

# **Outdoor Wireless including Linking Buildings and Wide Area Coverage**

04/04/2011

# 1 Introduction

The purpose of this document is to explain some of the principles and products that can be using for setting up wireless networks to do network bridging between buildings. For the purpose of this document a network can be just a single remote computer or a collection of networked computers: Both scenarios are discussed with real-life examples.

Generally, inter-building wireless links can be broken down into four types.

1. Simple single remote building direct to a single central building: So called point-to-point (PTP) link. A typical example might be you want to let a mate across the street piggy-back onto your internet connection or, you're a company and you want an office across the yard to connect into the main office network.
2. Multiple remote buildings direct to a single central building: So called point-to-multipoint (PTM) link. Typical examples are you want to share your internet connection with a number of mates down the street or, for example, a business that has several outlying buildings or, a holiday park site that wants to allow punters in their holiday homes (which could be 'proper' buildings or caravans) to access the internet coming into the clubhouse.
3. Single or multiple remote buildings connecting via repeaters to central building: So called multipoint-to-multipoint (MTM) link. This is similar to 1 and 2 but there is no direct line-of-site (LOS) between the remote clients and the central site. Therefore the network has to use a way-station or repeater to dog-leg around the obstruction.
4. Meshing systems. A **wireless mesh network** is a communications network made up of radio nodes in which there are at least two pathways of communication to each node. In practice there are normally two radio networks in operation on a typical mesh node device: A 'backbone' network that links the nodes together and facilitates transport of data between the nodes – this is the mesh network. Then each node has a secondary wireless network whose purpose is to facilitate wifi connection for local clients to the node and hence to the mesh. The coverage area of the backbone radio works as a single network creating a mesh cloud. Access to this mesh cloud is via the local secondary wifi network and (usually) also via the LAN port of the node devices. A mesh network is reliable and offers redundancy. When one node can no longer operate, all the rest can still communicate with each other, directly or through one or more intermediate nodes. Wireless mesh builds routes between nodes only as desired by originating nodes. It maintains these routes as long as they are needed by the originating node. Wireless mesh nodes forms paths in term of hops which connect together to form the wireless mesh network. Hops are the number of nodes between two a receiving and transmitting client i.e. Laptop, PC, Wi-Fi telephone, IP appliance, etc. Symbolically a Wireless Mesh network is represented by a network cloud.

A mesh network has key advantages over a generic, universal, wireless repeater based system:

- a) Typically, in a universal repeater setup each repeater forms a new wireless network with a different SSID (network name) than the source. So the whole network is effectively broken down into interconnected small wireless network areas each with a different name. Further the repeating routes of the network have to be specified and fixed at the time the network is installed. This can cause a lot of extra work and confusion when the network is created. With a meshed setup the connectivity between the nodes for the mesh backbone is automatically setup by the mesh nodes with a much smaller amount of user configuration.
- b) In a standard repeater network then data going from one cell to another cell results in ALL cells configured as repeaters in the system repeating the data; even if some cells don't cover the data source or destination. In a meshing system only those cells needed to complete the wireless data link actually transmit the data: The mesh repeating nodes create maps which allow them to choose which route or serial of nodes are required to most efficiently transport the data from source to destination. This dramatically reduces wireless congestion and significantly improves performance in a larger network.
- c) The meshing nodes dynamically alter their route maps which means, if one node goes out of action (e.g. someone parks a lorry in front of it) then the other nodes will automatically remake their maps in order to attempt so side step the blocked unit. This gives improved network reliability.

I'm sure, with some deep thought, you could probably dream up some more wireless scenarios however the 4 methods above should cover the majority of situations (or give clues on how to solve your problem).

However, before we got into some specifics, we need to cover some of the basics behind wireless links.

## 1.1 Clients and Access Points

---

### 1.1.1 Peer-to-peer or Ad-Hoc networks

An ad-hoc network is a network where stations communicate only peer to peer (P2P). There is no base unit and no one gives permission to talk.

Peer-to-Peer / Ad-Hoc

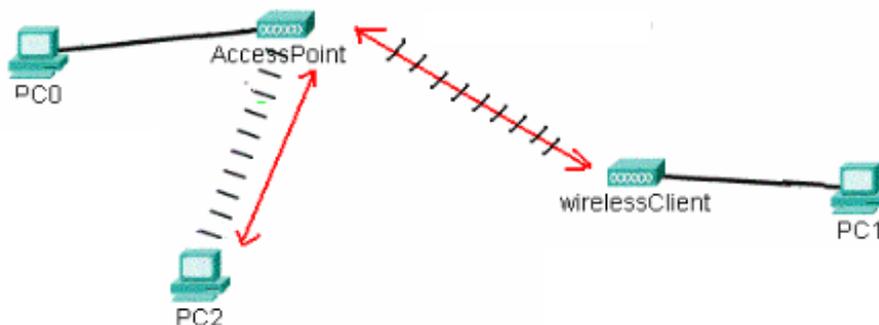


A peer-to-peer (P2P) allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network. It also the method used with meshing networks (using olsrd – see below). Ad-hoc networks are generally only used in networks using mobile or transient clients. Where links are required between fixed points then another type of wireless topology is used called ‘Infrastructure’ mode.

### 1.1.2 Infrastructure networks

In an infrastructure networks the wireless clients don’t communicate directly with each other but instead through a base station called an Access Point. The basis for a wireless link is a WiFi ‘client’ at one end and an ‘access point’ at the other. An Access Point (AP) is a wireless base station with a LAN connection (a wireless router is simply a router with a built in AP). A client could be a PC with a wireless card or built in wireless (Centreno) or it could be a bridge client. Essentially a bridge client is a wireless client device which has a LAN connection so that the remote PC (or other device) connects via its LAN port to the radio device.

For example:



So in this simple example you can see PC0 is connected via its LAN port to the AP. The AP has a wireless link to both PC2 (with built in wireless card) and, via the wireless client, to PC1. When it comes to remote wireless bridging between fixed points, infrastructure mode with clients and access points is usually preferred over a client only, peer-to-peer scenario because they provide a variety of benefits including increased range and better security.

When it comes to infrastructure mode remote wireless bridging then it’s preferable to use wireless clients rather than direct wireless links to your PC for three reasons:

- a) In order to get the best wireless signal you will almost always end up having to use an externally mounted antenna. Apart from the fact that most PC wireless cards or PC’s with built in wireless don’t have the ability to connect an external antenna the other point is you will need to mount the radio device (client) as close as possible to the antenna in order to keep the antenna cable as short as possible and thus reduce signal losses (it’s better to have a long LAN cable going from the client to the PC than to have the client close to the PC but have to use a long antenna cable).

- b) A bridge/wireless client will allow multiple computers to use the wireless link: Simply connect a normal network switch to the LAN port of the client (or connect the LAN port to you existing network) and you can then have several PC's using the link.
- c) Because there are no drivers or special software that has to be run on your PC then a bridge client is operating system independent i.e. the LAN device connected to the port on the client can be any PC or computer or even a LAN product which is not a tradition computer at all e.g. a network printer or an ADSL router.

## 1.2 Antenna and Signal Gain

---

Invariably, in order to cover any sort of distance with your wireless link then you are going to need to use alternative antenna. There are two reasons for this:

- a) Wireless don't like going through walls! So, if you can mount the wireless antenna outside the building then you get a significant boost to the signal. Even a single brick thick wall will reduce the signal by as much as 75% - a supporting or external wall will just about kill it altogether.
- b) If you want to go at high speed and/or a long distance then the puny indoor or built in antenna on normal CPE (Customer Premise Equipment) radio devices just ain't up to the job.

Now there's a lot of confusion with using antenna and what they will or won't do however the important things to remember are that an antenna doesn't amplify or boost the radio signal coming out of your radio device. An antenna is a passive device that works by focusing the wireless signal into a specific direction. The 'normal' built-in or small 'rubber-duck' style antenna fitted to a wireless card or home wireless AP/router is fairly low gain and sends out a roughly spherical shaped radio signal. The purpose, in this case, is to try and give all round reception so that you can connect to any point in any direction. However, when it comes to connecting to a specific remote link, then sending your signal all around, to places where you don't need it to go, means only a small fraction of the signal actually reaches the once place where you DO want it to go. Fitting a different, higher gain, antenna allows you the option of focussing the signal so it only goes where you want it to. A simple analogy is to think of a magnifying glass. With a magnifying glass you can take the light from the sun, which would normally be quite weak, and concentrate it onto a small spot so that it's strong enough to burn wood. Ditto, with a high gain antenna, you haven't somehow made the radio device turn up it's output power (just like, by using a magnifying glass you haven't sent a message to the sun to suddenly start burning hotter); instead you've taken the existing, scattered, signal and pointed into just the direction you want it to go.

BTW, don't be miss lead by 'so called' omni high gain antenna. At face value it would seem these would somehow amplify the signal but still allow all round coverage – Not true. What they actually do is flatten the signal into a higher powered thin, horizontal, disc. i.e. where as a 'normal' low gain omni antenna fitted to your radio device scatters the signal all round both up, down and side-to-side, what a high gain omni does is take the signal which would normally go up and down and instead concentrates it horizontally. This can mean that you actually get worse reception from device that are either below or above your level but an improvement for those at the same level.

Where a gain figure is quoted for an antenna it refers to the effective gain measured in the centre of the directed signal and is an addition to the signal coming into the antenna from the antenna cable. i.e. if there is, for example, 17dB coming out of the radio device and antenna cable into the connector on the antenna then, for an 8dB antenna the net gain coming out, in the centre of the antenna beam, is 25dB. The higher the gain of antenna then the more concentrated the signal so the smaller and tighter the signal beam. Generally, if talking about beam width and signal gain then, if you double the output power (i.e. add 3dB gain, for example in going from an 8dB directional antenna to an 11dB directional antenna) then you half the effective area covered by the beam (with reduces the beam width by about 30%).

The other point to remember about an antenna is, as well as concentrating the signal going out, it also concentrates the incoming signal. In this way, for example, an 8dB gain antenna will add 8dB to the signal received from the air before sending it down the antenna cable to the radio device. This is an important point. Since the ability of a radio device to transmit a long distance depends equally well both on how loud it can shout (net output gain) and also how well it can listen (which is a function of the loudness of the signal coming in from the air) then, it's possible, by lowing the output power from the radio device connected to the antenna, to reduce the effective output power but still retain the ability to receive weak signals (and hence improve the range). This is important in situations where you don't want to exceed a certain net power output level e.g. where there are local regularity reasons.

If you want to read up on some of the technical aspects behind wireless links covering aspects such as signal losses, line-of-site, effective range etc.. then you are advised to peruse some of our other technical articles:

<http://www.solwise.co.uk/networkingwireless.htm>

### 1.3 Design Considerations

---

Just a few pointers that you need to take into consideration when designing your wireless link:

1. Try to use externally mounted antenna wherever possible. Wireless doesn't like going through walls so even a single brick wall will seriously drop your signal strength.
2. For reliable operation you really must ensure that the antenna have a clear line of site between each other.
3. Try to keep antenna cables down to the absolute minimum in length – we recommend about 5m maximum when using '200' grade cable or about 10m for '400' grade cable. In situations where it's impossible to stick to sensible cable lengths then consider going for fully outdoor radio units which use 'power over ethernet' to send the power down the LAN cable to the device. If you have to use a long antenna cable because there isn't a convenient mains power socket then consider using a Power Over Ethernet system to send power up the LAN cable i.e. short antenna cable but long LAN cable taking date and power.
4. Try to be sensible with your antenna choice. Do a proper link budget (see <http://www.solwise.co.uk/los.htm>) to work out the size/gain of antenna you need. Using too high a gain antenna can actually make things worse rather better: For a start, the higher the gain sends the signal further and, therefore increases the chance of someone else picking up your signal behind you (i.e. with increased security problems). Secondly, a higher gain antenna concentrates the signal more which can make antenna alignment much trickier. This is particularly so with high gain omni antenna which concentrate the signal into a very thin, horizontal disc so that it can be hard to pickup the signal if the remote point is above of below the height of the sending end. Thirdly, using too high a gain can actually overload the receive circuits in your radio device. Although it's very unlikely you would ever cause any permanent damage, the effect of overloading the receive circuits will be to distort the signal and significantly reduce data throughput (in fact it might reduce data throughput to zero!). The table below shows typical antenna gain required **at each end** (e.g. for a distance of about 1.25Km you need antenna gain of about 7dB at each end of the link) vs. range for both 2.4GHz and also 5GHz wireless (5GHz wireless is discussed below):

Distance	Antenna Gain/dB for 2.4GHz operating at 11Mbps	Antenna Gain/dB for 5.4GHz operating at 11Mbps	Antenna Gain/dB for 5.4GHz operating at 54Mbps
620m	4	7	17
790m	5	8	18
1.25Km	7	10	20
2Km	9	12	22
5Km	13	16	26
12.5Km	17	20	reaching the limit of 5GHz
31Km	21	23	reaching the limit of 5GHz

5. Remember that radio kit that uses the 5GHz frequency band can offer several advantages over the much more common 2.4GHz WiFi ('normal' 802.11b or 802.11g WiFi is 2.4GHz band) i.e.
  - a. Better non-line-of-site (NLOS) capabilities.
  - b. Better penetration (roofs or walls for example)
  - c. Better security and lower problems with interference from other uses (there ain't many other 5GHz network users out there).
  - d. Higher, legal power limits meaning longer range whilst still keeping to the UK (EU) regulations.
  - e. Physical, smaller antenna size for same gain output.

If you want to read more on 5GHz networking then your are advised to check out our white paper - <http://www.solwiseforum.co.uk/downloads/files/intheuk5ghz.pdf>

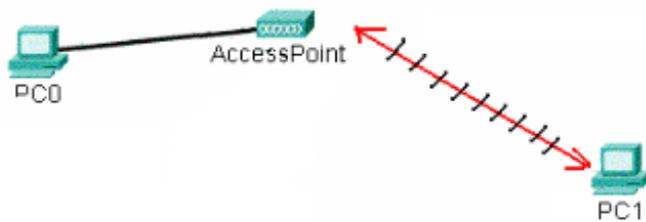
## 2 Wireless Link Designs

### 2.1 Basic, Point-to-Point links

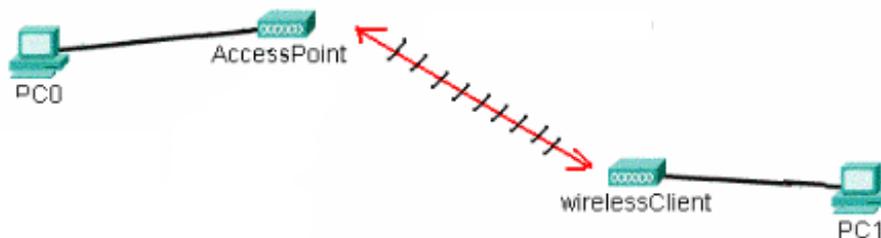
---

From above, it's clear that the most basic bridging wireless links would consist of, at one end, a bridge client with suitable antenna (and antenna cable if using an external antenna) and, at the other end, an AP with suitable antenna (and antenna cable if using an external antenna):

i.e. a wireless equipped PC talking back to an AP



or a PC connected to a remote wireless (bridge) client via a LAN cable



This is not hard and just extends the idea of an indoor access point based wireless network for use outdoors. The only new concept, which you might not have come across before, is the idea of a wireless (or bridge) client. This allows the remote computers and devices (e.g. games box) to connect to the wireless link via a LAN cable so you can easily mount the wireless device (client) close to where the outdoor antenna will be located (so as to keep the antenna cable short) and then run a LAN cable back to the PC.

So let's consider some specifics. Imagine you are linking over a distance of just a few hundred yards. Now, from my article discussing antenna transmission (<http://www.solwise.co.uk/los.htm>), it can be seen that, typically, for distances of a kilometre or less, smallish antenna of around 7-8dB are perfectly okay. This is using 2.4GHz equipment for speeds up to about 11Mbps. (For higher speeds or alternate frequency bands, like the 5GHz band, then higher gain antenna might be required - full details on our other technical articles and also discussed below.)

Point-to-Point links are nowadays normally configured using all-in-one outdoor cpe/bridge devices. These are outdoor proof units which contain the radio device and also the antenna in a single housing. Power for these is usually sent up the LAN cables using PoE (power over Ethernet). Solwise have a wide range of outdoor cpe/bridge devices with different antenna setups and for different operating frequencies. E.g. The EnGenius EOC-2611P is an outdoor 2.4GHz cpe with integral 10dBi directional antenna.

The beauty of a product like the EOC-2611P is the radio device and antenna are integrated into a proper, outdoor rated housing with a LAN (not antenna) cable running from housing to the building network. The system includes a POE (Power Over Ethernet) injector which sends power via the connecting LAN cable - hence there is no requirement to supply mains or other power at the housing location. The front panel of the housing incorporates a directional 9dB antenna. With this design the losses due to connecting antenna cables are kept to a minimum which gives a dramatic improvement in range - I've heard of situations of 2611 devices working over ranges exceeding 10Km!

### 2.1.1 Multiple users at the remote site

The examples above assume that the remote site is a single computer. For sites which have multiple remote computers then the easiest solution is to just install a network switch on the LAN cable at the remote site and then connect the multiple computers to the switch. Thus each remote computer appears as a separate IP device sharing the common wireless link. e.g. if you had 1 local PC (say PC0) and then two remote PC's (say PC1 and PC2) then the DSL router at the main site would see each PC (0 1 and 2) as a separate IP connection. Now there are sometimes reasons why you may NOT want the remote PC's to be separately addressed by the main router e.g. in an environment where you have a limited number of IP addresses available for the wireless network so you want the remote PC's (1 and 2) to only appear as a single address. Another reason might be for security reasons – in the type of network shown above then all users can 'see' each other. This might be something you do not desire. The easiest method to section the network like this is to use a router at the remote location.

## 2.2 Point-to-Multipoint links

---

Wireless link networks, where you have multiple remote points linking back to a single central source, are really just an extension of the basic, PTP, type network shown above. The only difference is usually the type of antenna used at the central source: For simple single point to single point links then you only need to use simple directional antenna at each end. However, when you have more than one remote site, then it's unlikely that all the remote sites will be arranged so that they all fall in line with the beam from a single directional antenna at the main site. In this case you will probably have to use an omni or sector style antenna at the main site. An omni antenna gives a 360degree coverage however a sector antenna gives a wide angle directional beam (typically 90 or 120 degrees)



e.g.

This is a typical, 8dB omni antenna. It gives a beam which circles 360 degrees around the antenna at roughly the same height as the antenna. It is therefore ideal when having to pick up signals from clients at any position around the antenna location.



This is a 120 degree sector antenna. It gives a strong signal in a clearly defined beam in front of the antenna – obviously, 120 degrees wide in this case 😊

Outdoor cpe devices like the EnGenius EOC-2611P have an antenna connector so that you can use a separate antenna instead of the built in directional antenna.

## 2.3 Wireless links using repeaters

---

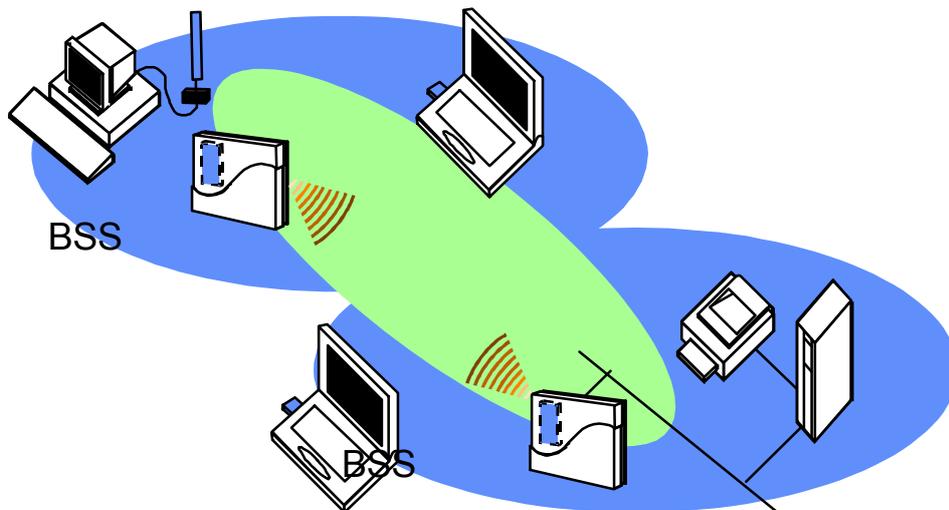
Up to now we've only considered fairly simple links where there are no problems with clear line of site between the wireless parties. However, what about where the two ends of the wireless link can't see each other? Well one answer is cross your fingers and hope, by a process of reflections and scatter, that the wireless signal is going to reflect off a neighboring building and hence dog-leg around the obstructions. The problem with relying upon reflection is it's very hit and miss: You just don't know if it's going to work and worse, if it's going to work reliably – it might work today and not tomorrow. If you want to (or are forced to because you cannot install repeaters, as discussed below, due to site restrictions) go the reflections and scattering route then you are advised to go for 5GHz equipment. 5GHz radio is much

better than 2.4GHz at reflecting and also much better at coping with the poor signal quality you get when radio signals are scattered in this way.

The other method to get around objects is to use repeaters. There are various wireless products which are supposed to support repeating but the only system that seems to work with any degree of confidence is WDS (Wireless Distribution System). Unlike 'other types' of repeater, which can be very choosy as to what they will and will not repeat from, WDS products seem to generally be fairly interchangeable with other makes of equipment. As such WDS products from different companies will usually work with each other without any problems.

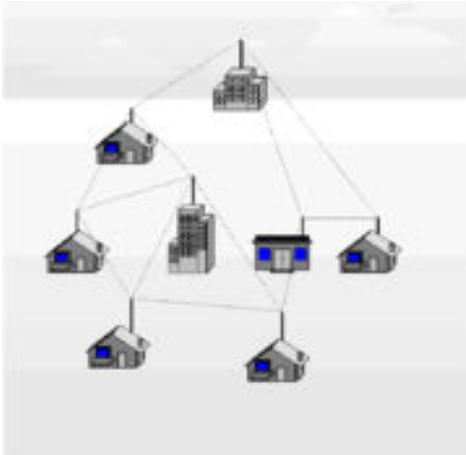
### 2.3.1 WDS

In proper IEEE 802.11 terminology a "Distribution System" is system that interconnects so-called Basic Service Sets (BSS). A BSS is best compared to a "cell", driven by a single Access Point (one of those circles in the diagram below). So a "Distribution System" connects separate cells of wireless coverage (each with a WDS configured AP in the middle) which link together to form a unified single wireless network and allows users within the area of coverage of each cell to network with each other.



Traditionally, WDS networks were first dreamt up as a system for allowing wireless coverage within buildings. This was necessary because there are big, inherent problems with trying to get wireless signals to go all round inside a building i.e. walls! Wireless don't like 'em ☹️ So WDS is one method to try and fix this. In practice the network would consist of several WDS mode AP's distributed around the building; each WDS AP must be positioned so that it can wirelessly link up with the last WDS AP down the chain and, if necessary, with the next AP up the chain. Then any client can simply connect to the nearest WDS AP and, because each AP is connected back to the last (and from there to all other WDS AP's in the system), hence network with any other client connected to any other AP in the system. Each WDS AP is the centre of a BSS cell.

## 3 Mesh systems



A **wireless mesh network** is a communications network made up of repeating, radio nodes which implement intelligent routing protocols to sensibly route data traffic within the network. The coverage area of the radio nodes, working as a single network, becomes a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. A mesh network is reliable and offers redundancy. When one node can no longer operate, all the rest can still communicate with each other, directly or through one or more intermediate nodes. Due to the high degree of redundancy and dynamic routing inherent in the system, wireless mesh networks can self form and self heal and, in multi node configurations, are far superior to WDS or any other repeating topology. They are therefore ideal for distributed wireless access systems e.g. public internet access where you need to provide internet access to large areas and users to caravan sites, etc.

Wireless mesh builds routes between nodes only as desired by originating nodes. It maintains these routes as long as they are needed by the originating node. Wireless mesh nodes forms paths in term of hops which connect together to form the wireless mesh network. Hops are the number of nodes between two a receiving and transmitting client i.e. Laptop, PC, Wi-Fi telephone, IP appliance, etc. Symbolically a Wireless Mesh network is represented by a network cloud.

Mesh nodes uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of nodes. Wireless Mesh Nodes builds routes using a route request, route reply query cycle. When a node desires a route to a destination for which it does not already have a route, it broadcasts a route request packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. The wireless nodes also collect other active nodes including IP address, current sequence number, and broadcast ID, and contains the most recent sequence number for the destination of which the source node is aware. A node receiving a route request may send a route reply when it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the route request. Nodes keep track of the route request through source IP address and broadcast ID. The nodes know when they receive a route request which they have already processed; they discard it and will not forward it.

As the backward pointers propagates back to the originating node, it then sets up forward pointers to the destination. Once the source node receives the backward pointers, it may begin to forward data packets to the destination. When the source later receives a backwards pointer containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route.

As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. Most wireless mesh nodes maintain routes for as long as the route is active. This includes maintaining hops for the life of the cloud. Because the network nodes can be mobile or shut down, it is likely that many link breakages along a route will occur during the lifetime of that route.

### 3.1 Network Structure

---

Wireless mesh architecture is a first step towards providing high-bandwidth network over a specific coverage area. Wireless mesh architecture's infrastructure is, in effect, a router network minus the cabling between nodes. It's built of peer-to-peer radio devices that don't have to be cabled to a wired port like traditional WLAN access points (AP) do. Mesh architecture sustains signal strength by breaking long distances into a series of shorter hops. Intermediate nodes not only boost the signal, but cooperatively make forwarding decisions based on their knowledge of the network. Such architecture provides high bandwidth, spectral efficiency, and economic advantage over the coverage area.

Wireless mesh network have a topology inherently more stable than a traditional WDS or universal repeating network. The traffic, being aggregated from a large number of end users, changes infrequently. Practically all the traffic is either

forwarded to or from a gateway, while in ad hoc networks the traffic flows between arbitrary pairs of nodes. A multi hop based nodes proactive routing scheme is used for traffic forwarding, since it easily allows flows aggregation and would minimize overhead, ensuring an optimal utilization of bandwidth.

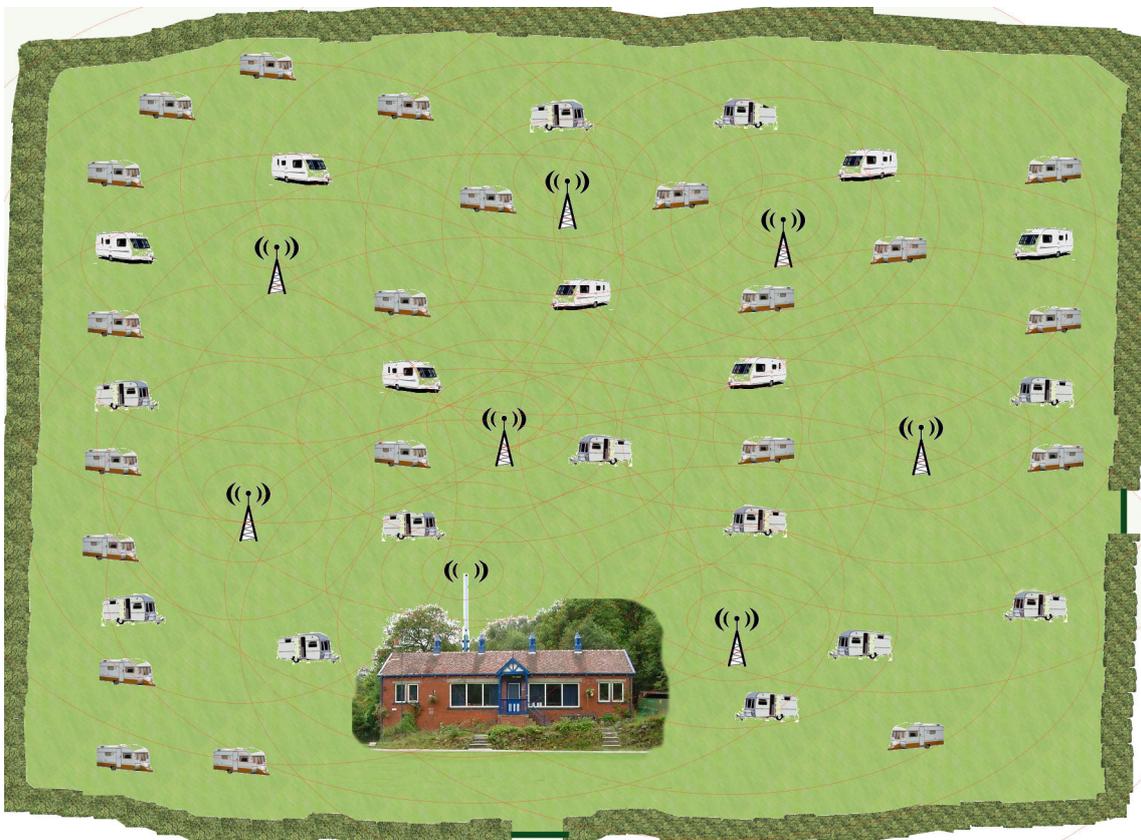
This type of infrastructure can be relatively inexpensive, and very reliable and resilient, as each node needs only transmit as far as the next node. Nodes act as repeaters to transmit data from nearby nodes to peers that are too far away to reach, resulting in a network that can span large distances, especially over rough or difficult terrain. Mesh networks are also extremely reliable, as each node is connected to several other nodes. If one node drops out of the network, due to hardware failure or any other reason, its neighbours simply find another route. Extra capacity can be installed by simply adding more nodes.

## 3.2 Caravan Site Example

Let's consider the problem with distributing wifi around a caravan site

### 3.2.1 Outline

See the figure below (apologies for the rather 'naïve' drawing style ☺):



The illustration depicts a 'typical' 'van site' where a number of 'vans exist where they want to receive wireless internet.



Wireless internet network originates at the 'club house'.

It's then 'repeated' over the site using a series of meshing nodes.

We intentionally use a high density of meshing nodes so that each 'van potentially has more than one node it can use for signal source and each node can see more than one other meshing node: This is something that would just not be possible using a WDS or 'Universal' repeater configuration because the massive resulting drop in performance would just make the whole network unusable! However, by using a high density of nodes then we significantly improve the likelihood that an end user client (someone sat in their 'van, using their wireless notebook to check an eBay bid for some Mickey mouse sunglasses) can get a good wireless connection. Also, multiple overlapping of the nodes means that there are multiple potential routes from source to destination which gives improved link stability: If any node goes out of action or any wireless path becomes blocked, then an alternative route for the traffic will be found and used.

### **3.2.2 Equipment**

The better meshing node devices use two (or more) radio interfaces. In this way they dedicate one radio interface for the mesh connectivity between the nodes and they have a second radio interface to give the local user connectivity. However two radio mesh nodes are a tad expensive ☹ It is often cheaper to use two separate radio devices: So you use one for the meshing part and then that connects via it's lan port to a second radio device that is just for the local user connectivity.

e.g. The EnGenius M5000 is a 5GHz single radio meshing device and the EOC-2611P is an outdoor 2.4GHz, non-meshing AP. So you could create a dual radio mesh node but combining at each point these two radio device and then connecting them by their lan ports. This way you get a solution giving the 2.4GHz local user connectivity and also a 5GHz mesh backbone.

### **3.2.3 Access Control**

The 'van site' example described above works very well and is a fairly cost effective means of feeding internet access into each van however one thing to consider is how you are going to charge and administer the access. One option is to just put it on as a levy on the normal fees (or even give it away free as a site perk) but then you have to worry about locking the wireless network down so that only user that have paid can use the link and also keeping track on the usage – if someone at the site downloads copyright material then it is the site owner, the person who's name is on the internet account, that takes the blame. A better, more secure option is to use a 'Hotspot router' like the Solwise WAS-105. The Hotspot router sits between the main, AP in the club house and the current ADSL router (assuming DSL access). It connects via LAN to the outgoing AP and also via LAN to the incoming DSL router and acts as a controller for any internet access going to the AP (and hence to the main site). It is also a wireless router and therefore also gives controlled internet access via local wireless. Using the hotspot you can either manually preset usage accounts or issue 'on demand' ticket or, even configured to do online PayPal charging to the customer. In either case the end user is given a unique, username and password (dynamically created if using on-demand ticket or PayPal) which they must enter from their browser screen when they want to access the internet. Access accounts can be setup to give short term access or longer usage, like the duration of the customers stay or on a weekly basis.

## 4 5GHz Wireless

All of the examples so far have been based around equipment using the common 2.4GHz license free wireless bands. 99.9% of all end user wireless equipment is designed for the 2.4GHz band – the equipment is low cost and there's plenty around ☺ However, there is another frequency band that can be used for licence free wireless and that is in the operating frequency range 5.1 to 5.8GHz (or, to be accurate, for outdoor use the bands are in the range 5470-5725 MHz or 5725-5825 MHz). For more details on the 5GHz band in the UK I advise you read our other technical article... <http://www.solwiseforum.co.uk/downloads/files/intheuk5ghz.pdf>. In summary though, the advantages for 5GHz are:

- i. Better non-line-of-site operation – better penetration, better scatter, superior multi-path signal rejection (OFDM).
- ii. Less effected by water vapour in the air (rain/fog etc.)
- iii. Higher legal power limits (though this is offset to some extent because of higher signal losses in the air)
- iv. More secure and less interference – at least at the moment when there is virtually no one using the 5GHz bands and, in any case, only people using 5GHz for building linking are legally allowed to use these channels ☺

The principles for the link design are the same as 2.4GHz i.e. AP at one end and Bridge Client at the other, WDS if you want repeating. The only difference is the model of antenna used (and gain – high gain is usually required, compared to 2.4GHz wireless, for the same distance) and radio device used.

However, the problem with using the 5GHz bands for building-to-building linking is one of legality. There are three 5GHz bands: A (5150-5350MHz), B (5470-5725MHz), and C (5725-5825MHz). Band A is indoor use only. Band B is indoor or outdoor BUT for outdoor use it's only allowed for use to mobile devices e.g. someone walking around in the garden with their notebook picking a signal up from a AP in the house. Band C is outdoor use ONLY and intended for building to building wireless linking. So it's Band C we should be thinking of. But Band C equipment is not, traditionally cheap ☹ To operate in the Band C region the radio equipment must conform to Ofcom regulation IR2007 and this is not easy. As such Band C devices tend to be a bit on the pricey side. The new Senao EOC-8610 units are extremely well priced for Band C equipment BUT they might well be out of the range for most, home or small users. Another consideration is that Band C is a licensed frequency range; you need to apply for an operators license from Ofcom. This is quite cheap (about £50 per network) and not hard to obtain (assuming, of course, your equipment conforms to IR2007) but needs to be included into the equation.

So, it's Band C 5GHz we shall be going for using IR2007 compliant, outdoor radio devices. i.e. the EnGenius outdoor eoc-5611P product is just the ticket and are very reasonably priced ☺