How to Use the Mesh Web Interface

Written by David Rivenburg, AD5OO

Table of Contents:

Please take note:

- Javascript and page redirection must be enabled in your browser for the web interface to work.
- Some operations can take several seconds, or even longer, to complete. There is currently no feedback while the node is working on your request. Be patient and wait for the web interface to respond before trying to click other buttons.
- Avoid the use of your browser's back, forward, and reload buttons. Every page has navigation controls to take you where you want to go.
- The various pages of the web interface are intended to be used by only one person at a time. This is especially important on the setup pages where using them from multiple browsers or multiple computers at the same time will almost certainly cause problems. Viewing different pages at the same time should not cause any conflicts.

Status Page

This is the first page you will see when accessing **http://localnode:8080/** or **http://your-node-name:8080/**. The top bar displays the node name and also a tactical name if one has been assigned. For more about tactical names see the Basic Setup section.

Below the name bar there will be a few control buttons. Some of these buttons may not be available depending on the current configuration:

- **Refresh** will update the page with current data.
- **Mesh Status** takes you to a page which shows what Neighbor nodes and Remote nodes are visible as well as what services are being provided through those nodes.
- **OLSR Status** takes you to the web pages that OLSR itself provides which gives you detailed information about the current state of the OLSR routing software.
- **WiFi Scan** provides a list of the WiFi networks that the node can see. It cannot show you which other nodes are visible, that is what the Mesh Status and OLSR Status pages are for. There is an automatic scan mode but it is recommended that it not be used continuously because the mesh performance will suffer due to the node spending much of its time on other channels looking for other networks.

- **Setup** takes you to the setup pages of the web interface. You will need to supply a username and password to access those pages. The username is always "root", and the password is the one you set on the Basic Setup page. If the node has not yet been configured, the password is "hsmm". Note that the password given to log in to the setup pages is encrypted in transit, so this is safe to do over a wireless connection.

- **Night Mode** switches the normal black on white color scheme to red on black. Black on white was chosen because it provides the best screen visibility on a laptop exposed to direct sunlight. Red on black is much better suited for night time use as it helps preserve night vision.

The left column contains the details of the network interfaces used on this node, the default gateway if one is available, and the IP address and name (if known) of the device accessing this page.

The right column contains the signal strength reading and other attributes of your node. The **Signal/Noise/Ratio** is a reading of the WiFi signal strength in dBm, and it is available only when the node is in a Mesh or Client configuration. The **Auto** button will take you to an automatically refreshing display of the current signal strength and an average of the last 20 readings. This is provided as an aid to assist in antenna aiming. It is of no use until another node is visible, so it is best used a a fine-tuning tool. Also, this reading is of little use if your node can directly see more than one other node. In this case you should temporarily change the wireless SSID of the two nodes you are aiming antennas for so that the other visible nodes will be excluded from this reading. Just remember to change the SSID back when you are finished. Note that the use of the **Auto** feature will negatively impact the mesh performance of the node it is running on so it is best used for short periods of time while aiming an antenna. For the best results it should be accessed from the LAN side of your local node. Running this page on a remote node will be less responsive due to the mesh performance degradation.

The **system time** is kept in UTC and begins at midnight on Jan 1, 2000. There is no internal battery or real time clock so the time will reset every time the node is booted. If an internet connection becomes available the internal NTP (network time protocol) client will connect with an internet time server and the time will be kept in sync with atomic time for as long as the internet connection is available.

The **uptime** shows how long the node has been running since its last boot, and the **load average** is the average number of processes that have been running for the last 1, 5, and 15 minutes. The load average will typically be less than 1 for each time slot.

Free space tells you how much space is available on local storage devices. Flash is the internal non-volatile storage where the operating system, configuration files, and software packages are kept. /tmp is a filesystem in RAM that stores the current state information and various temporary files. Memory is the amount of RAM available for running processes.

Basic Setup

This is where the basic networking settings are made for the node. Because of the way Broadband-Hamnet is designed you generally will not need to change any of the settings on this page other than the node name/type and password. Do not change any of the network settings unless you fully understand how the mesh works and why the default is not suitable for your application. One reason Broadband-Hamnet exists is to eliminate, as much as possible, the need to manually configure the network.

The buttons on this page work as follows:

- **Save Changes** will check the validity of all the entered information and save it to flash memory if no errors are found. A reboot is required to make most changes on this page take effect, and should be done as soon as possible to avoid configuration mismatch problems.

- **Reset Values** will reload the current settings from flash memory and undo any changes that have been made.

- **Default Values** will set all values to their default values except the Node Name and Password. These default values are not saved until Save Changes is clicked.

- **Reboot** will immediately reboot the node.

Node Name sets the hostname for the node. Hostnames can contain up to 63 letters, numbers, and dashes, but cannot begin or end with a dash. Underscores, spaces, or any other characters are not allowed. Hostnames are not case sensitive, but the case will be preserved.

As ham radio operators there are other requirements we must follow, namely identification of all transmitting stations. This hostname is beaconed automatically by the node every five minutes, so the hostname must contain your callsign. Recommended hostnames follow the (callsign)-(name) format, such as ad5oo-mobile or ad5oo-1. This is similar to the MYCALL setting you would give a packet TNC, but without the 0-15 restriction for the name part.

It is here that you can also set a tactical name for your node. A tactical name is just another name that your node is known by. If you are familiar with DNS records, this serves a purpose similar to a CNAME record. This is helpful in an emergency deployment situation where if for example several Red Cross shelters are being linked. In addition to the normal hostname you can give each node a tactical name such as shelter1, shelter2, shelter-north, etc. Tactical names have the same restrictions as hostnames, and are accessible through DNS like the main node names are.

To set a tactical name, put a slash after the the node name then give the tactical name. For example, "ad5oo-1/shelter5".

Node Type sets the operational mode of the device as follows:

- **Mesh Node**
  This is the main mode of the router, and the reason this firmware is running in the first place. The WiFi interfaces of multiple nodes form a mesh network, the LAN interfaces provide access to that mesh to other devices, and the WAN interface provides outbound network access, typically to the internet.

- **Mesh Access Point**
  In this mode the device is pre-configured to act as an access point providing standard wireless access to the LAN side of another mesh node. This is to be used on a second router whose LAN port is connected with the LAN port of a mesh node. It is a simple mode but there are special considerations, especially when you want to get out of this mode. See the section at the end called Mesh Access Point considerations for details.

- **Standard Access Point**
  In this mode the device acts like any other standard access point, although with fewer configuration options. It is provided mainly as a convenience if you need a basic access point. If you need a full featured access point, consider using either a stock router or one running conventional access point firmware.

- **Wireless Client**
  This mode allows you to connect a wired network interface to a wireless network. The WiFi interface acts as a client to a separate access point, and the LAN provides access to the wired device. This mode does not provide a wireless bridge, instead it uses NAT and is routed.

- **Wired Router**
  In this mode the WiFi is disabled and the LAN and WAN ports have their usual roles. This is "just a router" with no wireless functions.

Node Type sets the operational mode of the node. For our purposes it will be set to Mesh Node, but if needed it can also be set to one of the other modes, to be described at a later time.

The one mode I will mention is called Mesh Access Point. It is a configuration meant to be used to give standard wireless access to the LAN port of a mesh node. This is to be used on a second router whose LAN port is connected with the LAN port of a mesh node. When running a router in this mode it does not use OLSR and as a result its hostname is not available to the mesh. It can be accessed from the LAN by its IP address which by default is 172.27.0.2. Like the name "localnode", an automatically generated name exists called "localap" which is set to the localnode address plus one, but only when the node is operating in the default NAT mode.

Password is where you set the administration password for the node. It needs to be entered again in the Retype Password box to help ensure its accuracy. It is not necessary to enter a password unless you want to change its value, and the first time the node is configured it is required that you change the password. Note that these passwords entries are NOT encrypted in transit, so this is best done from a direct wired connection to the node.

The **WiFi**, **LAN**, and **WAN** boxes are where the details of each of these network interfaces are set.

In the **WiFi** box there are settings shown as being Active Settings. These settings can be changed without rebooting the node by clicking the **Apply** button, but unless they are saved they will revert to the previously saved values after a reboot.

The **Rx Antenna** and **Tx Antenna** settings of Right and Left are from the point of view from the front of the router. This is valid for the WRT54GL, but it is not unreasonable to expect that they may be reversed for some other router models. If you find this to be the case, contact the webmaster and it will be accounted for in the firmware.

The **Distance** setting adjusts the packet retry timer to account for stations that are very far away, presumably about 300 meters or more. The value should be set to the distance in meters to the farthest node that you expect to communicate with. A value of 0 sets it to automatic, which may or may not be suitable for your application. The only way to know is to experiment with it. Changes smaller than 150 meters do not affect the settings, so the value entered here will be reduced to the smallest multiple of 150 that produces the same effect.

The **LAN** box allows you to set the LAN IP Address of the node and the address range of the DHCP server, and these should be self explanatory. The **LAN Mode** is described in the next section.

The **WAN** box contains the settings used to connect with an upstream network, usually an internet connection. The DNS servers are set by default to the Google DNS servers and should not be changed under normal circumstances. More and more ISP's are adopting the "helpful" but broken behavior of taking you to an ISP generated web page if you incorrectly type in a URL or if the host you are trying to reach no longer exists. The proper behavior is for your browser to be able to detect these error conditions and report them accordingly. Google follows the rules and allows for the proper operation of the network.

When the WAN protocol is set to disabled you have the option of using a default gateway on the LAN. Integrating an existing LAN with a mesh node LAN is an expert level undertaking and there are far too many considerations to be covered here.

The other option in the WAN box is the **Mesh Gateway**. When a node has internet access from either the WAN or LAN, that access is available to the node itself and to any computer connected to the LAN port. When the Mesh Gateway is enabled, this node will advertise to the mesh that it has internet access and will act as a gateway and provide internet access to the rest of the mesh. By default it is disabled, so consider carefully your intentions for enabling it. Broadband-Hamnet is an FCC Part 97 amateur radio computer network, so be sure that any internet traffic that will be sent over radio will comply with Part 97 rules. If you just want local wireless internet access, consider using a standard Part 15 compliant access point instead of the Mesh Gateway function.

LAN Mode

The default mode is called **5 Host Direct** mode and in this mode every host on the LAN has direct access to and from the mesh. The LAN shares the same address space as the mesh. Port forwarding is not needed because NAT is not used, and there is no firewall in between the LAN and the mesh. This mode

was created because some services do not work well (or at all) through NAT, and to reduce the amount of manual configuration needed to provide services to the mesh.

The mesh address space is automatically managed, so in Direct mode the LAN is not user configurable. Those of you familiar with setting up commercial ISP access with static IP addresses should already be comfortable with this mode. Like commercial ISP access, you cannot decide for yourself what the network parameters are. You have to use the parameters which are given to you. But unlike most commercial ISP access there is a DHCP server available on the mesh node to configure the hosts that are attached to the LAN.

The only configurable option available in Direct mode is the size of the LAN subnet which can accommodate either 1, 5, or 13 LAN hosts. The one host subnet can be useful for either a single server or a commercial grade router using its own NAT which is capable of more advanced routing functions than those available from a mesh node.

It is important to not use a subnet larger than is necessary because the chances of an IP address conflict on the mesh increase with the size of the subnet. The LAN subnet parameters are automatically generated and depend on the IP address of the WiFi interface. If a conflict does occur it can be fixed by changing the WiFi IP address.

The other LAN Mode is NAT, which stands for Network Address Translation. In this mode the LAN is isolated from the mesh and all outgoing traffic has its source address modified to be the WiFi address of the mesh node. This is the same way that most routers use an internet connection, and all services provided by computers on the LAN can only be accessed through port forwarding rules. A single DMZ server can be set up to accept all incoming traffic that is not already handled by other rules or by the node itself.

Mesh Access Point considerations

When a device is configured in Mesh Access Point mode it is essentially 'transparent'. You are going through the device to reach a mesh node, and there is no need to get to the device unless you wish to change its configuration. When the time comes to reconfigure a device in this mode be aware that it is not running its own DHCP server because that is the job of the mesh node it is connected to. You will need some other way to configure your computer's network interface. There are two ways to do this:

1. Manual configuration
   Connect only your computer to the LAN port. Set your IP address to 172.27.0.100 and your netmask to 255.255.255.0. No other settings are needed.

2. Automatic configuration
   You will need another mesh node that is using NAT mode on its LAN, and using the default LAN IP address of 172.27.0.1. Both of these are required, otherwise this method will not work. Connect both your computer and the LAN of the Mesh Access Point to the LAN of the mesh node.

In this mode the default IP address on the LAN port is 172.27.0.2. After one of the above steps you should be able to send your browser to http://172.27.0.2:8080/. If you used automatic configuration you should also be able to go to http://localap:8080/. Like the name "localnode", an automatically generated name exists called "localap" which is set to the localnode address plus one, but only when the node LAN mode is set to NAT. If you changed the default IP address of a Mesh Access Point you will have to modify these instructions accordingly.

Port Forwarding, DHCP, and Services

The buttons on this page works as follows:

- **Save Changes** will do a basic validation of the entered data save it to flash memory if no errors are found. The settings take effect in about 20 seconds and a reboot is NOT required. Note that the checks performed are not comprehensive and it is possible to use settings that at best will not work and at worst will break the node's configuration.

- **Reset Values** will reload the current settings from flash memory and undo any changes that have been made.

- **Refresh** will reload the page and it is useful for two things. It will update the list of DHCP leases for any new hosts that have been configured on the LAN, and it will also validate the settings entered on the page and incorporate changed settings that may affect other settings. You should do this before saving the changes to make sure everything is set up as intended.

The way this page works depends on whether the LAN is operating in NAT mode or Direct mode. First we will cover NAT mode, where hosts on the LAN are insulated by a firewall and NAT from both the WiFi and WAN interfaces. This makes them inaccessible from either of these interfaces unless Port Forwarding is set up. Here are some common ports:

- **20** ftp-data
- **21** ftp - file transfer protocol
- **22** ssh - secure shell
- **23** telnet
- **25** smtp - simple mail transport protocol
- **53** dns - domain name service
- **80** http - hypertext transport protocol
- **123** ntp - network time protocol
- **698** olsr - optimized link state routing
- **1978** olsr http - olsr's web interface
- **2222** node ssh server
- **8080** node web server

So then what is port forwarding? Port forwarding is taking an inbound connection to a port from the WiFi or WAN interface and forwarding it to an IP address on the LAN. The port number need not be the same. If you have hosts on the LAN that provide services you want to make available to the mesh all it takes is a Port Forwarding rule to make that happen.

If you want to forward a range of ports, the **Outside Port** will accept a range in the form "2000-3000". Use a hyphen to separate the low and high values. When doing this, set the **Inside Port** to the low value of the port range. When forwarding a port range the outside and inside ports must be the same, moving them will not work.

If you want to forward every port that is not already in use to a single computer on the LAN, choose that computer's IP Address from the **DMZ Server** selector. There can be only one DMZ Server. Be aware that this bypasses the firewall in the node, so this computer should be running its own firewall to prevent unauthorized access.

Example:

On the LAN of a mesh node called ad5oo-mobile is an IP camera that is running its own web server. The address of that camera is 172.27.0.240. I want to make that camera available to everyone on the mesh so I set up a port forwarding rule on the WiFi interface whose outside port is 8100, IP address is 172.27.0.240, and inside port is 80. This takes all connections to port 8100 on ad5oo-mobile and redirects them to port 80 on 172.27.0.240. In a web browser on a computer connected to a different node you would go to http://ad5oo-mobile:8100 and would be connected to the IP camera.

Note that port forwarding to an FTP server, which uses both ports 20 and 21, can be done with a single rule using port 21 if the ftp client is capable of using passive ftp mode. Web browsers are able to do this and handle ftp downloads quite nicely.

Advertised Services

When you want to let others know about services you are providing, the Advertised Services will appear on the Mesh Status page of all other nodes on the mesh. All advertised services need a name, and no services can be advertised until at least one port forwarding rule or a DMZ server has been defined.

If the service is one that is accessible through a web browser, such as a web or ftp server, you can make the name appear as a clickable link by checking the Link box. All links need two parameters: a protocol and a port number. Web servers use the http protocol and ftp servers use the ftp protocol. Other servers may use other protocols. The port number should be the one used as the Outside Port in the forwarding rule through which the service can be accessed. In the last field you can enter an optional link suffix to give the link a more specific path if needed, such as the name of a specific page on a web server, or a directory or file on an ftp server.

DHCP Reservations

If you are providing services to the mesh from hosts on the LAN you will want to either override or make permanent the automatically assigned IP address for that host. The DHCP Reservations section is where you do that. In order for port forwarding to work, the IP address must match that of the host being forwarded to. If it is currently attached and has been set up by DHCP it will be listed under **Current DHCP Leases**. If you click the **Add** button next to the lease it will be added to the DHCP Reservations list. You can leave the information as it is or edit it to suit your needs. You can also enter your own information into the blank slots under DHCP Reservations and click **Add** to create your own entry.

For each of the sections on this page, simply entering information into the fields next to the **Add** buttons is not enough. The settings are not entered until the **Add** button is clicked. Before saving changes the Add fields must be either added or cleared.

Direct Mode Operation

When the LAN is operating in Direct mode both this page and the mesh work a little differently. Since in Direct mode the LAN hosts are accessed directly from the mesh and no port forwarding is involved, the advertised services are based upon which LAN hosts exist, and this is determined by the DHCP Address Reservations that are defined. After the DHCP Reservations have been made, services can be advertised in the same way as before with the additional requirement of selecting the name of the host that is providing the service.

Another difference in Direct mode is that the hostnames used in DHCP Reservations are also advertised to the mesh and therefore must be unique on the mesh. So, "webserver" would be perfectly suitable for a service name, but a very poor choice for a hostname because there can be only one host with this name on the entire mesh. Just as you used your callsign in the hostname for the node, it would also be a good idea to use it in DHCP Reservation hostnames. Therefore, "ad5oo-webserver" is a good choice of hostname as it is unique and only the callsign holder needs to keep track of the hostnames he has assigned himself.

The hostnames being discussed here are those that are defined in the DHCP Reservations and available to the mesh, not those that the LAN hosts call themselves. While it can be convenient for them to be the same, there is no reason that they must be. For example, the name "ad5oo-webserver" used above can be the name on the mesh for a host that calls itself "skywalker". But be aware that if this host is in fact a webserver, the webserver configuration should use the name "ad5oo-webserver" because the name "skywalker" will not be known on the mesh and any pages the webserver generates itself such as error pages may use the "skywalker" name.

There are two considerations to keep in mind regarding the size of the subnet chosen for the LAN. First, when using a one host subnet, the DHCP Reservation used for that single host will prevent any other host from receiving a DHCP lease. So if for some reason the original host is not connected to the LAN and you need to get back in to the node to reconfigure it, the easiest way is to access it from a different node on the mesh.

Second, if the node is already in Direct mode and you intend to reduce the size of the LAN subnet, you should first remove the DHCP Reservations that will fall outside of the address range of the smaller

subnet. Note that the automatically assigned network address will change if the subnet size is changed, and that internally the DHCP Reservations are stored as offsets from the network address, so address reservations which fall within the new subnet size will be translated into the new subnet address space.

Administration

Firmware Update is how new firmware is installed on the node. If you have a firmware image on your computer, click the **Browse** button and select the firmware file to upload. Click **Upload** and the file will be uploaded and installed. If the node has internet access (either from the WAN port or from the mesh) you can use the **Download Firmware** option. Click **Refresh** to get the list of available images. Select the image to download, click **Download**, and wait for the firmware to download and be installed.

A new feature in the 0.4.0 firmware is the ability to install firmware patches. This means that updated files can be installed directly on the node without having to replace the entire firmware. Except in cases where the patch contains updated configuration files, patches can be installed while preserving the existing node configuration. However, certain patches will require that the node be rebooted to take effect, and this will happen automatically when it is needed.

Package Management allows you to install and remove software packages on the node. **Upload Package** allows you to install a package file from your computer. **Download Package** allows you do retrieve a package over the internet from the Broadband-Hamnet website. Clicking **Refresh** will populate the list of packages available for download, but don't do this frivolously. The package information database gets stored locally and will use about 100KB of space in flash memory. The average user will probably never have to use this function.

The **Remove Package** list shows all packages on the node. Selecting a package and clicking **Remove** will remove the package. You will only be able to remove packages that you have installed. All installed packages are shown but the set that comes pre-installed is necessary for proper operation of the node and they cannot be deleted.

Authorized SSH Keys are useful for both developers and anyone managing a "fleet" of nodes. It allows connecting to a node via ssh without having to know the password. For developers, it also allows you to easily scp an updated file to the node without having to reinstall the firmware.

To generate a key on a Linux system, issue the command "**ssh-keygen -t rsa**" and hit enter at all the prompts to accept the defaults. It creates a file called **~/.ssh/id_rsa.pub**, which is the file you upload to install the key on the node. If you want to remove a key just select it and click the **Remove** button.

For fleet managers, having an authorized key installed is the best way gain access to a node for which you do not know the password. If you want to set the password to "abc", simply ssh to the node and run "**setpasswd abc**", then reboot. If you don't have an authorized key installed, the only way in is to use Failsafe Mode as described in a separate article.

Last Updated on Saturday, 03 August 2013 20:50