WiFi Solutions for Holiday Parks

1 Introduction

This article suggests possible scenarios for delivering broadcast WiFi for public areas such as holiday parks, caravan sites and marinas. I also discuss what you can do for user management. The purposes of this management could be so you can offer a chargeable service and/or so you can control and have traceability for site visits and usage: This final point might well be something that you need if Ofcom come knocking on your door accusing you of downloading a rip off DVD through your internet connection!

The WiFi broadcast methods discussed here centre around scattering WiFi nodes around the site to give complete WiFi coverage. However, before going through the various methods to achieve this, first of all we need to discuss the issues of where a signal will reach and where it will not. They key point is wireless doesn't go through walls or buildings or caravans! So you need to mount your outdoor wireless devices so that users can get clear line of sight to where the WiFi is being sent from. If the user is in a caravan or a metal hulled boat then that means the window of the caravan/boat needs to be aimed at where the WiFi is coming from. This means, when covering a park or 'van site, that you need to scatter WiFi transmitter nodes around the site to give all users clear connectivity. Of course you also want to keep the number of nodes down to reduce interference, boost throughput and to reduce costs. Deciding how many WiFi nodes to install and where to mount them for optimum coverage is, in my opinion, the hard part!

2 Methodology of Distribution

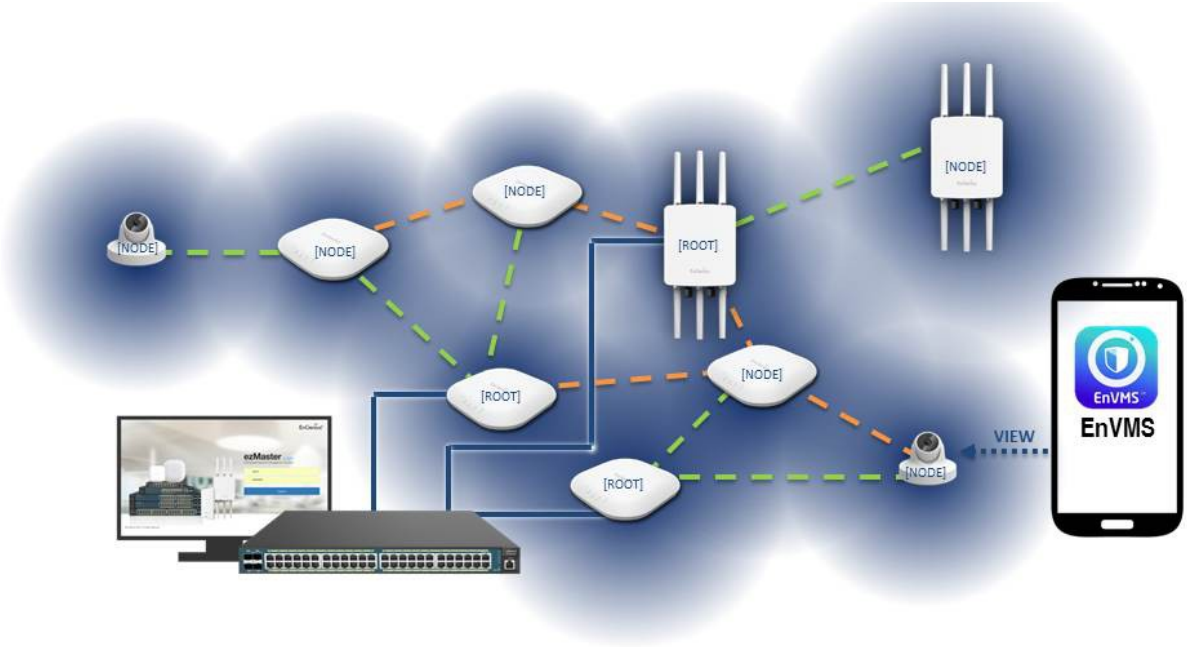
It would be great if the site could covered by just a single outdoor Access Point on the outside of the site club house. Unfortunately, unless the site is very small indeed, this is never the case. Most sites will therefore require multiple access point nodes, carefully sited to give seamless coverage. Once you've picked the best location for the access point nodes (see Physical Implementation below) the next problem is how do you get the network (Internet) to each node. There are a number of ways you can do this; each of them has its good points and its bad points:

1. Hardwired Access Points. This uses separate access points which are connected back to source via networking cable. This could be standard lan cables (cat5e for example), fibre cables, twisted pair cables (using 'Powerline or G.hn down twisted pair'). Each of these cable options has pluses and minuses (like maximum cable length, speed, cost) but the main issue is having to run the cable across the ground. What I mean is, unless you are very lucky and there's existing cable conduits connecting the various spots together, then you're going to have to get a spade out and dig some trenches in which to bury the cable! A hard-wired infrastructure to separate access points certainly gives you the fastest, most secure, and most stable interconnectivity but at the cost and inconvenience of laying the cable. One of the advantages of hard wired units is they can be placed much further from each other. In a repeater (or mesh) set-up then the nodes need to be close enough together so they can get a decent signal from the next unit along. If the backbone is hard-wired then this isn't important. As a consequence you can place the AP nodes twice are far apart.

2. Access Points with a wireless backbone. This is NOT the same as using WiFi repeaters or mesh nodes (see below). What this means is using discrete APs at each node location but then, connected to each AP, using another WiFi unit to bridge back to the network source. For example you might use separate 5GHz bridge units mounted with the node on your pole and the node (probably running 2.5GHz WiFi) is doing the local connectivity but the 5GHz bridge unit is joining the network back to the source. This is a sort of easier version of the hard-wired approach. Using the wireless backbone is obviously easier than having to dig trenches to run cable but you need to do some careful planning to ensure that the WiFi units making up the backbone can see back to the source location. Hopefully this can be done by single hops back to the source though, sometimes, you might have to resort of multi-point hops where you either use a single node to take the network signal in and then forward it on (though that immediately halves the throughput) or, for optimum performance uses two bridge units on the pole: One for the connection in and one for the ongoing connection.

3. Basic 'repeater' access points where the WiFi on the access point used for the local coverage and also the linking back to the source. So your access points are running with some repeating set-up e.g. WDS or 'Universal Repeater'. The advantage of this type of set-up is it's quick and relatively easy to install but that's about it! On the bad side:
    1. The repeating routes need to be fixed into each AP. What I mean is you have to set, in the set-up of the AP, which units to repeat from and to. So it's up to you, as the installer, to determine which units to repeat from what; which traffic routes are the most efficient. This means that if something changes in the topology then you have to go 'round and change this configuration.
    2. If the number of AP's is any more than 2 or 3 then the compound inefficiencies at each node (because each node is having to talk to potentially three ways at the same time – the data source, the local clients, the next node down the line) start to seriously stack up and the throughput drops right down. A single repeater halves the throughput (because the node is having to do receive and then send for each data packet). So add a few of these hops up and the performance is completely trashed.
    3. The nodes need to be close enough such that they can pick up a wireless link from the adjacent node.

4. The other type of repeating topology is using Mesh repeaters. This is really just a more efficient form of the repeating methodology described above. So although a mesh network still has potential throughput and coverage issues they do have several very important advantages as well:



1. One of the main advantage of a mesh set-up over simple repeaters is the 'mesh' system typically auto sets its self up deciding what node to repeat from what node. With traditional repeaters there can be a lot of planning and experimentation deciding which nodes to repeat from which. You don't simply want to set ALL nodes to repeat from ALL nodes because that results in significant performance issues and potentially traffic loops. Mesh system nodes should automatically set-up the repeating topology in such a manner to give best performance.
2. Intelligent routing. In order to optimise performance the mesh nodes constantly work out the optimum route for traffic from the client to the source or root. So depending upon where the client is located the back traffic is always going by the fastest route. This doesn't necessarily mean the smallest number of hops because a good mesh system might decide to route data by a larger number of hops simply to bypass one node that is overworked.
3. Auto-healing. The mesh system is continuously applying the features of auto set-up and auto-learning mentioned above to give a degree of self healing. i.e. if a node goes down then the mesh system will automatically re-plan the topology to maintain client traffic routing. 1. and 2. above. When this is allied with the ability of the nodes to automatically adjust their RF power then this should significantly help total network stability.
4. Multiple roots. A typical simple repeating network would consist of a single source node and then several repeating nodes coming off this. Where you have several repeaters with dozens of clients hanging off them then all that traffic has to come back and through that single source node. However, a good mesh network will allow you to install more than one source (or root) node, the back traffic is split over multiple source units. This gives a significant performance improvement and also helps with redundancy.

On the bad side mesh nodes are more expensive than the alternative of simpler nodes using a radio device for local coverage and another device for a WiFi backbone; even if you decide to use integrated dual radio devices which have two radio interfaces built in (one for local and one for backbone) then mesh nodes are

still typically twice the price. The other problem is coverage. Obviously for a node to repeat then it must be close enough from the previous node that it can pick-up a good WiFi connection. If the WiFi connection between the mesh nodes is poor then this will directly impede performance and stability. This means that the nodes must be close enough together to ensure each node can get good WiFi from it's neighbour. If you compare that to discrete nodes using a hard backbone (cable, fibre) this means, with a mesh, the nodes have to be 50% closer so that the WiFi from one node overlaps the next node up the line. This not only means higher overall costs but also increased WiFi interference.

Weighing up the various options my advice is go for APs using a hard-wired backbone. Failing that consider discrete APs with a a WiFi backbone. If the number of nodes is small and outright performance can be compromised then you could, perhaps, consider a repeater type configuration.

2.1 Roaming

One very important issue is it doesn't matter if you use discrete Access Points (APs) on the end of some lan cable or a repeater set-up, a traditional collection of Access Points still appears as separate WiFi sources as far as your client is concerned. This means that the client still sees them a different WiFi's (though you could use the same SSID/security so at least the clients don't have to redo the security password as they move around). However even using the same network set-up for each AP it still wont necessarily seamlessly hop from one AP to the other as you move around. That's called roaming and this behaviour is not intrinsic in WiFi clients i.e. they won't seamlessly hop from one AP to the next as you move around between nodes - there are protocols to help this is 'roaming' but the access points and the clients need to support it. What a client normally does is connect to the first node and then, as you move closer to the second node, if the signal drops out from the first node only then will it scan for a new node and, assuming it can find a stronger AP, then change connection. This can potentially cause signal and connection breaks which can last from an undetectable fraction of a second up to 10 or 20 seconds. What makes it worse is the signal might have to drop and dip several times before the client finally decides it's worth breaking the original connection and having a look for a better AP. During this time you might experience the affects of the poor connection i.e. data drop outs. It's a minefield which 99.99% of end users just aren't aware of; they think bang up a few APs so the site is covered with WiFi and that's it.... giving all the APs the same SSID, channel, security settings does NOT fix this because the WiFi signal from each AP still comes from a source with a different MAC address and ID.

As I say, there are protocols like 802.11k/r which help client migration (not 100% true roaming but pretty good), but the access point/nodes and also the client devices have to support this. Most cheaper APs DON'T!

2.2 Performance

Ten or twenty years ago it was much easier. I mean the number of WiFi users was very low and the amount of internet bandwidth required was very low. Things have now changed. It seems everyone wants to go on holiday in their caravan and then spend their time watching BBC iplayer or all day checking their social media! As such even a small site with only a couple of dozen 'van plots might well have 3 or 4 times that number of users requiring an internet connection. So you need to consider the number of connections each outdoor node will have to cope with and, more importantly, the bandwidth required. You

need to think about this not just for the final distribution node but also with any backbone link feeding the nodes. For example if you're doing distribution using 5GHz bridge units then check that the link is up to the bandwidth required at the source and the end. If the distribution is done using a chain of 5GHz bridges then the first link in that chain needs to be able to cope with the demand for all the nodes following on down the chain. Ditto, if you're using a single 5GHz node for distribution at the source and that unit is supporting three links then the limit is going to set by the performance of the starting unit; you might have three links which, on paper, are good for 50meg each but if all three are going to a single unit then the performance isn't going to be 50meg, it will be, at best a 1/3rd of 50 meg!
So carefully consider the link speeds e.g. sometimes you will need more than one source bridging node simply to improve performance.
Of course this assumes that the internet speed coming is is up to the job! It's amazing how many times we hear of people wanting to supply WiFi internet to a site of perhaps 50 or 100 vans (where there might be 200 to 500 actual users) and only have a single 38meg BT FTTC internet feed! Remember an iplayer feed might well be 2-3meg each so if 50% of the 'vans are watching in the evening then that's maybe over a 100meg of internet required!

2.3 Range

A VERY commonly asked question: What's the range of the access point? Well the first thing is if there's something in the way then the 'range' is as far as the obstruction. WiFi doesn't like going through things and the more substantial the obstruction the worse it gets. For example a typical 2 skin brick wall knocks the signal down maybe 75%. Even a person's hand will knock 50% off a signal, so if you're holding the phone and covering the built in antenna then that will have a serious effect on the signal. Anyway it's best to assume that if there's anything in the path of the signal, even if it's quite close, then the range is as far as that object. So let's say you have clear line of sight from the phone to the outdoor AP and you're also holding the phone so the antenna isn't covered and the signal isn't trying to go through your body or head! With decent kit at BOTH ends you can do a WiFi link of 10-20Km!! That's with line of sight and still being legal. The problem is the typical phone device has poor WiFi (it's not designed to go long distances). So decent products at BOTH ends of the link and this isn't a problem. Decent kit at one end to poor at the other is where you have problems. The analogy is you and I are stood at opposite ends of a football pitch trying to have a conversation. I'm shouting at you with a megaphone. You're replying with a whisper and your hand over your mouth. It doesn't matter how loud I shout we STILL can't have a conversation! So 'range' when one end is a decent outdoor AP and the other end is a phone is limited by the capabilities of the phone. In practice we advise people that even with a clear line of sight it's best to assume around 50m range for the WiFi from a phone. Okay it MIGHT go further and, obviously, some phones are better than others but if you stick to the 50m recommendation then you will probably be okay.

2.4 2.4GHz or 5GHz?

For the last stage of distribution to the end clients, should you use 2.4GHz or 5GHz WiFi? If you'd have asked this question a few years ago then the answer would have been go for the 2.4GHz. The reason being only a few client devices (phones, tablets, etc) actually supported 5GHz WiFi, plus APs that supported 5GHz were not exactly cheap. However things have changed i.e. most phones etc.. now support 5GHz WiFi and the cost of nodes (access points) with 5GHz are a lot cheaper than they used to be. There are also several

advantages with offering 5GHz for the final connection and that's WiFi congestion. The old 2.4GHz band really only has 3 non-overlapping 20MHz channels. This was fine 10 or 20 years ago but with the huge number of WiFi clients now around, having only 3 channels is a pain and means poor performance. The 5GHz band gives us 11 new outdoor 5GHz channels so using 5GHz can give a significant reduction is network congestion. You still need to support 2.4GHz as well because there are a number of clients out there that only support 2.4GHz however supporting 5GHz as well should improve network speeds and increase the number of clients a node can cope with.

3 Hard-wired Infrastructure

First thing is decide where to put your access points – see Physical Implementation/Site Survey below.

So you have a rough idea about where to put your access points to hopefully give blanket coverage. As to how to get the backbone network connection to each node, I'll leave that for you to sort out! Just bear in mind that there are several different hard wired options: There's normal cat5 cable: Fibre cable: Powerline down twisted pair wire. There might be other options but which ever way you go there are pluses and minuses not least of which is the issue of having to dig some trenches! The big advantages though of hard-wired nodes are maximum speed (no slow WiFi backbone), greater connection stability, and a much wider choice of Access Points.

3.1 Local AP Choices

If you want to stick to 2.4GHz only then a very popular outdoor AP is the ENS202EXT

http://solwise.co.uk/wireless-outdoor-bridging-el-ens202ext.html

This is a 300Mbps 11n 2.4GHz outdoor AP with two 5dBi omni antenna and gives a good, all round, coverage. It has built in PoE and comes with the PoE power supply included so you can use the lan cable for power and also data.

If you want a good outdoor unit which is 2.4GHz AND 5GHz then something like the ENS620EXT is ideal

https://www.solwise.co.uk/wireless-outdoor-bridging-el-ens620ext.html

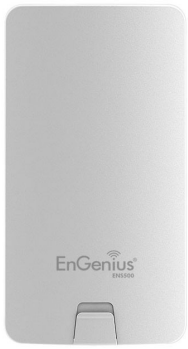
This is an outdoor omni device with dual band AP with 2.4 and 5GHz simultaneous WiFi using omni antenna (which could be replaced if needs be). It supports 300meg 11n 2.4GHz WiFi and also 866meg WiFi at 5GHz. A quick word about the 866meg 5GHz WiFi. The 5GHz on this unit is 11ac WiFi. This is WiFi that uses 80meg (that's 4x20meg channels) bandwidth. tbh this is a complete waste of channel space! What I mean is you don't need 866meg WiFi when installing a public WiFi solution! Think back to the arguments above about performance. The typical caravan site customer doesn't need a 866meg WiFi connection. All that does is waste 4 channels of the 5GHz WiFi. It would be much better to configure the 5GHz to operate at standard 300meg 11n. 300meg WiFi is perfectly fast enough for this sort of application; there's no point it giving all the clients a super-duper fast WiFi connection when the back-haul and the internet feed for the site isn't up to the job.

A quick note about the 5GHz WiFi in the ENS620EXT unit. One thing to bear in mind is if you are using a 5GHz bridge to link to the ENS device then you need to ensure that the 5GHz channels being used for the ENS620EXT don't interfere with the channels used by the bridge unit otherwise the interference might reduce performance.

4 WiFi Infrastructure

This isn't really much different than the hard-wired set-up: The essential broadcasting AP can be the same units e.g. the ENS202EXT or the ENS620EXT units as described above. However, instead of using some form of cabled backbone connectivity you instead use a separate WiFi infrastructure. In practice this could mean using 5GHz CPE units like the ENS500(EXT) or the ENStation5:

http://www.solwise.co.uk/wireless-outdoor-bridging-el-ens500.html



http://solwise.co.uk/wireless-outdoor-bridging-el-ens500ext.html

The ENS500(EXT) is ideal for distances up to a Km at 300meg 11n WiFi with throughput typically up to 50Mbps. The standard ENS500 has a built in directional 10dbi antenna. The EXT version has 5dbi omni. So for a simple point-to-point link then you'd use two of the ENS500 units. If you wanted two links going to a single source then you would probably need a wide angle antenna at the source so that's when you use the EXT version. So you'd have two remote ENS500 units that link back to a single ENS500EXT.

If you want a longer range for your link then you could use the ENStation5

http://solwise.co.uk/wireless-outdoor-bridging-el-enstation5.html

This is the same WiFi hardware as the ENS500(EXT) units but has a much higher gain integral directional antenna. This is good for perhaps 5Km in point-to-point or 2 Km when connecting to an ENS500EXT.

For much higher speed throughputs and/or longer distances then consider the ENStationAC

http://solwise.co.uk/wireless-outdoor-bridging-el-enstationac.html

This is an outdoor 5GHz bridging unit that uses 866MHz 11ac WiFi. It's capable of throughout speeds of up to 300+Mbps and distances of up to 10Km.

Another option, instead of using a separate access point for local coverage and then another, separate, radio device for the backbone is to go for a dual radio integrated radio device; so this is one product which contains both the 2.4GHz radio and the 5GHz radio. So you can use the 2.4GHz part for local connections and then the 5GHz for bridge linking. e.g. this might be the ENS620EXT as mentioned before

https://www.solwise.co.uk/wireless-outdoor-bridging-el-ens620ext.html

5 User Management

A site implementing a WiFi system should probably also consider how 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 proper site users that have paid can use the link. There are also EU rulings that need to be thought about with respect to secure WiFi and also keeping records of users:

In September 2016 the EU have said that you are no longer allowed to run an open WiFi public network are you must also collate contact details for each user!

http://www.theregister.co.uk/2016/09/15/eu_ends_anonymity_and_rules_open_wifi_hotspots_need_a_password/

You will probably need to consider some form of hotspot gateway to collect these user details. This can then collect user details using PayPal (if you want to charge) or via Facebook or a custom login page or simply noting them down when you give each user their unique access code.

e.g.
http://solwise.co.uk/wireless-hotspot.htm

A hotspot gateway/router will help you keep track on the internet usage because if someone at the site downloads copyright material then it is the site owner, the person whose name is on the internet account that takes the blame.

The hotspot router sits between the main, gateway network connection the broadband source e.g. the DSL or FTTC router on the internet connection. It connects via LAN to the public WiFi network and the incoming router and acts as a controller for any internet access going through to/from the public network. Using the hotspot you can either manually pre-set usage accounts or issue ‘on demand’ tickets 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 the want to access the internet. Access accounts can be set-up to give short term access or longer usage, such as the duration of the customers stay or on a weekly basis.

Tickets for on demand usage can be pre-created by the site operator using their own PC printer or using the special networked ticket printers. Using the special networked printers allows the operator to place ticket printers remote from the where the gateway is located.

Further functions include:

- Options for site and access logging (see below)
- Centralised authentication so you can run several gateway units connecting to a cloud service with a centralised user database
- Traffic statistics and graphs
- Facility to reserve certain MAC or IP address for authentication free connectivity; this is useful for people that want other devices to link back over the mesh to the internet e.g. site IP cameras.
- 1 or 2 or even 4 internet feeds so you can easily improve your connection speed by adding another internet connection (number of WAN ports is model dependant)
- Time allocations for when to or not to allow access

5.1 Legal Implications

One topic that comes up from time to time is what a site operator should do about illegal downloads. In this case 'illegal' can be thought of as either downloading illegal material such as kiddy porn or downloads which infringe copyright rules such as downloading rip-off DVDs. Various aspects of this were hinted at in the famous Digital Economy Act of 2010.

http://en.wikipedia.org/wiki/Digital_Economy_Act_2010

But the whole issue of illegal downloads was left intentionally unclear and vague because no time was taken for a proper consultation and to seek the correct expert advice. As a consequence end users and people wishing to operate services like public WiFi internet are to a large extent left to try and make the best assumptions they can about what they are supposed and not supposed to do.

Please note that ANY comments we make here are purely how we see things and should NOT be taken as legal advice or recommendations: This is just how we see the situation and we leave it up to the reader to make their own analysis of the act and make their own decisions about what their obligations are concerning what they have to do or does not have to do when operating a WiFi internet service.

In 2011 there was a document by Ofcom which contains some important definitions which should help those running a WiFi internet service:

http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf

Below are a few key extracts from this document:

"*In principle, operators of Wi-Fi networks would fall within the definition of internet service provider where the service is provided by means of an agreement with the subscriber, even where this is oral or implicit. Indeed, Wi-Fi operators would be regarded as offering a*

fixed service on the basis that it is offered from fixed locations and is not a licensed mobile network. It may not, however, apply to open access Wi-Fi networks where there is no payment from, and no agreement with, those making use of them. In those circumstances, the person making open access Wi-Fi available would themselves be a subscriber."

So, I take this to mean, where the operator of a WiFi service is supplying internet to end users as part of an agreement then the operator is an internet service provider and the end users are subscribers. Where there is no agreement then the operator is considered the subscriber.

However further on Ofcom say...

"*We consider that a person or an undertaking receiving an internet access service for its own purposes is a subscriber, even if they also make access available to third parties."*

So, this raises three points:

1. If a site operator has an internet connection for his own use but also supplies it onward then the site operator IS the subscriber (and therefore to blame for any infractions).
2. If the site operator has an internet service solely for third party use then the end users are the subscribers as long as there is some agreement between the end users and the site operator
3. However, if the site operator has an internet service solely for third party use but there is NO agreement in place then the site operator is the subscriber.

The gist of this is that it is best if the site operator has a) a dedicated internet connection and b) some form of agreement. This agreement can be implied or oral.

However this doesn't give any advice or help about what the responsibilities are of the operator or what the operator should be doing to protect themselves.

For these reasons it is perhaps prudent that anyone running or offering an internet service first of all supplies terms and conditions for access. There are various example copies of such T&Cs available out there on the internet but the key points which, in our opinion, should be covered include:

1. Limitations of what the service and operator should offer.
2. Statements that the service shall not be used for illegal operations
3. If you are going to maintain a log of the Internet Protocol ("IP") addresses of any devices which make use of the service and the times when they were accessed (using, for example, the logging facilities available in one of our hotspots) then you should warn the users and also advise them that this log might be shown to people, like the police, if so requested.
4. Following on from point 3 you need to ensure that you do not examine the use to which the client puts the service e.g. you don't monitor the content or interception of e-mails or look at any information downloaded since this might be construed as criminal liability by the operator of the service under the Data Protection Act.

6 Physical Implementation

So that covers the basics and explains the equipment involved, let's now consider the factors involved in an installation.

6.1 Site Survey

This is the hard part. The more time you spend getting the survey right then the quicker you'll get the installation up and working. You could go for the 'organic' approach i.e. put up a couple of units and just see what the coverage is like and, if you've got black spots, then just put extra units up, one at a time, until the site is covered. The organic approach is okay but not so easy if you want to turn up and bang the units straight up and have the system working in a day.

First have a look at the site and see where it's physically possible for you to mount the AP nodes. Remember they need to be at the right height to give the best coverage to people on the ground or in their 'vans/cabins. So you don't want them too high or the signal goes right over their heads and you end up with back spots close to/beneath where the nodes are mounted. Then again you don't want them too low or the signal ends up getting blocked by structures such as the neighbouring caravans: Remember the signal has to get clear line of sight so it can enter via the windows at the receiving end. If this is a mesh configuration then you also need to ensure that each mesh node can 'see' at least one other node and that there is a mesh route back to the source. However normally the nodes connecting to each other are not the problem: It's the people on the ground seeing the nodes that's this problem.

You then need a pole or structure to mount the node on, perhaps 4m high for a caravan site; maybe higher for a marina. You then need a source of mains power close or at the pole: The power is delivered to the AP or mesh node via a lan cable which can be technically be up to 100m long but we recommend keeping the lan cable as short as possible, maybe 20 or 30m maximum.

btw a common question we get asked at this stage is what's the range of the AP node. This is a question that tends to tell me the person hasn't understood the issues involved with WiFi connectivity. First of all remember that WiFi doesn't go through obstructions. Therefore the range of any WiFi signal is, at most, only going to be as far as the thing in the way. The next important issue is the capabilities of the client device. Where there is a WiFi link between a hand-held product and a professional grade outdoor unit then the weak part of the link is going to be the weedy client. The signal back from the client is going to be very weak or of very poor quality. So, for example, where a pair of mesh nodes with 9dbi antenna have probably got an absolute range of over 500m BUT if there's a caravan just 10 yards away that's blocking people stood behind it then the range is only 10 yards. If the client is an iproduct then, even with line of sight, don't expect anything better than 10 or 15 yards!

Once you've decided on spots where you could physically locate your nodes, next take each of those spots in turn, on a site map, and guestimate where the signal is going to reach assuming it radiates out in a straight line from the node. This will enable you to come up with a short list of potential mounting spots. The next part involves temporarily mounting a test node at each of these spots so you can test range to your chosen client

device. You don't need a network connection for the test unit: Simply mount the node device, power it up, and then walk around the site checking the signal strength with your client device (could be a hand held WiFi device). Check your map and see if the signal is reaching the areas you need to. To check properly you really need to look at the signal inside the 'van/cabin/boat – looking at the signal strength in the open air is going to be totally different to the signal strength actually inside the van or cabin!

6.2 Final Considerations

So now you've decided where the nodes are going to go and how they are going to be linked back to the source. You need to set-up the access point nodes with any WiFi security and SSID names you want though, tbh, we would normally advise using some form of user management with a hotspot gateway instead of WiFi security to control access because that puts less of a work load onto the APs. You might also want to consider setting a maximum number of clients for each node; if you have more clients in a particular area then consider adding another AP in the locale to distribute the users. Also configure each node on a different IP address.

With the nodes configured you can then install them at site along with any bridging set-up you are using, testing client connectivity and interconnectivity between the nodes as you go along.

The final stage is, if you have opted to use a hotspot gateway for user control, is to configure the gateway according to the type of set-up you need.

With that done that's pretty much the thing completed and the whole set-up should, fingers crossed, be delivering WiFi over the site as required.

Steve Mace, Solwise Ltd.