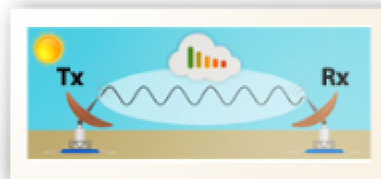
You should remember from **Module 03 - Radio Physics** that propagation losses are related to all attenuation of the signal that takes place when the signal has left the transmitting antenna until it reaches the receiving antenna.

The majority of the power of a radio signal will be lost in the air. Even in a vacuum, a radio wave loses some of its energy since (according to the Huygens Principle) some energy is always radiated in directions other than our link axis.

Note that this has nothing to do with air, fog, rain or any other influence that will further add losses.

Free Space Loss
The Free Space Loss (FSL) measures the power loss in free space without any kind of obstacles.

The radio signal weakens in free space due to its expansion in a spherical surface.



FSL is proportional to:

- the square of the distance; and
- the square of the radio frequency.

In decibel, that results in the following equation:

$$\mathrm{FSL\ (dB)} = 20\log_{10}(d) + 20\log_{10}(f) + K$$

d - distance
f - frequency
K - constant that depends on the units used for d and f

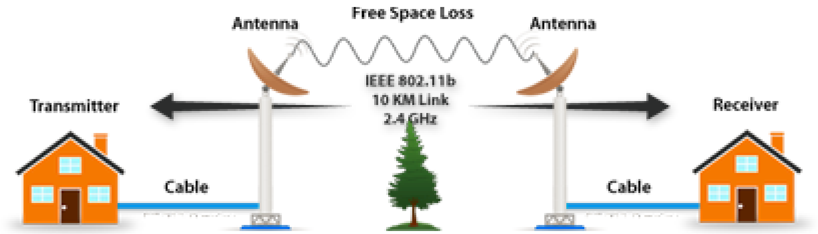
Establishing a Link Budget
Propagation Losses

As a rule of thumb in a 2.4 GHz wireless network, 100 dB are lost in the first kilometre (KM) and the signal is reduced by 6 dB every time the distance doubles.

For example, a 2 KM link has a loss of 106 dB, and 4KM link has a loss of 112 dB

How much loss do you think occurs in a 10km link?

Choose the correct option below and then click on Submit.



- ○ 100 dB
- ○ 112 dB
- ◉ 120 dB

Submit

The following table shows you the Free Space Loss (FSL) in dB for a set of distances and frequencies:

Distance	915 MHz	2.4 GHz	5.8 GHz
1 KM	92 dB	100 dB	108 dB
10 KM	112 dB	120 dB	128 dB
100 KM	132 dB	140 dB	148 dB

These values are theoretical values and can very well differ from your measurements.

The term 'free space' is never quite so 'free', and the losses can be many times larger due to terrain and climate conditions.

Information

In our example, we have a 10 KM link using 2.4 GHz.

This means that the total Free Space Loss is **-120db**.

Establishing a Link Budget

Receiver Side - Antenna Gain

Antenna Gain (G_{RX})
On the receiver side, antenna gain follows the same concept as on the transmitter side.

You should remember from Module 03 that there are many types of antenna.

Type of Antenna	Antenna Gain
Integrated	2 dBi
Omni-directional	5 dBi
Helical	20 dBi
Parabolic	30 dBi

If you are using a Helical antenna on the receiver side, how much antenna gain will there be?

Using the table as a guide, type in the amount of antenna gain on the receiver side, and then click on Submit.

dBi

Submit

Establishing a Link Budget
Receiver Side - Cable Loss

Cable

Cable Loss (CL_{RX})
Cable loss is the **same on the receiver side** as on the transmitter side. Here is a table that shows the typical loss for different types of cables in a 2.4GHz set-up.

Cable Type	Loss (dB/100m)
RG 58/BNC	100 dB
RG 213	50 dB
LMR-200	50 dB
LMR-400	22 dB
Aircom plus	22 dB
LMR-600	14 dB
1/2" Flexline	12 dB
7/8" Flexline	6.6 dB

Imagine we are using a **RG 213 cable**, which has a loss of **0.5dB/m** to connect a receiver to an antenna. We are using **9m** of cable.

Select the value of the loss 9m of RG 213 cable would cause.

- 1.5 dB
- 3 dB
- 4.5 dB
- 6 dB

Submit

Establishing a Link Budget

Now that you know a little about a link budget, we will go through each element of a link budget in detail, and show you an example of the contributions (in decibels) across the transmission path. Our example will be a 10km link working at 2.4 GHz.

T_P	+	CL_{TX}	+	G_{TX}	+	FSL	+	G_{RX}	+	CL_{RX}	=	Margin	-	R_S
+ 18dBm		- 7.5dB		+ 30dBi		- 120dB		+20dBi		- 6dB		-65.5 dB		

Margin: -65.5 dB

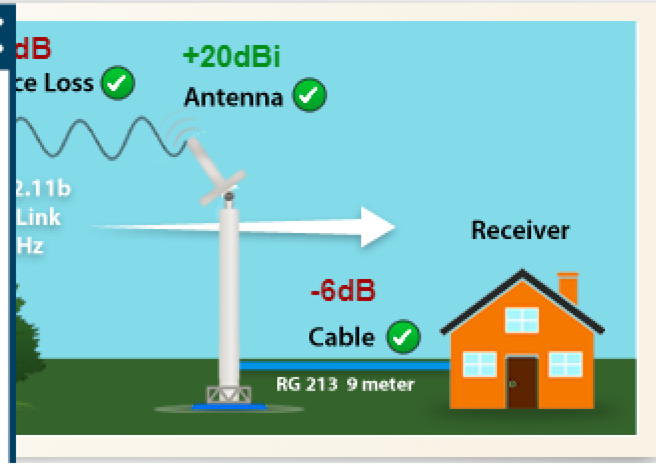
Additional Reading

At this point, you should now have calculated the total margin (-65.5 dB) which is the sum of all gains and losses across the transmission path up to the receiver.

Next you need to subtract the Receiver Sensitivity away from the total margin.

This looks like this:

Margin - Receiver Sensitivity



Establishing a Link Budget
Receiver Side - Receiver Sensitivity

Receiver

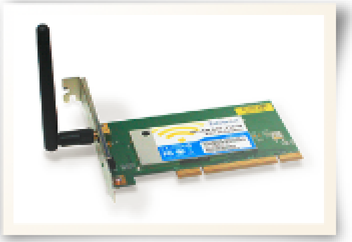
Receiver Sensitivity (R_s)
The sensitivity of a receiver is a parameter that deserves special attention as it indicates the minimum value of power that is needed to successfully decode/extract 'logical bits' and achieve a certain bit rate.

The lower the sensitivity, the better the radio receiver is. A theoretical value is -82 dBm for a 11 Mbps link and -94 dBm for a 1 Mbps link.

A 10 dB difference here (which can easily be found between different cards) is just as important as a 10 dB gain that might be gained by the use of amplifiers or bigger antennas.

Typical values of receiver sensitivity of major types of wireless network cards which support 802.11b

Card	11 Mbps	5,5 Mbps	2 Mbps	1 Mbps
Orinoco cards PCMCIA Silver/Gold	-82 dBm	-87 dBm	-91 dBm	-94 dBm
Senao 802.11b card	-89 dBm	-91 dBm	-93 dBm	-95 dBm



Information

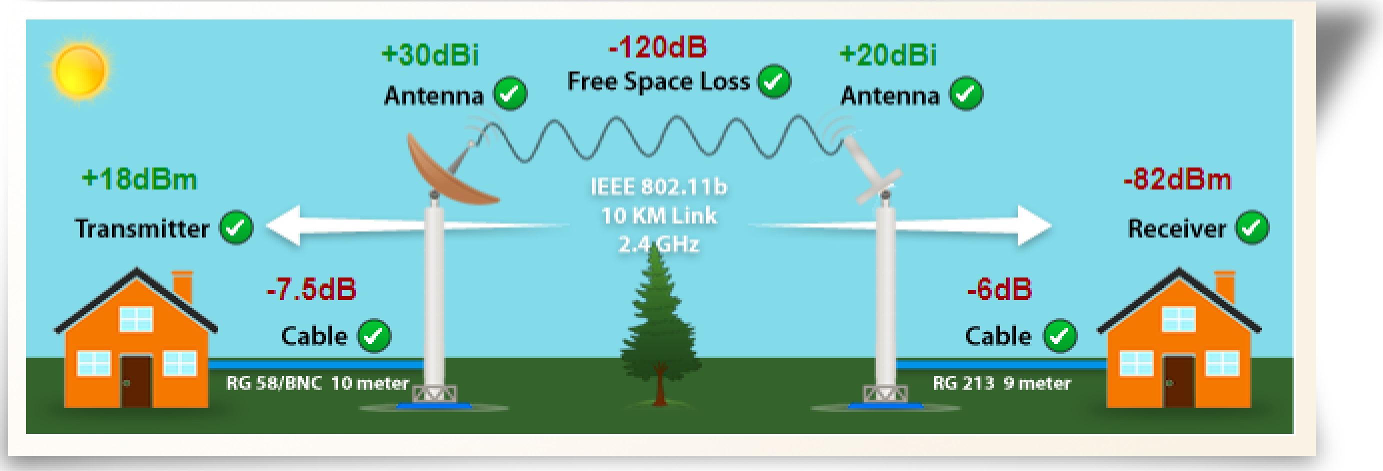
In our example, we are going to use an Orinoco Card at 11 Mbps which supports the 802.11b protocol. This results in a receiver sensitivity of **-82 dBm**.

Establishing a Link Budget

Now that you know a little about a link budget, we will go through each element of a link budget in detail, and show you an example of the contributions (in decibels) across the transmission path. Our example will be a 10km link working at 2.4 GHz.

T_P	+	CL_{TX}	+	G_{TX}	+	FSL	+	G_{RX}	+	CL_{RX}	=	Margin	-	R_S
+ 18dBm		- 7.5dB		+ 30dBi		- 120dB		+20dBi		- 6dB		-65.5 dB		- 82dBm

Radio Link Budget = Margin (-65.5 dB) - Receiver Sensitivity (-82 dBm) = +16.5dB



Now that you have been through the full calculation of a link budget, you should see that the Total Radio Link budget is **+16.5 dB.**

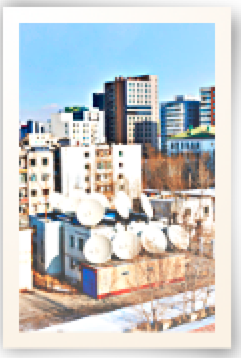
Establishing a Link Budget

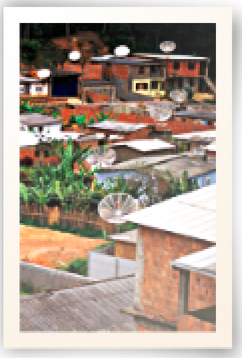
Signal-to-Noise Ratio

The final step when calculating a viable radio link, is to take account of the **noise levels** across the transmission path.

In most rural areas there will be little noise as there will be few (if any) other radio links operating.

In normal rural conditions without any other source in the 2.4 GHz band and without industrial noise, the noise level is around -100 dBm. Here the radio link is only limited by the sensitivity of the receiver. But in urban areas - where there may be many other radio links operating - it is common to see high levels of noise (such as -92 dBm).





In these conditions you will need to do a 'Signal-to-Noise' calculation to work out if your signal will be sufficient to counteract the noise and achieve your required bit rate.

This is known as the **'Signal-to-Noise ratio' (SNR)** and is worked out using the following formula:

Signal to Noise Ratio [dB] = 10 × Log10 (Signal Power [W] / Noise Power[W])

A typical requirement of SNR is:

- 16 dB for an 11 Mbps connection; and
- 4 dB for a 1 Mbps connection.

Establishing a Link Budget

Complete Link Budgets

Link Budget

Distance: 40 KM
Frequency: 2.4 GHz

Element	Value
Transmit output	+18 dBm
Cable and connectors	-10 dB
Antenna TX	+30 dBi
FSL	-131 dB
Antenna RX	+30 dBi
Cable and Connectors	-10 dB
Margin	-73 dB
Receive Sensibility	-89 dBm

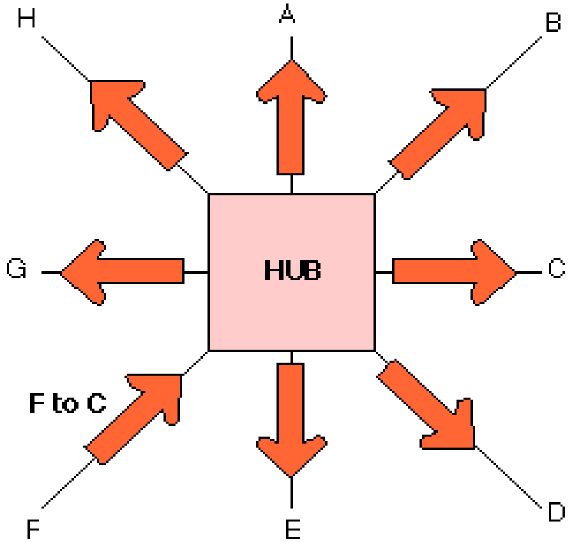
The Total Link budget of this link is +16 dB.

Network Infrastructure Components

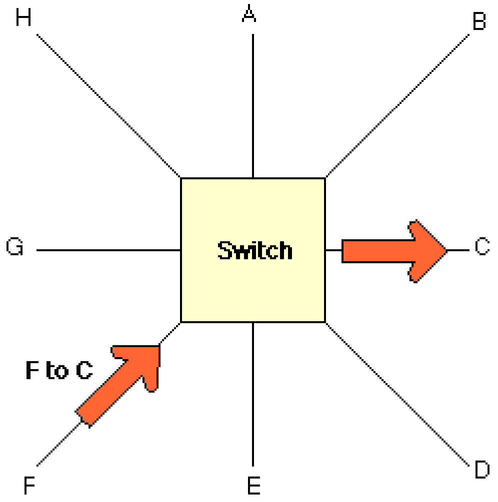
Switches

- N-Port bridge where N is equal to number of stations
- Switches resemble bridges and can be considered as multiport bridges
- Usually used to connect <u>individual computers</u> not LANs like bridge
- Allows more than one device connected to the switch directly to transmit **simultaneously**
- Can operates in **full-duplex** mode (can send and receive frames at the same time over the same interface)
- Performs MAC address recognition and frame forwarding in **hardware (bridge in software)**.
- For the case of a switch, the interconnected LAN segments may use different MAC protocols

Bridges (Switches) Vs. Hubs



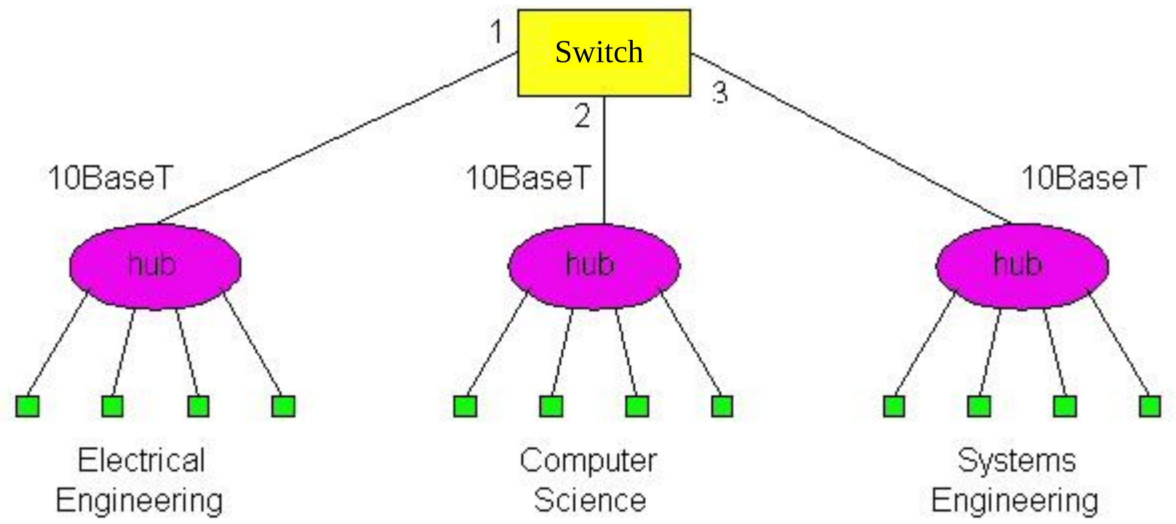
A Hub sending a packet form F to C.



A Switch sending a packet from F to C

Bridge/Switch features

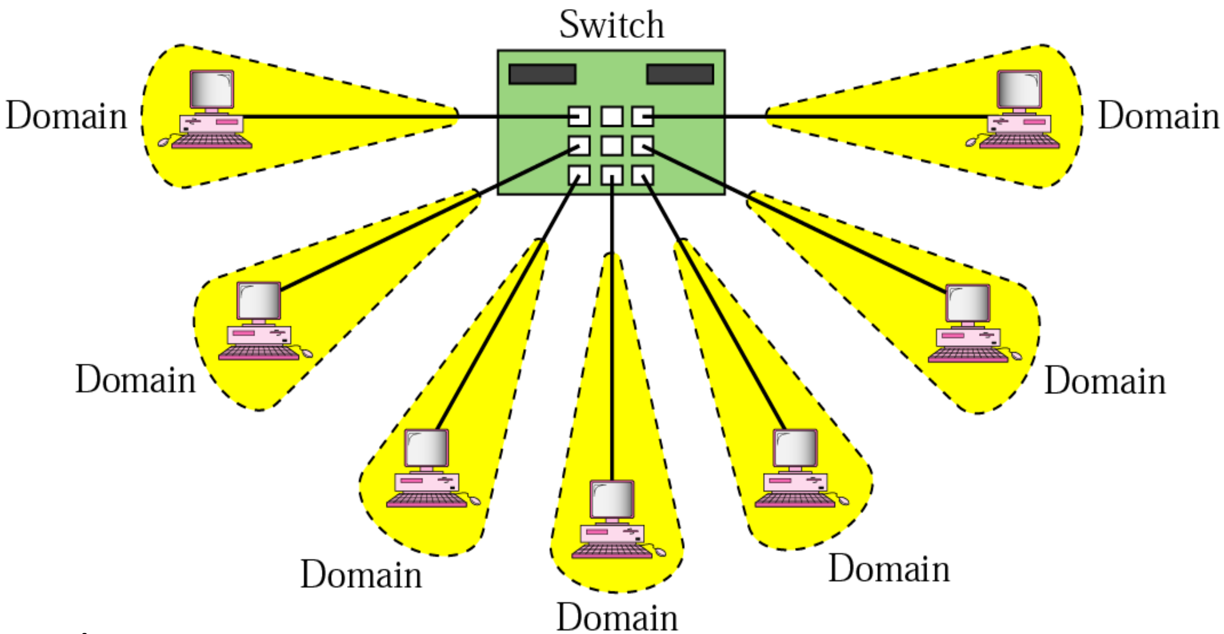
- Implements CSMA/CD
- Switches isolate collision domains (each LAN segment is a separate collision domain), THIS WILL REDUCE THE POSSIBILITY OF COLLISIONS AND result in **higher total max throughput**
- Switch forwards a frame with **broadcast address** to **all** devices attached to the whole network (**single broadcast domain**)
- **Transparent**: installing or removing a switch does not require the stations networking software to be reconfigured.
- ("**plug-and-play**"): *no configuration necessary* at installation of switch /switch or when a host is removed from one of the LAN segments



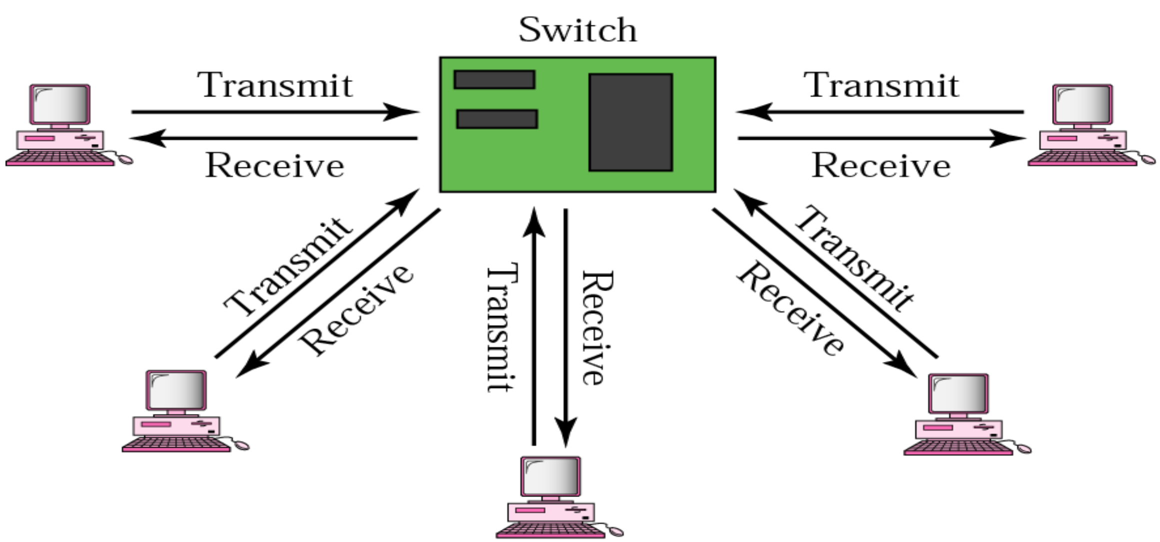
Example:

Three LANs connected through a bridge
Note: here we have ***three collision*** domains and *a **single broadcast*** domain

Isolated collision domains



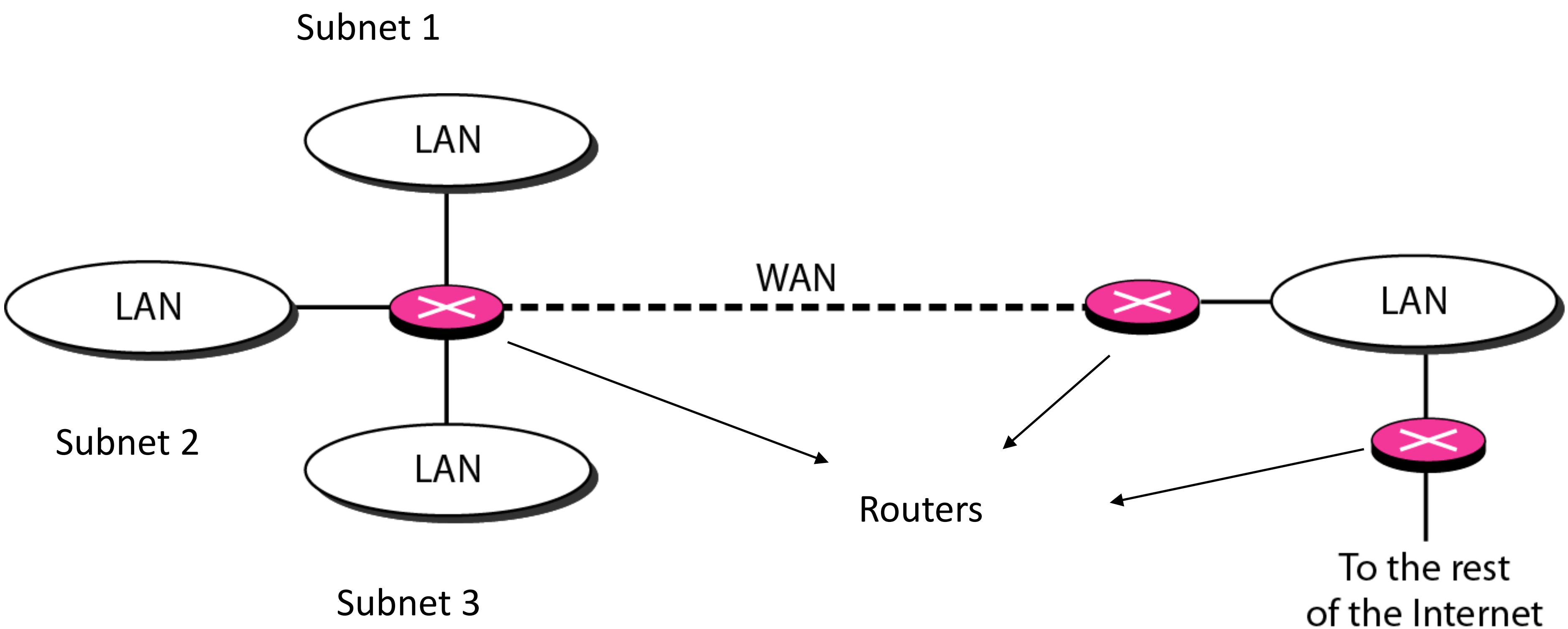
Full-Duplex operation



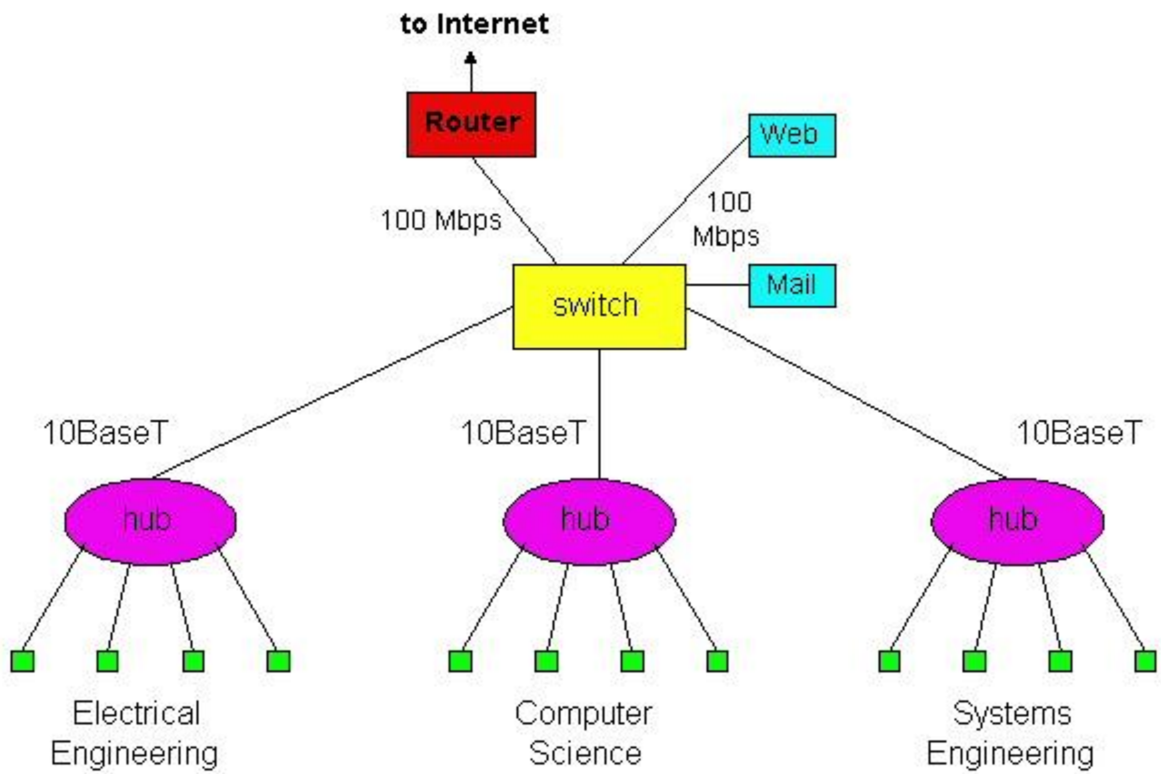
Routers

- Operates at network layer = deals with **packets,** not **frames**
- Connect LANs and WANs with similar or different protocols together
- Switches and bridges **isolate collision domains** but forward broadcast messages to **all LANs** connected to them.
- Routers **isolate both** *collision* domains and *broadcast* domains
- Acts like normal stations on a network, but have **more than one** network address (an address to each connected network)
- Deals with global address (network layer address (IP)) not local address (MAC address)
- Routers **communicate with each other** and exchange routing information
- Determine best route using **routing algorithm** by special software installed on them
- **Forward traffic if information on destination** is available otherwise **discard** it (not like a switch or bridge)

Figure *Routers connecting independent LANs and WANs*



An Institutional Network Using Hubs, Ethernet Switches, and a Router



Access Point and Wireless Repeater

- Access point is a layer 2 device – transfers signals from wireless devices to wired network.
- Wireless router is a layer three device
- Wireless router is capable of routing unlike an access point.

How the OSI and TCP/IP Models Relate in a Networking Environment

OSI Model Layer	OSI Model Name	Pneumonic	Equipment	Equipment Purpose	Data	Protocols	Words to Remember	TCP/IP Model
Layer 7	**A**pplication	**A**ll				Redirector, FTP, Telnet, SMTP, SNMP, Netware Core	Browsers	Application
Layer 6	**P**resentation	**P**eople	Computer		**D**ata		Common Data Format	Application
Layer 5	**S**ession	**S**eem		Regular Computer		NFS, SQL, RPC, X-Win	Dialogues and Conversations	Application
Layer 4	**T**ransport	**T**o	Computer		**S**egment	TCP and UDP	Quality of Service, and Reliability	Transport
Layer 3	**N**etwork	**N**eed	Router	Segment Network into Smaller ***Broadcast*** Domains	**P**acket	Routable Protocols. (IP, IPX, AppleTalk)	Path Selection, Routing, and Addressing	Internet
Layer 2	**D**ata Link -MAC -LLC	**D**ata	Bridge (2 Ports) or Switch and NIC	Segment Network into Smaller ***Collision*** Domains	**F**rame	NDIS, ODI, MAC Address, Ether Talk	Frames and Media Access Control (MAC)	Network Access
Layer 1	**P**hysical	**P**rocessing	Repeater, Hub (Multi-port), Cabling	One Collision AND One Broadcast Domain	**B**it	Physical	Signals and Media	Network Access

Network Topologies for a Wireless CN

Wireless Components and Modes

Wireless networks tend to consist of only a few fundamental components, in this section you will learn about some of these, including;

a Wireless Access Points

&

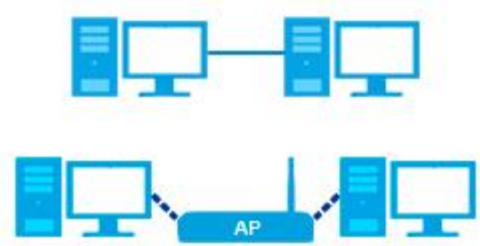
b Wireless Clients

The IEEE 802.11 suite of standards specify two modes of operation for wireless networks, which will be covered in this section, these are;

a Infrastructure mode

&

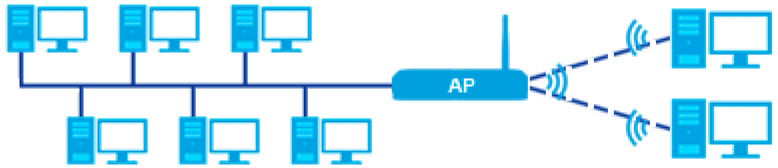
b Ad-Hoc mode



Wireless Components and Modes

Access Point

An access point is a wireless 'hub'. The transmitter/receiver connects together the wireless nodes and typically bridges them to the wired network.



An access point should be distinguished from a wireless router. A wireless router is a combination of an access point and a router and can perform routing tasks.

Consider a wireless router as a wireless bridge (between wireless and wired Ethernet) and a router (IP routing features).

From wireless clients' point of view (laptops or mobile stations), an access point provides a virtual cable between the associated clients.

A set of (coordinated) access points can be connected together to create a large wireless network.

Wireless Components and Modes

Access Point

Clients connect to the access points by knowing their 'identification'.

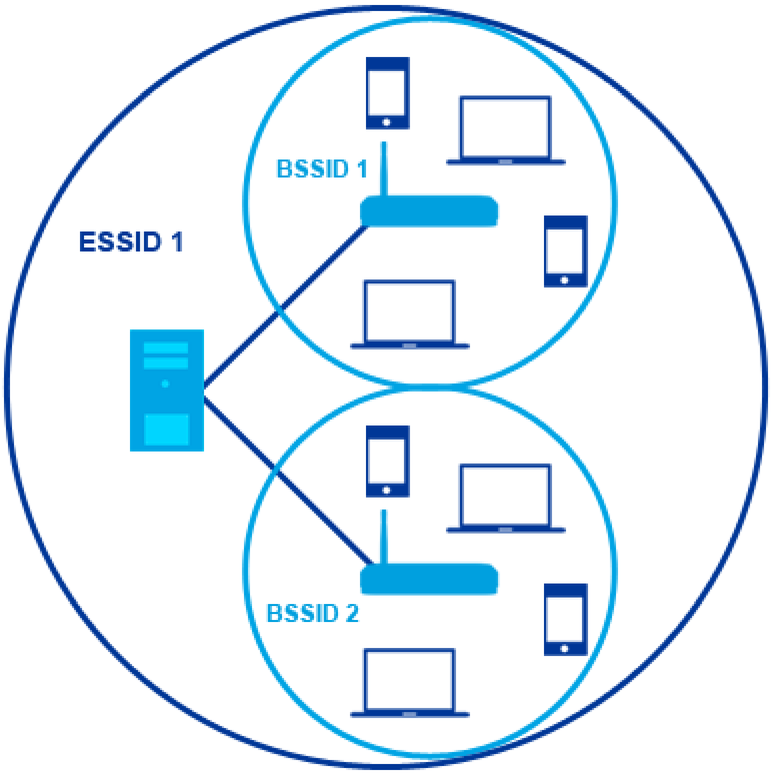
This identification is known as the Service Set Identity (**SSID**) and it should be shared by all members of the specific wireless network.

All the wireless clients and access Points within an Extended Service Set (ESS) must be configured with the same ID (**ESSID**).

Each access point in the ESS has its own Basic Service Set ID (**BSSID**) - usually the access point's MAC Address.

This allows wireless clients to roam between multiple access points while staying connected to the same network.

Connecting to a wireless network with SSID **x** is equivalent to plugging your computer into an Ethernet socket on the wall identified with the tag **x**.



Each access point has it's own unique BSSID, but they all share the same ESSID.

Wireless Components and Modes

Wireless Clients

A wireless client is any wireless station that connects to a wireless Local Area Network (LAN) to share its resources.

A wireless station is defined as any computer with an installed wireless network adapter card that transmits and receives Radio Frequency (RF) signals.

Some common wireless clients include laptops, PDA's, surveillance equipment and wireless VoIP phones.

Wireless Components and Modes

Wireless Modes

There are two fundamental wireless modes defined in the 802.11 suite of standards: **Infrastructure** and **Ad-Hoc**.

Infrastructure Mode

Most wireless networks function in **infrastructure** mode. In this case the wireless devices on the network all communicate through a single access point (usually a wireless router).

For example, there are two laptops sitting next to each other, each connected to the same wireless network. Even though they are sitting right next to each other, they are not communicating directly with each other - instead, they're communicating via the wireless access point.

They send packets to the access point, and it sends the packets on to the other laptop. **Infrastructure mode requires a central access point that all devices connect to.**

Ad-Hoc Mode

Ad-hoc mode is also known as **peer-to-peer** mode.

An Ad-hoc network does not require a centralized access point - instead, the wireless devices on the wireless network connect, and communicate directly with each other.

If you set up the same two laptops in ad-hoc wireless mode, they would connect directly to each other **without the need for a centralized access point**.

One disadvantage of ad-hoc wireless networks is if many devices are connected to the ad-hoc network, there will be more wireless interference - as each computer has to establish a direct connection to each other computer rather than going through a single access point.

Wireless Components and Modes

Infrastructure (BSS)

In infrastructure mode there is:

- a 'coordination' element; and
- an access point or base station.

If the access point is connected to the wired Ethernet network, the wireless clients can access the fixed network via the access point.

When several access points and wireless clients are interconnected, they must be configured to use the same SSID.

If we want to ensure that the overall capacity of your network is maximized do not configure all the access points in the same physical area to use the same channel.

The clients will discover (by means of scanning) which channel the access point is using and hence, there is no need for the clients to know the channel number in advance.

In IEEE 802.11 networks the denotation of the infrastructure mode is **Basic Service Set** (BSS).

A typical setup for an infrastructure network.

Setting	AP/Gateway	Node x1
Mode	Infrastructure	Infrastructure
SSID	Sets MY_SSID	Connects to MY_SSID
Channel	Sets channel x	Discovers the channel
IP address	Typically runs DHCP server (if router features are available)	Typically gets IP via DHCP lease

Wireless Components and Modes

Ad Hoc Mode (IBSS)

Ad hoc mode, also known as Peer-to-Peer, is a method for wireless clients to directly communicate with each other. By allowing wireless clients to operate in ad-hoc mode, there is no need to involve any central Access Points. All nodes of an ad hoc network can communicate directly with the other clients.

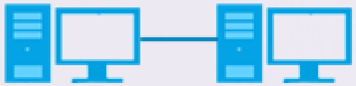
Each wireless client in an ad hoc network must set its wireless adapter in ad hoc mode and use the **same SSID** and **channel number/frequency**.

An ad-hoc network normally consists of a small group of devices located close to each other. Performance decreases as the number of nodes in the ad hoc network grows. In order to bridge an ad hoc network to a wired LAN or to the Internet, a special gateway must be installed.

Ad hoc mode can be used when we need to connect two stations directly for short period of time e.g. client to client. It can also be used inside of an office between a set of workstations.

In IEEE 802.11 networks the denotation of the ad hoc mode is **Independent Basic Service Set** (IBSS).

A typical setup for an ad hoc network.



Setting	Node 1	Node 2
Mode	ad hoc	ad hoc
SSID	MY_SSID	MY_SSID
Channel	Need to agree and know each other's	Need to agree and know each other's
IP Address	Typically Fixed	Typically Fixed

If one node is networked (e.g. Internet or intranet), it has control to share that network to the other node.

The Latin term 'ad hoc' means 'for this purpose' but is commonly used for an improvised and often impromptu events or solutions.

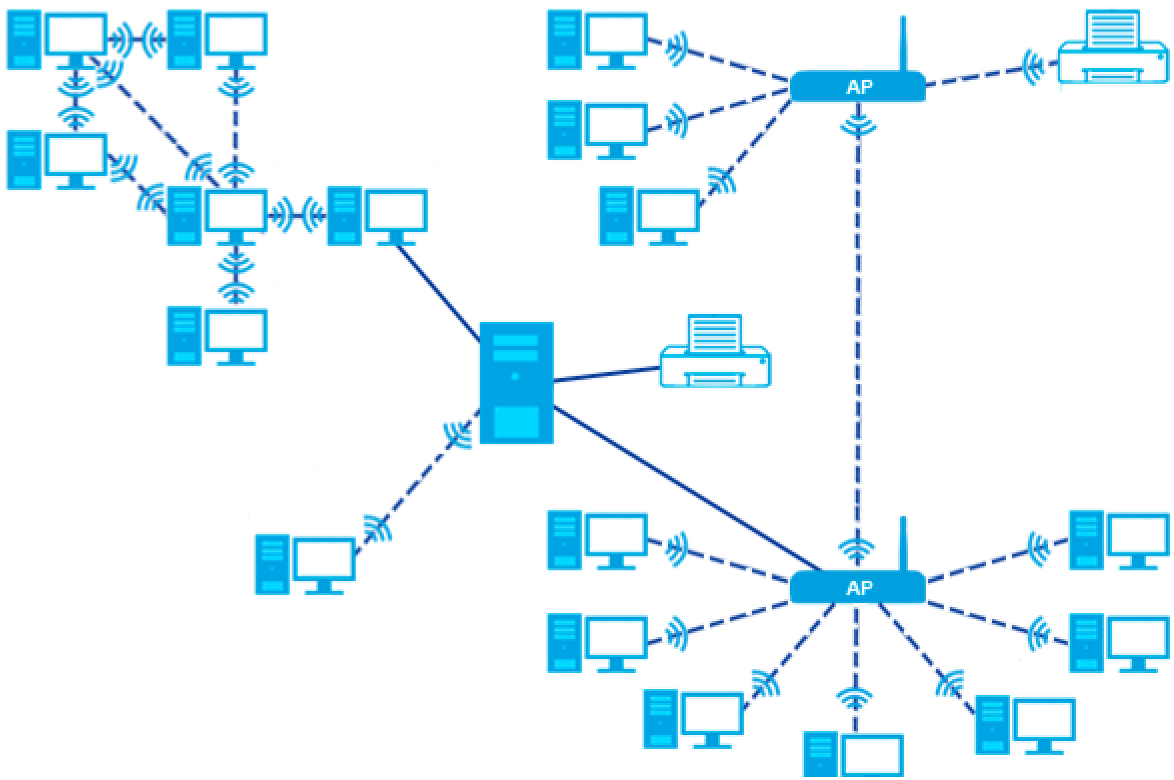
Relevant Network Topologies in Wireless Networking

Topology	Diagram	Is this topology relevant in wireless networking?	
Star		✔	Yes, the standard topology of a wireless network.
Line		✔	Yes, with two or more elements. A line of two nodes is a PtP link.
Tree		✔	Yes, typically wireless ISPs.
Ring		✔	Yes, possible but rarely found.
Full Mesh		✔	Yes, but mostly partial mesh.
Partial Mesh		✔	Yes.
Bus		✘	No. Studying the bus topology we will notice that each node is connected to all other nodes and since the place where one line meets the other lines is of no significance in the wireless case, this topology is fully equivalent to a (full) mesh network operating on single channel.

Real-Life Wireless Topologies

Real life wireless networks are very often combinations of different topologies.

This diagram shows an example which is comprised of **four** different topologies.



Real-Life Wireless Topologies

Mesh Topologies

Mesh topologies are an interesting option mainly in urban environment but also in remote areas whenever central infrastructure is hard to implement.

Some typical cases include **municipal networks**, **campus networks**, and **neighborhood communities**.

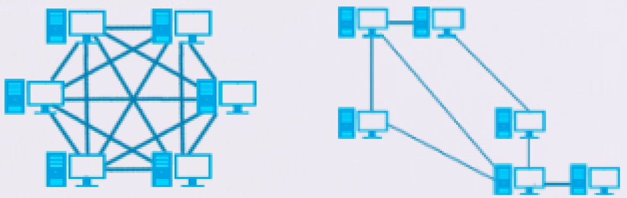
A mesh network is a network that employs one of two connection arrangements, full mesh topology or partial mesh topology.

In the full mesh topology, each node is connected directly to each of the others.

In the partial mesh topology, nodes are connected to only some, not all, of the other nodes.

All mesh nodes need to run the same mesh routing software (protocol), but can be of different operating systems, and hardware types.

Typical Mesh Parameters.



Setting	Node x1	Node x2
Mode	ad hoc	ad hoc
SSID	MY_SSID	MY_SSID
Channel	Channel x	Channel x
IP Address	Typically Static and manually set	Typically static and manually set
MAC Address	Might be fixed to one another's MAC	Might be fixed to one another's MAC

Using DHCP in mesh networks make difficult to manage, so static IP addresses are recommended.

The gateway nodes typically need additional settings to announce their presence.

Real-Life Wireless Topologies

Repeating

Repeating typically becomes necessary when the direct line of sight is obstructed or the distance is too long for one single link.

The wired equivalent of wireless repeating is a hub.

The setup of repeating depends on hardware and software specific factors and is difficult to describe in one generic way.

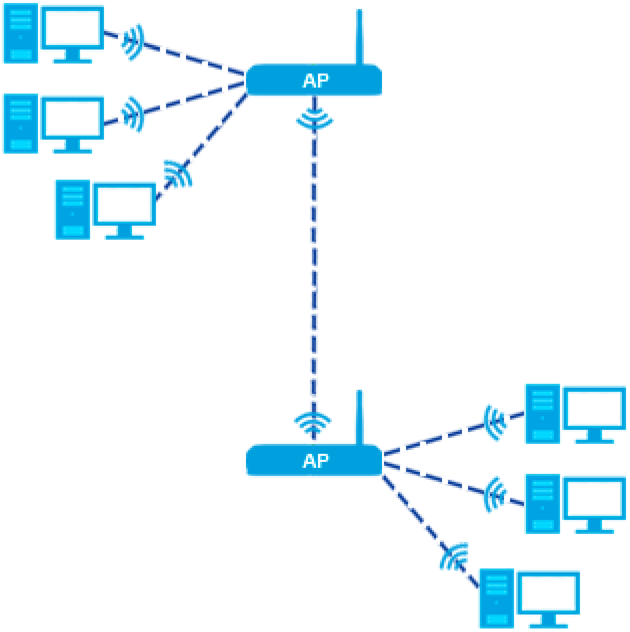
The repeating unit may consist of one or two physical devices and have one or two radios.

A repeater can also be seen as:

a receiving client AND a re-transmitting access point.

Typically, the SSID would be the same for all units.

Often the repeater ties to a MAC Address in addition to a SSID.



An example of repeating wireless infrastructure.

Real-Life Wireless Topologies

Star Topology

The star topology is by far the most common infrastructure for wireless networks. It is the typical topology for a hotspot, whether it is in a airport or a Telecenter.

The star topology is the typical **WISP** (Wireless Internet Service Provider) setup (think in a point to multipoint link).

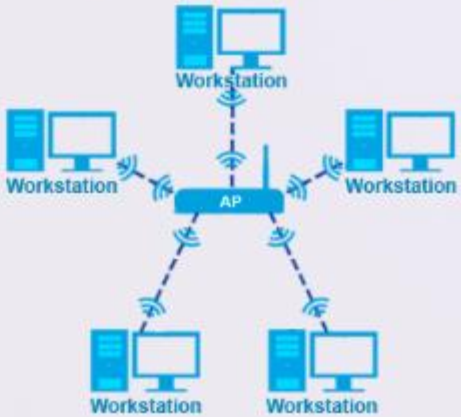
This type of network is often extended into tree topologies or developed in combination with other topology elements.

The main advantage of a star network, is that one malfunctioning node doesn't affect the rest of the network.

Wireless Access Point
Texas

Its main disadvantage is if the central computer fails, the entire network becomes unusable.

A typical setup for a star topology



Setting	AP/Gateway	Node x1
Mode	Infrastructure	Infrastructure
SSID	Sets MY_SSID	Connects to MY_SSID
Channel	Sets channel x	Discovers the channel
IP address	Typically runs DHCP server (if router features are available)	Typically gets IP via DHCP lease

Real-Life Wireless Topologies

Point to Point

Point to point (PtP) links are a standard element of a wireless infrastructure. On a topology level they may be part of a star topology, a simple 2-point line or other topology.

The mode of a PtP link can be ad hoc or infrastructure.

Settings of two nodes for Ad-hoc mode.

Setting	Node 1	Node 2
Mode	Any	Any
SSID	MY_SSID	MY_SSID
Channel	Will agree and know each others	Will agree and know each others
IP Address	Typically fixed	Typically fixed
MAC Address	Might be fixed to one another's MAC	Might be fixed to one another's MAC

A typical setup for a PtP link. The mode can be ad hoc or infrastructure but both nodes must be in the same mode.

For long distance PtP links advanced wireless settings are required to improve performance.

Benefits of Mesh Topology

- Easily scalable
- Robust – traffic can be re-routed if one link fails
- Failure during a single device won’t break the network
- No central control