



TEL: +44 (0) 1295 266277
FAX: +44 (0) 1295 268199
SALES@MSDIST.CO.UK

UNIT F121 CHERWELL
BUSINESS VILLAGE
BANBURY
OXFORDSHIRE
OX16 2SP

Setting up Wireless Links

Setting up a wireless link needs a little bit of knowledge about wireless and about computer systems. To cover all of it in one 'simple' document means information will be missing, but the information below is enough to get Wireless units up and running. It's divided into four sections:

- 1. Computer networks and 'IP addresses'**
- 2. Wireless networking**
- 3. How to change IP addresses on a PC running XP, Vista or Wins 7, and a on a wireless device**
- 4. Setting up Ubiquiti Airos V units in Bridge and Access Point/Client Modes**

You can skip any section entirely if you already know about it.

1. Computer networks and 'IP addresses'

If you know what an IP address is, what form it takes and why it must be a unique number, skip this section completely.

This section applies to PCs on a *network* – i.e. any PC that talks to another device somewhere else. A single home PC connected to the internet is part of a network. A standalone PC in an office with a wireless router attached is a network.

What's an IP address?

Every networked PC has an *address*, just as a house or business has an address so it can be found. 123, Acacia Avenue, Cheam, is an example of a UK address. In the world of computers this would be written as CR111AZ. Cheam. AcaciaAvenue.123. A PC's network address might typically be 83.200.132.254 and the highest number it can possibly be is 255.255.255.255. When the numbering system was invented (called IPv4) it was assumed that it would be enough to give a unique number to every computer ever likely to exist by providing 4.3 billion possible addresses, but on February 3, 2011 the numbers ran out, so a new system is coming on stream called IPv6 to allow for a lot more. This won't affect your reading of this document as implementation of IPv6 is a little way off yet.

The system was designed so that any IP address could be further divided by using a similar numbering principle called a subnet, the highest number available being 255.255.255.255. (This would be like dividing 123 Acacia Avenue into a very large number of very small flats). Typically the subnet mask is not used and is left at its default number of 255.255.255.0.

If you want to know more about the detail of IP addressing there's a very full explanation at http://en.wikipedia.org/wiki/IP_address but all we need to know now is that every PC on a

network has a unique IP address as four sets of three digits separated by a full stop – nnn.nnn.nnn.nnn

What are they used for and why?

Think of an office with 100 PCs in it. Each one needs its own IP address to identify it uniquely, and so does the office as a whole. This could be achieved, for example, by giving the entire office one address – let's say 192.168.2.254 – and giving the 100 PCs numbers 192.168.2.1 through to 192.168.2.100.

All the PCs are then wired back to a box (called a *router*) that picks up data from one machine and sends it to another, and the router would probably be number 254 in the example above. A router works like the Post Office, sending and delivering packets of data. It knows where to send them because every packet of data coming from one PC (think of an envelope containing a letter) has an IP address on the 'outside' of it saying where it's going and another IP address attached to it saying where it's come from. The router box *routes* the traffic on the network to the right places using the IP addresses attached to the data that's travelling through it. Usually, the router is attached to the *internet* too, so that data from the world outside the office can come in and out. Looked at from the outside world end, the entire office would have the IP address 192.168.1.254 and the office router handles data coming in from the outside and within the office to make sure it arrives at the right PC.

Why the IP address must be 'right'

If a PC user wants to look at something on a web page somewhere on the internet they would open up a *web browser* (Internet Explorer, Firefox, Safari, they all do the same job) and type in the name of the place they want to go in the form of www.bloggsLtd.co.uk. The browser sends this data to the router in the office, which then sends it on from its own IP address to web servers. Making a very long story short the web servers look up a huge list to find bloggsLtd.co.uk and discover what its IP address is. They then send on the request for a home page to the server at that address, which sends back the home page data all the way back to the office router, which passes that to the PC that asked for it and the user gets to see the page. The data request could travel through hundreds of routers and servers and back again in a fraction of a second and the system relies entirely on knowing the correct IP addresses right down the line. Thus IP addresses have to be exactly right or the data doesn't come back to the right place. What's more, if any of the 100 machines, which can currently 'see' all the others in the office were to have its IP address changed say from 192.168.2.80 to 192.168.3.80 it wouldn't 'see' any of the other machines and none of the others would see it (rather like it suddenly being moved to a different street). And if someone changed the address of PC number .100 to .99 there would suddenly be two machines on the network with address .99 which could confuse the poor router no end (just as the postman would have trouble with a letter addressed to Acacia Avenue number 123 AND number 122: he wouldn't know which house in Acacia Avenue to pop the letter into).

Where do IP addresses come from?

To save users having to learn all about IP addresses and how to set up a computer with an address to suit its use on a specific network, it is very common to have the router decide what the IP addresses for all the network PCs should be and tell them to just take the number they are given. The facility is known as *DHCP* and routers, or many other devices, can be set to hand out IP addresses to other devices by using DHCP. Where this facility is

used there is a setting in Windows to 'Obtain an IP address automatically' and the process is automated, and a new PC will normally be set up for automatic when it comes out of its box. It's important not to have two devices on a network both handing out DHCP! Also, if the automatic feature is used the IP address of each PC may change next time it or the network router is restarted. Sometimes it is better to give a PC a fixed number that it will keep permanently.

To sum up:

- Every PC has a unique address in the form of nnn.nnn.nnn.nnn (though it could be just n.n.n.n, or nnn.n.nn.n, or any combination of them, where n is less than 256)
- There is likely to be a subnet address for each PC, typically 255.255.255.0
- No two PCs can have the same IP address on the same network.
- If a PC is not in the right IP address range (one of the numbers other than the final numbers is not the same as all the others) it won't be able to communicate with any other PC because it's not on the same network.
- PCs may get their IP address automatically from a network router using DHCP.

Finally, until wireless networking came along, PCs were wired up on the network through cables connecting each one back to the router. Now the same thing can be done without the wire – i.e. wire-less-ly.

2. Wireless networks

If you already know about line of sight, frequencies, channels and choosing suitable antenna, skip this section.

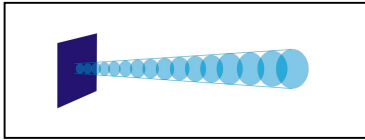
A wireless network is a system used to link two or more PCs together without using cables to do it. This can be very convenient and avoids the cost of laying cables in – which is very costly if you want to link two offices on opposite sides of town as it involves digging up roads, or renting a *leased line* from BT. If you want to shift vast quantities of data then a copper cable between the two points may be the only way to do it but typically costs many thousands of pounds a year for rental and is an expensive solution if the other office is just across the road. If you want to shift less data, then a wireless installation at one-off cost of just a few hundreds of pounds may offer a permanent solution, but wireless doesn't offer a solution in all cases.

What is needed to be able to make a wireless connection?

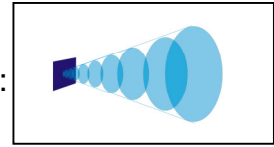
Wireless needs *line of sight* – that is the unit at one end must be able to 'see' the unit at the other with no obstructions in the path, just as you can. Typically a wireless unit has a radio and antenna inside it, so it sends out a radio signal. At the other end of the link another of the same unit listens for the radio signal then sends back data. To do this successfully the radio and antenna it is linked to must meet certain requirements:

- The radio must be good enough to send out a decent signal and sensitive enough to 'hear' the signal coming back. (There may be other wireless systems in the area sending out signals too, so when a unit is listening it must be able to find out which signals it should be listening to and ignore all the others in the area – more on this below.)

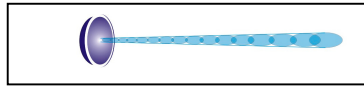
- The antenna must be able to pick up signals coming from the right direction. The antenna in most radio units sends out quite a narrow beam in just one direction so they need to be pointing at each other. (Think of two torches some distance apart – they must be shining directly at each other so that the beams line up.) Typically the beam is about 35 degrees up/down and left/right and looks like a cone:



But the width of the beam can be bigger:

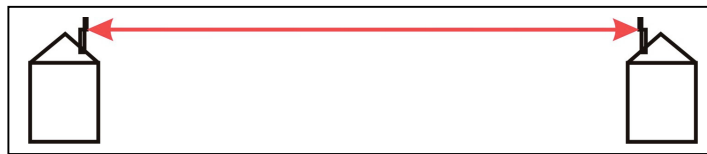


Or if the radio unit is connected to a dish antenna, the beam may be very narrow indeed:

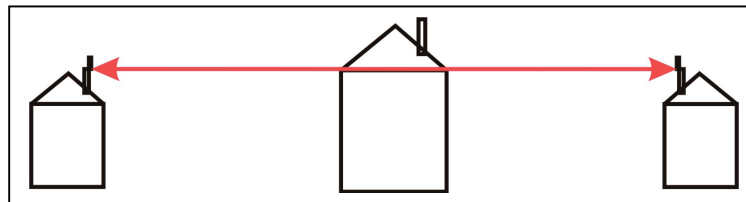


The wider the beam the more the signal is dissipated over a given distance, so if long-distance links are required a dish with a pencil beam would do well, but for a short link a wider beam is fine. The ‘power’ of the antenna is rated with a number which tells how much the beam is focussed in just one direction, so in the pictures above the wide beam might have a ‘gain’ figure of 10 dBi, while the dish has a gain of 28 dBi. How these numbers relate to each other, what dBi means and how the physical size of the antenna relates to the gain are beyond the scope of this document but more information is available at http://en.wikipedia.org/wiki/Antenna_gain but be prepared for the maths.

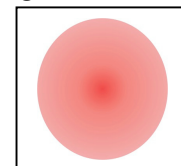
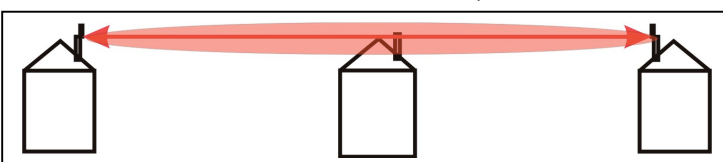
So, to link two points by wireless we need two radio units arranged something like this:



But because we must have line of sight, this link wouldn't work:



And neither would the one below, because quite a lot of the signal is above and below the centre line. Looked at end-on, the radio beam is really more like this:



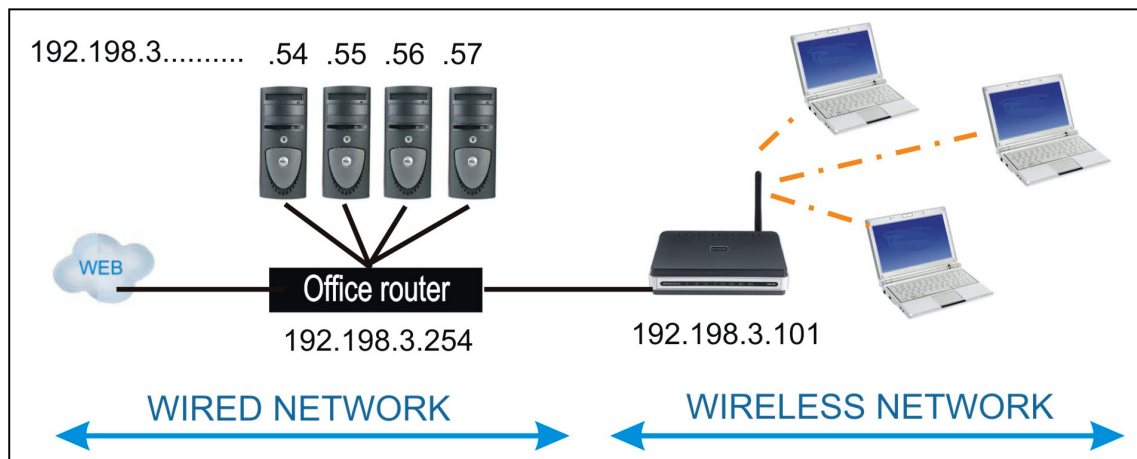
Looked at end-on, the radio beam is really more like this:

The line through the middle is the line of sight and the area around it is called the *Fresnel Zone*, which carries quite a lot of the signal. In fact, if you block 20% of the Fresnel zone you'll lose 40% of the signal, so it's not enough to be able to have a line of sight between two points like a piece of string – for example just over the top of a building to the point you can see on the far side – there must be plenty of clear space all around the centre line too. Just for the record, unlicensed wireless links in the UK operate on two

frequencies – 2.4 and 5.8 GHz – and at those frequencies line of sight is vital and the signal doesn't travel very far – perhaps 20 kms with a dish antenna, 5 kms with the smaller antenna. Signals can be stopped entirely with thick stone walls and trees are a real obstacle. (The only answer to trees in the path is a chain saw.) Mobile phones, which work on a lower frequency, can penetrate stone and brick more easily, which is why users don't have to stand outside – though they may have to in poor signal areas – and for the same reasons the units used for wireless networks really are best placed outside a building in free space and preferably at least 3 metres above ground level.

Spectrum overcrowding and how channel numbering may help.

The radios used in these units will pick up signals from every other wireless network in the area. In the office with 100 PCs there may be some laptops which their users want to be able to use anywhere without having to plug a network cable into them. All laptops now have radios built-in and a wireless router could be connected to the network on 192.168.2.101 following the example above to broadcast a wireless signal that the laptops can use to connect to the network.



This works well until the office next door installs a wireless router as well, the coffee shop across the road installs a free hotspot, the people in the flats next door all install wireless routers too and the result is lots of signals all whizzing about at the same time and interfering with each other. The radios hear all the signals and have to sort out which ones they want to listen and talk to (more on that under SSIDs below) but will be under quite a heavy load as they struggle to sort out which signal is the one they want. When they're struggling they work more slowly because they're trying to process a lot more incoming radio data before they can even start to concentrate on the data packets that they want to pass on to their network.

There is a part solution to this. On the 2.4 GHz range the available airspace is split into 13 channels, and all the users on one network can be set to stick with one particular channel number that isn't used by another local system. With 13 channels available this should give plenty of room for everyone, but unfortunately each of the 13 channels spills over into two adjacent channels, so if there is a local user with a strong signal on channel 6 then channels 5, 6 and 7 will be occupied as well so the next lowest channel number that's usable is 3, which will use up 2, 3 and 4. The next highest will be 9, which will use up 8, 9 and 10. So really there are only 4 sets of usable channels out of the 13 available, which can sometimes make for difficulties depending on how busy the local radio environment is. Another solution is to use radios that work on the 5.8 GHz band as it is far less crowded – at least for the time being. 5.8 GHz kit tends to give better results in urban environments.

Point to Point (PTP) and Point to Multipoint (PTMP).

Wireless units can operate in different ways, called modes. You might want to just link two places together (Point to Point – think of a wire strung between two buildings) or one central unit might be required to talk to many others (Point to MultiPoint – think of a telephone pole in the street with wires running from it to many buildings). Wireless units need to be told the first time they are set up which mode they need to use. *Bridge Mode* means Point to Point: the unit at each end is set up in Bridge mode so they can only talk to each other. For Point to MultiPoint use the unit to be used as the central point is set in *Access Point Mode* and the many satellite units are set in *Client*, or *Station*, mode.

To sum up

- Wireless networks need line of sight
- Line of sight means a direct line between two points and a fair amount of free space around that line, with no intrusion by buildings or trees into the fresnel zone.
- Units need to be chosen that will perform at the distance required and the beam pattern and gain of the antenna must be carefully considered
- Channels available can be quite busy on 2.4 GHz so 5.8 GHz may be a better choice
- PTP or PTMP must be selected and each unit set up in the appropriate mode to do the job required of them.

If you want to find out what other radio devices may be using certain channels, download Netstumbler from <http://www.netstumbler.com/downloads/>. It's free. Install it and run it to see what devices are in your area and what channels they are using. Be aware that sometimes radios are set up to hide that information and that you may need VistaStumbler from <http://www.vistumbler.net/> if you are using Vista on Windows 7.

3 How to change IP addresses on a PC running XP, Vista or Wins 7

If you already know how to check and change a network computer's IP address in order to set up a wireless unit for use on the network, skip this section.

This section will deal with setting up Ubiquiti radios running AirOS V operating system for use with networks running Windows XP, Vista and Windows 7.

Ubiquiti networks units show on the end of their box what the number of the installed operating system is and that number should be 5 or higher for use with the instructions below. Earlier versions follow the same principles but the screenshots may not be exactly the same as those shown here. By default, the IP address of any Ubiquiti unit is always **192.168.1.20** out of the box.

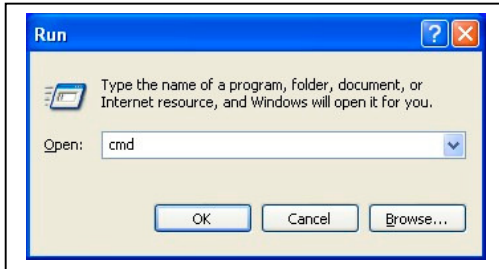
If your network or computers are using the IP address range of 192.168.1.1 to 192.168.1.255 you are very lucky and can skip a lot of this section **unless** you already have a PC on the network using 192.168.1.20, in which case you will need to change that unit's address to a different end number. .250 is usually a good choice as a temporary measure while the PC is used to set up the Ubiquiti units.

If you need to look at the IP addresses of all the PCs on the network to find an IP address that is free on the network, download Superscan from <http://www.softpedia.com/get/Network-Tools/Network-IP-Scanner/SuperScan.shtml>, install it, and run it to get a list of all devices on the network and their IP addresses.

To set a Ubiquiti unit's IP address you need to be able to connect to it using a web such as Internet Explorer, Mozilla, Safari etc. BUT the PC from which you do that MUST be on the address range **192.168.1....** or it won't see the Ubiquiti unit at all. This may mean that the PC must have its IP address changed and the instructions below cover how that is done. The routine is:

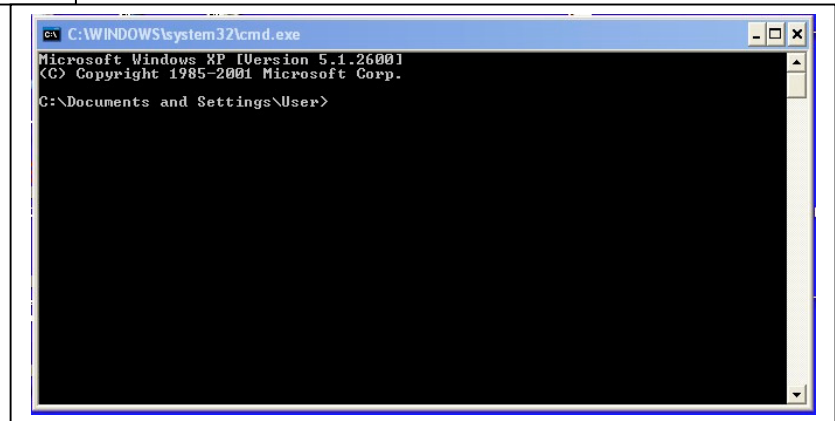
- put the PC on the same IP address range as the Ubiquiti unit
- connect to the Ubiquiti unit
- change the IP address of the Ubiquiti unit to match the network IP address range
- change the PC's address back to what it was before you started
- connect to the Ubiquiti unit again with the web browser to set it up.

It takes a while and it's a bit cumbersome, but is straightforward.



From the Windows desktop click Start, then click Run to get a box on screen like this:

Type **cmd** in the box next to the word 'Open:' and click OK. A new window will open like this



To make life easier. click anywhere on the box, then type `cd..` and press return, then do it again, until you get to just `C:>` on the left of the screen. Now you can use the *Command Line interface* (that's what it's called) for the next step.

Type **ipconfig** and press Enter. You should have returned to you four lines of text. The middle two lines are the important ones and the numbers you see will probably be different to these:

Ethernet Adapter Local Area Connection

Connection-specific DNS suffix.....:

IP address.....: 192.148.3.54

Subnet mask.....: 255.255.255.0

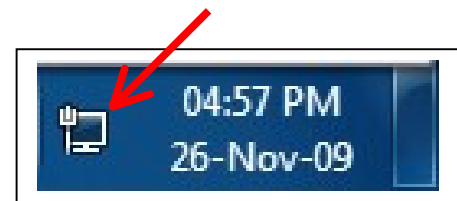
Default Gateway.....:192.148.3.250

This tells us that the network address range for the PC you are using is 192.168.3 and this PC has the number 54. The subnet mask has conveniently not been changed.

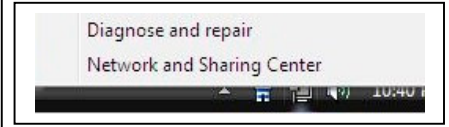
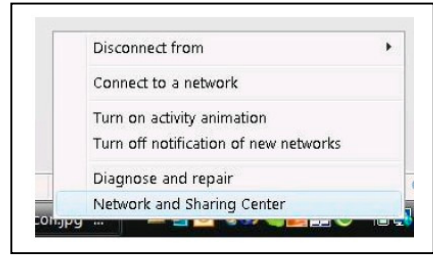
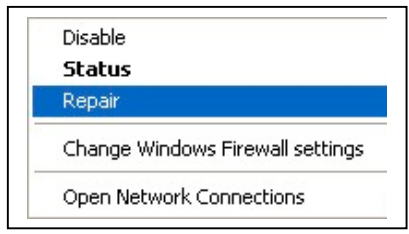
First we change the PC's IP address to it can see the Ubiquiti unit, which is on **192.168.1.20**. Click on the Network icon in the bottom right corner of the PC's screen:



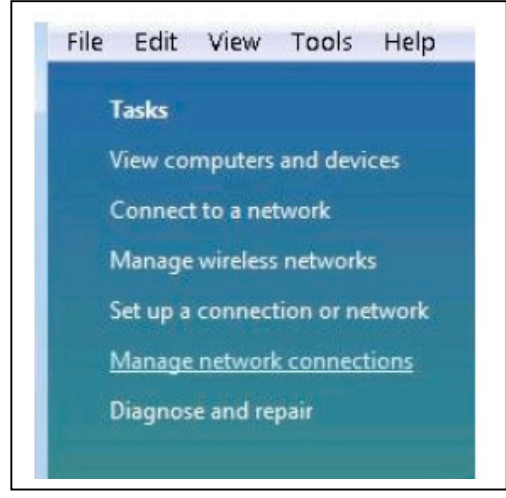
In Windows 7 the icon looks like this:



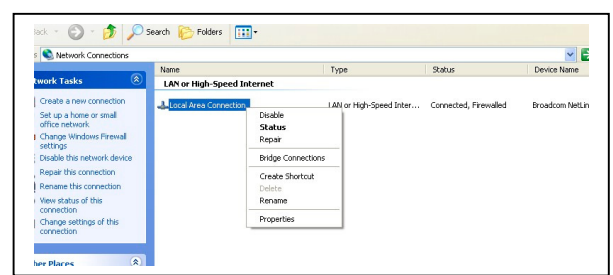
(If you don't have the icon, click Start\Control Panel\network connections and skip down this page a bit.) A new window will pop up. In Windows XP choose **Open Network Connections**. In Windows Vista and 7 choose **Network and Sharing Center** [sic – we can excuse American English spelling]



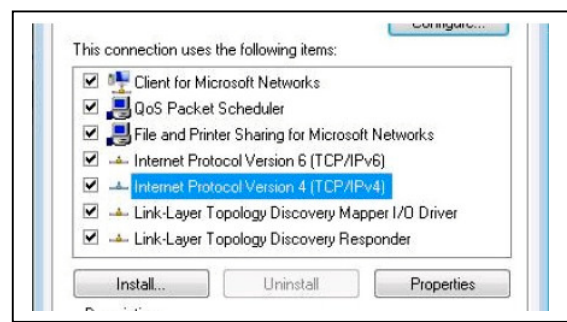
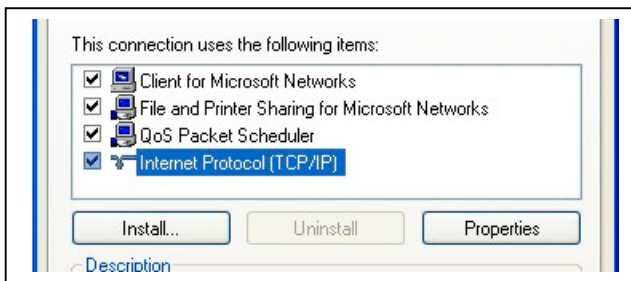
In Vista, choose Manage Network Connections



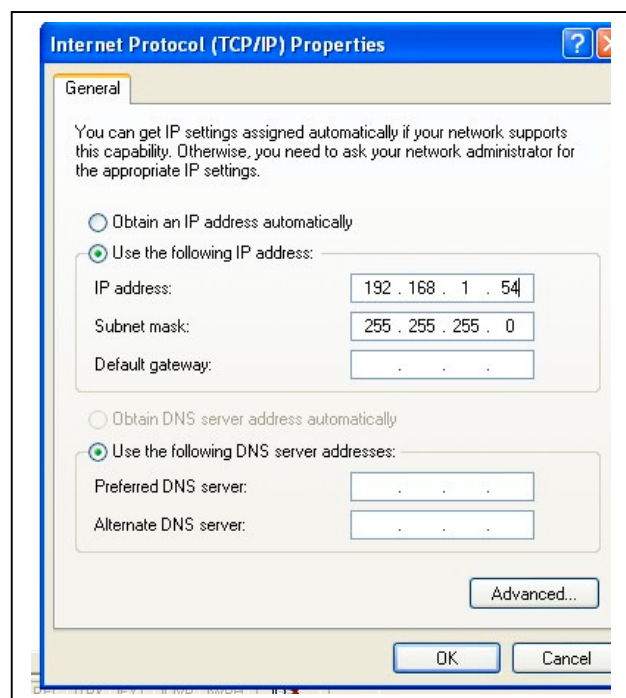
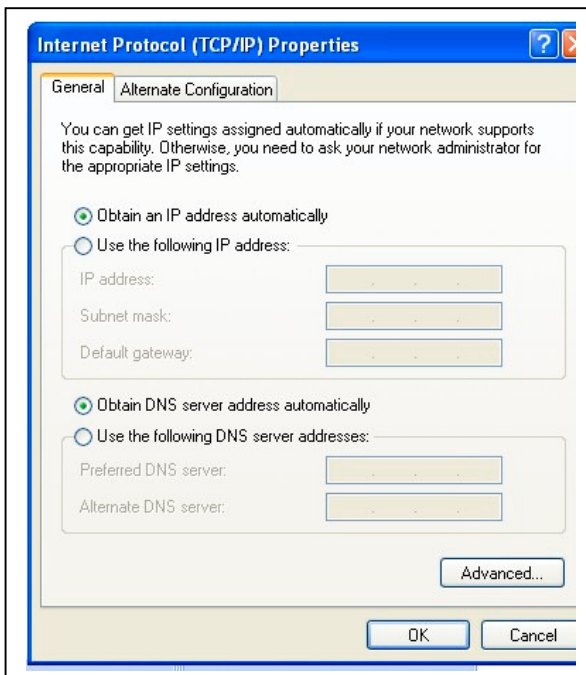
Next there's another box. In XP, Vista and Windows 7 all have a different layout, but look for the **Local Area Connection** and click on it. Click **Properties** at the bottom of the box that appears.



Next screen - click on **Internet Connection Properties** or **Internet Protocol Version 4** to select the line, then click the **Properties** button. In Windows 7 you can click on the Properties button straight away – whatever screen you have in front of you find **Properties** and click on it.



XP, Vista and Windows 7 all now present a very similar screen. If the PC was set to obtain an IP address automatically (the router is doing the DHCP) there will be a blob in 'Obtain an IP address automatically.' If the blob is in 'Use the following IP address' there will be an IP address that someone has previously entered. If there are numbers showing, write them down somewhere safe because they're about to be changed temporarily and if they are not put back **exactly** as they are now in due course the PC will disappear from the network.



The IP address of the PC must now be changed to match the range that the Ubiquiti unit uses by default. The first 3 numbers **MUST** be **192.168.1....** and the last number can be anything **except 20** – which the Ubiquiti will soon be using. Type the numbers in, keep the subnet mask as 255.255.255.0, and click OK. Now back out of all the previous screens until you are at an empty desktop.

If you want to be sure that the IP address is set correctly, open up the cmd window again and type ipconfig as you did before. This time the IP address should be

192.168.1.[whatever number you chose - and it mustn't be 20 - here]

The next step is to set up the Ubiquiti units to match the address that the PC network you are dealing with is on. In this example the address range is 192.148.3.... so the Ubiquiti unit (or a pair of units if you are just creating a PTP Bridge) will now have to have its IP address changed as the next step in the setup.

Remember that when the Ubiquiti unit(s) have been set up, this PC will need to be returned to its original IP address by going through the procedure again and setting it either to 'Obtain an IP address automatically' or have the correct IP address put back as it was when you started. It's a much faster procedure after you've done it once....

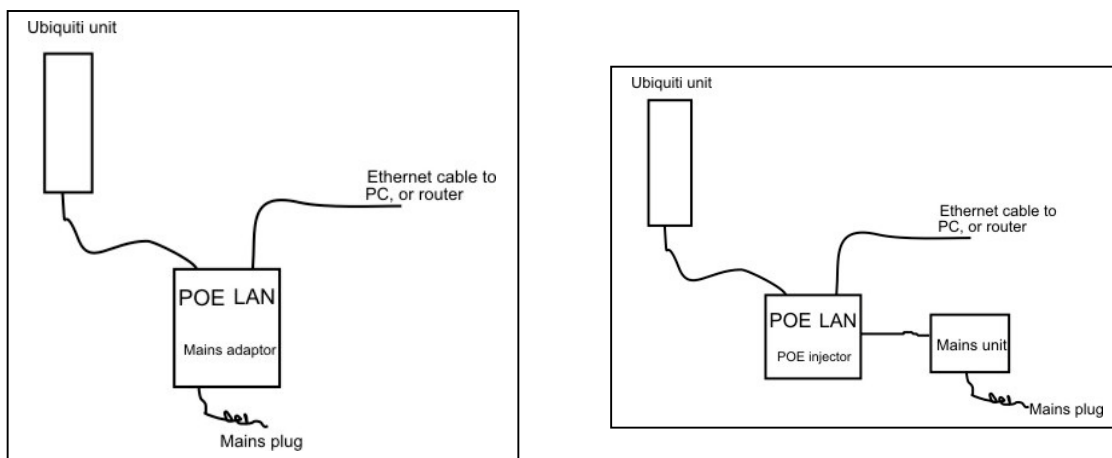
4. Setting up Ubiquiti Airos V units in Bridge and AP/Client Modes

This section deals with setting up Ubiquiti wireless ethernet units for use on a network in Bridge or AP/Client modes.

Ensure that the PC you are using to connect to the Ubiquiti unit has an IP address in the range 192.168.1. n [where n is between 1 and 254 and is NOT 20].

All Ubiquiti units have an ethernet port. Some have two. Where there are two, use the one marked 'MAIN.'

There are two possibilities for wiring, depending on whether your mains unit has a *Power Over Ethernet* socket built in, or whether you have a separate mains supply and a POE injector. This is how they hook together to supply data and power via the ethernet cable to the Ubiquiti unit:



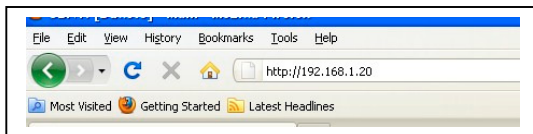
The length of the ethernet cable is important. Although it will carry the data up to 100 metres, the power is carried by two spare pairs of wires in the cable and because the wires are thin (typically 22 AWG) the voltage delivered at the other end of the cable is reduced and the longer the cable is the more it's reduced. A 10 metre cable will not make a significant voltage drop, 20 metres will, and a 50 metre cable will reduce the power available at the radio unit a lot, to the point that it may not work well, or may not work at all. As the cable length increases, the transmission power of the unit will drop, because the radio does not have enough power available for it to work properly. For this reason we don't recommend using more than 20 metres of ethernet cable with Ubiquiti radios when using a 24 volt supply: lower supply voltages will deliver proportionately less power to the radio over the same length of cable, so 24 volts is a good starting voltage, but don't go higher than that with Ubiquiti gear, it won't stand it.

Hook up as per the diagram and switch the power on at the mains. **NEVER insert an ethernet plug with power on it into the radio unit. ALWAYS switch the power on**

and off at the mains supply to the mains unit. ‘Hot plugging’ applies a large current to the power supply regulators in the radio unit which they are not designed to handle. Switching the power on at the mains unit allows the current to rise to the level required more slowly. **Wrecking the power regulators by hot plugging is not covered by warranty – it is misuse.**

Ubiquiti radios do not support 48v power supplies as are sometimes found on hubs and switches. If you connect a Ubiquiti unit to such a switch or hub, the unit will not survive and damage caused is not covered by warranty.

Your radio unit should now be running and the LED with the power symbol should be lit. There may be additional LEDS lit but for the moment you can ignore them. If you have no power LED lit, check that you have everything wired as per the diagram and the power is on.



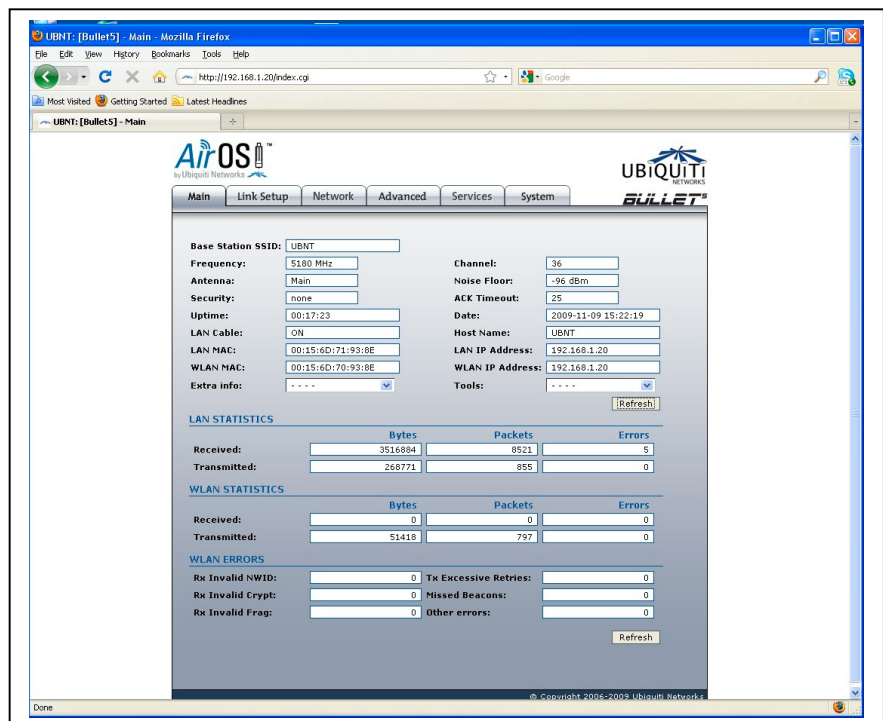
Start up your preferred browser and type into the address bar 192.168.1.20 and press enter. (You may find that http:// is inserted for you by the browser, but it is not necessary to connect to the

radio unit.

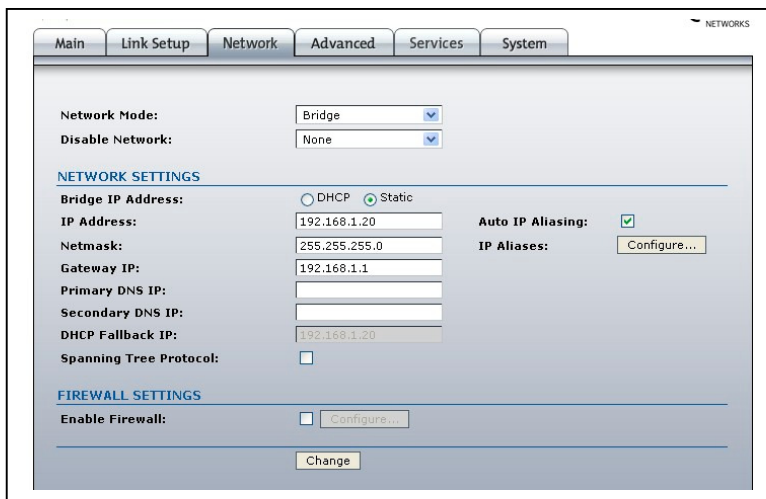
Your web browser should return a screen asking for a username and password, which by default are **ubnt** for both – this is written on the box the unit came in for reference. The exact screen that is presented depends on how the browser has been set up by the user but in all cases the username and password are what needs to be entered.



You should now see a screen like this, and you are logged into the Ubiquiti unit and on the Main page. Bear in mind that the screens you see from here onwards will be like this one, with five tabs across the top, but the exact appearance and the boxes and legends will vary a little according to which Ubiquiti unit you have connected. The pictures you see here are for 5.8 GHz units.



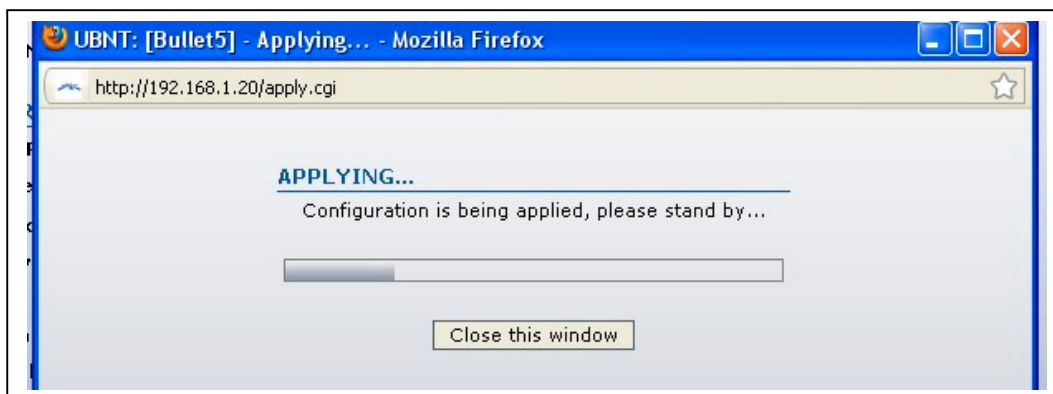
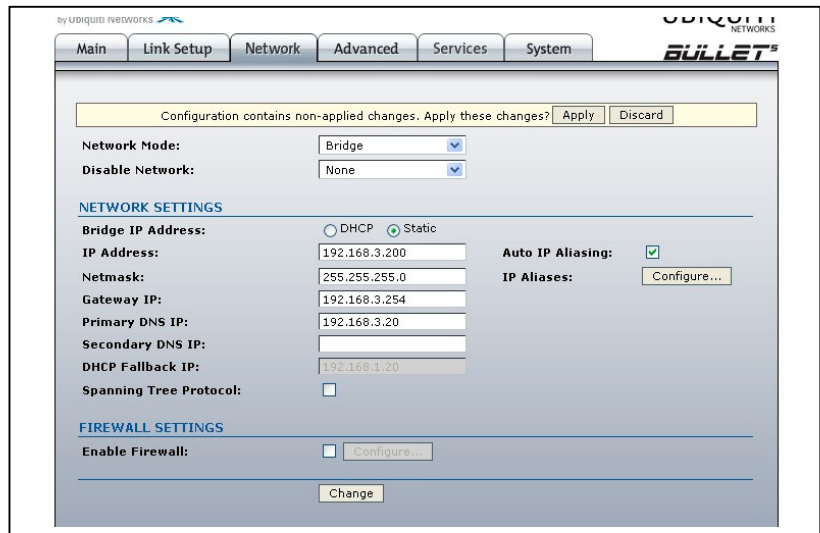
The first step is to set the unit up with an IP address that suits the network. Our example has the network address range 192.148.3.nnn, so we need to change the *network* settings of the unit. Click the **Network** tab to get a screen like this



and make sure there is a blob in **Static** in the row *Bridge IP address*. Now overtype the IP Address with the number you want. (For the moment, 200 is a good candidate as the final number in the IP address, but you will have checked already that this number will be free and available on the network)

Here are the changes. If you don't have Primary DNS IP use the same number as the IP address. If you don't have a Gateway IP number to hand use 254 as the last three digits for the moment.

Click **Change** and you will get a confirmatory message at the top of the screen – **Apply** the changes. Remember that this unit is about to disappear entirely, as the PC will no longer be able to talk to it because it's on a different IP address range.



Once this screen has completed the unit cannot be seen from the PC you are using. If you are setting up other units for the network, now would be a good time to connect them and change their IP addresses, always setting them so that the number they have is unique but within the address range of the network you wish to use them on. If we were setting up a pair of units as a bridge, for our example, we might use addresses 200 and 201.

When you have set the IP addresses for all your Ubiquiti units so that they are on the IP address range for the network, you need to return the PC you're using to the IP address

range for the network. Follow the steps in section 3 above using the original IP address you wrote down for the PC.

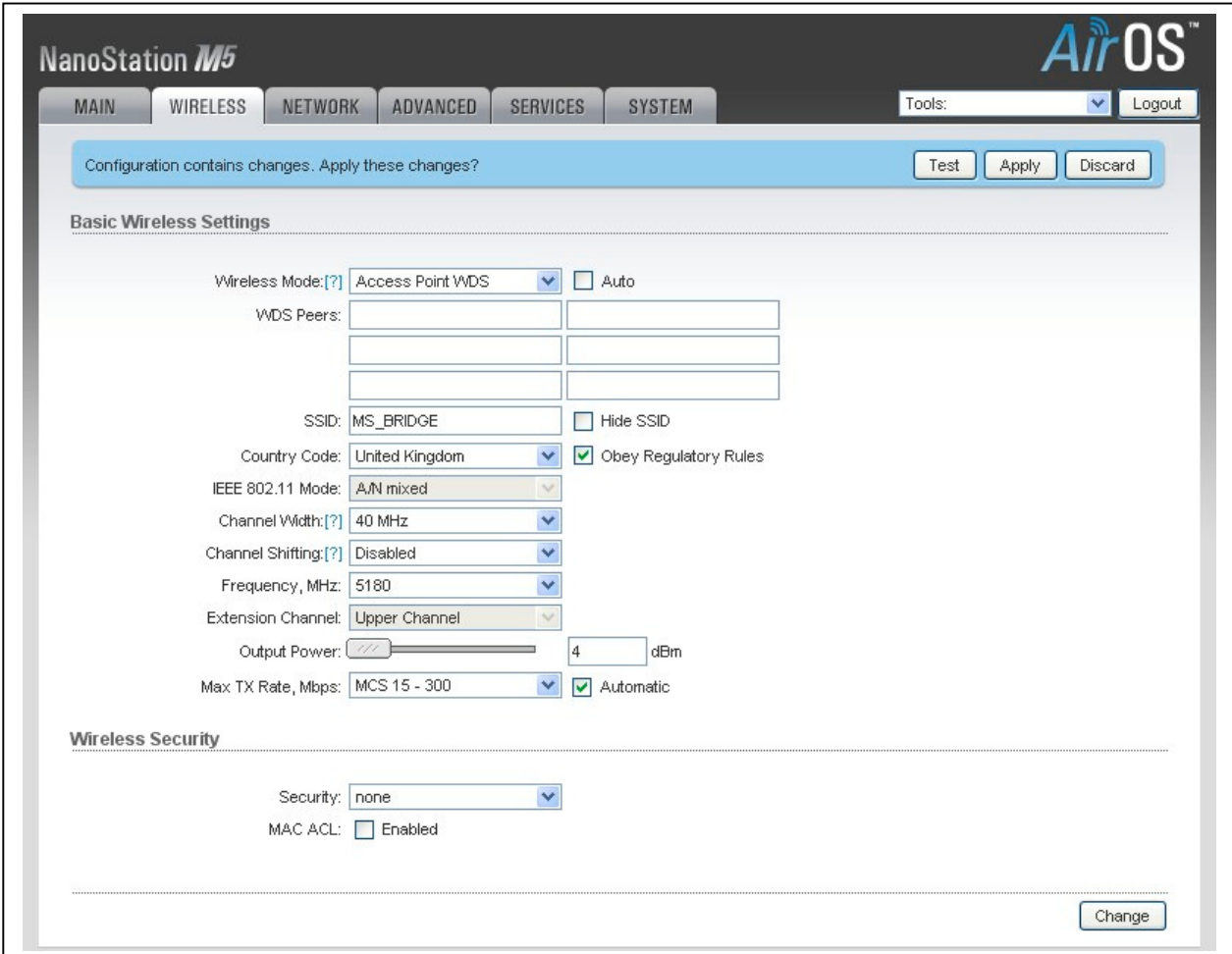
You now have your PC back on the network, and the Ubiquiti units can be seen on the network too.

Setting up the wireless units to talk to one another

Do this from one place, on a bench, before taking units out to install them in remote locations. This will ensure that they are all talking to each other before you go climbing on roofs.

1) As a Bridge

Connect both Ubiquiti units to the network. We will stick with our example IP addresses in which the units have been set up as 192.168.2.200 and 192.168.3.201. Web browse into 200 first. We will set this as one end of the bridge. Click the **Wireless** tab



The screenshot shows the NanoStation M5 AirOS configuration interface. The 'WIRELESS' tab is selected. A notification bar at the top indicates 'Configuration contains changes. Apply these changes?' with buttons for 'Test', 'Apply', and 'Discard'. The 'Basic Wireless Settings' section includes:

- Wireless Mode: [?] Access Point WDS (selected) Auto
- WDS Peers: [] [] [] []
- SSID: MS_BRIDGE Hide SSID
- Country Code: United Kingdom Obey Regulatory Rules
- IEEE 802.11 Mode: A/N mixed
- Channel Width: [?] 40 MHz
- Channel Shifting: [?] Disabled
- Frequency, MHz: 5180
- Extension Channel: Upper Channel
- Output Power: [] [] [] [] 4 dBm
- Max TX Rate, Mbps: MCS 15 - 300 Automatic

The 'Wireless Security' section includes:

- Security: none
- MAC ACL: Enabled

A 'Change' button is located at the bottom right of the configuration area.

This screen is setting up a Nanostation Airmax M5. Some of the graphics are a little snazzier, but the functions are the same. There are three settings that have to change.

- Set the **Wireless Mode** as **Access Point WDS**. (This is counter-intuitive – we’d expect ‘Bridge’ as an option, but Ubiquiti use Access Point WDS so we must go with that.)

- Decide on a *Service Set Identifier (SSID)*. This sounds complicated but just means a name for the link. We're using MS_BRIDGE for this example. Type in your preferred name – no spaces before, no spaces after and no spaces anywhere else either.
- Select the **Country Code** and if you want to stay within the legal limits as you should, put a tick in **Obey Regulatory Regime** too.
- Click the Change Button, then remember to Apply the changes.

Now web browse into the unit that will be used as the other end of the bridge. Set the wireless mode as **Station WDS**, the SSID *exactly* the same as the name you used for the other end (check for no spaces before and after), and the Country Code and regulatory Regime. Click the Change button followed by Apply.

You should now have a working bridge. If you want to be 100% certain that all is well, connect the second unit (201) directly into a laptop (on the same IP range of course), and check in a way you prefer: you can start the command window and ping 192.168.1.200 and you should get a reply, or if you're using Superscan just scan the network and you'll see 200 in the list – and every other PC on the network too. Or just open My Computer and look for the other PCs on the network.

The LED lights on the unit are helpful: the first shows that power is on, the second shows activity on the wired network and the last four show signal strength of the wireless link. You are looking for four greens, with no ambers or reds.

Remember: Set up as a bridge the Ubiquiti Units can see only the other end of that particular bridge, and will not talk to any other radio unit at all.

2) As an Access Point with Satellite stations

Follow the same procedure as for a bridge above, but set the central unit as an **Access Point** and each client that wants to talk to the Access Point as a **Station**. All of the units must have the same SSID and country settings. Note that these are NOT Access Point WDS and Station WDS!

You can check in the same way as above that each station can talk to the Access Point.

Quick Tips

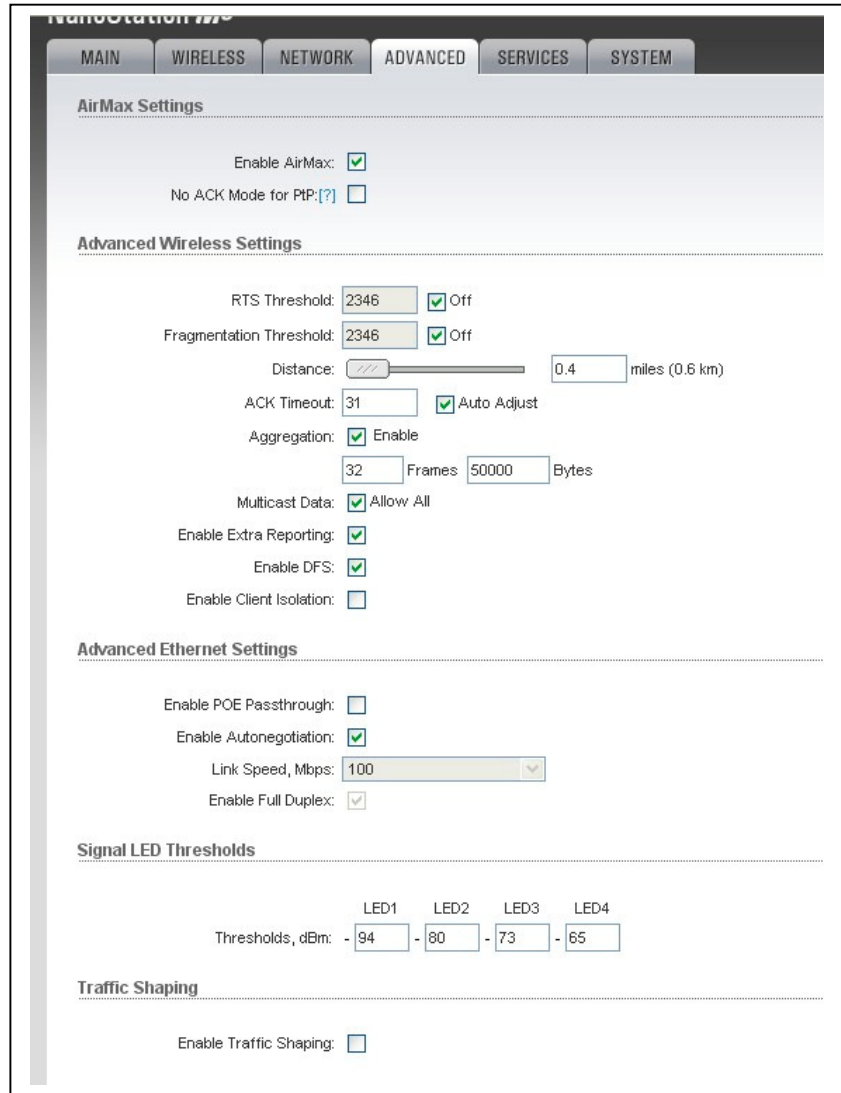
For security a range of encryption is available and you can also specify the MAC address of the unit at the other end if you wish to make doubly sure that one unit will only pass traffic to that MAC address and no other. If you want to encrypt your data, we recommend WPA2-AES. Get the units installed and talking to each other *before* you set encryption on or apply a MAC address.

The screenshot shows the 'Wireless Security' configuration page. The settings are as follows:

- Security: WPA2-AES (dropdown menu)
- WPA Authentication: PSK (dropdown menu)
- WPA Preshared Key: [masked] (text input field)
- MAC ACL: Enabled (checkbox)
- Policy: Allow (dropdown menu)
- Below the Policy dropdown, there is an empty text input field and an 'Add' button.
- Below that, there is a scrollable list area with an empty entry and a 'Rem' button.

For short links (under 300 metres) click the Advanced tab and move the **Distance** slider fully to the left and save the change. This will speed up short distance performance. For longer distance links, over 300 metres, set this distance at 25% above the distance to the unit furthest away.

There are many, many settings available to optimise the performance of Ubiquiti units as a glance through the software setup screens reveals. This document is intended to get you up and running speedily. Far more detailed information is kept up-to-date at the Ubiquiti Wiki site link below. The AirOS v5 User Guide is a document you should be acquainted with, if not in detail at least to know roughly what's in it. Especially useful when



setting up links is to be aware of the utilities available to help align the antenna, survey for other radio units in the area, ping other radios directly, conduct speed tests and understand how to use the mini-spectrum analyser built into AirosV, as well as direct links to every Ubiquiti device currently available. You can find the document at http://www.ubnt.com/wiki/Main_Page

Please note that our Trade Partners and Resellers would be expected to have consulted this document, and the Ubiquiti Forum, before seeking Technical Support from us.

The final page below shows what a good working link looks like using a Nanostation M5 running as one end of a link. It is easy to miss the blue links in the Monitor section which offer further very useful screens.



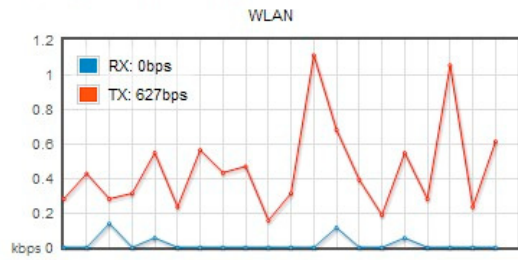
Status

| | |
|---------------------------------------|---|
| Device Name: UBNT | AP MAC: 00:15:6D:8E:4E:4A |
| Network Mode: Bridge | Connections: 1 |
| Wireless Mode: Access Point WDS | Noise Floor: -94 dBm |
| SSID: MS_BRIDGE | Transmit CCQ: 60 % |
| Security: none | AirMax: Enabled |
| Version: v5.2.1 | AirMax Quality:  86 % |
| Uptime: 02:19:03 | AirMax Capacity:  62 % |
| Date: 2010-09-13 20:22:01 | |
| Channel/Frequency: 36 / 5180 MHz | |
| Channel Width: 40 MHz (Upper) | |
| ACK/Distance: 30 / 0.3 miles (0.5 km) | |
| TX/RX Chains: 2X2 | |
| WLAN MAC: 00:15:6D:8E:4E:4A | |
| LAN MAC: 00:15:6D:8F:4E:4A | |
| LAN1/LAN2: Plugged / Unplugged | |

Refresh

Monitor

[Throughput](#) | [Stations](#) | [ARP Table](#) | [Bridge Table](#) | [Routes](#) | [Log](#)



Refresh