MeshAxis Wireless Router Documentation

Operational / User Manual

FCC ID: RC4-MESHAXIS

Note: This unit has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna. —Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help.

Commensurate with EIRP limits specified in FCC Rules 15.247b, this device may not be used with antennas that exceed 36dB of gain in point-to-mulit-point applications.

Radiation Exposure Statement
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

Caution
Changes or modifications not expressly approved by Netunwired LLC could cause harmful interference and void the user's authority to operate the equipment.

MeshAxis - MeshAP Documentation
Quick Setup Guide
MeshAxis MeshAP
1. Register at Netunwired.org to receive an encryption key and management of nodes.
2. Email Netunwired login name to nodes@MeshAxis.com.
3. Node will be transferred to your account.
4. Nodes are set up for Infrastructure mode with the ESSID of MeshAxis and DHCP client on the Ethernet interface.
If your DHCP server does not hand out an address due to an incompatibility, use the following instructions to set a static IP on the box.
Connect wirelessly and obtain an address. From there, using SSH, log into the unit using the gateway address on the laptop you are using. The login username is root and the password terra7. From there, enter the following commands:
vi /etc/STATIC <ENTER>
Then edit the file as follows:
Hit <INS> key and enter
192.x.x.x 255.x.x.x
192.x.x.1
Where the ip address you want on the unit is the first 192.x.x.x, the subnet is the 255.x.x.x and the gateway is 192.x.x.1. Change those values to whatever makes sense for your network.
Then hit <ESC> and then :wq <ENTER>.
Type reboot <ENTER> and start a ping to see if the box is communicating via the Ethernet port.

MeshAxis - MeshAP Documentation
General Use
Once you receive your MeshAP, plug the unit into a DHCP enabled connection and use an SSH program such as Putty to log into the box.
Default username: root
Default password: terra7
Once into the box execute the command Netunwiredregister and enter the email address that is registered with www.Netunwired.org. This will allow easy configuration and advanced monitoring. While continued use of Netunwired.org is not required, the tools that are given there are extremely handy.
Using Netunwired
Register nodes
For manual registration follow this link and enter the hardware key of the machine.
Alternatively run Netunwiredregister at the command line of the node.
XX registered
Click here to see the list of nodes and check in status
Realm manager
Use the realm manager to setup and maintain users on the network

MeshAxis - MeshAP Documentation
Node details
Hardware Key: d47c8c1c20ed397c076d7b63257a6649
This 32 character value identifies your node uniquely. To find the hardware key of a mesh node that you are logged into type the command hardwarekey at the command prompt Version: 0 - Build: 24
Major releases of the MeshAP software are counted in "builds". This value reports the current build installed on this node

Netunwired certified IP: 1.214.163.220
Each node has a wireless IP number. These start off as random 10.x.x.x numbers. Once registered NETUNWIRED assigns fixed 1.x.x numbers
Node certificate live or **Node certificate ready - hit Make Changes**
Each node has a digital certificate. Once they are live they are used to drive the encryption and authentication checks between nodes.
Node configuration
Set the primary wireless communication parameters in this section
Node name:
Netunwired reports will show this node name, which can be easier to remember than the hardwarekey or IP number
ESSID:
Set the ESSID of the wireless network here.
Captive portal:
The captive portal controls access to services by clients using the network. Turning it off lets users go straight in to the network without first reaching a login page.
The *Old System* setting is a compatibility function for legacy installations. Not needed in normal circumstances.

Portal mode:
Fine tune the captive portal settings. Both lets guests in freely, and is useful for early stages,
. Both Auth and Open - Allow logins by recognized users *and* guests
. Auth Only - stops guest access.
. Guest Access open - Everyone's a guest?
. No Access - Node is closed - e.g. use this for maintenance periods
Portal timeout (hours):
Set the time that each login session lasts for.
Portal style: There are a variety of kinds of portal that you can set here:
. NETUNWIRED based
. nocatsplash
. ticketed
. remote
Ticket timeout:
When using single use tickets, set the time they give on the network here in minutes
GUI:
Turn the internal graphical user interface on the MeshAP on or off here. Turning this off preserves system resources.

PCMCIA support:
Use this option for installation with a PCMCIA wireless card; turn it off to save loading unnecessary drivers
Atmel support:
Use this option for to load the Atmel USB drivers, turn it off to save unnecessary loading faster boot up:
This option skips some checks during booting, saving about 10 seconds
First interface Wireless mode:
Set the mode between adhoc and infrastructure. Beware that a node on one mode can't talk to a node on the other mode, so change with care, and work from the outer reaches of the network back to the centre when making changes.
First interface Wireless Channel:
Set the channel carefully and ensure that there are other machines within range

that can communicate on this channel too.
WEP:
Infrastructure mode can support WEP, but ad-hoc mode does not. This is currently supported on Prism adapters only.
WEP key:
The WEP key must be shared with other clients using this cell
Second interface Wireless mode:
Secondary interface settings apply to twin radio nodes. Beware that a node on one mode can't talk to a node on the other node, so change with care, and work from the outer reaches of the network back to the centre.
Secondary ESSID:
Set the ESSID of the second wireless network here.
Second interface Wireless Channel:
5

Set the channel carefully and ensure that there are other machines within range that can communicate on this channel too.
WEP:
Infrastructure mode can support WEP, but ad-hoc mode does not. Currently supported on Prism adapters only
WEP key:
The WEP key must be shared with other clients using this cell
Extra features
Additional functions are set here.
Hybrid protocol:
Set to YES allows the take up of additional protocols as they become available.
Band extension:
Recommended set to NO. On some networks setting YES will allow seamless roaming between nodes.
Bandwidth revenue:
Will enable future features for brokering traffic between other nodes.
CCTV USB web cam:
Check this to YES if you want to use a web cam. Find the web cam images at http://1.Netunwired.ip.number:10192/singleframe.html (replace *1.Netunwired.ip.number* with YOUR node's actual Netunwired Certified IP address)
Max wired clients:
Limit the number of local clients that can connect via the Ethernet interface
Max wireless clients:
Limit the number of local clients that can connect via the wireless network interface
6

Mesh nodes to use:
Limit the number of other mesh nodes that this node will talk to within one hop.
DHCP services:
Defaults to YES. Set to "NO" to stop offering DHCP services. Use this setting on a machine that is only working as a repeater.
DHCP NAK wrong nets:
Use NO on ad hoc networks that are overlapping their wireless DHCP services and giving confused DHCP leases. Otherwise leave as YES
DNS services:
Defaults to YES. Set to NO to stop offering DNS services over the network. Normally matched with the DHCP service
IPSEC:
This option turns the IP Security between nodes on and off.
Always mesh IPSEC:

Setting this to YES stops the mesh talking to un-certificated nodes; this can make it hard to get new nodes on the network, but makes the security tighter.

Radius only local:
Defaults to YES. When YES the local radius realm is used as set below.

Radius local prefix:
This value is set by the system and should not be changed in normal circumstances.

Lock to realm prefix:
Select a local realm, as defined in the realm manager that this node will use for authentication

Minimum cell signal:
7

To avoid poor quality links through marginal connections, set this value above zero. The exact value to use will depend upon your network characteristics. Observe signal strengths on the Mesh Monitor (on drop down menu in GUI).

Mesh watchdog:
The mesh watchdog is only suitable for use in well saturated networks, where the node should expect to see a lot of neighbors. If no other mesh nodes can be seen the watchdog assumes that connectivity is lost, and goes into a network search, to try to re-establish a connection as a client, so that it can download its settings and get back on the mesh.

Internal watchdog:
Set to YES this watchdog will reboot the machine if processes lock-up.

Wireless sensitivity:
Adjusts the sensitivity value for receiving on supported network cards.

Wormhole capable:
Wormholes are VPNs that link meshes together over the internet. See Wormhole Hubs.

Wormhole hub address:
Enter the Netunwired IP or private LAN address of the hub here

Wormhole key:
Each node needs to enter the shared key here

Wormhole type:
Internet wormholes use the Netunwired IP, LAN wormholes go over a private network. P2P not supported yet.

Wormhole transport:
Use UDP unless your network blocks it, in which case use TCP

Traffic Shaping
Shaping values set here define the parameters for managing bandwidth at the node.
8

Mesh traffic is the data passed through this node from carried on behalf of other nodes in the mesh. Routing traffic is the data sent between nodes to establish routes.

enable shaping:
Turn Shaping on or off

optimize traffic:
Optimization should improve performance

eth bandwidth:
Define the speed of the Ethernet network

wlan0 bandwidth:
Define the speed of the wireless network

mesh down: mesh up: mesh down burst: mesh up burst:
Mesh upload and download rates are set here, they can be exceeded up to the value of the burst limit if there is spare capacity available on the network.

routing down: routing up: routing down burst: routing up burst:

Routing bandwidth settings are important to ensure that the network can remain intact.

Client Shaping

Client shaping defines the rules that are used to deliver bandwidth to users of the mesh. Users can have one of four classes, Owner, Public, Member, and Unknown. These values relate to the class defined in their Realm user settings.

Client shaping rules are applied on a per user basis.

Each class of user has rules for their bandwidth rights, defined separately for upload and download. In addition to their regular bandwidth they can also use a limited number of

"burst" events, where they request data at a higher rate for a short period. This improves interactive response without giving away too much bandwidth on an ongoing basis. Burst settings allow greater bandwidth use if spare capacity is available.

unknown down:
unknown up:
unknown down burst:
unknown up burst:
public down:
public up:
public down burst:
public up burst:
member down:
member up:
member down burst:
member up burst:
owner down:
owner up:
owner down burst:
owner up burst:

Firewalling

Firewall settings are applied in relation to user class. By default higher classes of users don't get blocked.

Apply block to Owner users:
Apply block to Member users:
Apply block to Public users:
Allow FTP port 21:
Allow SSH port 22:

Allow TELNET port 23:
Allow SMTP port 25:
Allow HTTP port 80:
Allow POP3 port 110:
Allow RPC port 111:
Allow HTTPS port 443:
Total block on incoming wired:

This locks down a wired LAN that is connected via the mesh, to make a high security fire walled connection.

Root password:

Set the root password here.

Privacy cipher:

You can use this value to secure the data on your mesh.

Mesh Port mappings:

These options will allow port mappings - *not yet implemented*

Bluetooth

These features apply to the Bluetooth meshing functions, which are available as a separate commercial module.

Bluetooth:
Enables the Bluetooth functions
Bluetooth data:
offer mesh as modem:
GPRS backhaul:
Provides internet connectivity using a GPRS equipped phone
GSM backhaul:

Provides internet connectivity using a GSM modem
Bluetooth Options:
Bluetooth fileserver:
Bluetooth audio:
Bluetooth mp3/ogg stream:
Bluetooth phone emulation:
PSTN phone handoff:
Bluetooth web cam:
Bluetooth admin:
admin auto notify:
root presence lock:
Admin MAC:
Bluetooth Cell ID:
Bluetooth meshing:
Bluetooth SMS emulation:
GSM SMS handoff:
Dialup settings
Use these settings to configure a dial-up internet connection on the MeshAP. These can be used for demonstrations or backups, but are unlikely to be the primary internet connection for the mesh. Email mailto:support@locustworld.com for more information on these settings if you need them.
Dialup back haul: Dial on demand:
Dialup type:
. Analogue
. ISDN
. ATM
. Cable
Dialup port:

. Serial port 1
. Serial port 2
. Internal card
Phone number:
ISP username:
ISP password:
Auth type:
. CHAP
. PAP
. Login
. None
Core settings
These settings define the hardware configuration of the node
Flash type:
Enter the memory capacity of the boot device used in the node. For hard disc use

"Other".
These settings should not normally need to be changed.

Preserve settings:
When set to YES the machine's custom settings will be maintained during a software upgrade. When set to NO the machine will come up on standard settings after a software upgrade, and it will need to check in to download them again and re-certify.
VGA mode:
Defines the resolution of the GUI
. 800x600x16
. 1024x768x8
. 1024x768x16
. 640x480x24
. 640x480x16
Soft Booting:
. Suitable for the ISO CD image
External radius:
Enter the IP number of the remote radius server
static eth addr:
If the node is on a LAN without DHCP set the IP number that it should have here. Should match settings in */etc/static*
static eth net mask:
If the node is on a LAN without DHCP set the net mask that it should have here
static eth gateway:

If the node is on a LAN without DHCP set the IP number of the gateway machine here
static eth DNS:
If the node is on a LAN without DHCP set the IP number of the DNS server here
Cell ID 1:
Each node maintains two cells. The first cell is used for the DHCP services on WLAN0 and the inter-node VPN cell number in IP gateway tunnel mode.
Cell ID 2:
This second cell id is used for twin radio installations
Gateway tunnel:
. PPP
. IP
PPP tunneling gives more capacity for VPNs than IP tunnels, which are more suited for smaller meshes.
Hostmapping
Host mapping allows you to map a public internet address (or LAN address) from your gateway point to a remote wireless or wired device connected to a remote MeshAP anywhere on the mesh.
Setting up host mapping is intended as something done as an installation. That is to say that the configuration doesn't change that frequently. Hostmapping is intended for advanced users.
What you need to know:
1) Remote server's LAN side IP address. It is recommended to set it to a static IP in the top end of the range 192.168.X.220-240 in the range of the DHCP that the MeshAP it is connected to is giving out.
2) The first cell ID of the node it is connected to

3) The public / LAN address you want to map.
Check list:
Hostmapping is only supported in tobuild25dev42 onwards.
Remote node gateway type is IP and not PPP
Cell IP does not conflict with any others (Netunwired will warn you) Local wired side of the remote MeshAP does not conflict with elsewhere on the
mesh. It can be changed to a specific range, changing the "X" quoted above.
Ranges should be 1-120 for that part of the subnet. - this only applies if the remote device is connected via the remote MeshAP Ethernet or if an AP is connected to that Ethernet that the remote device is then connected to wirelessly.
note: You can technically have overlapping wired cells but this could cause confusion later. You can also overlap them with the LAN range of the network that the gateway is attached, but this makes the remapped IP's unreachable from the gateway as it thinks they are remote IP's on the mesh. In short - not recommended but possible in large networks if you get short of cell ranges.
Check that the IP you are redirecting is in the same subnet as the gateway, it is possible to map addresses not in that range, but this requires a special net mask setting not covered here.

In the Hostmapping specification, enter a line which reads as follows.
12.34.56.78 210 192.168.5.220
These are:
Public IP - Cell ID - Remote address.
Update the node and it should then start remapping. You must make sure the remote device is authenticated or traffic cannot flow - use of an automac is recommended for this and of course the automac can represent a user and a traffic class, so you can traffic shape remote servers if required.

Protocol support:
Not all protocols are supported yet; web email etc and any TCP/UDP based service should run fine. For windows file sharing, it's possible to enter the IP address URL, into windows and it will connect directly to the file share. This should work outbound from any mesh client already, even without host mapping.
With a host mapped host you can access it's file share simply by typing its IP into the address bar of windows explorer preceded by \
e.g.: \10.0.0.1
Note that host map is a 1:1 IP mapping between the hosts, so Host mapping opens up security implications for the remotely attached device.
The host map also only runs when the remote node has internet gateway connectivity, if this link breaks the connectivity to the host mapped device will also be broken until the link is re-established.

Splash page customization

HTML insert:
Allows the captive portal page to be customized. The HTML is added at the top of the page.

Make Changes:
Click here to schedule an update. Once clicked, the next time the node check in it will download these settings and apply them. A message will appear in red at the bottom of the reloaded page to indicate you have a scheduled operation.

Ticketing

To utilize one time ticketed passwords, follow the procedure below:

Create a new realm on your Netunwired account called TICKETED
Edit this realm and use the "Create Tickets" button to produce tickets as required for the various login classes.
Click "Email all passwords" button to receive a copy of all the passwords for the realm via email.
On the nodes concerned, manage their settings and ensure that the following options are in place:
. Captive Portal = capture ON
. Portal Mode = Auth Only
. Portal Style = Netunwired based
. Ticket Timeout = time you want each ticket to last in minutes
. Radius only Local = YES
. Lock to realm prefix = Ticketed
Click update for the node and after next check-in it should allow access once for each ticket. Tickets are removed live from Netunwired, so it is easy to track progress and to receive an updated mailing of remaining tickets.

Client Connections

Win XP

Win2K

Select the wireless configuration control panel or system tray icon and set your wireless device for either the ESSID of the network or ESSID of Any or default or blank depending on your device. Scan for the network and your connection should automatically get an IP address.

Win9x

Linux

Set your wireless device to the correct settings, usually managed mode with either a blank ESSID or the ESSID of the mesh network you wish to connect to. The iwconfig command should show the status of your wireless device and whether it has associated. Then use DHCP client software to obtain IP address settings.

Mac OS X

Show airport status in menu bar (from Networks System Preferences). Click on the airport icon on the menu bar. You should see the ESSID of the WiFi network you wish to connect to (the default is *MeshAxis*). Select it - this will connect you to the mesh network.

Mac OS 9

All

To access anything on a default network, you will first need to open a web browser. Going to any page will take you to the Redirect splash page. There is a login field, if you have set up user accounts, or a guest button. Clicking on one of these will open your access. Configuration of the authentication settings are done under NetunwiredSettings.

Setting up VPN end users

While the mesh is encrypted end-to-end, wireless end-user clients connect over an unencrypted connection to their local cell.
To provide a secure and robust authentication a VPN protocol is used. At this time, the MeshAP software supports PPTP VPNs, which are typical of Microsoft Windows computers and implementations exist for many other platforms as well.
VPN users work within a realm, using the realm manager you must first have created your realm and user within that realm. Select VPN as the type for the user. Note that VPN logins can only be used with VPN connections.
Make sure your local node is set to "Radius only Local" and Lock to realm of the realm you wish to utilize on the local cell.
On the client end, the settings required are:

MS-CHAP v2 authentication Require encrypted connection - disconnect if none Server host name / address is: vpnhost. Compression off
Note the full stop / period mark at the end of vpnhost - this is important for it to work on all platforms.
The username and password are those from the username/password of the realm user.
This has been successfully tested with Windows 2000 and Windows XP; reports are welcomed from other platforms.
Mac OS X
Connect using *Internet Connect*. Under *File* you will see the option *New VPN Connection Window*. Under *Server Host* put in "vpnhost." Under username and password put in the username and password created under your realm for VPN clients. Click connect.

Wormhole Hubs
Wormholes link networks of nodes together through other network links. Typically non wireless but delivered over IP. Such as the Internet, a local LAN or a point to point connection such as an eps9 circuit.
This facility allows you to join together geographically distributed meshes into a single unified network.
With Internet connections, some MeshAP may be behind NAT and so cannot accept incoming connections. Typically a "wormhole hub" is used to link NAT'ed connections like this together.
Designate one machine which has full IP connectivity as the hub. Set the Netunwired "Wormhole key" to a secure password which your hub connected machines will share. Select the appropriate Wormhole type, e.g. "Internet"
Update the settings on the wormhole hub machine. Nothing is entered in the "hub address" field for the hub machine.
On all the other machines which you wish to connect in to the hub, manage their Netunwired settings and enter the same key and wormhole type. On these "wormhole client" machines, set the wormhole hub address as the literal Netunwired IP address of the hub node. eg, 1.96.23.121
Update the settings and you should find that in time, you can simply ping one network from another. Interconnections between the networks will expand the routing tables, but connecting to a host will open the route up.
The wormholes use blowfish encryption and compression on every packet. Intramesh communications over the worm hole also use individually negotiated host encryption ensuring privacy even over shared managed mesh links.
If your node which is connecting in to a hub cannot support UDP via a NAT proxy or firewall, then switch the mode to TCP. Likewise if your hub is behind a firewall, then you need to port redirect port 51010 with both UDP and TCP if possible. If you can't redirect UDP then all the nodes connecting in to the hub should be set to TCP mode.

Wormhole hubs can currently only be used in infrastructure mode. This may change in the future.
Technical Specifications
Wireless
IEEE 802.11b
Frequency Band 2.412 – 2.462 GHz
Modulation DSSS (CCK, DQPSK, DPPSK
TX power 100mW
Media Access Protocol CSMA/CA with ACK
RX Sensitivity -94 dBm (1 Mbps)
Data rates supported 11.5.5,2,1 Mbps
128/40 bit WEB

Impedance: 50 ohms
Antenna connection RS-SMA
Networking
DHCP server
DHCP relay
TCP and VPN session persistent roaming without client software
Full VPN Compatibility
Full 802.11b Client compatibility
Management
SNMP V2
HTTPS to on board management tools
Secure local and remote management tools via HTTPS
Web-based management tool
Configuration save and restore via NETUNWIRED.ORG
Security
Full VPN compatibility
VPN filtering – rejects non-VPN traffic
Mac address access control lists
HTTPS to on board management tools
AES encryption of wireless control protocol
NAT support with port forwarding
128/40 bit WEP
HTTPS element management security

Mesh node digital certification
2048 bit encryption for inter node communications
Environmental Specifications
Operating temperature 0° C to 50° C
Humidity 95% non-condensing
Approvals:
FCC CFR47 Part 15, Class A
UL/cUL Listed
UL 60950
Plenum rated
CAN/CSA -C22 No 60950
Package Contents
MeshAxis
Power adaptor
Hardware installation guide
Quick start guide
Antennae sold separately
Hardware Specifications
Auto sending 10/100BaseT Ethernet
Auto sending Bluetooth
2 USB
Power Input options
External wall plug-in AC power supply 120-140 AC
Power over Ethernet 802.3af
Dimensions:

Table of Contents

Linux programmer Software build 25

The following are email replies that Linux programmer has made regarding build 25. between

August 2003 and December 1, 2003

Ad-hoc and infrastructure Modes

You can mesh between infrastructure and ad-hoc mode with orinoco based hardware for the ad-hoc side. This is due to features of the orinoco firmware which appear to allow several addressing modes to operate at once.

Mixing ad-hoc with infrastructure on other chipsets is unlikely to work. Typically the ad-hoc network cannot hear the infrastructure network.

Software Module Manager

If you are running build25 - the latest is tobuild25dev68 then go to manage that node and select the software module manager, then enable the apache+php module and the mysql module if you want that as well.

Click update.

Leave the meshbox for 6 hours, you should then find that it installs apache and mysql on the box. You willl probably want to create a symbolic link from the documents directory to the /drv2 partition that will be automatically created by the meshap for any space beyond 32mb on the CF. You may well want to copy the entire /htdocs over to drv2 and create a symbolic link to that.

Security

The mesh encryption is much much stronger than WEP and with the PPTP signon you've got a very secure setup. You can use WEP as well if you like.

Firmware on Radio Cards

You do not need to change the firmware on any PCI card with the MeshAP.

Upgrade Splash

The username and password work instantly, the automac if used works at the next checkin.

If anyone wants to use the MAC and username and password pair feature, then you'll probably need the splashup upgrade.

getandverify splashup

Preventing External DHCP from getting through Meshbox

If its build25, set the "never gateway" option as "box function" on the Netunwired management page for the node. This stops it getting a dhcp lease of the wire it is connected to.

Were you using static IP when you set it up at your house? If so you need to remove the static ip options before deploying it wirelessly.

Wired Repeaters

The wired repeater is just using the same range as your gateway network.

You can change the address range for the wired side on the Netunwired management pages if you like. You'd probably also want to enable "wired captive portal" feature so that wired clients on the wireless repeater are also asked to authenticate before access is given.

Atmel Drivers Infrastructure Mode

From the front page of the first site:
* no promiscous, monitor or station mode and no
support for libpcap, i.e.
it does not work with Kismet or Airsnort and it cannot act
as an WLAN access
point. This is a restriction imposed by the current
firmware.
From the second site:
* ad-hoc mode
* infrastructure mode (ie. connect to an access point)
* scan mode for both ad-hoc and infrastructure
* WEP

What you need is the infrastructure master or AP mode
listed. Neither of these drivers does it as it needs a
firmware from atmel that they use in their access points
and as I said they wanted $40k for it last time someone
asked.

Iptable Routing

to avoid syntactical problems.

USB Network Cards

Atmel or Prism2, but the performance isn't ideal.

Using Access Point to link to the Mesh

Erm.. best not to have them as the same essid and channel.
Ideal configuration is the ap in the back of the Meshbox
repeater's Ethernet port then it asks as another local
channel.

Syntax on Mac Addresses

The syntax for mac addresses is NN:NN:NN:NN:NN:NN not
NNNNNNNNNNNN

Channels and mixing ESSID

Just to add in to this mix. In Europe you can use channels
1-13 which gives even more spread or the potential for more
channels to be used at once.

Channel Mixing

Or if you talk to some of the theorists, you can actually
do this..
MeshAP 1 MeshAP2 MeshAP3
1 - 8 8 - 4 8 - 11 etc.

The theory is that channels 1,4,8,and 11 only interfere
with the
adjacent channel by 2% as that is the extreme part of the
lobe.
DSS signals look like this (crudely):
4
..
3 . . 5
.. . . ..
. .. .. .
. . . .6
2
The numbers are channels. This is why most people will
tell you that 1,6,11 are the only true non-interfering

channels. What the theorists are saying it that channel 4 uses almost none of channel 2 and channel 1 uses almost none of channel 3. The most important channels for interferences are the side lobes or channels 3 and 5 in the diagram. Channel 1 would use 0 and 2 primarily, so that leaves little interference on 3 for the next radio.

Infrastructure Mode vs. Ad-Hoc

In ad-hoc mode all clients talk directly, in infrastructure clients talk to an ap (in this case MeshBoxes) ad-hoc mode is cool except that it doesn't have power sensitive roaming, so you can lock on to any node you can hear, not just the nearest.

It also has "helpful" features built in the firmware such as automatically switching channels to one with an ad-hoc network. We used ad-hoc on the mesh until we could get it working in infrastructure mode. You should see a more reliable network with infrastructure mode.

Traffic Shaping

With the Ethernet side of things, you can change your maximum to 100mbit and maybe your Ethernet can support this, but it doesn't make much sense to then shape and load balance only a small segment of that because compared to your wireless side the Ethernet is overpowered and so the additional 90mbit of capacity can't be used anyway.

If you set your owner traffic to be 5mbit and 6mbit burst, what you are doing is telling that node that whatever else is going on, it has to reserve 5mbit of all traffic for the owner class. So it wont transmit any other data whilst keeping that open. That means traffic for any other classes or traffic being repeated from another mesh node.

All the traffic shaping values should generally be left alone. If you want to do something like give the owner class more than 3mbit, then set the burst values only to a higher value, eg 4mbit. Bursting traffic is the maximum that a class can use when the airwaves are free. You can allocate more burst than you actually have (within reasonable limits) and this value acts as a top speed maximum.

Gateway Max per node

This setting is the Gateway max per node that refers not to any forwarding traffic but specifically to Internet gatewaying. So if two nodes are downloading off the network, the max per node indicates the maximum speed each could utilize, preventing one node from hogging the entire uplink.

Typically I've been recommending people set the max per node to half their uplink speed, but it depends on the type of network, number of remote clients you're trying to serve and exactly what type of bandwidth you're looking to deliver.

Optimizing Netunwired

I'm on a laptop, which is connected wirelessly to an AP, which is in the back of a Meshbox 3 hops from the gateway.

I'm able to reach all of the sites mentioned here without any problems.

32

MeshAxis - MeshAP Documentation

Please check the following settings are set the same throughout any misbehaving meshes:
Gateway tunnel = IP
Gateway use DHCP dns = NO
following optimizations enabled:
Gateway max per node = 1024 kbit
Gateway optimization priority = High bandwidth
Gateway compress traffic = Yes

DNS Priorities

MeshAxis - MeshAP Documentation

If the local node tries to resolve the node and at that instant there is a connectivity failure lasting for say 40 seconds. The local dns server would cache the fact that the remote nameserver for that specific domain were unreachable. The result is that subsequent requests would also return a blank result. Negative caching is normally handled pretty well and I wouldn't expect even a failure condition like this to persist for more than 20 minutes.
If negative caching is the problem then you'd see the problem occur possibly for all users for a period of time, but then go away and perhaps occur on another site. If it’s always the same sites then it points to either an incompatible way of handling dns or some other low level IP problem, which needs special handling.

Auto Mac Updates

That is the absolute latest. Automac's are used in production environments on this release without any problems. It does take approx 0-30 minutes before an auto mac change is applied over your network. Perhaps this is frustrating testing?

Automatic Level Control

As Kenny says, the latest dev builds are recommended, dev54 is good and we're testing dev55 at the moment.
The values to use are 100mW or Auto depending on the type of card. Personally I'm running 100mW on all PCI devices with excellent results.
If you're using the 100mW setting then the "automatic level control" feature should be off.

Syntax on Mac Addresses

Last time I had this reported it was due to the mac address supplied not being the same as the card in use. Double check that and ensure you use the syntax 00:00:00:00:00:00 for mac addresses.

34

MeshAxis - MeshAP Documentation

The differences between dev48 and dev54 are roughly:

Slightly later development drivers - supposed minor bug fixes routing fixes when no good route exists, previously it could do some like you have

a-b-c
C goes offline and b notices this, it asks for an alternate route and A says, hey go via me to C, but of course A's route to C goes back via B, which is what causes things to appear in the routing table with long hops, but are not reachable. This logic bug fixed.
Additionally even when routes are in use, every 3 minutes it checks the
Route for alternate and better routes. On top of this some routes never timed out that is also now fixed.
Other stuff to do with shutting down the wireless, which caused approx 1 in 10 MeshBoxes to crash during reboot - the more neighbors they have the more likely it was to happen. I think I've cleared this up now, but let me know if you get any nodes crashing during reboot.
There is also an approx 10% speedup when using the high bandwidth mode, on top of the existing speed up.
RTS used to turn itself off on the previous release of the drivers, this and fragmentation thresholds are now fully working.
If dev48 is aok then that’s cool, but consider dev54 if you have any problems.
The highbandwidth and compression only needs to be set on the gateway, the downstream nodes use the setting that the gateway offers them. Eg the type of connection (low latency/high bandwidth) is controlled by the gateway. Not having this set on non-gateway nodes should have no effect at all.

Client IP Address

Client IP address won’t interfere with various MeshBoxes, they'll give out addresses in different ranges.

You can set the static IP options for your gateway in the Netunwired configuration or by creating a /etc/STATIC file.
Change your "Gateway tunnel type" to IP rather than PPP as an optimization.
The 34 number you're referring to is the measured signal strength; in the version you're using this runs from about 20-50.

Host mapping

How to use hostmapping
Host mapping allows you to map a public internet address (or lan address) from your gateway point to a remote wireless or wired device connected to a remote meshbox anywhere on the mesh.
Setting up host mapping is intended as something done as an installation, that is to say that the configuration doesn't change that frequently. Hostmapping is intended for advanced users.
What you need to know:
1) Remote server's lan side IP address. It is recommended to set it to a static ip in the top end of the range 192.168.X.220-240 in the range of the dhcp that the meshbox it is connected to is giving out.
2) The first cell ID of the node it is connected to

3) The public / lan address you want to map.
Check list:
Hostmapping is only supported in tobuild25dev42 onwards.
Remote node gateway type is IP and not PPP
Cell IP does not conflict with any others (Netunwired will warn you)
Local wired side of the remote meshbox does not conflict with elsewhere on the mesh. It can be changed to a specific range, changing the "X" quoted above. Ranges should be 1-120 for that part of the subnet. - This only applies if the remote device is connected via the remote meshbox

ethernet or if an AP is connected to that ethernet that the remote device is then connected to wirelessly.
Note: You can technically have overlapping wired cells but this could cause confusion later. You can also overlap them with the lan range of the network that the gateway is attached, but this makes the remapped ip's unreachable from the gateway as it thinks they are remote ip's on the mesh. In short - not recommended but possible in large networks if you get short of cell ranges.
Check that the ip you are redirecting is in the same subnet as the gateway, it is possible to map addresses not in that range, but this requires a special netmask setting not covered here.
So for example. Our remote server is 192.168.5.220 set to a static ip on a direct-wired ethernet on a remote meshbox. The first cell id of that Meshbox is 210. The remote Internet address we're mapping to it is 12.34.56.78
Enable port mappings and host mappings (if displayed) in the Netunwired management page.
In the hostmapping specification, enter a line which reads as follows.
12.34.56.78 210 192.168.5.220
With a space between each entry. These are:
Public IP - Cell ID - Remote address.
Update the node and it should then start remapping. You must make sure the remote device is authenticated or traffic cannot flow - use of an automac is recommended for this and of course the automac can represent a user and a traffic class, so you can traffic shape remote servers if required.
Important note:

settings as invalid ones are not handled very well at the moment.
Protocol support:
Not all protocols are supported yet, web email etc and any tcp/udp based service should run aok. I'm not sure what will happen if the remote mapped box is also a nat gateway itself!!
For windows file sharing, its possible to enter the IP address url, into windows and it will connect directly to the fileshare. This should work outbound from any mesh

client already, even without host mapping.
With a hostmapped host you can access it's fileshare simply by typing its ip into the address bar of windows explorer preceded by \\
eg: \\12.34.56.78
Note that hostmap is a 1:1 IP mapping between the hosts, so hostmapping opens up security implications for the remotely attached device.
The hostmap also only runs when the remote node has Internet gateway connectivity, if this link breaks the connectivity to the hostmapped device will also be broken until the link is re-established.
Testing needed on PPTP and IPSEC tunneling as well.

Multiple Gateway Balancing

Gateways are currently already balanced, but you need to set the max gateway per node to be either the speed of your uplink total or less than it. So for example if you have 1mbit Internet connection you could set the gateway max per node at 512kbit. This would mean in theory that each node cannot use more than half of your total upstream.
When combined with compression this amount is variable so they can burst up to the full speed of your connection on easily compressible data and get the 512kbit when they're downloading pre-compressed files.

Performance

Okay well I'm sure we can get to the bottom of the speed issues. Good news that it’s all working.
Check the following settings in Netunwired.
Transmit power set to 20dbm - this is the best value I've found for dev48 build. You can also try the "auto" option as an experiment if you like, but so far I recommend 20dbm over auto.
Mesh any essid set to no - a useful feature but creates a lot of interference if the mesh is near normal access points.
On your gateway you can change the setting from Low Latency to High bandwidth and switch compression on on your gateway. After the gateway reboots and the remote nodes reestablish, see how that performs. Various setups get better performance with different settings. The gateway high bandwidth and compression options only have any effect on the gateway.

Software Modules

Okay disable (uncheck) all the software modules. I'll post to the list about this. They're not ready yet.

Grub Failure

Make Key

> I had a nose around /hj and found a 'makekey' (IIRC). I ran that and my node pickeed up the Netunwired IP 1.x.x.x no problem. (I had done a 'distread' beforehand though). Maybe

Jon can tell us if this is safe or not?
Its not a recommended or safe way of doing it, but it might work in certain situations.
If your node is online with a 10.x address, Netunwired will cause it to re-request its 1.x address. It is best to let this happen automatically; typically it shouldn't take more than a few hours.

Manually calling the splash page

http://vpnhost.:5280/
Note the dot colon after vpnhost.
That will show the splash and shows that meshbox dns is working locally as is the splash server.
Perhaps this is a power related issue. Change the power setting to Auto in Netunwired for that node, however there was a recent wireless driver bugfix, you can try getandverify tobuild25dev48 for the most recent version.
Does your gateway have a direct connection to the internet?
It sounds like a dns related issue. When you can't bring up the splash page, can you get an address of:
http://vpnhost.
Note the trailing .

Flashing larger Compact flashes

Its only available via a getandverify upgrade at the moment
getandverify tobuild25dev45

is the current latest.
Please note this is an experimental development release, whilst being the latest version of the software, may not be suitable for general production use.

RAM

The "low memory" version of the MeshAP is over a year old now. I'd recommend the regular release; just disable GUI in the Netunwired settings. It will run fine> in 64mb, 32mb maybe, I haven't tried that for a while. I can't even buy anything less than 128mb SDRAM these days.

VPN

1st off - take a peek at the wiki documentation (http://www.locustworld.com then click on "Project Tracker / FAQ" in the left panel).
The latest version of Windows XP displays the "insecure connection, no WEP key" message to try to scare people to turn WEP on. Our MeshAP doesn't need this, because if you want privacy you can connect securely through a VPN instead, and all internode communications are certificated and encrypted. Sort of leaves WEP crying in to it's digital pint.
In NETUNWIRED realm manager, a user is set up with a either "Owner", "Member", "Guest"(public) or "Vpn" class. "Vpn" class allows VPN login only, while the others allow login through the splash page only. (I am ignoring AutoMAC here for simplicity.)
For the NETUNWIRED management settings, I defer to Jon's own words:-

---
"With your realm set up, you need to apply the following settings to the meshbox to use your specific logins. Set the options in the management page as follows:
* Captive Portal = capture ON
* Portal Mode = Auth Only
* Portal Style = Netunwired based
* Radius only Local = YES
* Lock to realm prefix = name_of_your_realm

Click "make changes" and wait for the node to check in and load the new settings, after that it will use the realm login details on the fly.

Forcing Gateway Advertisement

It sends the gateway advertisement every 2 minutes at the moment. Issuing:
killall sleep
Will cause it to send immediately. The timing of this was reduced by 25%
(faster) in the most recent builds.

Aggregation

You mean it doesn't have an internal ADSL modem. The article is talking about aggregating multiple remote adsl connections so you have 3 different connections at different sites and the wireless user gets all of that bandwidth combined.

Wired Internet Connection

Any ethernet ADSL router will work fine. There was some support for the USB adsl modem made by alcatel, but it doesn't work on more recent models. The recommended way to interface with ADSL is with an ADSL ethernet router.

Time Zones

Yep, I had to take timezones out of previous builds when I ran out of space, but they are planned to be added back in. As the change is largely cosmetic it hasn't been a top priority. I'd expect to have it in place within a month.

Netunwired Status Icons

These only appear if your node is build25, more data the later the dev build. You can hover the mouse over the icons and click them for more or alternate data screens. It is still experimental at the moment but provides lots of useful data.

Securing the ESSID

Yes, build25 has a "routing key" which is an encryption key used for meshing. Changing this key will make it impossible to mesh unless someone else has the changed key. Support for changing all your node's keys via Netunwired is likely in a few weeks.

PCI Cards

he chipsets on the cards vary even within the same model number. This is a very annoying habit of the hardware manufacturers. All of the listed card models could be prism2, but are not always.

The Meshbox resellers maintain a stock of compatible cards, buying from them should ensure compatibility.

Frottle

I checked out frottle when it was released and it is designed for centrally planned networks, eg a single master with many slaves. It might work in the mesh if it was rewritten as a traffic control module rather than a packet queuing system. I discussed this with the author who said it was a good idea but I don't believe there has been any further development with it.

There is a certain amount of this already in the system, but I could probably optimize performance by adding a specific "mesh aware" traffic control module.

Changing Owners Rights

Yes, and you can also downgrade the bandwidth allocation for the owner class by modifying the burst value for owner up and down.

Forcing External Splash Page

The text probably isn't included anywhere where the javascript could be active.

I guess the best solution would be to add in hidden html into the form to replace the destination redirection url. I could probably add another field like "adverturl" and it would redirect to the advert after the user clicks the guest button.

The other alternative is to allow more data in the splash insert or to manually modify the splash page so that it is your advert and upon clicking the guest button, the user reaches their original url.