EnRoute50x/51x

User's Guide

Rev. D2

Communicate Without Boundaries

Tranzeo Wireless Technologies Inc.
19473 Fraser Way, Pitt Meadows, BC, Canada V3Y 2V4
www.tranzeo.com
technical support email: support@tranzeo.com

FCC Notice to Users and Operators

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for 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 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

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 14cm from all persons.

Any changes or modification to said product not expressly approved by Tranzeo Wireless Technologies Inc. could void the user's authority to operate this device.

The Tranzeo EnRoute500 Mesh Router must be installed by a trained professional, value added reseller, or systems integrator who is familiar with RF cell planning issues and the regulatory limits defined by the FCC for RF exposure, specifically those limits outlined in sections 1.1307.

Table of Contents

1 Working with the EnRoute500

Thank you for choosing the Tranzeo EnRoute500 Wireless Mesh Router. The EnRoute500 allows a wireless mesh network to be rapidly deployed with minimal configuration required by the end user. This user's guide presents a wide array of configuration options, but only a limited number of options have to be configured in order to deploy a mesh network of EnRoute500s.

1.1 EnRoute500 Variants

There are four EnRoute500 variants available, as shown in Table 1.

Model Number	External AC Power Connector	Included Antennas
EnRoute500	No	AP 5dBi, Mesh 8.5dBi
EnRoute501	Yes	AP 5dBi, Mesh 8.5dBi
EnRoute510	No	AP 7.5dBi, Mesh 10.5dBi
EnRoute511	Yes	AP 7.5dBi, Mesh 10.5dBi

Table 1. EnRoute500 variants

Throughout the manual, "EnRoute500" will be used to collectively refer to this family of products. Where the functionality of the variants differ, the actual model number will be used.

1.2 EnRoute500 Capabilities

The EnRoute500 is capable of automatically forming a mesh network that allows devices that are connected to it, either with a wired or a wireless connection, to communicate with each other and external networks that are accessed through gateway nodes. The EnRoute500 has two radios, an 802.11a mesh backhaul radio and an access point radio for 802.11b/g-client devices. An EnRoute500 will currently support up to four access points (APs), each with different access and performance settings. It is also possible to connect devices to an EnRoute500 using an Ethernet connection.

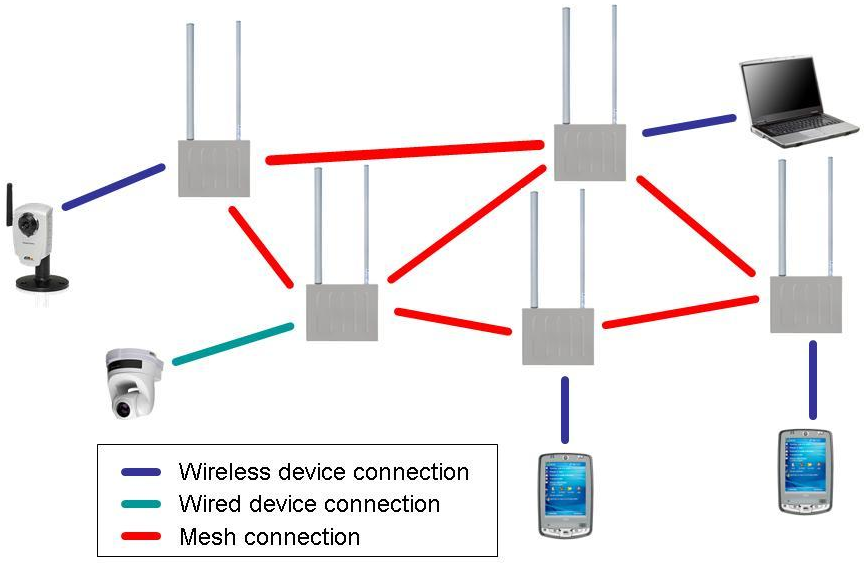

Figure 1. EnRoute500 sample network – devices attach to the EnRoute500 through both wired and wireless connections

1.3 Network Topology

EnRoute500s can be used to create two network topologies: a stand-alone network or an Internet extension network that attaches to a network with connectivity to the Internet.

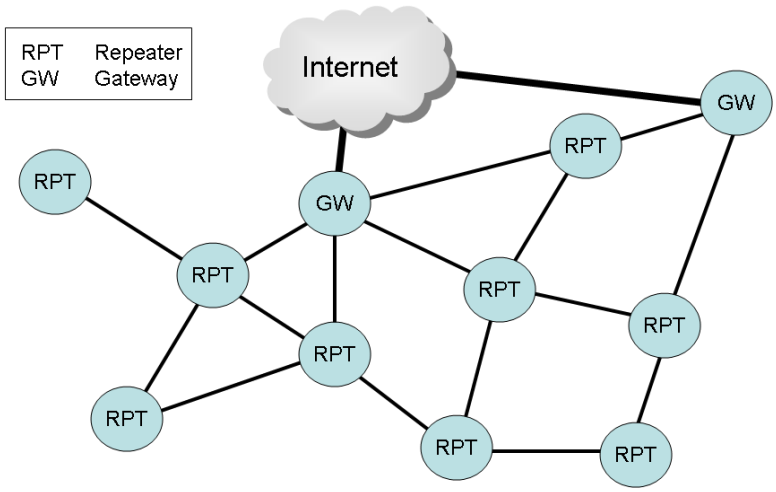

Figure 2. Internet extension network

An Internet extension network (shown in Figure 2) is typically used when the goal is to provide Internet access to a number of clients that connect to the mesh network. Alternatively, this configuration can be used to provide access for client devices to remote resources on a private network. The key feature to note is that there is a gateway node that provides access from the mesh network to an external network.

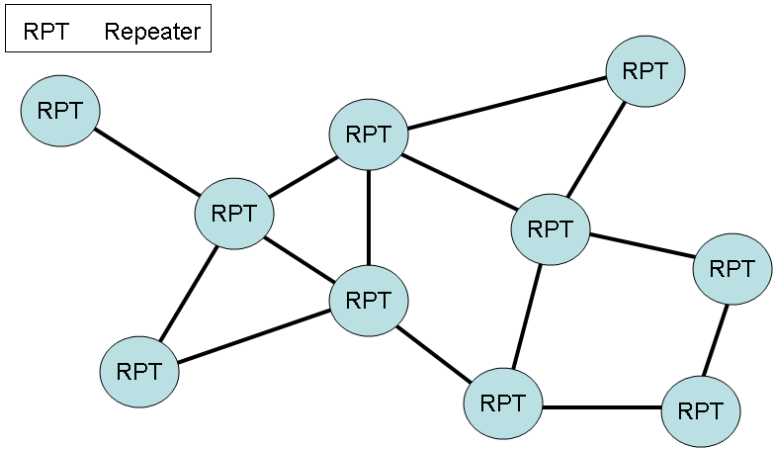

Figure 3. Stand-alone network

In a stand-alone network, as shown in Figure 3, all nodes are configured to operate in the same mode (repeater mode). This network configuration is suitable for applications where the clients using the mesh only need to communicate with each other and do not need to access the Internet or other remote network resources that are not directly connected to the mesh.

1.4 Network Terminology

The following terms will be referred to throughout this manual.

Mesh cluster – a group of two or more EnRoute500 nodes with at least one configured as a gateway

Mesh cloud – a group of EnRoute500 nodes configured as one or more mesh clusters

Mesh node – a single EnRoute500 node that is part of a mesh network

1.5 EnRoute500 Interfaces

The interfaces available on the EnRoute500 are Ethernet and two radio ports. On the EnRoute5x1 models, an external AC power port is also present.

Figure 4. EnRoute500 interfaces. EnRoute501 shown

Interface	Description
Power (EnRoute 5x1 only)	Power input (100-240VAC 50-60 Hz)
Mesh radio port	N-type antenna connector for mesh radio
AP radio port	N-type antenna connector for access point radio
Ethernet	10/100 Mbit Ethernet interface
Passive PoE	PoE secondary power input (9-28VDC, 12W) *Not compatible with IEEE 802.3af*

Table 2. EnRoute500 Interfaces

1.5.1 Ethernet and PoE

The EnRoute500 has a 10/100 Ethernet port that supports passive Power over Ethernet (PoE). The PoE power injector should supply an input voltage between 9-28VDC and a minimum of 12W. The pinout for the Ethernet interface on the EnRoute500 is provided in Table 3.

INFO

The EnRoute500 is equipped with an auto-sensing Ethernet port that allows both regular and cross-over cables to be used to connect to it.

Pin	Signal	Standard Wire Color
1	Tx+	White/Orange
2	Tx-	Orange
3	Rx+	White/Green
4	PoE V+	Blue
5	PoE V+	White/Blue
6	Rx-	Green
7	Gnd	White/Brown
8	Gnd	Brown

Table 3. Ethernet port pinout

1.5.2 Antennas

Attach the supplied antennas to the mesh and access point (AP) radio ports on the EnRoute500. The antennas used for the two radios are band-specific and therefore it is important to correctly match the antennas with the radio ports.

1.6 Deployment Considerations

The EnRoute500's radios operate in the unlicensed 2.4 GHz and 5.8 GHz ISM bands. It is possible that there will be other devices operating in these bands that will interfere with the EnRoute500's radios. Interference from adjacent EnRoute500s can also degrade performance if the EnRoute500s are not configured properly.

It is advisable to carry out a site survey prior to installation to determine what devices are operating in the two bands that the EnRoute500 uses. To detect the presence of other 802.11 devices, a tool such as Netstumbler (http://www.netstumbler.com/downloads/) can be used. A spectrum analyzer can be used for further characterization of interference in the band.

1.6.1 Mesh channel selection

The mesh radio channel must be the same for all EnRoute500s in a given mesh cluster. Adjacent mesh clusters will get a performance benefit if they are on different channels as the clusters will not interfere with each other. The 802.11a channels that the EnRoute500 mesh radio can be configured to use are all non-overlapping.

1.6.2 AP channel selection

The access point radio channels used by the EnRoute500s in a mesh cluster may differ. It is advisable to use different access point channels for adjacent mesh nodes to reduce interference.

However, it may be more important to select the access point channel based on the presence of other 802.11 devices in the area rather than configuring it to be different than that of an adjacent EnRoute500. A site survey should be conducted to determine which access point channel will provide the best performance.

Some of the 802.11b/g channels that the EnRoute500 access point radio can be configured to use are overlapping. Only channels 1, 6, and 11 are non-overlapping.

2 Using the Command Line Interface

All configurable EnRoute500 parameters can be accessed with a Command Line Interface (CLI).

The CLI allows you to:

- Modify and verify all configuration parameters
- Save and restore device configurations
- Reboot the device
- Upgrade the firmware

2.1 Accessing the CLI

The EnRoute500's command-line interface (CLI) is accessible through the device's network interfaces using an SSH client. Any of the network interfaces can be used to establish the SSH connection to the EnRoute500. However, connecting through the Ethernet port is recommended for devices that have not previously been configured.

The EnRoute500 has a dedicated configuration interface that is accessible via the Ethernet port. This interface is present regardless of the EnRoute500's standard Ethernet interface configuration. The IP address and netmask of this interface are provided in Table 4.

Since the configuration IP address (shown in Table 4) is the same for all EnRoute500s, you should not simultaneously connect multiple EnRoute500s to a common LAN and attempt to access them using the configuration IP address.

Parameter	Setting
IP address	169.254.253.253
Netmask	255.255.0.0
Protocol	SSH v2
User name	admin
Default password	mesh

Table 4. EnRoute500 Ethernet configuration interface settings

To use this interface:

1. Configure a computer with an IP address on the 169.254.0.0 subnet
2. Connect the PC to the EnRoute500 using an Ethernet cable. A standard or cross-over cable will work.

3. Login to the node using an SSHv2-capable client application with the credentials provided in Table 4.

Windows XP does not include an SSH client application. You will need to install a 3rd-party client such as SecureCRT from Van Dyke software (http://www.vandyke.com/products/securecrt) or the free PuTTY SSH client (http://www.putty.nl/) to connect to an EnRoute500 using SSH.

If you are configuring multiple EnRoute500s with the same computer in rapid succession, it may be necessary to clear the ARP cache since the IP addresses for the EnRoute500s will all be the same, but the MAC addresses will vary. The following commands can be used to clear the ARP cache

Windows XP (executed in a command prompt window)

```
arp -d *
```

to clear the entire cache, or

```
arp -d 169.254.253.253
```

to just clear the EnRoute500 entry

Linux

```
arp -d 169.254.253.253
```

When you log in to the node, the CLI will present a command prompt. The shell timeout is displayed above the login prompt. The CLI will automatically log out a user if a session is inactive for longer than the timeout period. Section 6.11 describes how to change the timeout period.

```
Shell timeout: 3 minutes.

Press '?' for help..
>
```

2.2 User Accounts

There are two user accounts for accessing the EnRoute500: 'admin' and 'monitor'. With the 'admin' account all parameters can be set and viewed. The 'monitor' account only allows users to view a subset of the parameters available. Parameters that affect access to the network, such as encryption keys, are not viewable by the 'monitor' user. The only parameter that can

be set by the 'monitor' user is the shell timeout (see section 6.10). The passwords for both users can only be set by the 'admin' user. The procedure for changing passwords is described in section 6.1.

2.3 CLI Interfaces

The CLI provides the user with a number of interfaces that contain related parameters and controls. Some of these interfaces are actual hardware interfaces, such as Ethernet, while others are virtual interfaces that contain a set of related parameters.

The available interfaces are:

- mesh0 – controls for the mesh radio
- wlan1, wlan2, wlan3, wlan4 – controls for the APs supported by the EnRoute500
- eth0 – controls for the Ethernet interface
- firewall – controls firewall settings for client device, mesh node and mesh network access
- qos – controls Quality of Service (QoS) settings
- version – displays version information for the installed firmware
- system – system settings

The currently selected interface is shown as part of the command prompt. For example, when the mesh interface is selected, the command prompt will be

```
mesh0>
```

After logging in, no interface is selected by default. Before setting or retrieving any parameters, an interface must be selected.

2.4 CLI Features

The CLI has a number of features to simplify the configuration of the EnRoute500.

2.4.1 Control of the Cursor

The cursor can be moved to the end of the current line with Ctrl+E. Ctrl+A moves it to the beginning of the line.

2.4.2 Cancel a Command

Ctrl+C cancels the input on the current command line and moves the cursor to a new, blank command line.

2.4.3 Searching the Command History

The command history can be searched by pressing Ctrl+R and entering a search string. The most recently executed command that matches the string entered will be displayed. Press 'Enter' to execute that command.

2.4.4 Executing a Previous Command

By using the up and down arrow keys you can select previously executed commands. When you find the command you wish to execute, you can either edit it or press 'Return' to execute it.

2.5 CLI Commands

The usage of all CLI commands is explained in the following subsections. The command syntax used is

```
command <mandatory argument>

command [optional argument]
```

2.5.1 '?' command

Syntax `?`

Description Pressing '?' at any time in the CLI will display a help menu that provides an overview of the commands that are described in this section. It is not necessary to press 'Enter' after pressing '?'.

2.5.2 'whoami' command

Syntax `whoami`

Description Displays the name of the user you are logged in as.

2.5.3 'help' command

Syntax

```
help [command|parameter]
```

where [command] is one of the CLI commands or [parameter] is a parameter in the currently selected interface.

Description

When no argument follows the help command, a help menu showing a list of available commands is displayed. When a command is supplied as the argument, a help message for that particular command is displayed. When a parameter in the current interface is specified as the argument, help information for it is displayed.

Example

```
help get
```

will display the help information for the 'get' command. With the 'sys' interface selected

```
sys> help scheme
```

displays help information about that 'scheme' parameter, as shown below

```
scheme : wireless node type
```

2.5.4 'show' command

Syntax

```
show
```

Description

Displays all available interfaces. An interface in this list can be selected with the 'use' command.

2.5.5 'use' command

Syntax

```
use <interface>
```

where <interface> is one of the EnRoute500's interfaces. A complete list of interfaces is available with the 'show' command.

Description

Selects an interface to use. By selecting an interface you can view and modify the parameters associated with the interface.

Example

```
use mesh0
```

will select the backhaul mesh radio interface and change the CLI prompt to

```
mesh0>
```

to reflect the interface selection.

2.5.6 'set' command

Syntax

```
set <parameter>=<value>
```

where <parameter> is the parameter being set and <value> is the value it is being set to.

Description

Sets a configuration parameter. Note that is only possible to set the parameters for the currently selected interface. If the value of the parameter contains spaces, the value must be surrounded by double quotes (" ").

If a valid 'set' command is entered, it will output its result and any effects on other parameters. If changes are made to attributes of other interfaces as a result of changing the parameter, these attributes are preceded by a '/' to signify that they are in another interface.

Changing certain parameters will require the node to be rebooted.

Example

With the 'sys' interface selected

```
set id.node=2
```

will set the node ID to 2, while

```
set id.mesh=1
```

will have an impact on a larger number of parameters as can be seen in the output below.

```
             id.mesh : 1
private.nets.default : "172.29.0.0/16 10.1.0.0/16"
/mesh0.routes.static : 224.0.0.0/4,10.1.0.0/16
splash.local_network : "172.29.1.0/24 10.1.0.0/16"
       /mesh0.cellid : 00:05:88:01:0a:01
   /mesh0.ip.address : 172.29.1.7
Reboot needed.
```

Note that changes were made to variables in the 'mesh0' interface, as indicated by the '/' at the beginning of those lines.

2.5.7 'get' command

Syntax

```
get <parameter>
```

where <parameter> is the parameter whose value is being fetched.

Description

Gets the value of one or more configuration parameters for the currently selected interface. The '*' character can be used to specify wildcard characters. This allows multiple values to be fetched with a single command.

Example

With the 'sys' interface selected

```
get id.node
```

will return the node's ID, while

```
get id.*
```

will return all parameters that begin with 'id.'

```
sys.id.lanprefix = 10
sys.id.mesh = 4
sys.id.meshprefix = 172.29
sys.id.node = 7
```

2.5.8 'list' command

Syntax `list`

Description Lists all parameters for the selected interface

Example With the 'firewall' interface selected

```
list
```

will display

```
firewall.gateway.enable : prevent uninitiated incoming connections
past the gateway?
 firewall.node.allowc2c.eth0 : allow clients to see each other if
.role=access
 firewall.node.allowc2c.wlan1 : allow clients to see each other if
.role=access
 firewall.node.allowc2c.wlan2 : allow clients to see each other if
.role=access
 firewall.node.allowc2c.wlan3 : allow clients to see each other if
.role=access
 firewall.node.allowc2c.wlan4 : allow clients to see each other if
.role=access
 firewall.node.enable : firewall enabled? if not, nothing else
here matters.
 firewall.node.tcp.allow.dest : tcp dest ports (space separated)
to allow to this node
 firewall.node.tcp.allow.source : tcp source ports (space
separated) to allow to this node
 firewall.node.udp.allow.dest : udp dest ports (space separated)
to allow to this node
 firewall.node.udp.allow.source : udp source ports (space
separated) to allow to this node
```

2.5.9 'ping' command

Syntax `ping <IP address or hostname>`

Description Pings a remote network device. Halt pinging with Ctrl+C

Example `ping 172.29.1.1`

2.5.10 'ifconfig' command

Syntax `ifconfig <eth0|wlan[0-4]>`

Description Displays information, such as IP address and MAC address, for the specified network interface.

Example `ifconfig wlan1`

will display

```
wlan1     Link encap:Ethernet  HWaddr 00:15:6D:52:01:FD
          inet addr:10.2.10.1  Bcast:172.29.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2434 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:233128 (227.6 Kb)
```

2.5.11 'route' command

Syntax `route`

Description Displays the current route table.

2.5.12 'clear' command

Syntax `clear`

Description Clears the screen

2.5.13 'history' command

Syntax `history`

Description Shows the command history since the node was last rebooted

Example After switching to the 'wlan1' interface, inspecting the ESSID setting, and then changing it

```
history
```

will display

```
1: use wlan1
2: get essid
3: set essid=new_ap_essid
```

2.5.14 '!' command

Syntax

```
!<command history number>
!<string that matches start of previously-executed command>
!!
```

Description

Executes a previously-executed command based either on a command history number or matching a string to the start of a previously-executed command. Note that there is no space between the '!' and the argument.

The 'history' command shows the command history, with a number preceding each entry in the command history. Use this number as an argument to the '!' command to execute that command from the history.

When a string is provided as an argument to the '!' command, the string will be matched against the beginning of previously-executed commands and the most recently executed command that matches will be executed.

Use '!!' to execute the last command again.

Example

If the command history is as follows

```
1: use wlan1
2: get essid
3: set essid=new_ap_essid1
4: use wlan2
5: set essid=new_ap_essid2
```

the command

```
!1
```

will execute

```
use wlan1
```

The command

```
!use
```

will execute

```
use wlan2
```

2.5.15 'exit' command

Syntax `exit`

Description Terminates the current CLI session and logs out the user

2.5.16 'quit' command

Syntax `quit`

Description Terminates the current CLI session and logs out the user

3 Using the Web Interface

The EnRoute500 has a web interface accessible through a browser that can also be used to configure the node and display status parameters.

3.1 Accessing the Web Interface

You can access the web interface by entering one of the node's IP addresses preceded by "https://" in the URL field of a web browser (see section 2.1 for a description of how to access an unconfigured node using its Ethernet interface). When you enter this URL, you will be prompted for a login and password. The login and password used for the web interface is the same as for the CLI (see Table 4 in section 2.1).

The node IP must be preceded by "https://", not "http://", to access the web interface

Figure 5. Login window for web interface

Since the certificate used in establishing the secure link to the node has not been signed by a Certification Authority (CA), your browser will most likely display one or more warnings similar to those shown below. These warnings are expected and can be disregarded.

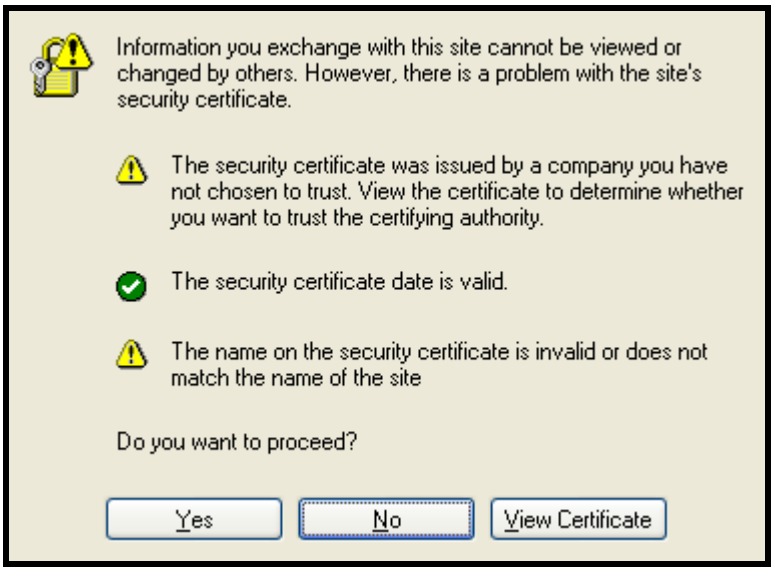

Figure 6. Certificate warning

3.2 Configuration Overview Page

A configuration overview page is loaded by default after the login process has been completed. This page contains the following information

- System type (gateway or repeater)
- System uptime
- Interface IP addresses
- VLAN status and ID for all interfaces
- Mesh interface channel and ESSID
- Access point status, channel, ESSID, and encryption type
- Ethernet interface use (client access or backhaul)
- Firmware version

To access the status page from any other page in the web interface, click on the "Status" button on the left side of the page.

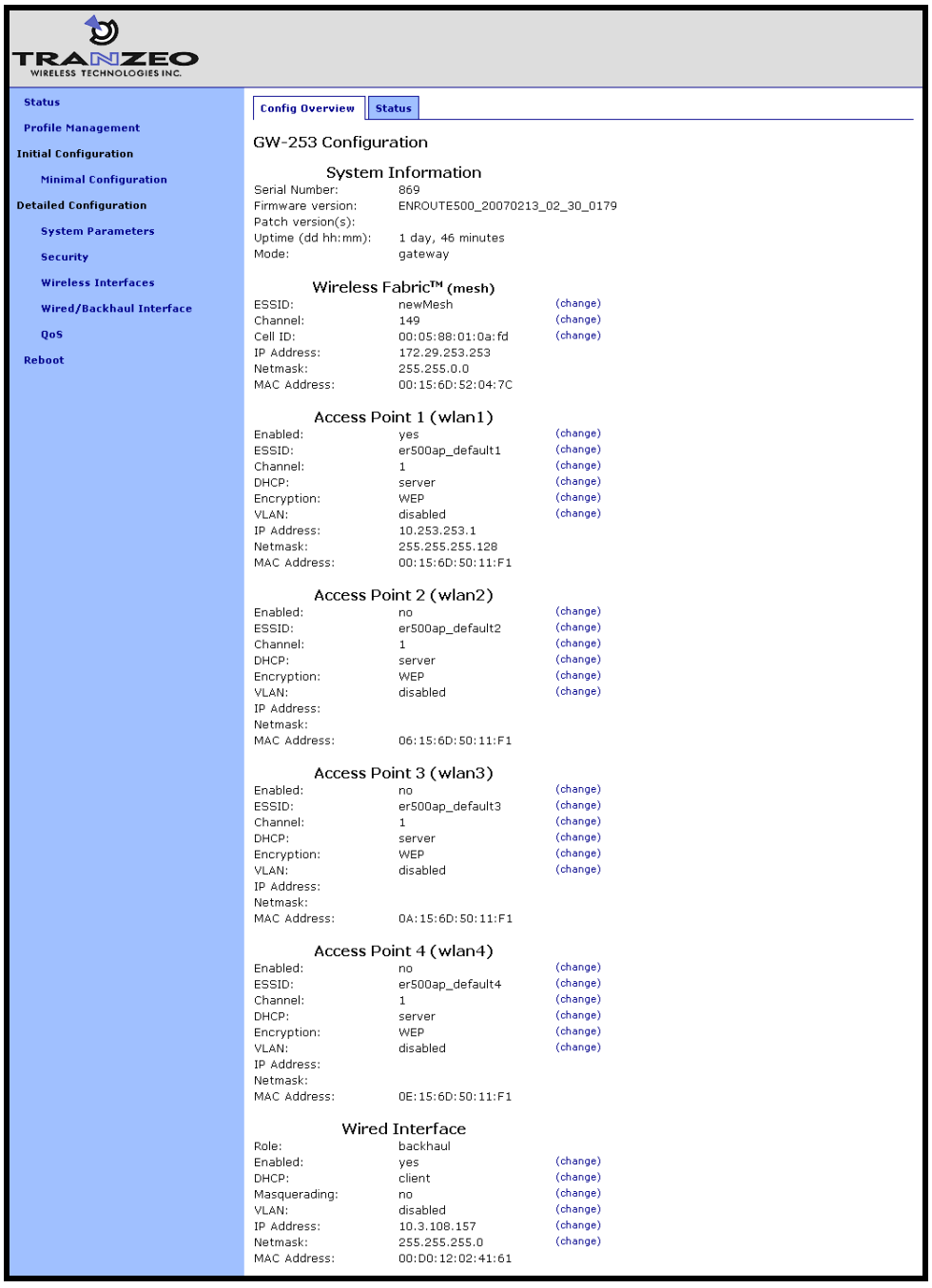

Figure 7. Sample status page

3.3 Setting Parameters

Many of the web interface pages allow you to set EnRoute500 operating parameters. Each page that contains settable parameters has a "Save Changes" button at the bottom of the page. When you have made your changes on a page and are ready to commit the new

configuration, click on the "Save Changes" button. It typically takes a few seconds to save the changes, after which the page will be reloaded.

For the changes to take effect, the node must be rebooted. After a change has been committed, a message reminding the user to reboot the node will be displayed at the top of the screen.

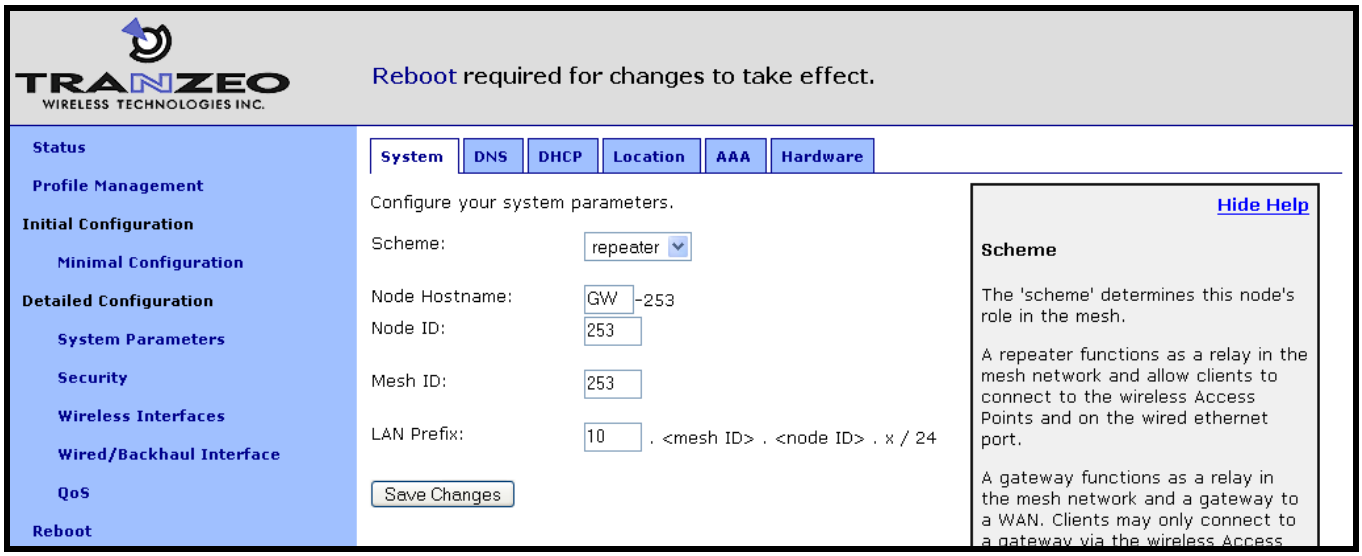

Figure 8. Sample page showing "Save Changes" button and message prompting the user to reboot

3.4 Help Information

Help information is provided on most web GUI pages. The help information is shown on the right-hand side of the page. The help information can be hidden by clicking on the 'Hide Help' link inside the help frame. When help is hidden, it can be displayed by clicking on the 'Show help' link.

3.5 Rebooting

Click on the "Reboot" link on the left of the page and then click on the "Reboot Now" button to reboot the node. Any changes made prior to rebooting will take effect following completion of the boot process.

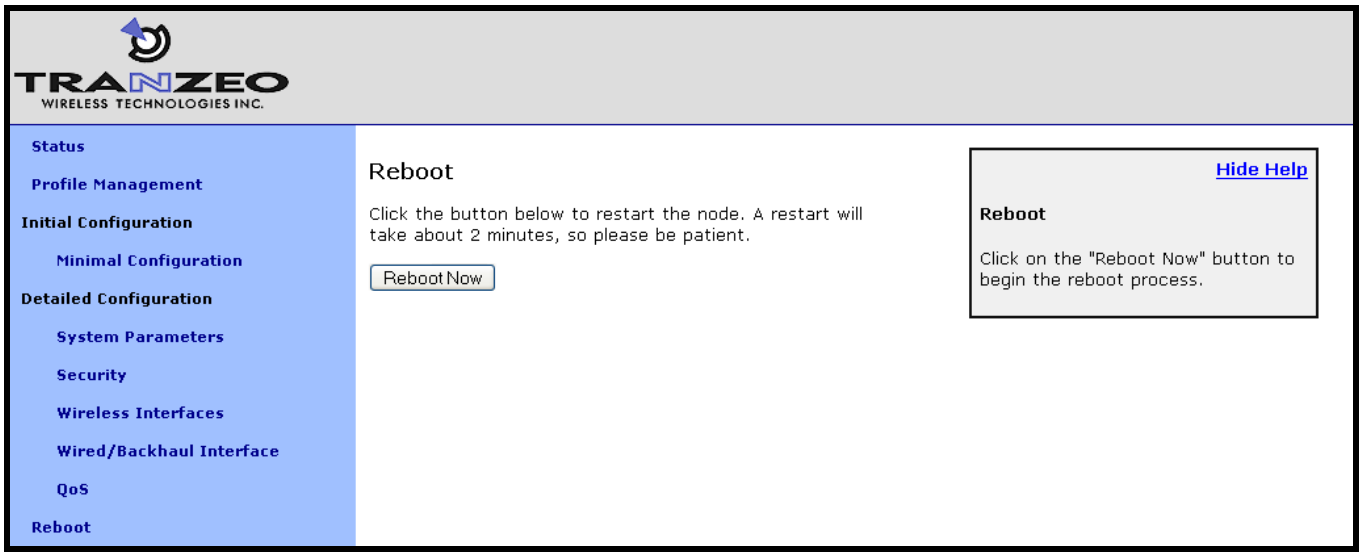

Figure 9. Rebooting the node

4 Initial Configuration of an EnRoute500

This user's guide provides a comprehensive overview of all of the EnRoute500's features and configurable parameters. However, it is possible to deploy a network of EnRoute500s while only changing a limited number of parameters. The list below will guide you through a minimal configuration procedure that prepares a network of EnRoute500s for deployment.

1	**Change the 'admin' and 'monitor' passwords.** The default passwords should be changed to prevent unauthorized access to the node.	See section 6.1
2	**Set the operating scheme for the node** Most nodes will be configured as repeaters, with at least one node per mesh cluster configured as a gateway.	See section 6.2
3	**Set the node and mesh IDs** The node and mesh IDs uniquely identify a node and determine which mesh cluster it is part of.	See section 6.3
4	**Set the DNS servers** Specify DNS servers to allow hostnames to be resolved.	See section 6.6
5	**Set the mesh radio channel** The mesh radios on all nodes in a mesh cluster must be set to operate on the same channel.	See section 7.1
6	**Set the mesh ESSID** Set the mesh interface ESSID to a common value for all nodes in a mesh cluster. It should be different than the ESSID for any adjacent mesh clusters.	See section **Error! Reference source not found.**
7	**Set the AES encryption key for the mesh** Change the default AES encryption key to prevent unauthorized access to the mesh. The mesh encryption key must be the same for all nodes in a mesh cluster.	See section 7.3
8	**Set the mesh radio transmit power** Set the mesh power to the maximum allowed value to achieve the best possible connectivity between mesh nodes.	See section 7.4

After these settings have been changed, the EnRoute500s will be able to form a mesh cluster and you will be able to configure the nodes from a central location. This minimal configuration must be performed prior to deployment, but all other configuration can be carried out after deployment.

To simplify initial configuration, the web GUI has a page that allows the user to change all the parameters listed in this section on a single page. This page can be accessed by clicking on the 'Minimal configuration' link that is present on the left-hand side of all web GUI pages.

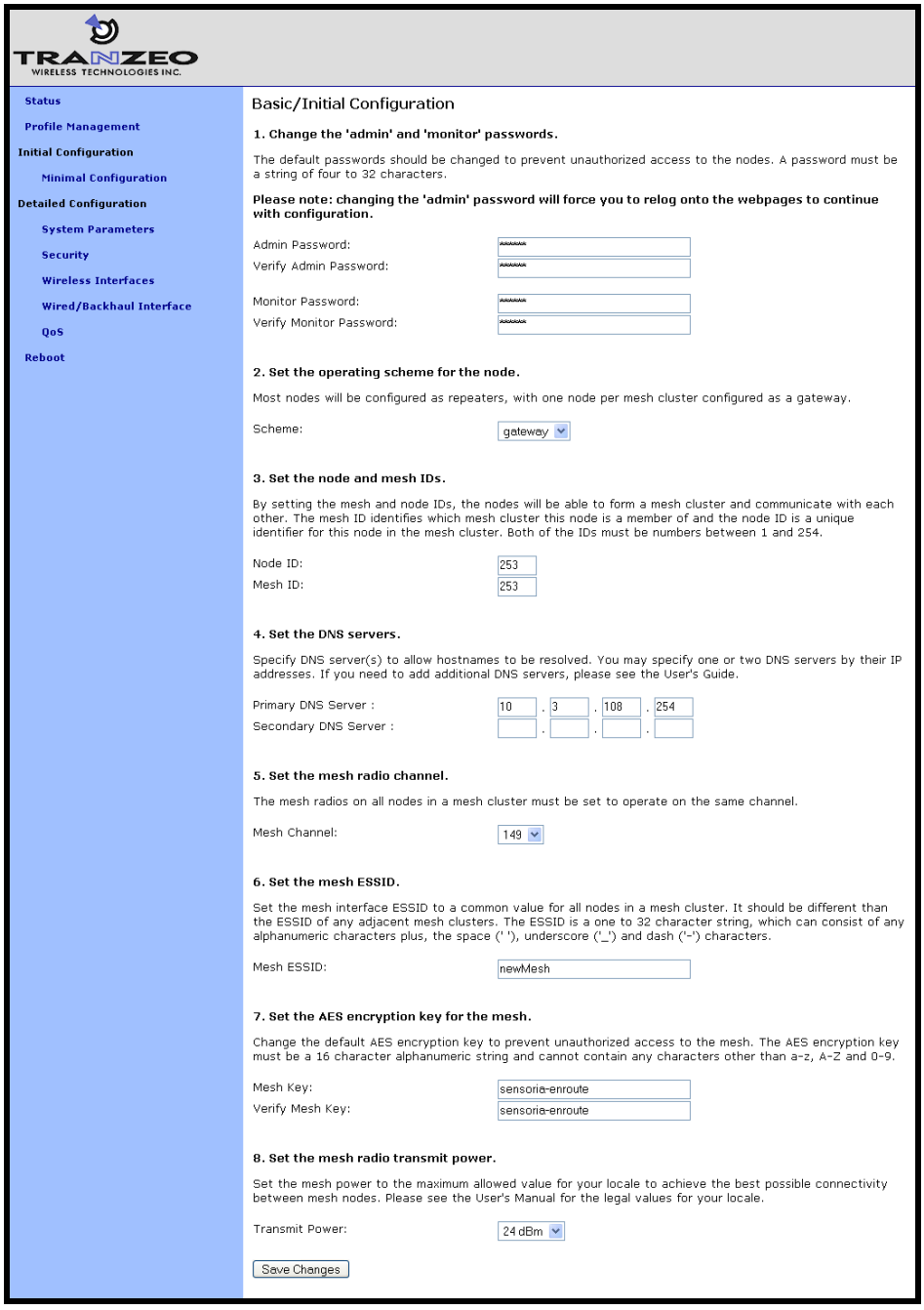

Figure 10. Initial configuration web page

5 Configuration Profile Management

Configuration profiles describe an EnRoute500's configuration state and can be created to simplify the provisioning and management of nodes. The EnRoute500 supports the following configuration profile-related tasks:

- Saving the current configuration as a configuration profile
- Applying a configuration profile stored on the node
- Downloading a configuration profile stored on the node to a computer
- Uploading a configuration profile from a computer to the node
- Deleting a configuration profile stored on the node

Currently configuration profile management is only supported via the web interface.

5.1 Saving the Current Configuration

The current configuration can be saved on the "Save" tab on the "Profile Management" page. Enter a profile name or select an existing profile name from the list of existing configurations, and then click on "Save Profile". The saved profile is stored locally on the node and will appear in the "Existing profiles" text box. Use the "Download from Node" tab to download it to a different device.

Figure 11. Save a configuration profile

5.2 Load a Configuration Profile

A configuration stored on the node can be loaded on the "Load" tab on the "Profile Management" page. This profile must either have been saved earlier or uploaded to the node. Choose a profile name from the "Existing Profiles" box and then click on "Load Profile". It is necessary to reboot the node for the loaded profile settings to take effect.

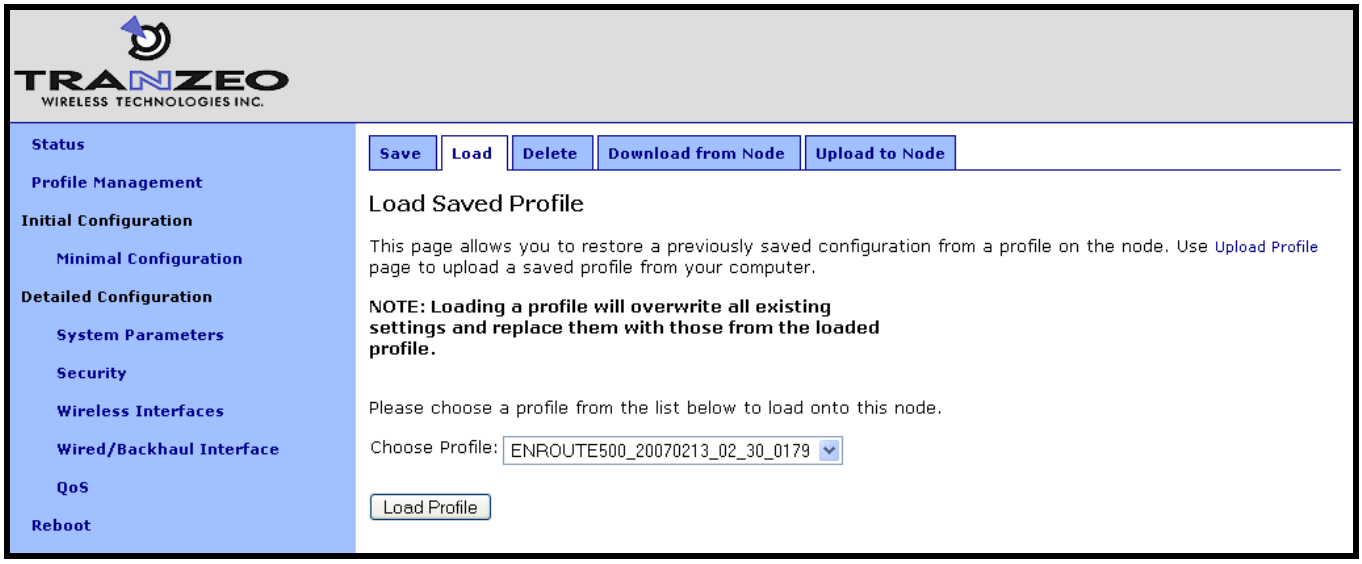

Figure 12. Load a configuration profile

5.3 Delete a Configuration Profile

A locally-stored configuration profile can be deleted using the "Delete" tab on the "Profile Management" page. Choose a profile to delete from the profile drop-down box on the page and then click on "Delete Profile".

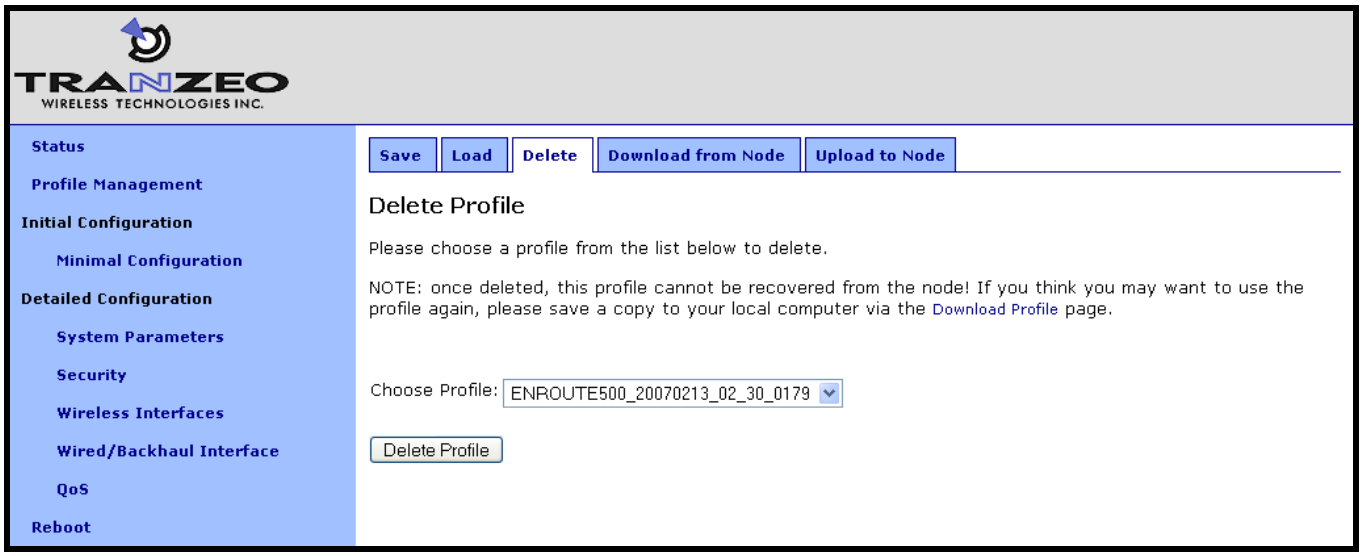

Figure 13. Deleting a configuration profile

5.4 Downloading a Configuration Profile from a Node

A configuration profile can be download from a node using the "Download from node" tab on the "Profile Management" page. The existing configuration profiles are listed on this page. Click on the one that is to be downloaded to your computer and you will be given the option to specify where the profile should be saved on the host computer.

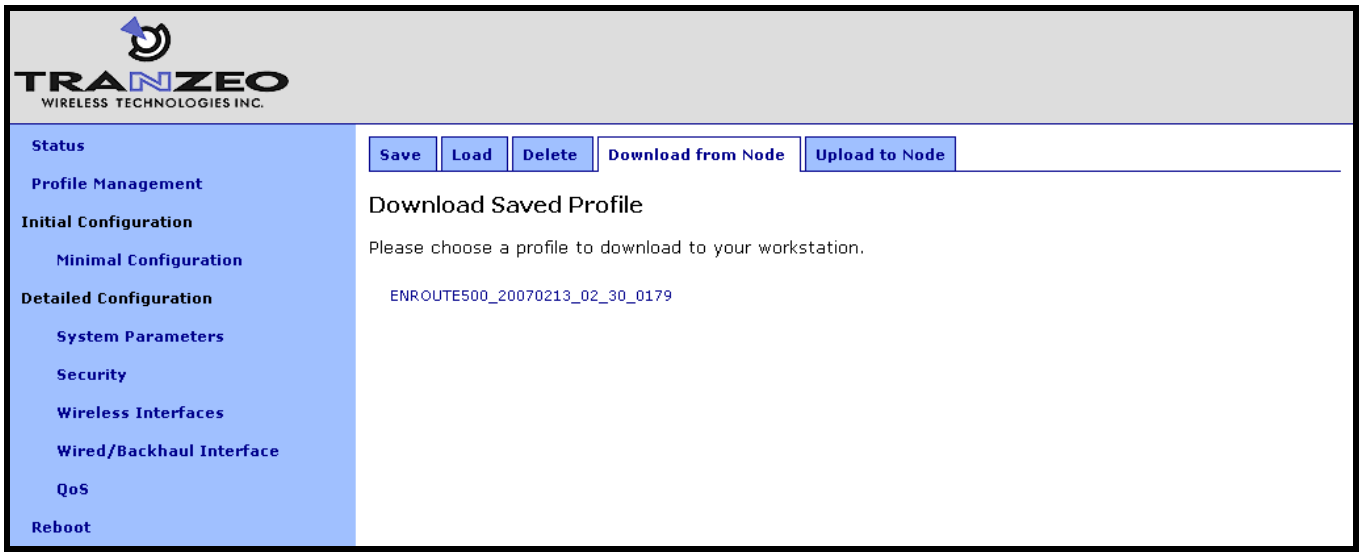

Figure 14. Downloading a configuration profile from a node

5.5 Uploading a Configuration Profile to a Node

A configuration profile can be uploaded to a node using the "Upload to node" tab on the "Profile Management" page. Use the "Browse" button to select a profile file on your host computer for upload to the node. Alternatively, enter the file name by hand in the text box adjacent to the "Browse" button. Click on the "Upload Profile" button to upload the selected file to the node.

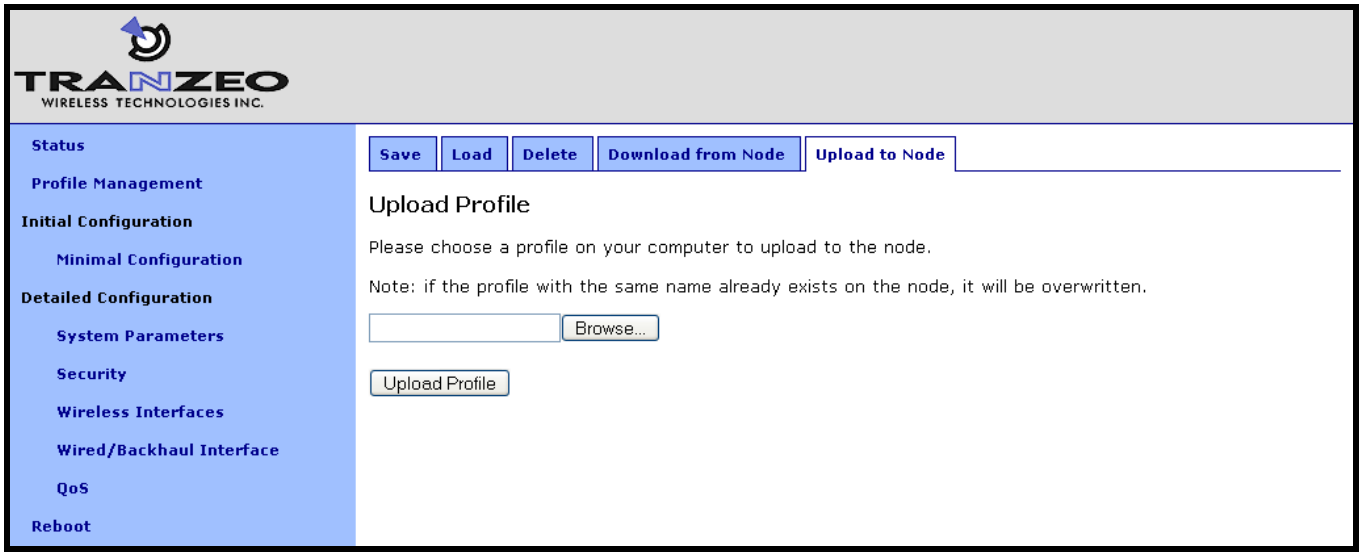

Figure 15. Uploading a configuration profile to a node

6 System Settings

This section describes settings that are applicable to the overall operation of the EnRoute500, but are not related directly to a particular interface.

6.1 User Passwords

The passwords for the 'admin' and 'monitor' users are configurable. The default password for both accounts is 'mesh'.

CLI

The passwords for the 'admin' and 'monitor' users can be set using the 'password.admin' and 'password.monitor' parameters in the 'sys' interface. The passwords will not be displayed when using the 'get' command with these parameters. Note that the 'monitor' account password can only be changed by an 'admin' user. The example below shows how to set the 'admin' password using the CLI.

```
> use sys
sys> set password.admin=newpass
```

Web GUI

The passwords can be changed via the web interface using the "Passwords" tab on the "System Parameters" page. The passwords can be changed independently – if only one password is modified, the other password will remain unchanged.

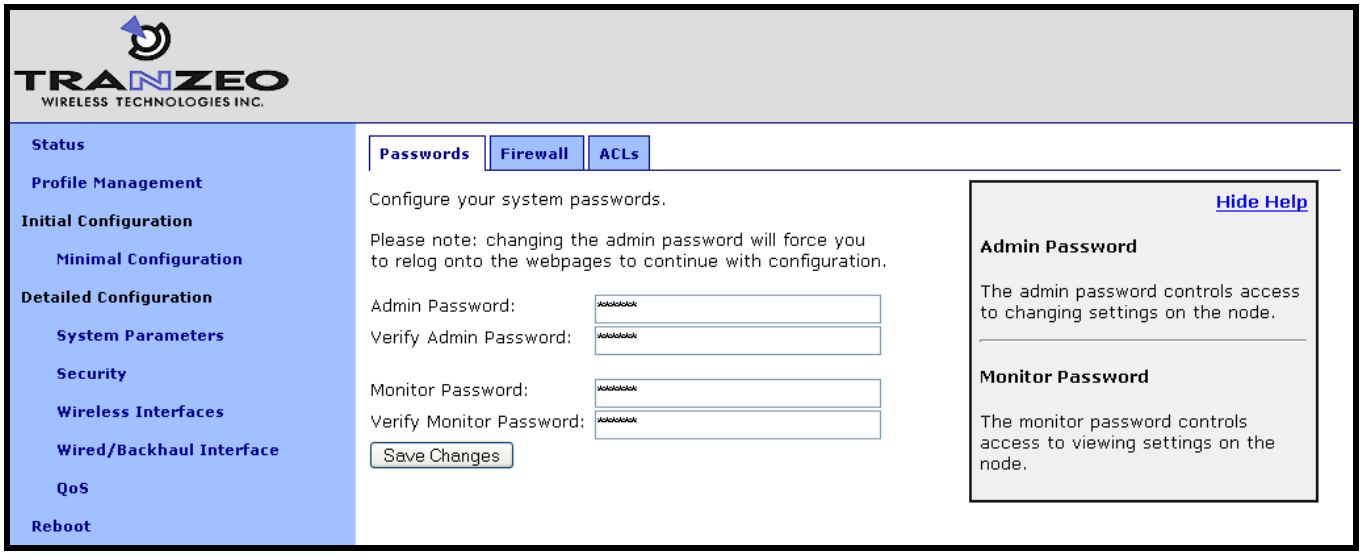

Figure 16. Passwords page

6.2 Operating Scheme

The operating scheme determines a node's role in the mesh network. Typically one of two configurations will be used in a network:

- All EnRoute500s will be configured as repeater nodes to create a stand-alone mesh cluster
- At least one of the EnRoute500s in a mesh cluster will be configured as a gateway node, with the remaining nodes configured either as gateways or repeaters. The gateway nodes are connected to an external network using the nodes' Ethernet interfaces. This network configuration will create an Internet extension network.

Mode	Description	Ethernet interface
Repeater	The EnRoute500 will function as a relay in the mesh network. Client devices can connect to the node using both wired (10/100 Ethernet) and wireless (built-in APs) interfaces. The node can provide IP addresses to clients on both the wired and wireless interfaces.	Client devices can connect to it. IP addresses can be provided to client devices using DHCP or be manually configured.
Gateway	The EnRoute500 will function as a relay in the mesh network and a gateway to a WAN. Client devices can only connect to the node using the wireless (built-in APs) interfaces. The node can provide IP addresses to clients on the wireless interface.	Used to connect the mesh cluster to a larger network. Will expect to be provided an IP address by a DHCP server or have a static IP address assigned to it.

Table 5. EnRoute500 operating schemes

CLI

The EnRoute500's operating scheme is set with the 'scheme' parameter in the 'sys' interface. Valid values are 'apgateway' and 'aprepeater'. For example, set the operating scheme to gateway mode with:

```
> use sys
sys> set scheme=apgateway
```

Web GUI

The operating scheme can be set via the web interface using the "System" tab on the "System Parameters" page.

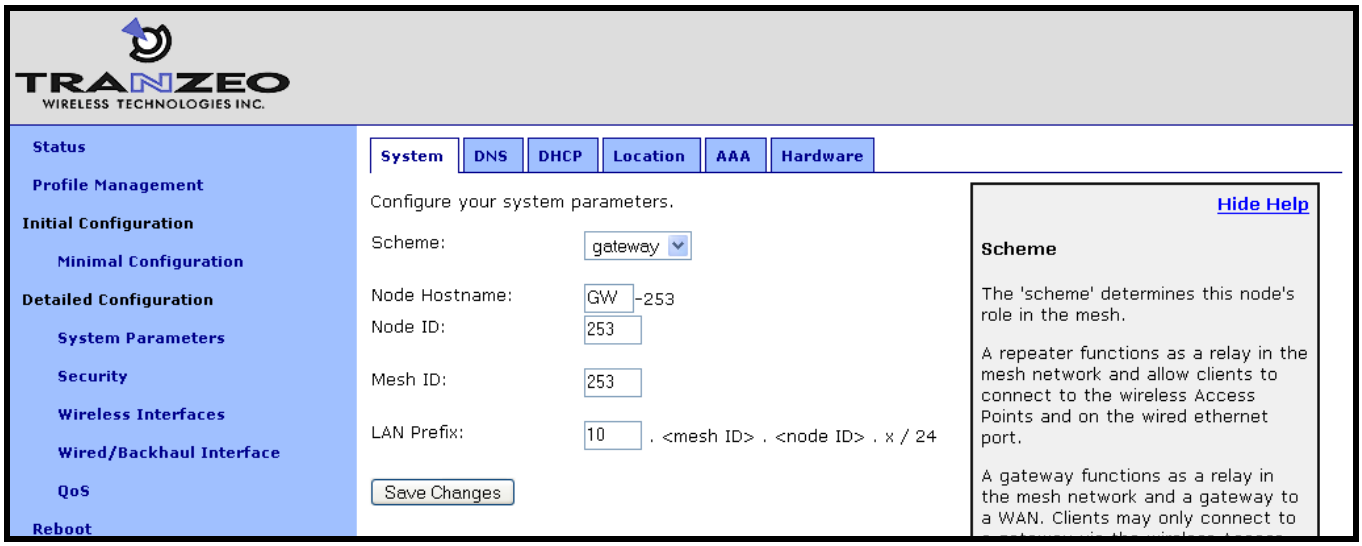

Figure 17. Setting the operating scheme

6.3 Mesh / Node ID

An EnRoute500 must be assigned mesh and node IDs before it is deployed as part of a mesh cluster. Together, these values uniquely identify a node within a mesh cluster and no two nodes in a cluster are allowed to have the same node ID.

The mesh ID must be the same for all nodes in a cluster The range of valid mesh IDs is 0 through 254.

The node ID is part of the node's IP address as shown in Figure 18. The allowable range for node IDs is 1 through 254.

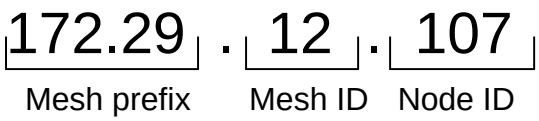

Figure 18. EnRoute500 mesh interface IP address

CLI

The mesh ID is set with the 'id.mesh' parameter in the 'sys' interface as shown below.

```
> use sys
sys> set id.mesh=12
```

The node ID is set with the 'id.node' parameter in the 'sys' interface as shown below.

```
> use sys
sys> set id.node=107
```

Web GUI

The mesh and node IDs can be set via the web interface using the "System" tab on the "System Parameters" page.

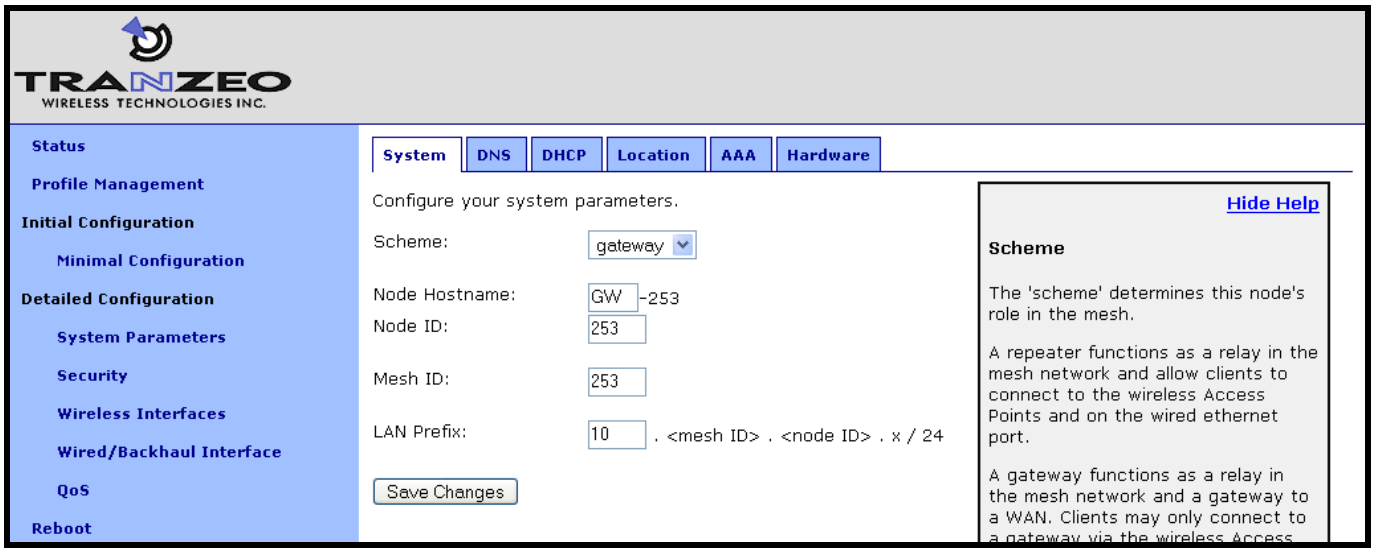

Figure 19. Setting the mesh and node IDs

6.4 Mesh Prefix

The mesh prefix parameter sets the first two octets of a node's mesh interface IP address. It must be set the same for all nodes in a given mesh cluster. The allowed range of values is 172.16 through 172.29.

It is recommended that the mesh prefix is not changed from its default value 172.29.

CLI

The mesh prefix is set with the 'id.meshprefix' parameter in the 'sys' interface as shown in the example below.

```
> use sys
sys> set id.meshprefix=172.29
```

Web GUI

The mesh prefix can be set via the web interface using the "Mesh" tab on the "Wireless Interfaces" page.

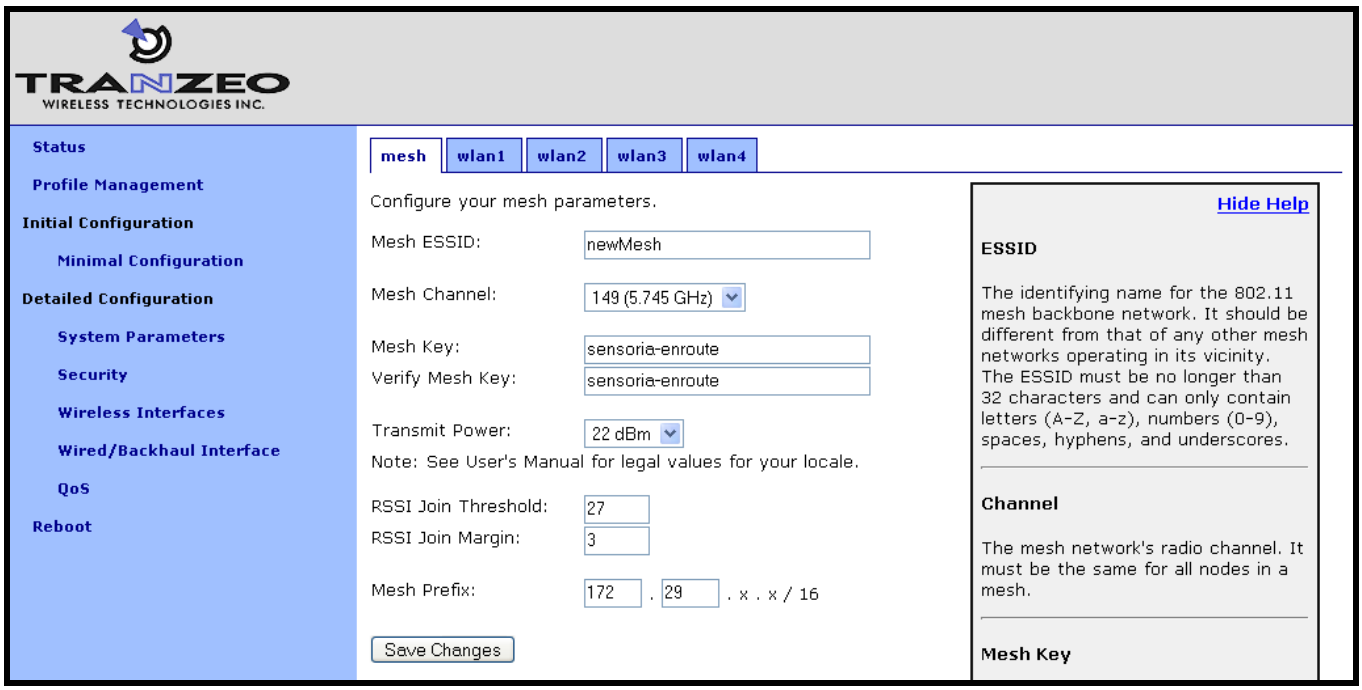

Figure 20. Setting the mesh prefix

6.5 LAN Prefix

A Class C subnet is shared between a EnRoute500's access point and Ethernet interfaces. The subnet address space is based on the mesh ID, node ID, and LAN prefix. The suggested values for the LAN prefix are 10 and 192. The LAN prefix must be the same for all nodes in a mesh cluster.

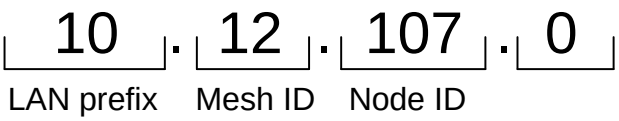

Figure 21. Subnet address structure

By default the subnet is split between a node's interfaces as shown in Table 6. See sections 8.1.4 and 9.6.3 for instructions on how to adjust how the subnet is segmented between interfaces.

Interface	Interface address	Broadcast address	Client address range
wlan1	subnet.1	subnet.127	subnet.2-126
wlan2	subnet.129	subnet.159	subnet.130-158
wlan3	subnet.161	subnet.191	subnet.162-190
wlan4	subnet.193	subnet.223	subnet.194-222
eth0	subnet.225	subnet.255	subnet.226-254

subnet = <id.lanprefix>.<id.mesh>.<id.node>

Table 6. Default subnet segmentation between interfaces

CLI

The LAN prefix is set with the 'id.lanprefix' parameter in the 'sys' interface as shown in the example below.

```
> use sys
sys> id.lanprefix=10
```

Web GUI

The LAN prefix can be set via the web interface using the "System" tab on the "System Parameters" page (see Figure 19).

6.6 DNS / Domain Settings

At least one DNS server must be specified for a node to be able to resolve host names. This DNS server is also provided to client devices that acquire an IP address from the local DHCP server on a node.

If a gateway node acquires DNS server information through DHCP, this DNS server information will overwrite the 'dns.servers' setting. Note that the DNS server settings will not be passed to repeater nodes that are in the same mesh cluster that the gateway is serving – you will need to set this on each of the repeater nodes.

CLI

The DNS server(s) used by the node are specified with the 'dns.servers' parameter in the 'sys' interface. To specify multiple DNS servers, list them as a space-delimited string enclosed by quotes as shown in the example below

```
> use sys
sys> set dns.servers ="10.5.0.5 192.168.5.5"
```

Web GUI

A primary and secondary DNS server can be set via the web interface using the "DNS" tab on the "System Parameters" page.

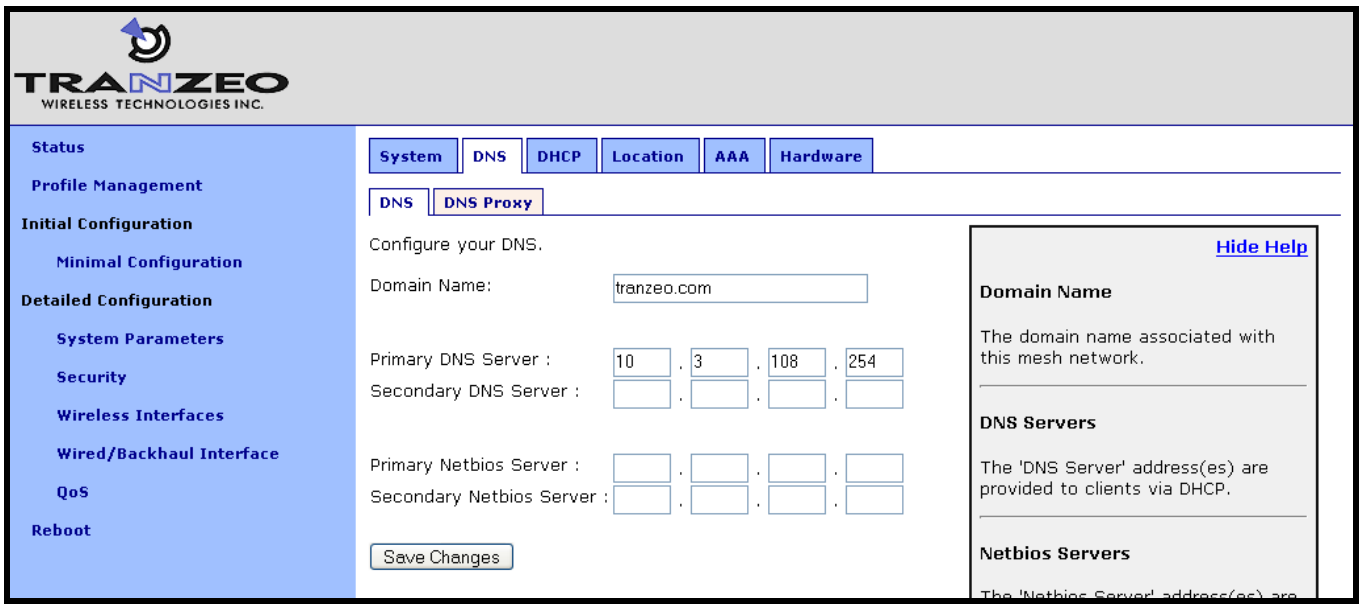

Figure 22. Setting the DNS server(s)

6.7 DNS Proxy Configuration

DNS proxy entries can be added to an EnRoute500 to force local resolution of host names to IP addresses.

CLI

A list of hostname/IP address to be resolved locally can be specified using the 'dnsproxy.hosts' parameter in the 'sys' interface. If multiple hostname/IP address entries are specified, they must be separated by semi-colons, as shown in the example below. DNS proxying must be explicitly enabled using the 'dnsproxy.enable' parameter in the 'sys' interface after the list of hosts has been specified.

```
> use sys
sys> set dnsproxy.enable=yes
> use sys
sys> set dnsproxy.hosts="server1.domain.com=10.0.0.1;server2.domain.com=10.0.0.129"
```

Web GUI

DNS proxying can be enabled through the Web GUI as shown in Figure 23. Hostname/IP address pairs can be added through the web interface as well.

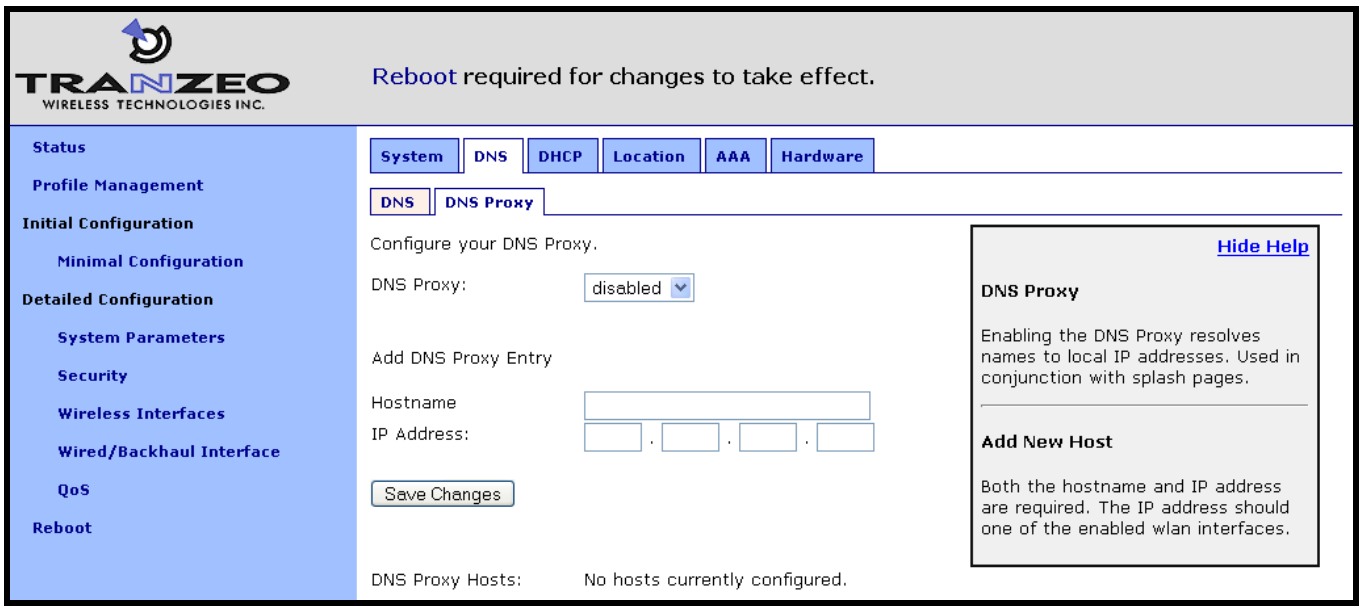

Figure 23. Configuring DNS proxying

6.8 NetBIOS Server

The NetBIOS server parameter is used to define a NetBIOS server IP address that is provided to client devices by the local DHCP server.

CLI

The NetBIOS server is set with the 'netbios.servers' parameter in the 'sys' interface. To specify multiple NetBIOS servers, list them as a space-delimited string enclosed by quotes as shown in the example below

```
> use sys
sys> set netbios.servers ="10.6.0.5 192.168.6.5"
```

Web GUI

A primary and secondary NetBIOS server can be set via the web interface using the "DNS" tab on the "System Parameters" page.

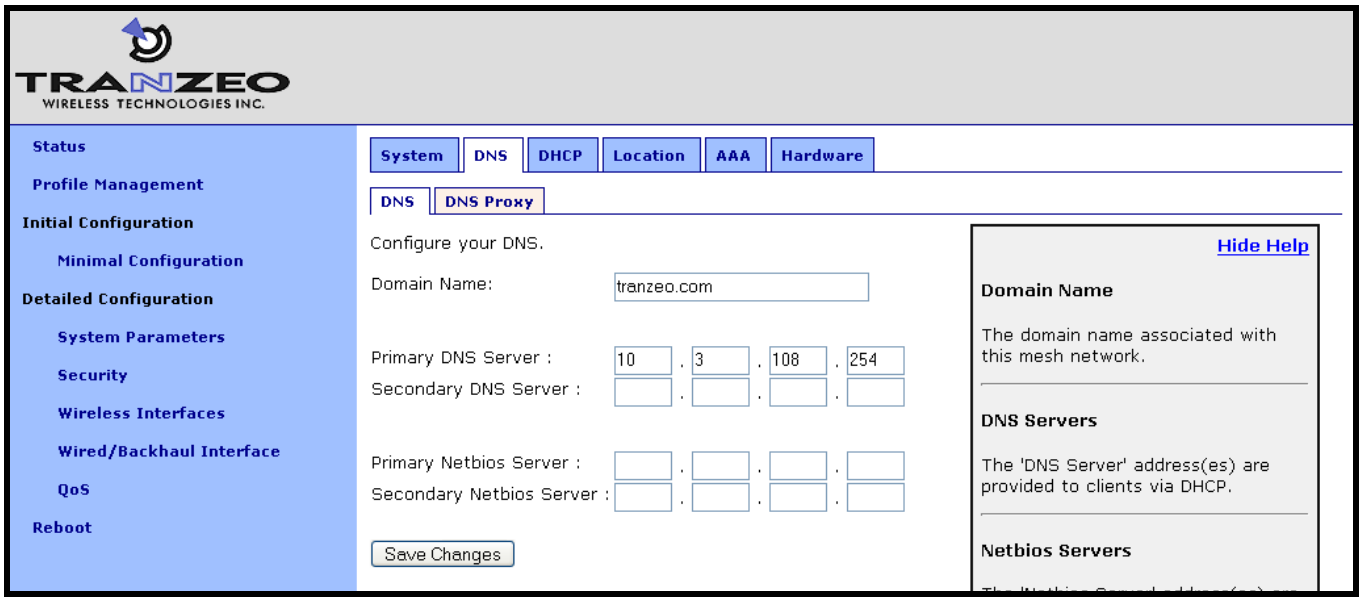

Figure 24. Setting the NetBIOS server(s)

6.9 Location

Two types of node location information can be stored:

- Latitude/longitude/altitude
- Postal address or description a node's location

Note that these values are not automatically updated and must be entered after a node has been installed. Altitude is in meters. Latitude and longitude must be given in geographic coordinates, with latitude ranging from -90 to 90 (with negative being south, positive being north) and longitude ranging from -180 to 180 (with negative being west, positive being east).

CLI

The GPS location of the node can be stored in the following fields in the 'sys' interface:

- sys.location.gps.altitude
- sys.location.gps.latitude
- sys.location.gps.longitude

For example, you can set the latitude value as follows.

```
> use sys
sys> set location.gps.latitude="34.01"
```

A description of the node's location can be stored in the 'location.postal' field in the 'sys' interface. For example, you can set the location value as shown below.

```
> use sys
sys> set location.postal="Light post near 123 Main St., Anytown, CA"
```

Web GUI

The location information can be set via the web interface using the "Location" tab on the "System Parameters" page.

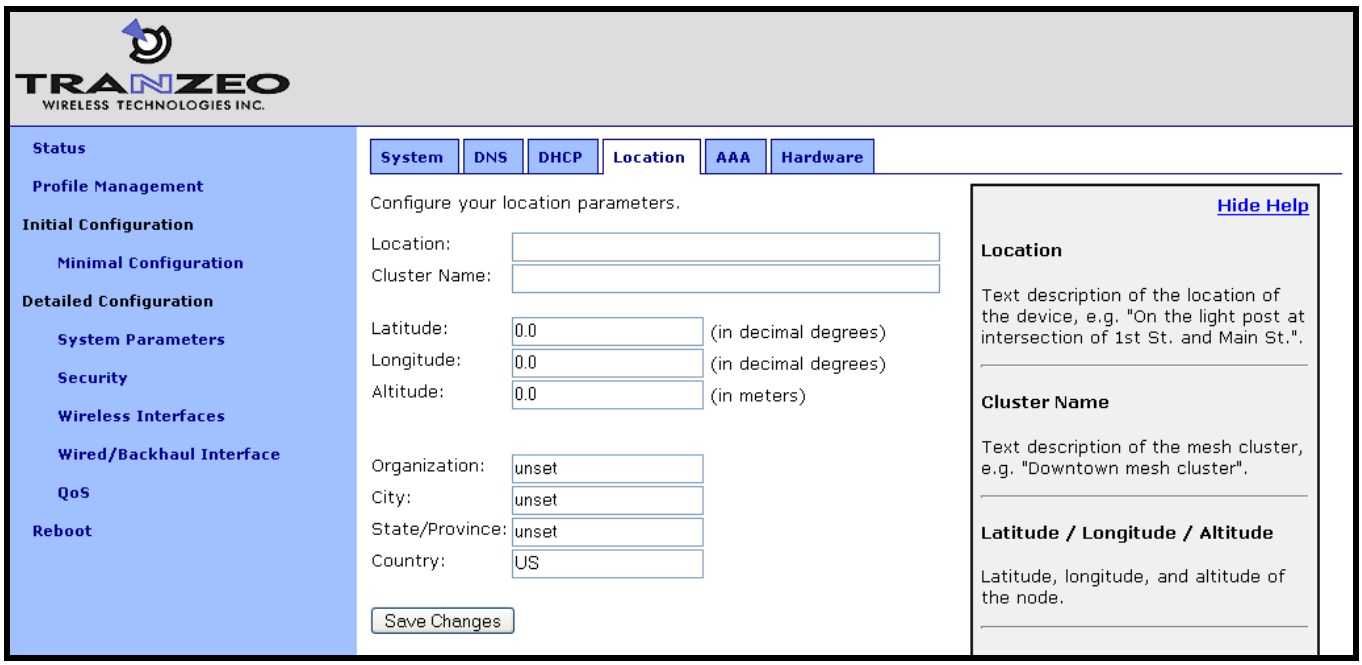

Figure 25. Setting location information

6.10 Certificate Information

A certificate for use with splash pages and the web interface is locally generated on the node. The information embedded in this certificate can be defined by the user. A new certificate is automatically generated when any of the following parameters are changed.

CLI

The information used in certificate generation can be set using the 'organization' parameters in the 'sys' interface. These parameters are:

- sys.organization.name –name of organization (must be enclosed in quotes if it contains spaces)
- sys.organization.city – city name (must be enclosed in quotes if it contains spaces)

- sys.organization.state – state name
- sys.organization.country – two-letter country abbreviation

Web GUI

The certificate information can be set via the web interface using the "Location" tab on the "System Parameters" page.

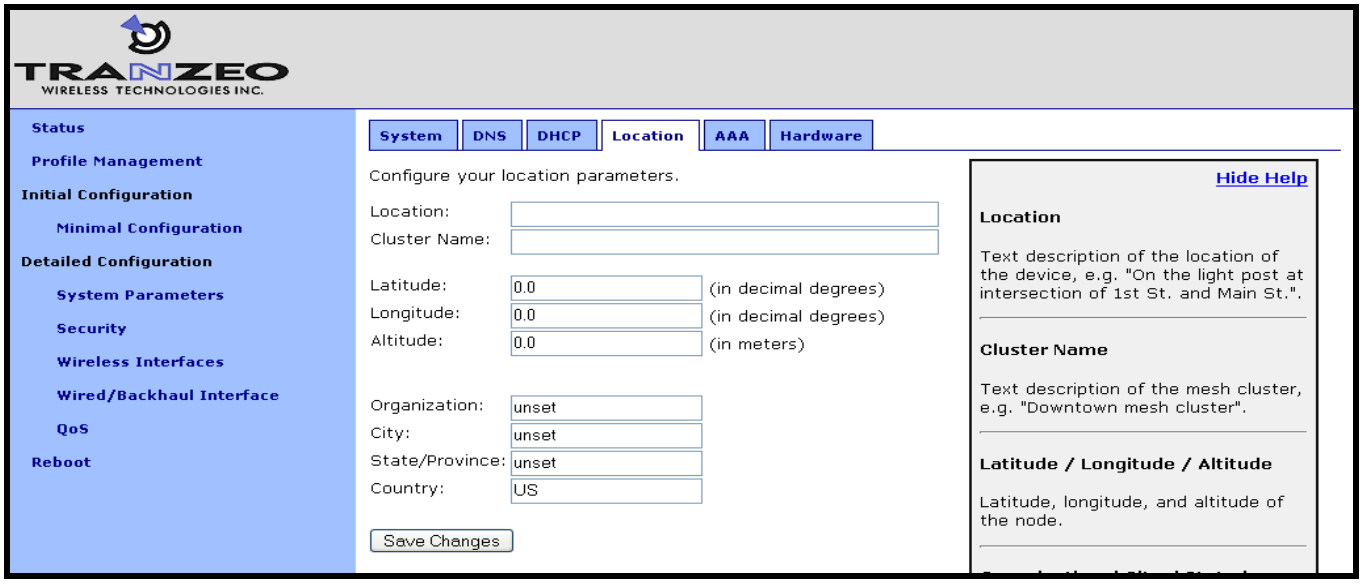

Figure 26. Setting certificate information

6.11 CLI timeout

The CLI will automatically log out a user if the interface has remained inactive for a certain length of time. The time, in seconds, that a shell must remain inactive before a user is automatically logged out is set with the 'shell.timeout' parameter in the 'sys' interface, as shown in the example below. The maximum idle time that can be set is 21600 seconds (360 minutes).

```
> use sys
sys> set shell.timeout=300
```

7 Mesh Radio Configuration

The EnRoute500 has an 802.11a radio dedicated to mesh backhaul traffic. The settings for this radio are independent of any settings for the radio used for the EnRoute500's built-in access points. The majority of the mesh radio settings must be the same on all nodes in a given mesh cluster for the nodes to be able to communicate.

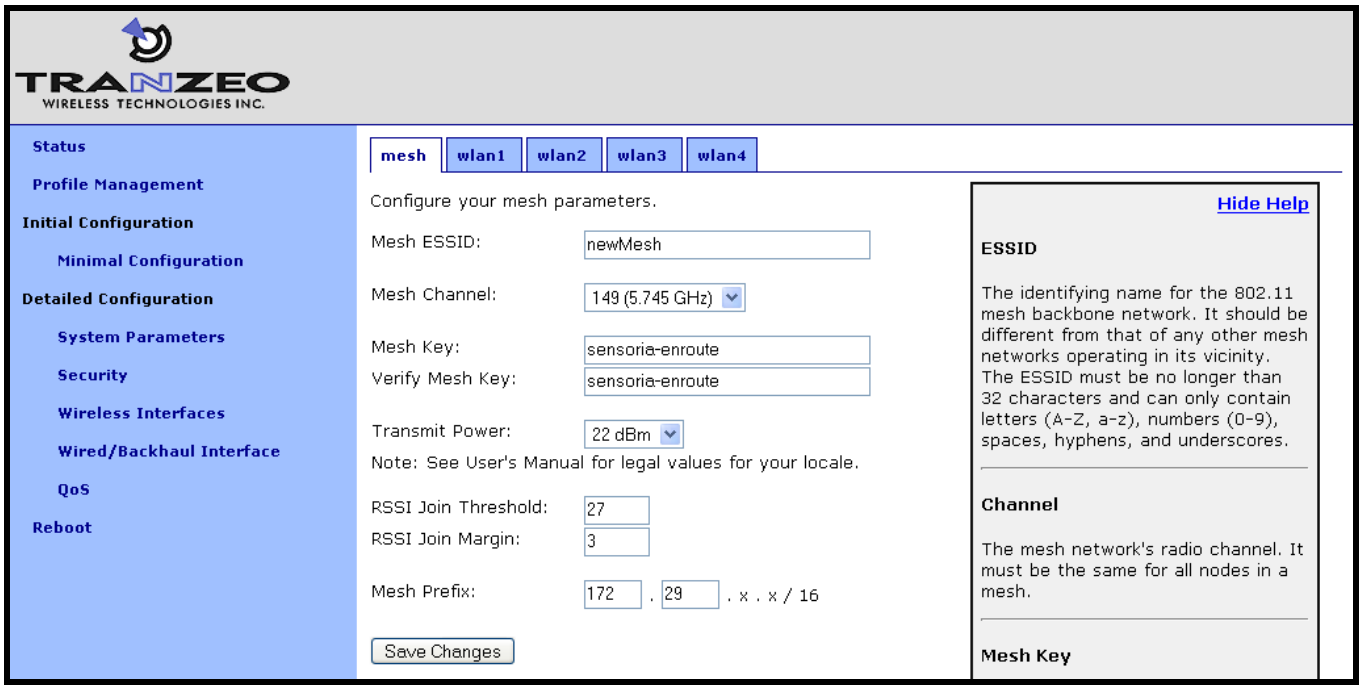

Figure 27. Mesh interface parameters

7.1 Channel

The 802.11a radio can be set to operate in the channels listed in Table 7. All these channels are non-overlapping.

Channel	Center Frequency (GHz)
149	5.745
153	5.765
157	5.785
161	5.805
165	5.825

Table 7. Mesh radio channels and frequencies

All the nodes in a mesh cluster need to be configured to use the same 802.11a channel.

CLI

The mesh radio channel is set with the 'channel' parameter in the 'mesh' interface as shown in the example below.

```
> use mesh0
mesh0> set channel=157
```

Web GUI

The mesh radio channel can be set via the web interface using the "Mesh" tab on the "Wireless Interfaces" page (see Figure 27).

7.2 Service Set Identifier (SSID)

The Service Set Identifier, or SSID, is used in 802.11 communication to identify a particular network. It differentiates logical networks that operate on the same radio channel. The mesh radio SSID for all the nodes in a mesh cluster must be the same. If you have adjacent mesh clusters where one or more nodes from each cluster are within communication range of each other, the SSID for the clusters must be different.

The SSID value must be a text string that has a maximum length of 32 characters. It must only contain alphanumeric characters, spaces, dashes ("-"), and underscores ("_"). The SSID setting is case sensitive.

It is possible to hide the mesh SSID by restricting it from being broadcast. You will generally want the mesh SSID to be hidden, and it is hidden by default.

CLI

The mesh radio SSID is set as shown in the example below. When setting an ESSID that contains spaces, the SSID value must be enclosed by quotes. The quotes are optional otherwise.

```
> use mesh0
mesh0> set essid="enroute500_mesh"
```

The broadcast of the SSID can be controlled with the 'hide_essid' parameter in the 'mesh0' interface. The example below shows how hiding of the SSID can be enabled.

```
> use mesh0
mesh0> set hide_essid=yes
```

Web GUI

The mesh radio SSID and its broadcast state can be set via the web interface using the "Mesh" tab on the "Wireless Interfaces" page (see Figure 27).

7.3 Encryption

The mesh radio link can be protected with an encryption key to prevent unauthorized users from intercepting or spoofing mesh traffic. Each node in a mesh cluster must have the same encryption key.

CLI

To enable encryption, set the 'key' parameter in the 'mesh0' interface. The examples below illustrate how to set the encryption key. The 'key' parameter can either be specified as a 16-character ASCII string preceded by "s:" or a 32-character hexadecimal string.

Encryption can be enabled using an ASCII key with

```
> use mesh0
mesh0> set key="s:abcdefghijklmnop"
```

or using a hexadecimal key with

```
> use mesh0
mesh0> set key="0123456789abcdef0123456789abcdef"
```

Encryption can be disabled by specifying a blank value as shown below.

```
> use mesh0
mesh0> set key=
```

Web GUI

The mesh radio encryption key can be set via the web interface using the "Mesh" tab on the "Wireless Interfaces" page (see Figure 27). The same encryption key must be entered in both the "Mesh Key" and "Verify Mesh Key" text boxes for the new key to be accepted.

Only ASCII keys can be entered using the web interface. Unlike the CLI, an ASCII key should not be preceded by "s:"

7.4 Transmit Power

The transmit power of the mesh radio is configurable. Increased output power will improve communication range, but will also extend the interference range of the radios. It is suggested that the transmit power is initially set to the maximum level for an installation and is then reduced if it is determined that the transmit power far exceeds the level required to maintain links. It is also recommended that a common transmit power value is used for all nodes in a mesh to reduce the likelihood of asymmetric links. The default transmit power is 22dBm.

The mesh radio's transmit power value must be less than the default value to be in compliance with FCC regulations. Setting a value greater than the default power is prevented by the software.

CLI

The example below shows how to set the mesh radio's transmit power with the 'txpower' parameter in the 'mesh0' interface . Note that the parameter specified in the CLI is not in dBm. Refer to Table 8 for converting between CLI parameter values and dBm.

```
> use mesh0
mesh0> set txpower=33
```

txpower	Output Power (dBm)
1	9
9	10
14	12
18	14
22	16
26	18
29	20
33	22

Table 8. Mesh radio output power settings in the CLI

Web GUI

The mesh radio transmit power can be set via the web interface using the "Mesh" tab on the "Wireless Interfaces" page (see Figure 27).

7.5 RSSI Threshold Levels

The mesh networking algorithm evaluates link qualities to neighboring mesh nodes and only considers links with a received signal strength indicator (RSSI) value equal to or greater than

the 'RSSI Join' value specified to be usable. The 'RSSI Join' value is set to 27 by default. This value reflects the lowest RSSI that will allow the mesh radio to operate at its highest data rate. It is possible to achieve longer link ranges, at the cost of reduced throughput, by reducing the 'RSSI Join' value.

In combination with the 'RSSI Join' value, the 'RSSI Margin' value is used to set the RSSI level at which links are dropped. A link will be considered broken when its RSSI drops below the 'RSSI Join' level by the amount specified with 'RSSI Margin'. For example, with an 'RSSI Join' value of 27 and an 'RSSI Margin' value of 3, the link will be dropped if the RSSI goes below 24.

CLI

The example below shows how to set the mesh radio's RSSI thresholds with the 'fabric.rssi.join' and 'fabric.rssi.margin' parameters in the 'mesh0' interface .

```
> use mesh0
mesh0> set fabric.rssi.join=27
> use mesh0
mesh0> set fabric.rssi.margin=3
```

Web GUI

The mesh radio RSSI thresholds can be set via the web interface using the "Mesh" tab on the "Wireless Interfaces" page (see Figure 27).

7.6 IP Configuration

The IP address, broadcast address, and netmask associated with the mesh radio interface can be viewed through the CLI and the web GUI interfaces. It is not possible to directly set these values though. To change the mesh interface IP settings, the node and mesh ID settings must be changed (see sections 6.3 and 6.4).

CLI

In the CLI, the mesh IP settings can be viewed with

```
> use mesh0
mesh0> get ip.address
 ip.address = 172.29.2.4   [read-only]
mesh0> get ip.broadcast
 ip.broadcast = 172.29.255.255   [read-only]
mesh0> get ip.gateway
 ip.gateway =    [read-only]
mesh0> get ip.netmask
 ip.netmask = 255.255.0.0   [read-only]
```

Web GUI

The mesh radio IP settings are available through the web interface on the "Status" page.

7.7 Neighbor Status

Information on mesh neighbors is provided on the mesh status page of the web GUI, accessible under the 'Status' tab on the 'Status' page. The signal strength of each mesh neighbor device, it's MAC address, its IP address, and the time since data was last received from it are listed. A sample of the mesh neighbor status page is shown in Figure 28.

The minimum RSSI required for a link to be established and maintained are set with the 'RSSI Join' and 'RSSI Margin' parameters (see section 7.5).

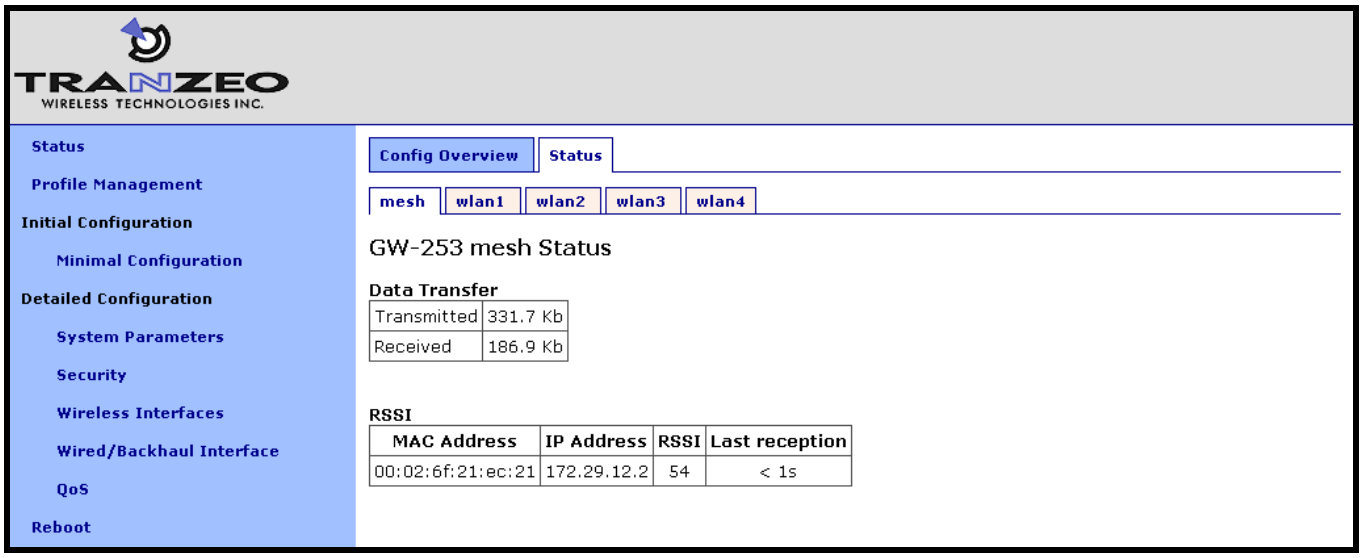

Figure 28. Mesh neighbor status information

8 Ethernet Interface Configuration

The function of the Ethernet interface (eth0) depends on the operating scheme that has been selected (see section 6.2). In repeater mode, the Ethernet interface can be used to connect client devices to the mesh cluster. In gateway mode, the Ethernet interface is used as a backhaul interface that connects the mesh cluster to a WAN. Client devices cannot connect through the Ethernet interface in this mode.

8.1 IP Configuration for Repeater Nodes and Their Clients

When an EnRoute500 is configured as a repeater, client devices can connect to it via the Ethernet interface to access the mesh network. These client devices can either be assigned their IP configuration using DHCP or be manually configured.

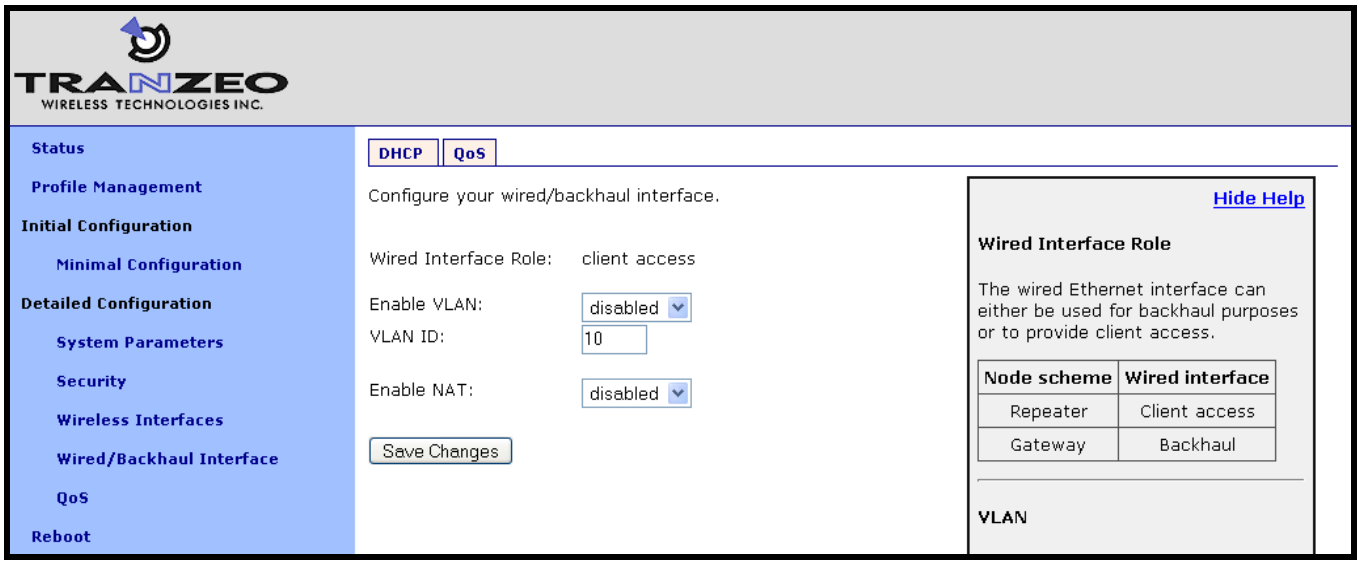

Figure 29. Wired interface parameters with EnRoute500 in repeater mode

8.1.1 Ethernet Client Device Address Space

The Ethernet interface, when the node is in repeater mode, is assigned a segment of the class C address space that each node has to share between its client interfaces, which include eth0, wlan1, wlan2, wlan3, and wlan4. The start address of the address segment and its size can be set with the IP address range start address and size parameters. The following restrictions are placed on the address segment configuration:

- Each active client interface must be assigned an address segment.

- The IP address range start address ('ip.start.requested' in the CLI) must be one of the following values: 1, 33, 65, 97, 129, 161, 193, 225.
- The IP address range size ('ip.size.requested' in the CLI) must be one of the following values: 31, 63, 127, 255.
- The IP address range size and start address must be chosen such that the address segment does not cross a netmask boundary. Table 9 lists allowed combinations.
- The address spaces for enabled interfaces must start at different addresses.
- The address spaces for enabled interfaces should not overlap.

	ip.size.requested			
ip.start.requested	**31**	**63**	**127**	**255**
1	Yes	Yes	Yes	Yes
33	Yes	No	No	No
65	Yes	Yes	No	No
97	Yes	No	No	No
129	Yes	Yes	Yes	No
161	Yes	No	No	No
193	Yes	Yes	No	No
225	Yes	No	No	No

Table 9. Allowed address segment start address and size combinations

Each of the enabled interfaces' address segments should be configured to avoid overlap with the other interfaces' address segments. In the case where a node is not configured such that this requirement is met, address spaces will be automatically reduced in size to prevent overlap.

CLI

In the first example below, the Ethernet interface is set to use the entire class C address space (this requires that all the other client interfaces, wlan1-4, are disabled). In the second example, the Ethernet interface is set to use the upper half of the class C address space.

```
> use eth0
eth0> set ip.start.requested=1
eth0> set ip.size.requested=255

> use eth0
eth0> set ip.start.requested=129
eth0> set ip.size.requested=127
```

The actual start address and size of a segment are accessible via the 'ip.start.actual' and 'ip.size.actual' parameters.

Web GUI

The eth0 address segment start address and size can be set via the web interface using the "DHCP" sub-tab on the "DHCP" tab on the "System Parameters" page (see Figure 30).

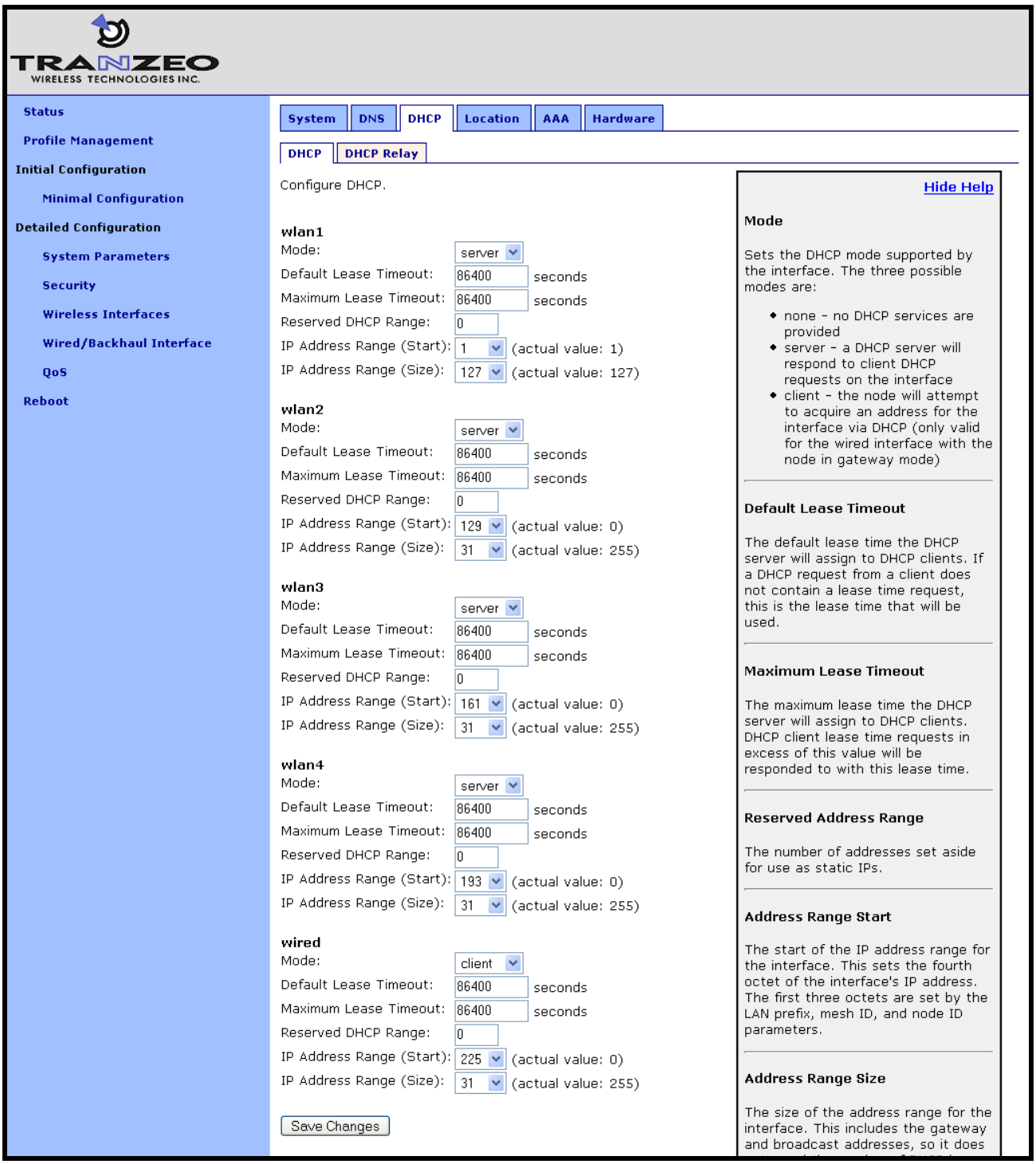

Figure 30. 'eth0' DHCP and address space settings

8.1.2 Ethernet Interface IP Address

The EnRoute500's Ethernet interface IP address should not be changed directly when it is in repeater mode. To set the IP address to the desired value, modify the node ID, mesh ID, and LAN prefix parameters (see sections 6.3 and 6.5).

CLI

You can view the IP settings for the Ethernet interface with the 'ip.*' parameters in the 'eth0' interface as shown in the example below.

```
> use eth0
eth0> get ip.*
 ip.address = 10.2.4.225   [read-only]
 ip.address_force =
 ip.broadcast = 10.2.4.255   [read-only]
 ip.broadcast_force =
 ip.gateway =    [read-only]
 ip.gateway_force =
 ip.netmask = 255.255.255.0   [read-only]
 ip.netmask_force =
 ip.size.actual =    [read-only]
 ip.size.requested = 31
 ip.start.actual =    [read-only]
 ip.start.requested = 225
```

When the node is in repeater mode, the Ethernet IP settings can be changed by altering the 'id.node', 'id.mesh', and 'id.lanprefix' parameters in the 'sys' interface and the 'ip.start.requested' parameter in the 'eth0' interface

Web GUI

The Ethernet IP settings are available through the web interface on the "Status" page. The Ethernet IP settings can be changed by altering the node ID, mesh ID, and LAN prefix settings on the "System" parameters tab on the "System Parameters" page.

8.1.3 IP Configuration of Client Devices via DHCP

When configured as a repeater, the EnRoute500 can be set to serve IP addresses to clients on the Ethernet interface using DHCP. Two distinct modes for providing IP addresses via DHCP exist. These are described in depth in section 10.

8.1.4 Manual IP Configuration of Client Devices

The client devices connected via the Ethernet interface that use static IP addresses must have addresses that are within the subnet of the Ethernet interface.

If the local DHCP server is enabled for the Ethernet interface, IP addresses must be reserved for statically-configured devices by setting the DHCP reserve parameter. This will reserve the specified number of IP addresses at the bottom of the IP range for the interface. For example, if the interface has been assigned the IP address 10.2.4.225, the netmask 255.255.255.224, and the DHCP reserve value 5, the IP addresses 10.2.4.226 through 10.2.4.230 will be available for use by statically configured devices. The remaining IP addresses in the interfaces address space can be assigned by the DHCP server to other client devices.

CLI

The number of IP addresses reserved for statically-configured devices connected to the Ethernet interface is set with the 'dhcp.reserve' parameter in the 'eth0' interface.

Web GUI

The DHCP reserve value can be set via the web interface using the "DHCP" sub-tab on the "DHCP" tab on the "System Parameters" page (see Figure 30).

8.2 IP Configuration for Gateway Nodes

When an EnRoute500 is configured as a gateway, the Ethernet interface is used to provide backhaul capability by connecting it to a WAN or directly to the Internet. Clients cannot connect to the EnRoute500 through the Ethernet interface when operating in this mode. The Ethernet interface IP address can either be acquired from a DHCP server on the WAN or be set manually.

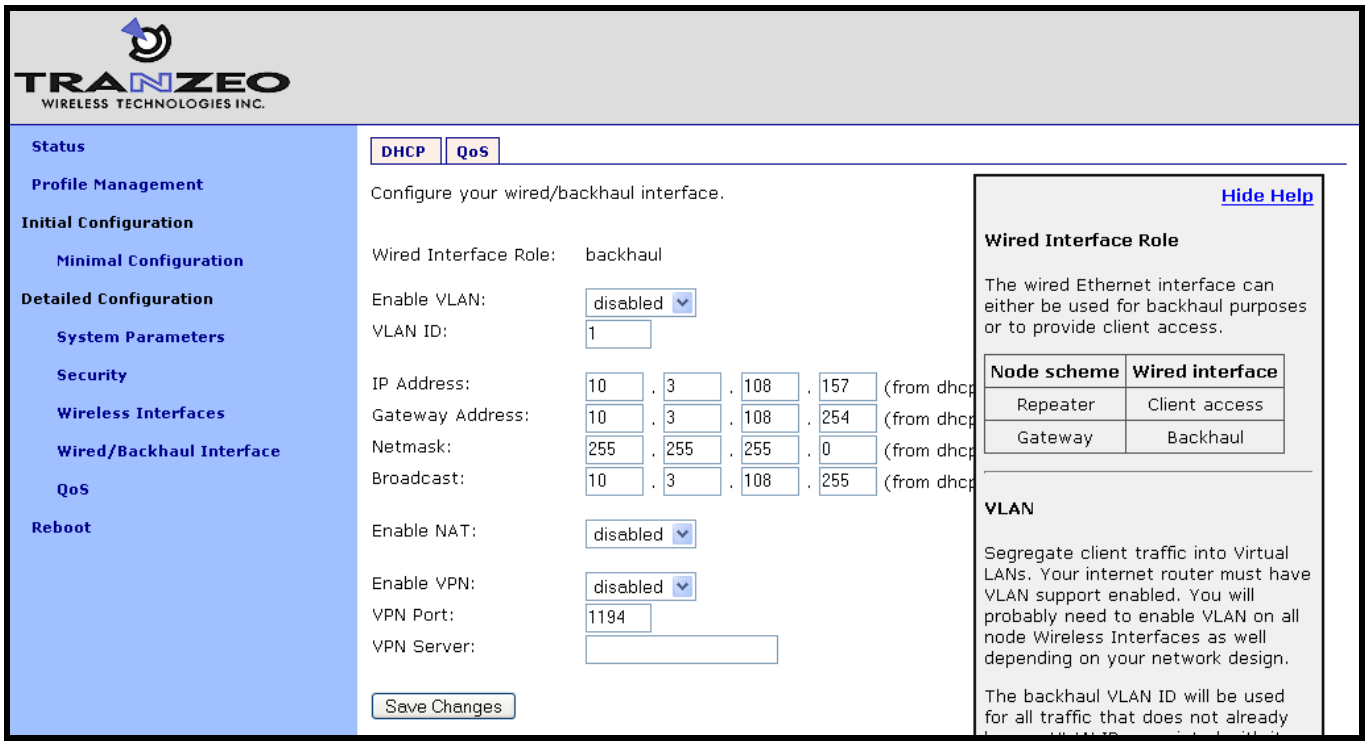

Figure 31. Wired interface parameters with EnRoute500 using wired interface for backhaul

8.2.1 DHCP

When configured as a gateway, the EnRoute500 can be set to obtain an obtain an IP address for its Ethernet interface using DHCP. To enable the DHCP client mode on the Ethernet interface, set the value of the Ethernet DHCP role parameter to 'client'. When configured as a DHCP client, the EnRoute500 will continually attempt to contact a DHCP server until it is successful.

INFO

The DHCP reserve parameter (described in section 6.1.1) has no effect when the DHCP role parameter is set to 'client'.

To disable Ethernet DHCP client mode, set the DHCP role parameter to 'none'. If DHCP client mode is disabled, the IP configuration must be carried out manually, as described in the next section.

CLI

To enable the DHCP client mode on the Ethernet interface, set the value of the 'dhcp.role' parameter in the 'eth0' interface to 'client', as shown in the example below.

```
> use eth0
eth0> set dhcp.role=client
```

To disable Ethernet DHCP client mode, set the DHCP role parameter to 'none' as shown below.

```
> use eth0
eth0> set dhcp.role=none
```

Web GUI

The Ethernet DHCP role value can be set via the web interface using the "DHCP" sub-tab on the "DHCP" tab on the "System Parameters" page (see Figure 30).

8.2.2 Manual IP Configuration

When a node is configured as a gateway, there are no limitations imposed by the EnRoute500 on the IP address assigned to the Ethernet interface. If the Ethernet DHCP role parameter is set to 'none', the manually configured IP address will be used. The default IP configuration that is assigned to the interface based on the node and mesh ID settings is available through the CLI and the web GUI.

Note that for the manually configured IP address to be used, the Ethernet DHCP role setting must be set to 'none' if the node is connected to a network which provides access to a DHCP server.

The IP configuration settings shown in the 'eth0' interface in the CLI and on the "Wired/Backhaul Interface" page of the web interface do not necessarily reflect the current settings of the interface. They are the requested settings and do not take into account whether the interface has been configured via DHCP. If the Ethernet DHCP role parameter is set to 'client', the 'ip.address', ip.broadcast', 'ip.gateway', and 'ip.netmask' parameters will respond to a 'get' command with '<dhcp>' to indicate that the parameters will be assigned by a DHCP server instead of any values assigned via the CLI. Use the 'ifconfig eth0' command in the CLI or access the "Status" page in the web interface to get current interface settings.

CLI

The Ethernet default IP configuration is available through the following read-only parameters:

- ip.address – IP address
- ip.broadcast – IP broadcast address
- ip.gateway – default gateway
- ip.netmask – netmask

These parameters cannot be set though. These default parameters can be overridden with the parameters listed below.

- ip.address_force
- ip.broadcast_force
- ip.gateway_force
- ip.netmask_force

The example below, shows how a custom IP address can be set for the Ethernet interface

```
> use eth0
eth0> set dhcp=none
eth0> set ip.address_force=192.168.1.2
eth0> set ip.broadcast_force=192.168.1.255
eth0> set ip.gateway_force=192.168.1.1
eth0> set ip.netmask_force=255.255.255.0
```

Web GUI

When the node is in gateway mode, the Ethernet IP address, gateway, netmask, and broadcast address parameters can be set via the web interface using the "Wired/Backhaul Interface" page (see Figure 31). The current IP values can be viewed on the "Status" page.

9 Access Point (AP) Configuration

The EnRoute500 has an 802.11b/g radio dedicated to access point traffic. The settings for this radio are independent of any settings for the radio used for the mesh backhaul traffic. The settings for the access points can vary from node to node in the mesh, but typically it is desirable to set certain parameters to the same value for all the access points in a mesh to allow clients to roam seamlessly within the mesh network.

An EnRoute500 has four access points that can be configured to suit different application needs. With the exception of the 'wlanN.channel' parameter, all access point parameters can be configured independently of each other.

INFO

The interfaces for the access points will be referred to as 'wlanN' when it applies to all four access points. 'wlan1' will be used in all examples.

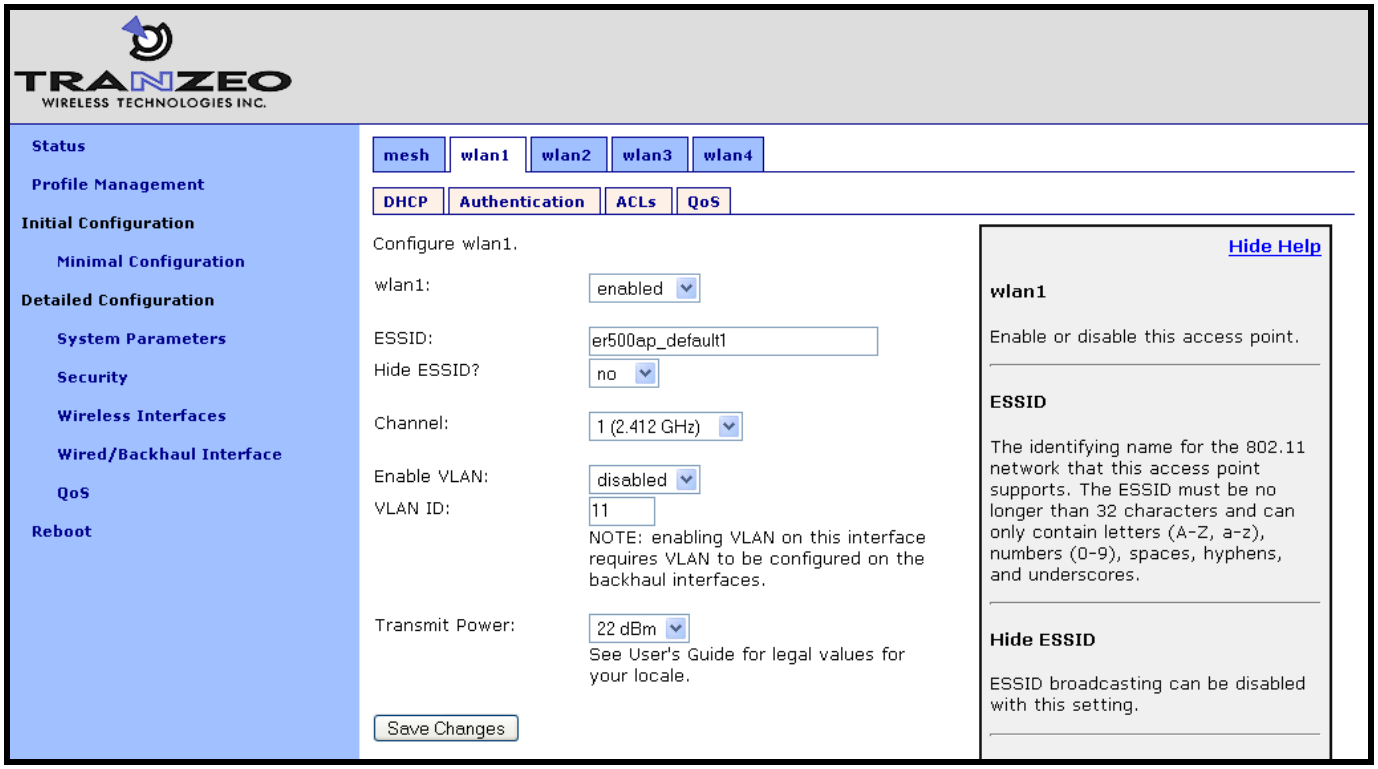

Figure 32. Access point interfaces

9.1 Access Point Interfaces

There are four access point interfaces that are used to configure the access points: wlan1, wlan2, wlan3, and wlan4. The access points have equivalent configuration capabilities and

there is no inherent prioritization or preference for one access point. The section on quality-of-service settings (section 13) describes how prioritization on a per-access point basis can be configured.

9.2 Enabling and Disabling Access Points

Access points can be individually enabled or disabled. An access point can be configured when it is disabled and parameter settings are retained when it is disabled.

CLI

An access point can be enabled with the 'enable' parameter in the 'wlanN' interface as shown below.

```
> use wlan1
wlan1> set enable=yes
```

An access point can be disabled with the following commands.

```
> use wlan1
wlan1> set enable=no
```

Web GUI

The access point status can be set via the web interface using the appropriate "wlanN" tab on the "Wireless Interfaces" page (see Figure 32).

9.3 Access Point Client Device Address Space

The enabled wlanN interfaces are assigned segments of the class C address space that each node has to share between its client interfaces, which include eth0, wlan1, wlan2, wlan3, and wlan4. The start address of the address segment and its size can be set with the IP address range start address and size parameters. The following restrictions are placed on the address segment configuration:

- Each active interface must be assigned an address segment.
- The IP address range start address ('ip.start.requested' in the CLI) must be one of the following values: 1, 33, 65, 97, 129, 161, 193, 225.
- The IP address range size ('ip.size.requested' in the CLI) must be one of the following values: 31, 63, 127, 255.
- The IP address range size and start address must be chosen such that the address segment does not cross a netmask boundary. Table 9 lists allowed combinations.
- The address spaces for enabled interfaces must start at different addresses.

- The address spaces for enabled interfaces should not overlap.

Each of the enabled interfaces' address segments should be configured to avoid overlap with the other interfaces' address segments. In the case where a node is configured such that this requirement is not met, address spaces will be automatically reduced in size to prevent overlap.

CLI

In the example below, the WLAN interfaces are set up to use the lower half of the class C address space. This assumes that the Ethernet interface is either used for gateway purposes or is assigned to an address segment in the upper half of the class C network.

```
> use wlan1
wlan1> set ip.start.requested=1
wlan1> set ip.size.requested=31
wlan1> use wlan2
wlan2> set ip.start.requested=33
wlan2> set ip.size.requested=31
wlan2> use wlan3
wlan3> set ip.start.requested=65
wlan3> set ip.size.requested=31
wlan3> use wlan4
wlan4> set ip.start.requested=97
wlan4> set ip.size.requested=31
```

The actual start address and size of a segment are accessible via the 'ip.start.actual' and 'ip.size.actual' parameters. These may differ from the requested values if incompatible requested values have been set for different interfaces.

Web GUI

The eth0 address segment start address and size can be set via the web interface using the "DHCP" sub-tab on the "DHCP" tab on the "System Parameters" page (see Figure 33).

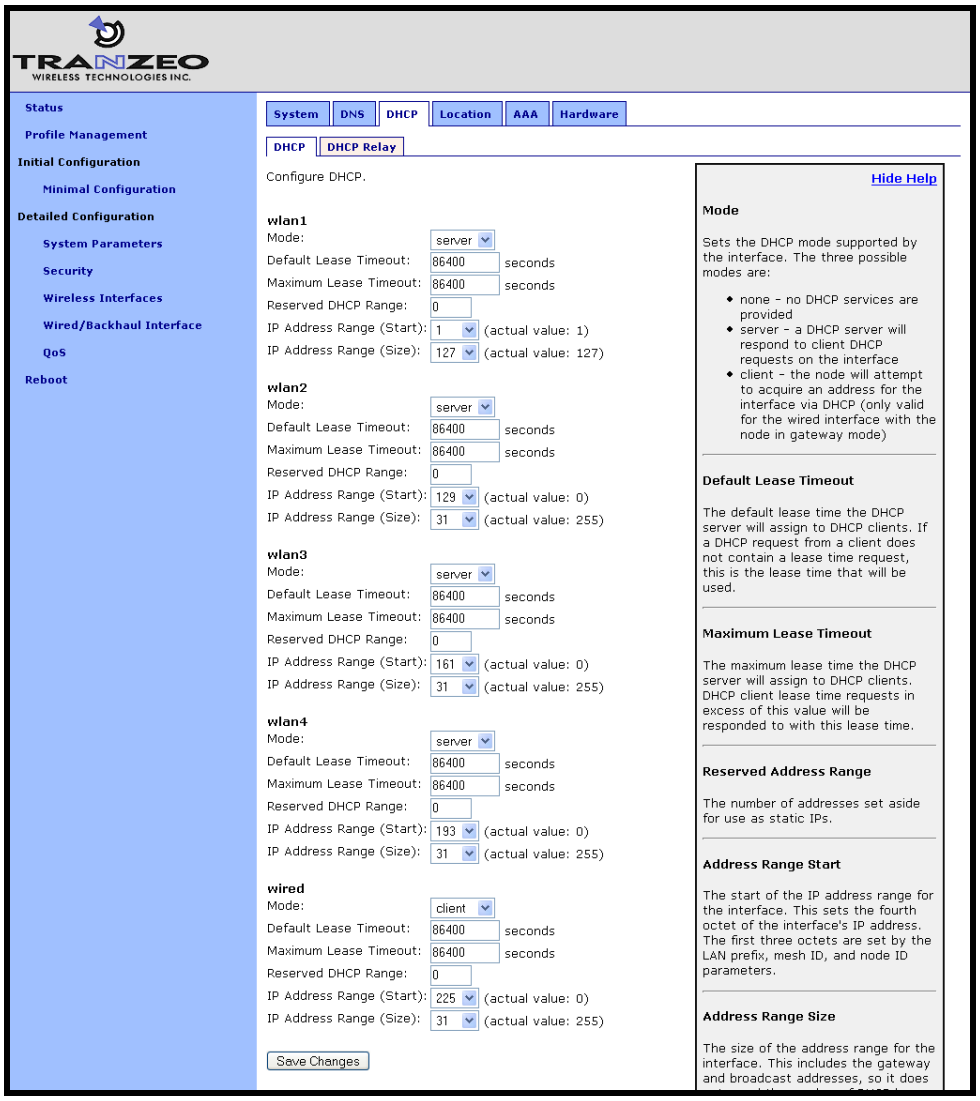

Figure 33. 'wlanN' DHCP and address space settings

9.4 Channel

The 802.11b/g radio can be set to operate in the channels listed in Table 10.

Channel	Center Frequency (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

Table 10. Access point channels and associated center frequencies

Note that only channels 1, 6, and 11 are non-overlapping.

It is not possible to configure access points to use different channels. If the channel for wlan2 is changed, the channel will be changed for wlan1, wlan3, and wlan4. However, different nodes in a mesh cluster can be set to use different access point channels in order to reduce co-channel interference.

CLI

The AP channel is set with the 'channel' parameter in the 'wlanN' interfaces. The example below shows how to set the AP channel to 6.

```
> use wlan1
wlan1> set channel=6
```

Web GUI

The access point channel can be set via the web interface using the appropriate "wlanN" tab on the "Wireless Interfaces" page (see Figure 32).

9.5 ESSID

The ESSID, or Extended Service Set Identifier, is used in 802.11 infrastructure networks to identify a particular network. It is used to differentiate logical networks that operate on the same channel.

INFO

Each access point can be configured with a different ESSID. This allows network traffic to be separated based on ESSID. Assigning unique ESSIDs to the access points in a mesh has the benefit of allowing a user to configure a client device to connect to a specific node in the mesh. Typically a mesh will be deployed with the access point ESSIDs having the same set of values for each EnRoute500 in order to support seamless roaming.

The ESSID value must be a text string that has a maximum length of 32 characters. It must only contain alphanumeric characters, spaces, dashes ("-"), and underscores ("_").The ESSID setting is case sensitive.

It is possible to hide an AP ESSID by restricting it from being broadcast. Whether it is appropriate for an AP ESSID to be hidden depends on the application.

CLI

The access point ESSID is set as shown in the example below. When setting an ESSID that contains spaces, the ESSID value must be enclosed by quotes – the quotes are optional otherwise.

```
> use wlan1
wlan1> set essid="wlan1_ap"
```

The broadcast of the ESSID can be controlled with the 'hide_essid' parameter in the 'wlanN' interface. The example below shows how hiding of the ESSID can be enabled.

```
> use wlan1
wlan1> set hide_essid=yes
```

Web GUI

The access point ESSIDs and its broadcast state can be set via the web interface using the appropriate "wlanN" tab on the "Wireless Interfaces" page (see Figure 32).

9.6 IP Configuration for Nodes and Their Clients

The access point interfaces allow client devices to connect to access the mesh network. The client devices can either be assigned their IP configuration using DHCP or be manually configured.

9.6.1 Access Point IP Address

The IP address, broadcast address, and netmask associated with an access point interface can be viewed, but not directly changed through the CLI or web GUI. To set the IP address to the desired value, modify the node ID, mesh ID, and LAN prefix parameters (see sections 6.3 and 6.5). You can view the resulting settings for the AP interface with either the CLI or the web GUI.

CLI

You can view the IP configuration settings for the AP interface with the 'ip.*' parameters in the 'wlanN' interface as shown in the example below.

```
> use wlan1

wlan1> get ip.address
 ip.address = 10.2.4.1
wlan1> get ip.broadcast
 ip.broadcast = 10.2.4.127
wlan1> get ip.gateway
 ip.gateway =
wlan1> get ip.netmask
 ip.netmask = 255.255.255.128
```

Web GUI

The access points' IP settings are available through the web interface on the "Status" page.

9.6.2 IP Configuration of Clients Devices via DHCP

The EnRoute500 can be set to serve IP addresses to clients on the access point interfaces using DHCP. Two distinct modes for providing IP addresses via DHCP exist. These are described in depth in section 10.

9.6.3 Manual IP Configuration of Client Devices

Client devices that use static IP addresses must have an IP address that is within the subnet of the access point interface that they connect to.

If the local DHCP server is enabled for an access point interface, IP addresses must be reserved for statically configured devices by setting the DHCP reserve parameter. This will reserve the specified number of IP addresses at the bottom of the IP range for the interface. For example, if the interface has the IP address 10.2.4.1, the netmask 255.255.255.128, and the DHCP reserve value 5, the IP addresses 10.2.4.2 through 10.2.4.6 will be available for

use by statically configured devices. The remaining IP addresses in the interfaces address space can be assigned by the DHCP server to other client devices.

CLI

The number of IP addresses reserved for statically-configured devices connected to the Ethernet interface is set with the 'dhcp.reserve' parameter in the 'eth0' interface.

Web GUI

The 'dhcp.reserve' value can be set via the web interface using the "DHCP" sub-tab on the "DHCP" tab on the "System Parameters" page (see Figure 33).

9.7 Client Devices

Each access point has a status page that displays information about attached clients and total throughput through the access point. The signal strength of each client device, it's MAC address, its IP address, and the time since data was last received from it are listed. The status pages can be accessed under the 'Status' tab on the 'Status' page, as shown in Figure 34.

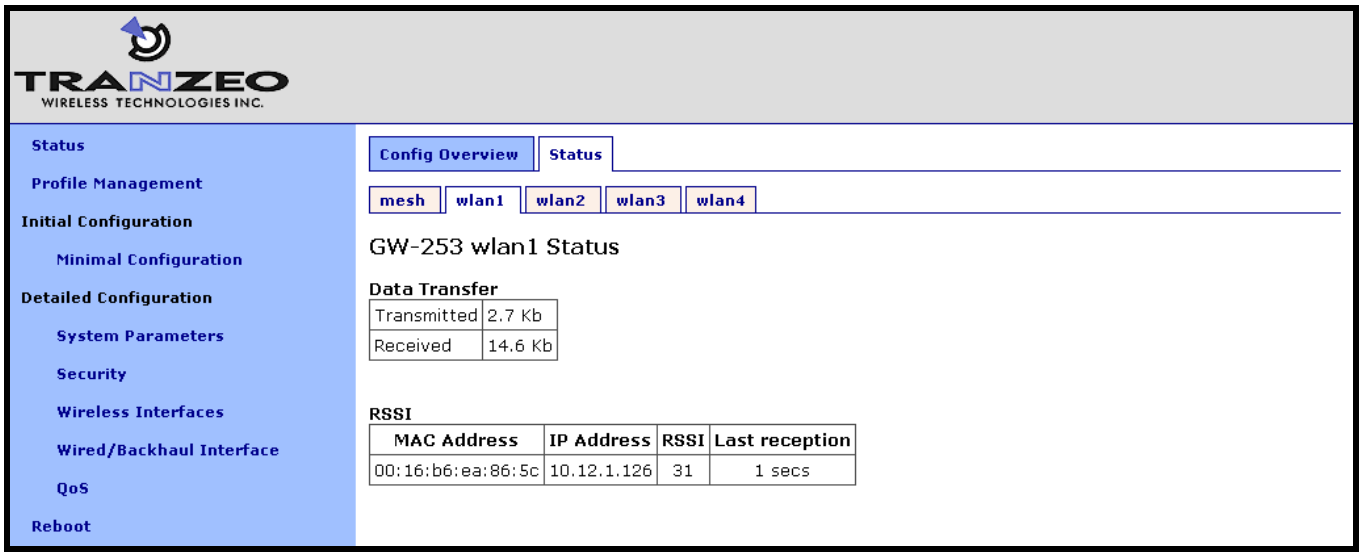

Figure 34. Access point client status information

9.8 Encryption and Authentication

The EnRoute500 supports several common encryption/authentication schemes, including WEP, WPA, and WPA2, to provide secure wireless access for client devices. WEP keys with 40-bit or 104-bit lengths, pre-shared WPA keys, and multiple WPA-EAP modes.

The WEP and WPA configuration settings for each access point are independent. An access point can only support one of the encryption/authentication modes at a time, but the APs in the EnRoute500 do not all have to use the same encryption/authentication scheme.

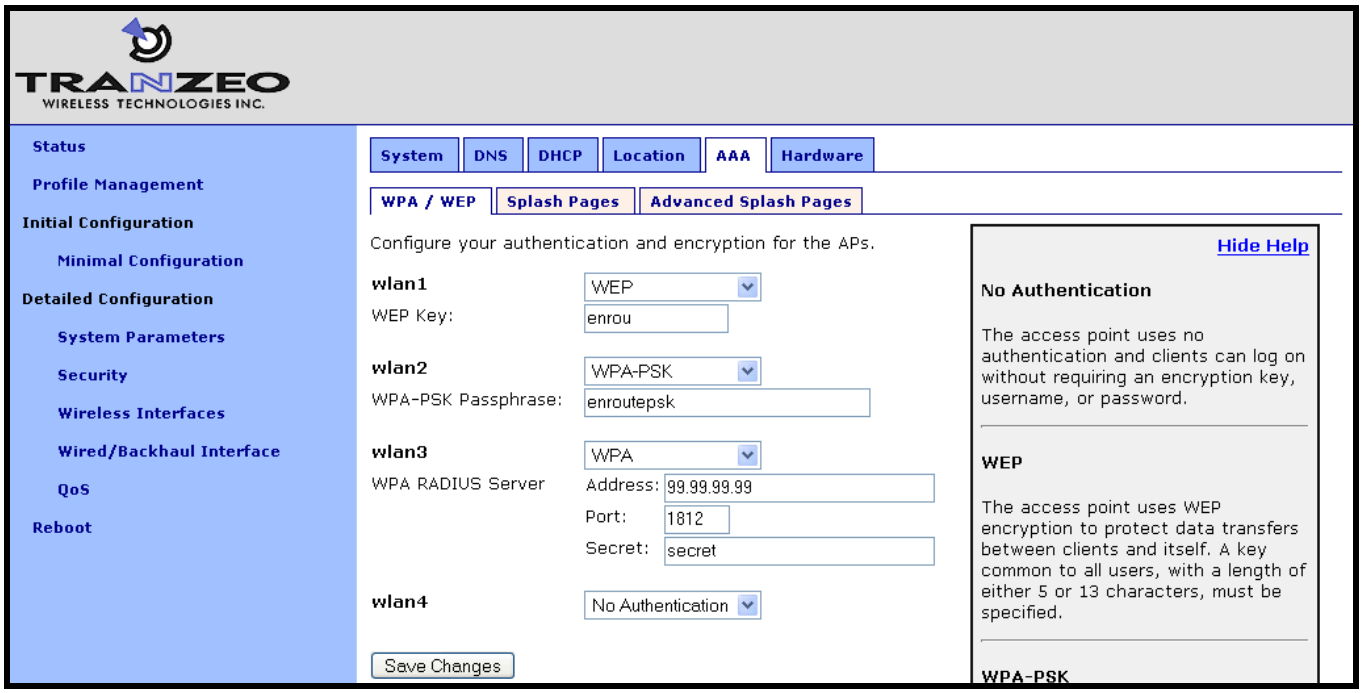

Figure 35. Access point authentication and encryption settings

9.8.1 WEP Encryption

The access points can be protected with a WEP-based encryption key to prevent unauthorized users from intercepting or spoofing traffic.

CLI

To enable WEP-based encryption, set the 'key' parameter in the 'wlanN' interface. The length of the encryption key is determined by the format used to specify the 'key' value. Valid key formats and the corresponding encryption type and key length are listed in Table 11.

If WPA is enabled for an interface ('wpa.enable' CLI parameter in the 'wlanN' interfaces), the WPA settings will be used for encryption and authentication and the 'key' value used to enable WEP will be ignored.

Key format	Encryption format	Encryption key length
s:<5 ASCII characters> <10 hex values>	WEP	40 bits
s:<13 ASCII characters> <26 hex values>	WEP	104 bits
<blank>	None	N/A

Table 11. WEP encryption key formats

For example, 104-bit WEP encryption can be enabled using an ASCII key with

```
> use wlan1
wlan1> set key="s:abcdefghijklm"
```

or using a hexadecimal key with

```
> use wlan1
wlan1> set key="0123456789abcdef0123456789"
```

WEP encryption can be disabled by specifying a blank value as shown below.

```
> use wlan1
wlan1> set key=
```

Web GUI

WEP encryption can be enabled and the key can be set via the web interface using the "WPA/WEP" sub-tab under the "AAA" tab on the "System Parameters" page (see Figure 35). Select "WEP" as the type of encryption from the drop-down menu for the access point you wish to configure and set the WEP key in the text box below the drop-down menu. In the example in Figure 35, 'wlan1' has been configured to use WEP.

9.8.2 WPA Pre-Shared Key Mode (WPA-PSK)

In WPA pre-shared key (PSK) mode, a common passphrase is used for clients connecting to an EnRoute500 AP. To set the WPA-PSK mode, enable WPA for the interface and set the pre-shared key value as shown below. The passphrase must be between 8 and 63 characters in length.

INFO

The minimum number of characters required for the WPA passphrase is 8. However, it is recommended that a longer passphrase, on the order of 15-20 characters, is used to increase the strength of the encryption used for the wireless link.

CLI

The example below shows how to enable WPA-PSK mode for wlan1. The 'wpa.key_mgmt' parameter must also be set to indicate that PSK mode is being used, as shown below.

```
> use wlan1
wlan1> set wpa.enable=yes
wlan1> set wpa.key_mgmt="WPA-PSK"
wlan1> set wpa.passphrase=long_passphrases_improve_encryption_effectiveness
```

Web GUI

WPA-PSK can be enabled and the pre-shared key can be set via the web interface using the "WPA/WEP" sub-tab under the "AAA" tab on the "System Parameters" page (see Figure 35). Select "WPA-PSK" as the type of encryption/authentication from the drop-down menu for the access point you wish to configure and enter the WPA-PSK key in the text box below the drop-down menu. In the example in Figure 35, 'wlan2' has been configured to use WPA-PSK.

9.8.3 WPA EAP Mode

In WPA-EAP mode, a client device is authenticated using an 802.1x authentication server, which is typically a RADIUS server.

The supported EAP modes are:

- TLS (X509v3 server & client certificates)
- PEAP-TLS (X509v3 server & client certificates)
- TTLS (X509v3 server certificate)
- PEAP-MSCHAPv2 (X509v3 server certificate)

The following information must be provided about the RADIUS server:

- address – the IP address of the 802.1x server that will be used for authentication
- port – the port that the authentication server is listening on (UDP port 1812 by default)
- secret – the shared secret for the authentication server. The secret must be a string that is no longer than 32 characters in length.

CLI

To configure the EnRoute500 to support 802.1x authentication, the following parameters in a 'wlanN' interface must be set:

- wpa.enable
- wpa.key_mgmt
- wpa.auth.server.addr

- wpa.auth.server.port
- wpa.auth.server.shared_secret

The 'wpa.key_mgmt' parameter must be set to indicate that both PSK and EAP modes can be supported, as shown in the example below.

The example below shows how to enable WPA EAP mode.

```
> use wlan1
wlan1> set wpa.enable=yes
wlan1> set wpa.key_mgmt="WPA-PSK WPA-EAP"
wlan1> set wpa.auth.server.addr=1.2.3.4
wlan1> set wpa.auth.server.port=1812
wlan1> set wpa.auth.shared_secret=enroute500_radius_secret
```

Web GUI

WPA-EAP can be enabled and the authentication server parameters can be set via the web interface using the "WPA/WEP" sub-tab under the "AAA" tab on the "System Parameters" page (see Figure 35). Select "WPA-EAP" as the type of encryption/authentication from the drop-down menu for the access point you wish to configure and set the authentication server IP address, port, and secret in the text boxes below the drop-down menu. In the example in Figure 35, 'wlan3' has been configured to use WPA-EAP.

9.9 Transmit Power

The transmit power of the access point radio is configurable. Increased output power will improve communication range, but will also extend the interference range of the radios. The default power level is 22 dBm.

The output power for any 'wlanN' interfaces must be no greater than the values listed in Table 12 to be in compliance with FCC regulations. Note that the power limit is dependent on the channel selected.

Channel	Output power (dBm)	CLI setting
1-11	22 dBm	25

Table 12. Access point transmit power limits

INFO

When setting the output power for an access point, consider the output power of the clients that will be communicating the access point. If these devices have output power levels that are far lower than that of the access point, an asymmetric link may result. Such a link exists when the received signal strength at clients is sufficient for a downlink to the client be established, but the received signal level at the access point is not sufficient for an uplink from the client to be established.

CLI

The example below shows how to set the access point radio's transmit power using the CLI. Note that the value is not specified in dBm. Refer to Table 13 for correlation between output power and the value set through the CLI.

```
> use wlan1
wlan1> set txpower=13
```

CLI txpower Value	Output Power (dBm)
1	18
10	20
13	22

Table 13. AP radio output power settings in the CLI

Web GUI

The access points transmit power can be set via the web interface using the appropriate "wlanN" tab on the "Wireless Interfaces" page (see Figure 32). Drop-down menus display a list of output power choices in dBm.

10 Client DHCP Configuration

Two configuration options exists for assigning IP addresses to client devices using DHCP:

- Each EnRoute500 hosts a local DHCP server and supplies IP addresses to devices attaching to any of the client interfaces
- A centralized DHCP server supplies IP addresses to client devices, with the EnRoute500s relaying DHCP messages between client devices and the centralized server.

All client interfaces in a mesh cluster must use the same DHCP mode or have DHCP disabled.

10.1 Using Local DHCP Servers

The EnRoute500 can be set to serve IP addresses to clients on enabled access point interfaces and the Ethernet interface on repeater nodes using DHCP. The DHCP role parameters in the 'wlanN' and 'eth0' interfaces control DHCP behavior. When the role is set to 'server', the EnRoute500 will respond to DHCP requests received from client devices connected to the interface.

The IP addresses provided by the DHCP server will be in the subnet defined by the LAN prefix ('sys.id.lanprefix'), mesh ID ('sys.id.mesh'), node ID ('sys.id.node') and the IP address range start address and size parameters in the appropriate client interface ('<intf>.ip.start.actual' and '<intf>.ip.size.actual'). For example, for the 'wlan1' interface, the start and end of the address range are:

Start address = <LAN prefix>.
<Mesh ID>.
<Node ID>.
<wlan1 IP address range start address> + 1
End address = <LAN prefix>.
<Mesh ID>.
<Node ID>.
< wlan1 IP address range start address > -
< wlan1 IP address range size > - 2

The EnRoute500 can be configured to set aside a number of IP addresses for client devices that will use a static IP address. These IP addresses are taken from the pool that DHCP assigns IP addresses from. Thus, increasing the number of IP addresses set aside for devices with static IP addresses will reduce the size of the DHCP address pool. The DHCP reserve parameter controls the number of IP addresses that will be reserved for static use. By default, this parameter is set to zero, assigning the maximum possible number of IP

addresses to the DHCP pool. You may reserve the entire range of IP addresses, but the EnRoute500 will use at least the highest address in the range for DHCP.

If the 'dhcp.reserve' value is non-zero, the DHCP range start address will be affected as shown below

Start address = <LAN prefix>.
<Mesh ID>.
<Node ID>.
<wlan1 IP address range start address> + 1 - < wlan1 DHCP reserve>

CLI

The examples below show how to set the DHCP server state for the 'wlan1' interface.

```
> use wlan1
wlan1> set dhcp.role=server
```

To disable the DHCP server, set the 'dhcp.role' parameter to 'none'

```
> use wlan1
wlan1> set dhcp.role=none
```

The example below shows how to set the DHCP reserve parameter

```
> use wlan1
wlan1> set dhcp.reserve=5
```

Web GUI

The access point and wired interface DHCP servers' state can be set via the web interface using the "DHCP" sub-tab under the "DHCP" tab on the "System Parameters" page (see Figure 36). All of the access points' DHCP settings can be configured on this page.

The DHCP reserve setting for all access points and the wired interface can be set via the web interface using the "DHCP" sub-tab under the "DHCP" tab on the "System Parameters" page (see Figure 36).

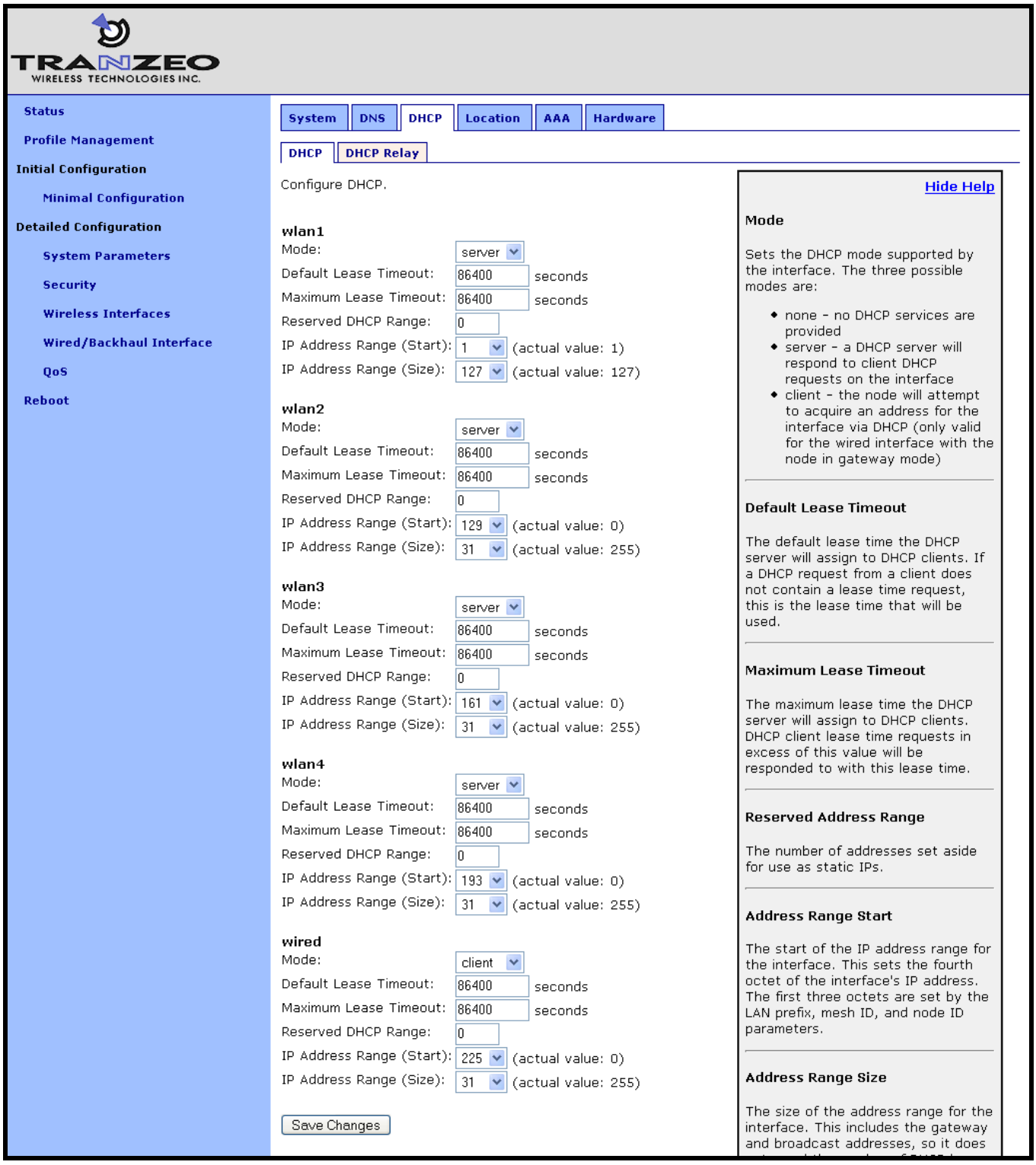

Figure 36. Access point DHCP configuration

10.2 Using a Centralized DHCP Server

DHCP relay enables assignment of IP addresses to wireless clients from a common remote DHCP server. The remote DHCP server may reside either on a host connected to the mesh gateway's wired segment, or on a server that is beyond one or more routers. When using a common DHCP server, wireless clients are assigned IP addresses from a single address pool, and are allowed to keep their IP address while roaming seamlessly from AP to AP. Even though they will not move seamlessly from one node to another, wired clients can also have their IP addresses assigned by a centralized server.

There are three classes of entities that must be configured when using this DHCP mode:

1. The individual EnRoute500s, including the repeaters and the gateway node
2. The central DHCP server
3. Any intermediate router(s) in the path between the DHCP server and the mesh cluster gateway node

When using a centralized DHCP server, an address space, from which client IP addresses are assigned, must be defined. The client interfaces on the EnRoute500s (there can be up to 5 per node) must also have IP addresses that belong to this address space in order to facilitate DHCP relay and selection of client IP addresses from the correct DHCP scope on servers that serve hosts connected to different subnets. The client interface IP addresses need to be configured statically. It is recommended that a contiguous range of IP addresses at either the beginning or the end of the address space be set aside, one for each client interface on the mesh nodes.

Consider the example where a mesh cluster consists of 3 nodes, including the gateway node. The DHCP server resides on a host that also acts as the upstream router and is connected to the mesh gateway's wired segment. We will set aside 15 IP addresses for the mesh nodes' client interfaces (3 nodes, up to 5 interfaces per node). Assuming the client address space is 192.168.5.0/24, with available addresses from 192.168.5.1 to 192.168.5.255, we will use 192.168.5.1 for the server hosting the DHCP server, 192.168.5.2 for the mesh gateway's backhaul interface, set aside 192.168.5.3 to 192.168.5.18 for the mesh AP interfaces, and configure the remote DHCP server to serve IP addresses in the range of 192.168.5.19 to 192.168.5.254 to wireless clients. We will keep 192.168.5.255 as the broadcast address for the mesh cluster.

10.2.1 Configuring the EnRoute500s

When operating in centralized DHCP mode, Each EnRoute500 in a mesh cluster must be configured to use centralized DHCP mode and to use the same centralized DHCP server. The IP address of the central DHCP server is set with the DHCP relay server parameter. The server must be reachable through the mesh cluster gateway's wired backhaul interface.

Each client interface on the EnRoute500 that is to support centralized DHCP mode must be configured to be in DHCP server mode for it to support relay of IP addresses to clients from a central DHCP server. This configuration is set with the DHCP role parameter in each of the client interfaces (eth0, wlan1-4).

It is possible to disable DHCP address assignments to clients on a per-interface basis and have them use static IP addresses instead. To disable DHCP for an interface, set the DHCP role parameter associated with the interface to 'none'.

The address space that is to be used for the wireless clients is a subnet specified with the Client Address Space parameter. This subnet can either be a class A (/8), class B (/16), or class C (/24) network. The value must be specified in CIDR notation (a subnet and its size separated by a '/'), e.g. '192.168.5.0/24'

The IP addresses of the client interfaces (eth0, wlan1-4) need to be manually assigned to each of the nodes in the mesh cluster. This is done by setting the Address Base parameter for the interfaces, which is assigned to the first enabled client interface. Addresses for the remaining client interfaces are determined by successively incrementing the Base Address by 1. It is recommended that the gateway in a mesh cluster be assigned the lowest available value (3 in the example in the CLI section below) and the repeaters in the mesh cluster are given successively higher values, with an increment of 5 between them (5 is the maximum number of client interfaces available on each mesh node, including the Ethernet interface on mesh repeaters).

CLI

DHCP relay mode is enabled using the 'dhcp.relay.enable' and 'l2.client_mac_fwd' parameters in the 'sys' interface as shown in the example below.

```
> use sys
sys> set dhcp.relay.enable=yes
sys> set l2.client_mac_fwd=yes
```

In the example below, the central DHCP server resides on a host on the same segment to which the mesh gateway's wired interface is connected.

```
> use sys
sys> set dhcp.relay.server=192.168.5.1
```

The example below shows how to set the DHCP role parameter for the wlan1 and wlan2 interfaces.

```
> use wlan1
wlan1> set dhcp=server
> use wlan2
wlan2> set dhcp=server
```

To disable distribution of centralized DHCP addresses on an interface, set the interface's 'dhcp.role' parameter to 'none' as shown below.

```
> use wlan3
wlan3> set dhcp=none
```

The Client Address Space value is set with the 'dhcp.relay.dhcp_subnet' parameter in the 'sys' interface. This value should be a class A, B, or, C subnet specified using CIDR notation as shown in the example below.

```
> use sys
sys> set dhcp.relay.dhcp_subnet=192.168.5.0/24
```

The Base Value, which sets the IP address of client interfaces on a node, is set through the 'dhcp.relay.base' parameter in the 'sys' interface. The example below shows the configuration for a mesh cluster consisting of 3 nodes.

On the gateway:

```
> use sys
sys> set dhcp.relay.base=192.168.5.3
```

on the first repeater node:

```
> use sys
sys> set dhcp.relay.base=192.168.5.8
```

and on the second repeater node:

```
> use sys
sys> set dhcp.relay.base=192.168.5.13
```

Note that the value of the fourth octet increases by 5 for each node since that is the number of client interfaces that each node has, and each interface requires one IP address.

Web GUI

DHCP relay mode can be enabled via the web interface on the "DHCP Relay" sub-tab under the "DHCP" tab on the "System Parameters" page (see Figure 37). The external DHCP server IP address, the Client Address Space parameter, and the Base Value can also be set on this page. The DHCP role parameters for all interfaces can be set on the "DHCP" sub-tab under the "DHCP" tab on the "System Parameters" page.

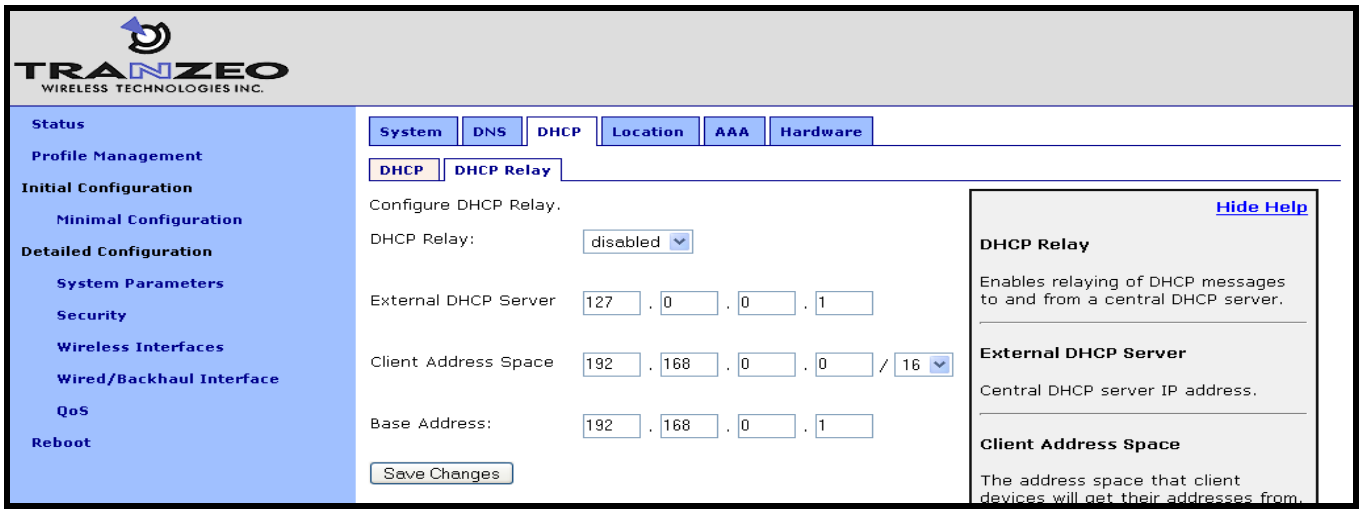

Figure 37. DHCP relay settings for use with a centralized DHCP server

10.2.2 Configuring the Central DHCP Server

Guidelines for configuring the central DHCP server are provided below. The full configuration of the central DHCP server will depend on the type of DHCP server that is used and is beyond the scope of this document.

Typically the following information must be available in order to configure the server:

1. The local interface (to the DHCP server) over which the DHCP-related messages from the mesh cluster arrive
2. The parameter(s) that define the address lease time
3. Whether DNS and domain names are to be provided by the DHCP server to clients
4. The range of the flat IP address that is used for assigning IP addresses to clients. The range must not include the IP addresses set aside for the client interfaces on each mesh node.

The following is a segment of the dhcpd.conf file for a Linux DHCP server (ISC DHCP server) that illustrates the scope settings for the mesh network:

```
subnet 192.168.5.0 netmask 255.255.255.0
{
        option broadcast-address        192.168.5.255;
        option subnet-mask              255.255.255.0;
        option domain-name              "domain.com";
        range                           192.168.5.18 192.168.5.254;
}
```

Note that in this definition no "routers" option is needed. If a global "routers" option is defined, it will be set to the correct value for proper operation inside the mesh network. In this example,

the mesh network includes 3 mesh nodes, 2 IP addresses are set aside for the DHCP server and the mesh gateway, and therefore the address pool starts from 192.168.5.18.

11 Connecting an EnRoute500 Gateway to a WAN

The options for connecting an EnRoute500 gateway to a WAN are described below.

11.1 Manual Configuration

An EnRoute500 gateway can be directly connected to a WAN without using Network Address Translation. With this gateway configuration, the router on the network that the gateway is attached to must be configured to forward the mesh subnet and the LAN subnets to the gateway's Ethernet IP address. The subnets that need to be forwarded are:

Class B subnet: <LAN prefix>.<Mesh ID>.0.0
Class C subnet: <Mesh prefix >.<Mesh ID>.0

In the case where the LAN prefix is 10, the mesh ID is 2, and the mesh prefix is 172.29, the subnets the router would need to forward to the gateway are 10.2.0.0/255.255.0.0 and 172.29.2.0/255.255.255.0.

CLI

The subnet information can be retrieved from the 'sys' interface as shown below.

```
> use sys
sys> get id.*
 sys.id.lanprefix = 10
 sys.id.mesh = 2
 sys.id.meshprefix = 172.29
 sys.id.node = 4
```

Web GUI

The LAN prefix and mesh prefix can be obtained by inspecting the IP addresses available on the "Status" page. Alternatively, the mesh ID can be obtained from the "Mesh" tab on the "Wireless Interfaces" page and the LAN prefix can be obtained form the "System" tab on the "System" page.

11.2 Network Address Translation (NAT)

Network Address Translation (NAT) isolates a mesh cluster from the WAN network that its gateway is connected to. The mesh nodes and their client devices are able to communicate with devices connected to the external network that the mesh gateway is connected to.

However, devices on the external network cannot initiate communication with any nodes in the mesh cluster, or their clients, other than the mesh cluster gateway.

The advantages of using NAT are:

- You can easily attach a mesh cluster to an existing network. You do not need to modify any settings on the router on your existing network to forward packets to the IP addresses used in your mesh cluster.
- The nodes in the mesh cluster are shielded from the network that the gateway is attached to.
- You only consume a single IP address on your existing network when connecting the mesh cluster to it.

The main disadvantage of using NAT is

- You are not able to initiate connections with nodes in the mesh cluster or their clients from outside the mesh cluster.

CLI

To set the NAT state, use the commands

```
> use sys
sys> set nat.enable=<yes|no>
```

Web GUI

The NAT state can be set via the web interface on the "Wired/Backhaul Interface" page (Figure 38).

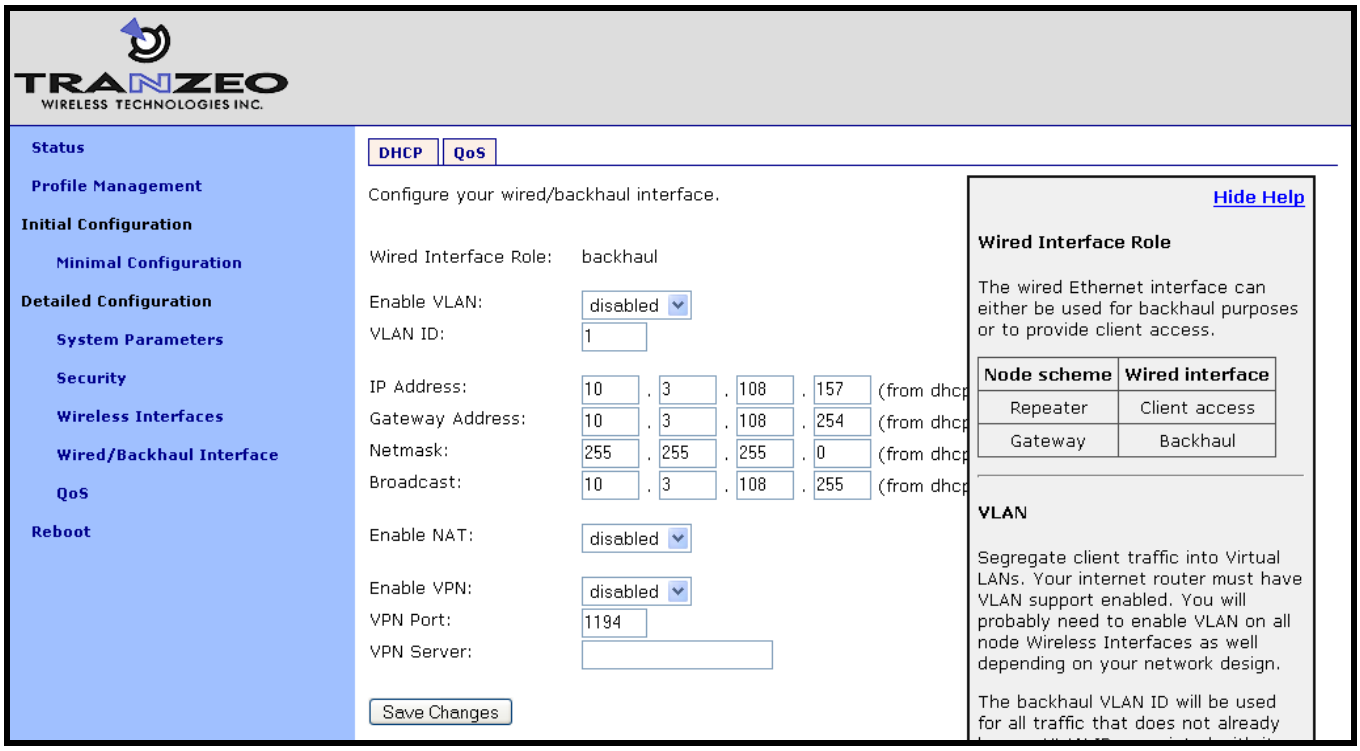

Figure 38. NAT setting

11.3 VPN Access to a Mesh Gateway

An EnRoute500 configured as a gateway can establish a VPN connection to an OpenVPN server. This VPN connection provides the following capabilities:

- Any node in the mesh can be contacted directly from a remote host, even when NAT is enabled on the gateway node. This allows remote access to nodes to monitor their behavior or reconfigure them
- A secure path between the mesh and a host, which can be used to monitor and reconfigure the mesh, is established. The control and status traffic passing between the mesh and the host is protected if it passes over a public network at any point.

The state of the VPN client on the EnRoute500 is set with the Enable VPN parameter. The IP address of the VPN server and its port are specified with the VPN Server and VPN Port parameters. Note that the VPN server parameter can either be an IP address or a resolvable host name.

CLI

The example below shows how to enable the VPN connection ('vpn.enable' in the 'sys' interface) and set the server and port parameters ('vpn.server' and 'vpn.port' in the 'sys' interface).

```
> use eth0
sys> set vpn.enable=yes
sys> set vpn.server=192.168.0.1
sys> set vpn.port=1194
```

Web GUI

These parameters can be set via the web interface on the "Wired/Backhaul Interface" page when the node scheme is set to 'gateway'.

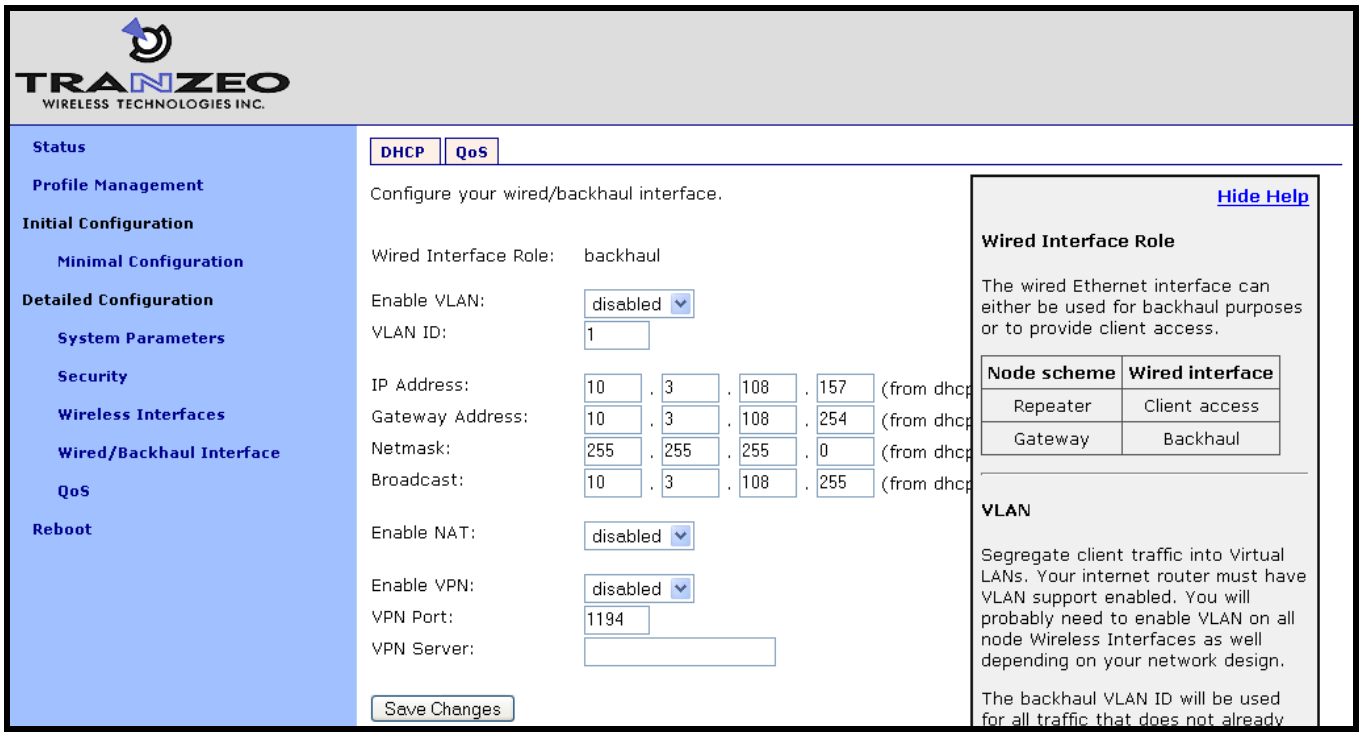

Figure 39. VPN client settings

12 Controlling Access to the EnRoute500

The EnRoute500 supports the following features for restricting access to the mesh node, inter-client device communication and access to mesh nodes and client devices from an external network:

- Firewall
- Client-to-client communication blocking
- Gateway firewall

It further supports controlled network access by client devices through MAC address black lists and mesh association through MAC white lists.

12.1 Firewall

The EnRoute500 has a firewall that blocks traffic destined for the EnRoute500. This prevents client devices attached to a node and devices on the mesh gateway WAN from connecting to the node.

INFO

The firewall only affects packets destined for the EnRoute500. All traffic destined for devices 'past' the EnRoute500 is not affected by the firewall. This means the firewall needs to be enabled on every EnRoute500 or connected clients will have full access to the EnRoute500's private ports.

By default, the ports listed in Table 14 are set to be allowed.

Function	Port	Type	Protocol
SSH	22	Source & destination	TCP
HTTPS	443	Destination	TCP
HTTP redirect	3060	Destination	TCP
DNS	53	Source & destination	UDP
DHCP	67	Destination	UDP
DHCP	68	Destination	UDP
Roaming support	7202	Destination	UDP
Roaming support	7203	Destination	UDP

Table 14. Source and destination ports allowed by default

If ports that are open by default are reconfigured to be closed, certain EnRoute500 functions will be affected. It is strongly recommended that all of the ports listed in Table 14 be kept open.

CLI

The firewall is enabled by selecting the 'firewall' interface and setting the 'node.enable' parameter.

```
> use firewall
firewall> set node.enable=yes
```

Lists of allowed source and destination ports for inbound TCP and UDP traffic can be specified. These lists can be set with the following parameters in the 'firewall' interface:

- node.tcp.allow.dest
- node.tcp.allow.source
- node.udp.allow.dest
- node.udp.allow.source

The list of allowed ports must be a space-delimited string enclosed by quotes. The example below shows how to set the TCP source ports parameters.

```
> use firewall
firewall> set node.tcp.allow.dest="22 23 80 5280"
```

12.2 Gateway Firewall

The gateway firewall blocks connections originating outside the mesh cluster from entering the mesh via the gateway, protecting mesh nodes and their clients from unwanted traffic. The gateway firewall will permit return traffic for connections that originate inside the mesh cluster or on mesh clients.

The gateway firewall should only be enabled on EnRoute500's that are configured as gateways. It is possible to have the gateway firewall set to be enabled on a repeater node, but it does not have any effect on the flow of traffic through the node's Ethernet interface.

If you have enabled NAT (see section 11.2) on the Ethernet interface 'eth0', you will have an implicit firewall that limits the type of inbound connections that are possible.

CLI

The state of the gateway firewall is controlled with the 'gateway' parameter in the 'firewall' interface. Enable the gateway firewall with

```
> use firewall
firewall> set gateway=yes
```

disable it with

```
> use firewall
firewall> set gateway=no
```

12.3 Blocking Client-to-Client Traffic

Client-to-client traffic can be blocked or permitted on a per-interface basis. By enabling client-to-client traffic blocking for one or more of an EnRoute500's client interfaces, the clients that attach to that particular interface will not be able to communicate with any clients attached to that or any other client interface in the mesh. Client-to-client traffic can be controlled for interfaces wlan1, wlan2, wlan3, wlan4, and eth0.

CLI

The parameters that control client-to-client access are all in the 'firewall' interface. They are:

- node.allowc2c.eth0
- node.allowc2c.wlan1
- node.allowc2c.wlan2
- node.allowc2c.wlan3
- node.allowc2c.wlan4

To block client-to-client traffic, select the 'firewall' interface and set the parameter for the appropriate interface to 'no', To allow traffic between clients, set the parameter to 'yes'. The examples below illustrate the how to configure these parameters.

To block client-to-client traffic for clients attached to wlan1:

```
> use firewall
firewall> set node.allowc2c.wlan1=no
```

To allow client-to-client traffic for clients attached to eth0:

```
> use firewall
firewall> set node.allowc2c.eth0=yes
```

Web GUI

The client isolation parameters can be set via the web interface using the "Firewall" tab on the "Security" page (see Figure 40). By setting an interface's client isolation parameter to 'yes',

clients connecting to that interface will not be able to communicate with any other clients in the mesh.

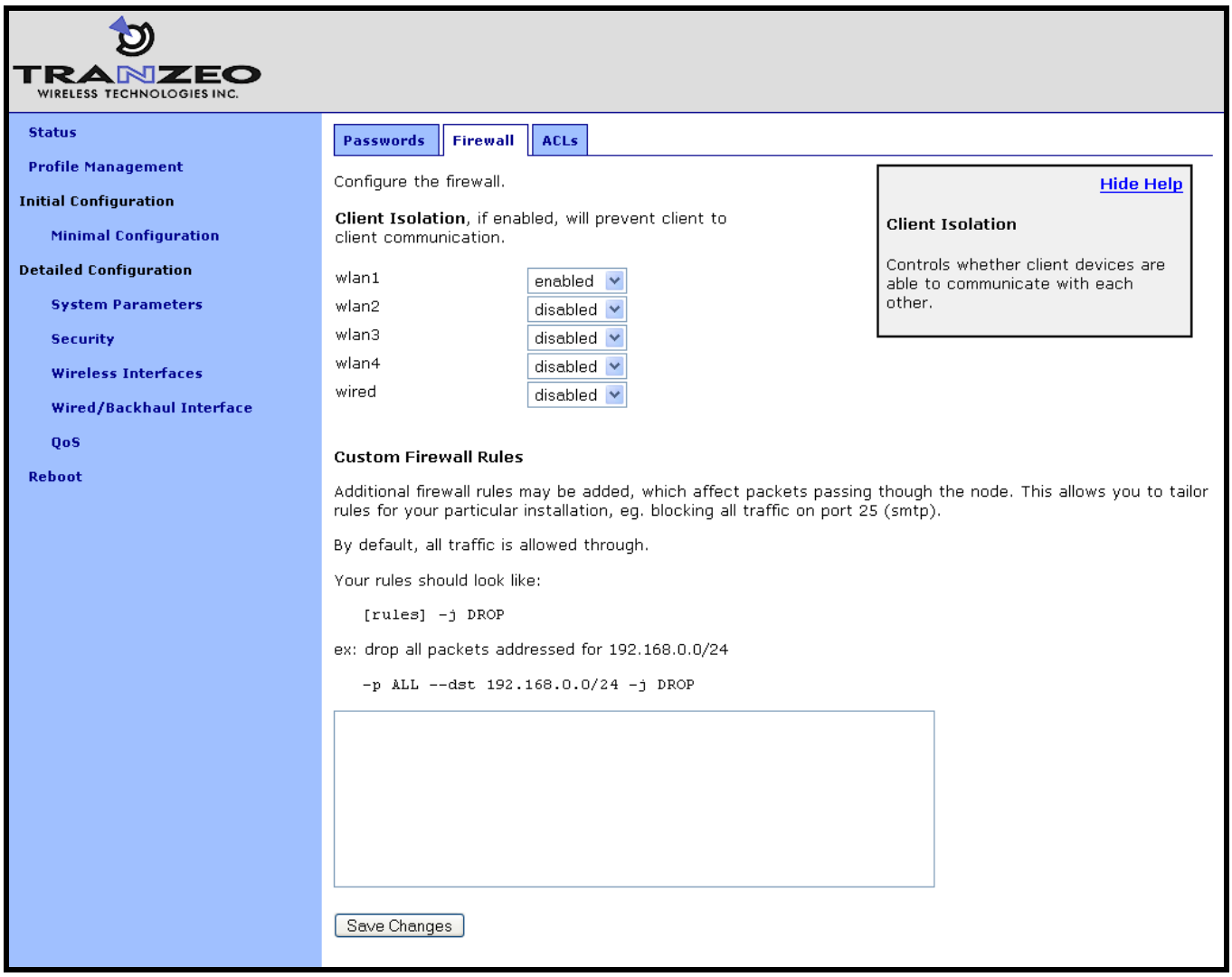

Figure 40. Client-to-client firewall settings

Note that devices connected to different interfaces can only communicate with each other if client-to-client isolation is disabled for both interfaces.

Client-to-client isolation is only enabled if the EnRoute500 node firewall (firewall.node.enable) is enabled (section 12.1).

12.4 Access Control Lists (ACLs)

Access control lists can be created for each of the access point interfaces and the mesh interface.

12.4.1 Access Point Access Control Lists (ACLs)

The access control lists (ACLs) for the access point interfaces (wlan1-wlan4) block access to any device with a MAC address matching those on the list. Individual ACLs can be defined for each access point.

Web GUI

The ACLs can be defined via the web interface on the appropriate "wlanN" sub-tab under the "ACL" tab on the "Security" page. Enter a MAC address and click on the "Add MAC" button to add the address to the ACL for that access point. Once an address has been added, it will appear at the bottom of the page. To delete a MAC address in an ACL, click on the "Delete MAC" button next to the address.

The ACL for an access point must be enabled after it has been created. Choose "blacklist" from the drop-down menu and click on "Change ACL Mode" to enable the list. Choose "none" from the drop-down menu and click on "Change ACL Mode" to disable the ACL.

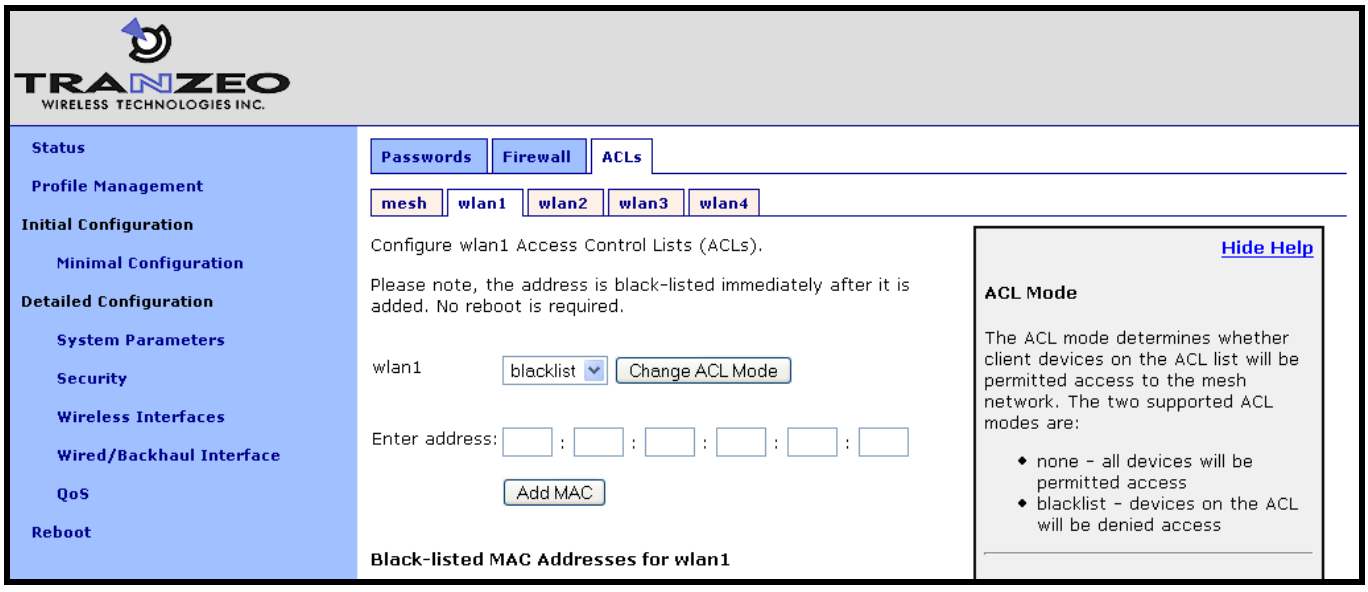

Figure 41. AP ACL configuration

12.4.2 Mesh ACL

The access control list (ACL) for the mesh interface blocks access to the node via the mesh interface for any node whose mesh MAC address is not listed in the ACL.

It is possible to isolate a mesh node from other nodes in the mesh if the mesh ACL is incorrectly configured. If the mesh ACL is enabled and no MAC addresses are present on the list, or the wrong addresses are present, it will not be possible for other mesh nodes to communicate with the node.

Web GUI

The mesh ACL can be defined via the web interface on the "Mesh" sub-tab under the "ACL" tab on the "Security" page. Enter a MAC address and click on the "Add MAC" button to add the address to the ACL for that access point. Once an address has been added, it will appear at the bottom of the page. To delete a MAC address in an ACL, click on the "Delete MAC" button next to the address.

The ACL for an access point must be enabled after it has been created. Choose "whitelist" from the drop-down menu and click on "Change ACL Mode" to enable the list. Choose "none" from the drop-down menu and click on "Change ACL Mode" to disable the use of the ACL for the mesh interface.

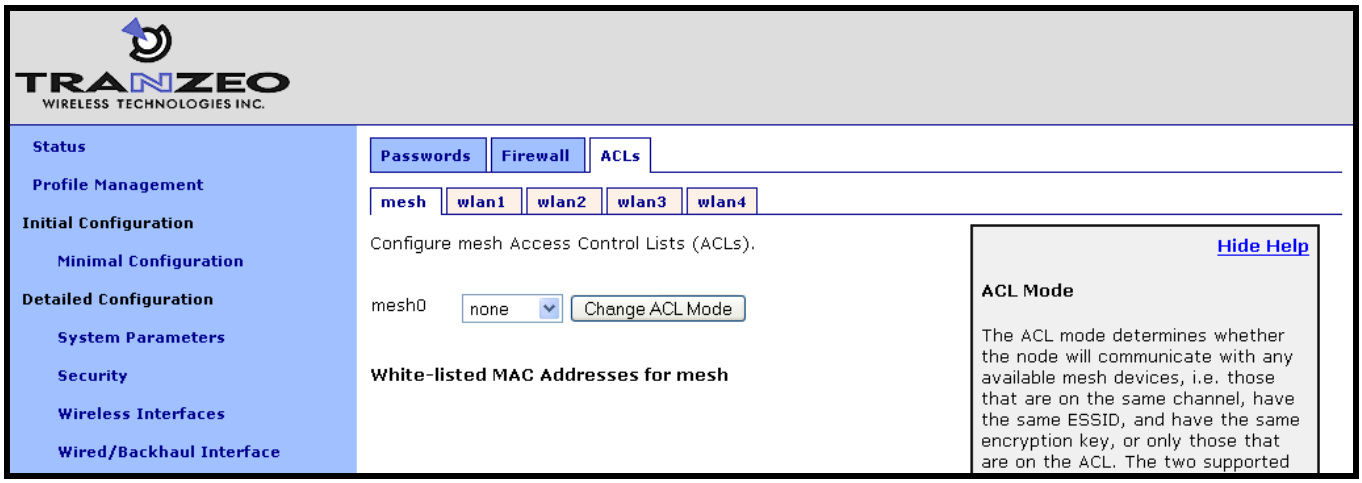

Figure 42. Mesh ACL configuration

13 Quality of Service (QoS) Configuration

The EnRoute500 has extensive support for quality of service settings that allow traffic to be prioritized based on the source interface, destination interface, and type of traffic. The EnRoute500 QoS scheme allows both rate limiting and rate reservation for all interfaces.

13.1 Priority Levels

The Flow Priority parameters set the relative priority of outbound traffic based on the source interface. These parameters can be set to an integer value in the range from 0 to 99, with a higher number indicating a higher priority. If a priority level parameter is set to 'inherit', the interface will assume the default priority level.

Traffic originating from an interface with a higher priority will take priority over traffic from all interfaces with a lower priority value until the higher-priority interface has no more data to send. If multiple interfaces have the same priority level, their traffic will be given equal access to the outbound interface. Rate reservation and rate limiting, described in the following sections, can be used to avoid one interface dominating the use of the mesh interface bandwidth.

As a rule, locally generated traffic should **always** have the highest priority so that EnRoute500 control traffic has precedence over client traffic and the mesh can be maintained.

The absolute value of the priority settings do not have any weighting effect. If a priority is higher for one interface than another, the former will always be prioritized with any remaining bandwidth allocated to the other one.

The Max/Min Hardware Priority parameters can be used to limit the hardware priority queues that traffic from a particular interface can use for outbound traffic. Valid values for these parameters are from 1 to 4, which are the priority levels listed in Table 15.

Abbreviation	Description	Priority level
VO	Voice	4 (highest)
VI	Video	3
BE	Best Effort	2
BK	Background	1 (lowest)

Table 15. Priority levels

When sending data out through any of the wireless interfaces (wlanN, mesh0), these priorities map directly to the hardware priority output queues on the wireless card. The default level is Best Effort.

To increase the hardware priority of traffic from a particular interface, set the value of Min Hardware Priority to a value larger than 1. This will force all traffic from the chosen interface to use a hardware queue equal to or greater than the Min Hardware Priority value set. To reduce the maximum hardware priority of traffic from an interface, set the Max Hardware Priority parameter to a value less than 4. To disable hardware prioritization, set the Min/Max Hardware Priority parameters to '0'.

Changing hardware priorities does **not** affect the rate limiting and reservation (section 13.2), it only affects which output hardware queues are used.

CLI

Flow priority levels are set with the 'in.<intf>.flow_priority' parameters in the 'qos' interface, where <intf> is one of the following: default, local, eth0, mesh0, wlan1, wlan2, wlan3, wlan4. 'local' refers to traffic originating on the node itself, not from its clients (in practice this means mesh network control traffic). The example below sets locally generated traffic to have top priority and wlan1 to have priority over all other interfaces.

```
> use qos
qos> set in.default.flow_priority=10
qos> set in.local.flow_priority=90
qos> set in.wlan1.flow_priority=20
qos> set in.wlan2.flow_priority=inherit
qos> set in.wlan3.flow_priority=inherit
qos> set in.wlan4.flow_priority=inherit
qos> set in.eth0.flow_priority=inherit
```

Hardware priority levels are set with 'in.<intf>.hwpri{max,min}' in the 'qos' interface, where <intf> is one of the following: default, local, eth0, mesh0, wlan1, wlan2, wlan3, wlan4.

The example below shows how to configure the system such that all traffic from 'wlan1' with a 'Voice' or 'Video' priority will be reduced to a 'Best Effort' priority. Traffic with 'Best Effort' and 'Background' priorities will not be affected.

```
> use qos
qos> set in.wlan1.hwpri.max=2
```

The example below shows how to configure the system such that all traffic from 'wlan2' with a 'Background' or 'Best Effort' priority will be increased to a 'Video' priority. Traffic with 'Video' and 'Voice' priorities will not be affected.

```
> use qos
qos> set in.wlan2.hwpri.min=2
```

Web GUI

Flow priorities can be set via the web interface under the "QoS" tab on the "QoS" page (see Figure 43). The hardware priority levels can be set for each interface under the "Advanced QoS" tab on the "QoS" page (see Figure 44).

Figure 43. QoS settings

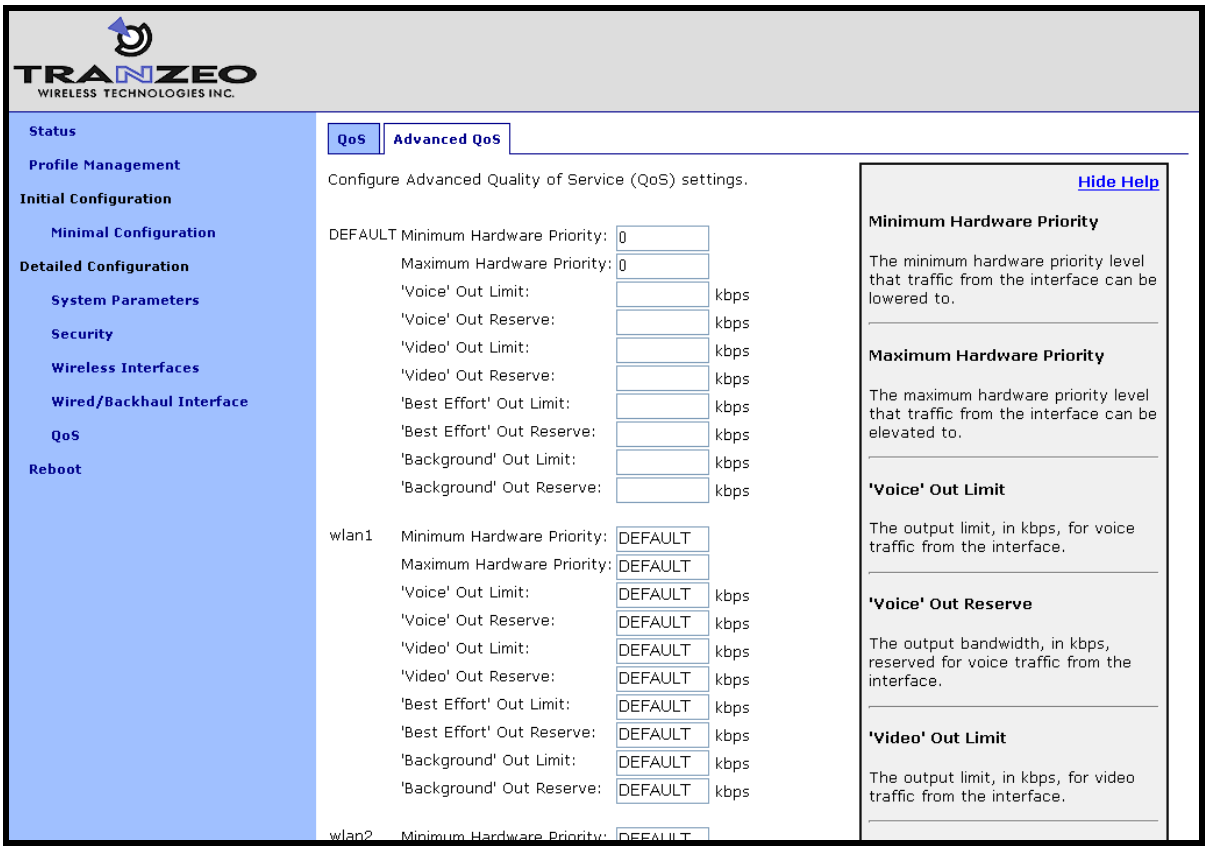

Figure 44. Advanced QoS configuration (only settings for some interfaces are shown)

13.2 Rate Limiting

A rate limit can be set at each QoS Control Point shown in Figure 45. The Control Points can be split into three groups, listed below in decreasing order of importance:

- Interface output limit
- Interface output limit of traffic from a particular interface
- Interface output limit of traffic of a certain type from a particular interface

INFO

All rate limit parameter values are in kbps. If no rate limit parameter is set, rate limiting will be disabled for that interface or interface and traffic combination.

The maximum output data rate for interfaces can be limited with the Output Limit parameters for each client interface. The default output limit value is applied to interfaces that have the Output Limit parameter set to 'inherit'.

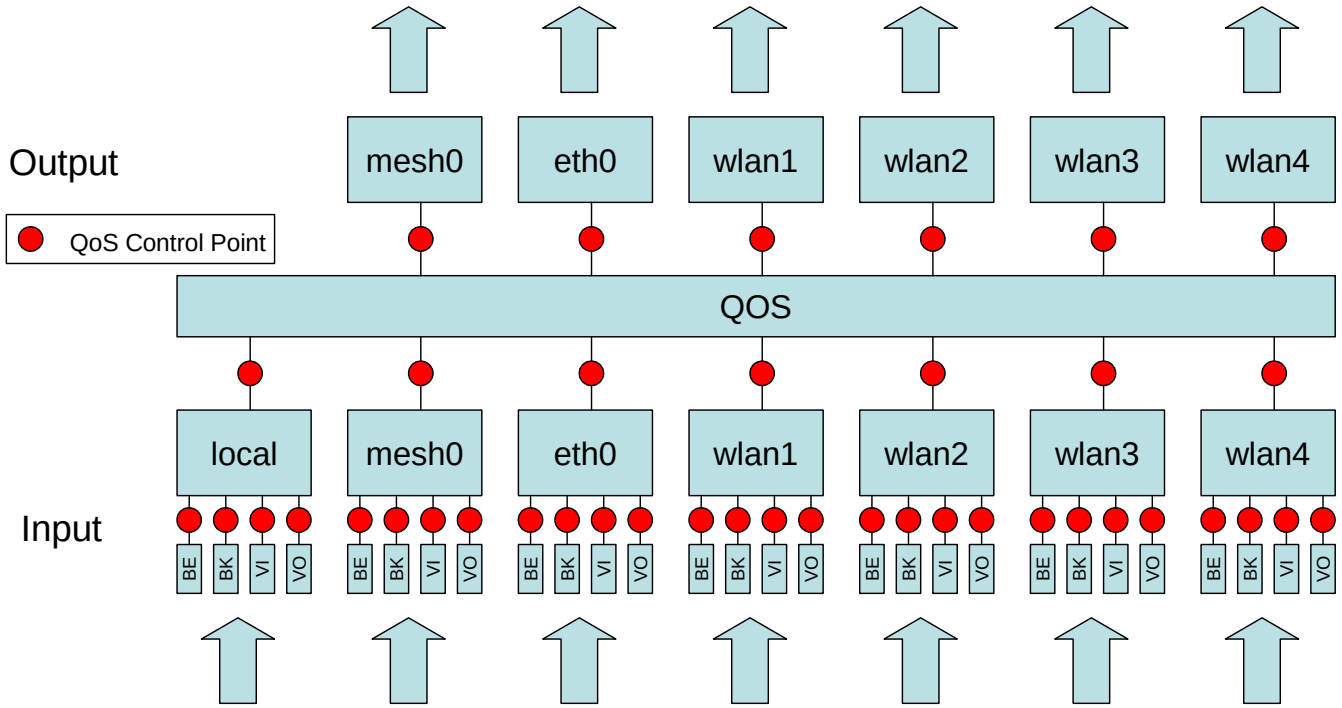

Figure 45. Quality of Service rate limit control points

Data rate limits can also be imposed based on traffic type through an interface. The maximum data rate for a certain type of traffic that enters the EnRoute500 through a particular interface and exits it through another interface can be limited.

INFO

There is no standalone input rate limiting. Limiting the input rate of an interface only makes sense in the context of the output for another interface(s). In most cases you are concerned with mesh0 as the output interface.

CLI

The example below shows how to limit the maximum output rate of the mesh0 interface to 8 Mbps and the maximum output rates of all four wlanN interfaces to 2 Mbps each.

```
> use qos
qos> set out.mesh0.limit=8192
qos> set out.wlan1.limit=2048
qos> set out.wlan2.limit=2048
qos> set out.wlan3.limit=2048
qos> set out.wlan4.limit=2048
```

The maximum data rate for traffic that enters the EnRoute500 through a particular interface and exits it through another interface can be limited with the 'out.<output intf>.<input intf>.limit' parameters in the 'qos' interface, where <output intf> is one of the following: default, eth0, mesh0, wlan1, wlan2, wlan3, wlan4; and <input intf> is one of the following: default, eth0, local,

mesh0, wlan1, wlan2, wlan3, wlan4. The 'out.default.default.limit' value is applied to interfaces that have the 'out.<output intf>.<input intf>.limit' parameter set to 'inherit' or is left blank.

The example below shows how to limit the maximum output rate of data from wlan1, wlan2, wlan3, and wlan4 through the mesh0 interface to 2 Mbps, 1 Mbps, 512 kbps, and 256 kbps, respectively.

```
> use qos
qos> set out.mesh0.wlan1.limit=2048
qos> set out.mesh0.wlan2.limit=1024
qos> set out.mesh0.wlan3.limit=512
qos> set out.mesh0.wlan4.limit=256
```

Traffic type limits can be set with the 'out.<output intf>.<input intf>.<traffic type>.limit.' parameters in the 'qos' interface, where <output intf> is one of the following: default, eth0, mesh0, wlan1, wlan2, wlan3, wlan4; <input intf> is one of the following: default, eth0, local, mesh0, wlan1, wlan2, wlan3, wlan4; <traffic type> is one of the following: 'vo', 'vi', 'be', 'bk' (see Table 15 for description of traffic types).

The example below shows how to limit the maximum output rate of voice, video, best effort, and background traffic from wlan1 through the mesh0 interface to 256 kbps, 1 Mbps, 256 kbps, and 256 kbps, respectively.

```
> use qos
qos> set out.mesh0.wlan1.vo.limit=256
qos> set out.mesh0.wlan1.vi.limit=1024
qos> set out.mesh0.wlan1.be.limit=256
qos> set out.mesh0.wlan1.bk.limit=256
```

Web GUI

The interface- and traffic-based Output Limit parameters can be set via the web interface under the "QoS" tab on the "QoS" page (see Figure 43).

13.3 Rate Reservation

Rate reservation is used to guarantee bandwidth for certain types of traffic. Rate reservations can be made for traffic based on:

- The traffic input and output interfaces
- The traffic type, input interface, and output interface

For rate reservations to be enforced, a rate limit must be set for the traffic type that the reservation is made for. Setting a rate limit for a broader traffic type, of which the one the reservation is made for is a subset, is also acceptable. For example, when making a rate reservation for voice traffic from wlan1 to mesh0 ('out.mesh0.wlan1.vo.reserve'), a limit must be set with 'out.mesh0.limit', 'out.mesh0.wlan1.limit', or 'out.mesh0.wlan1.vo.limit'.

Rate reservations guarantee bandwidth for a particular traffic type, but if no such traffic is present, the bandwidth reserved will be returned to the pool of available bandwidth for other traffic types to use. The points at which rate reservations can be made are shown in Figure 46. These points are similar to where rate limits can be placed, except that rate reservations require both an input and output interface, whereas rate limits can be made without specifying an input interface.

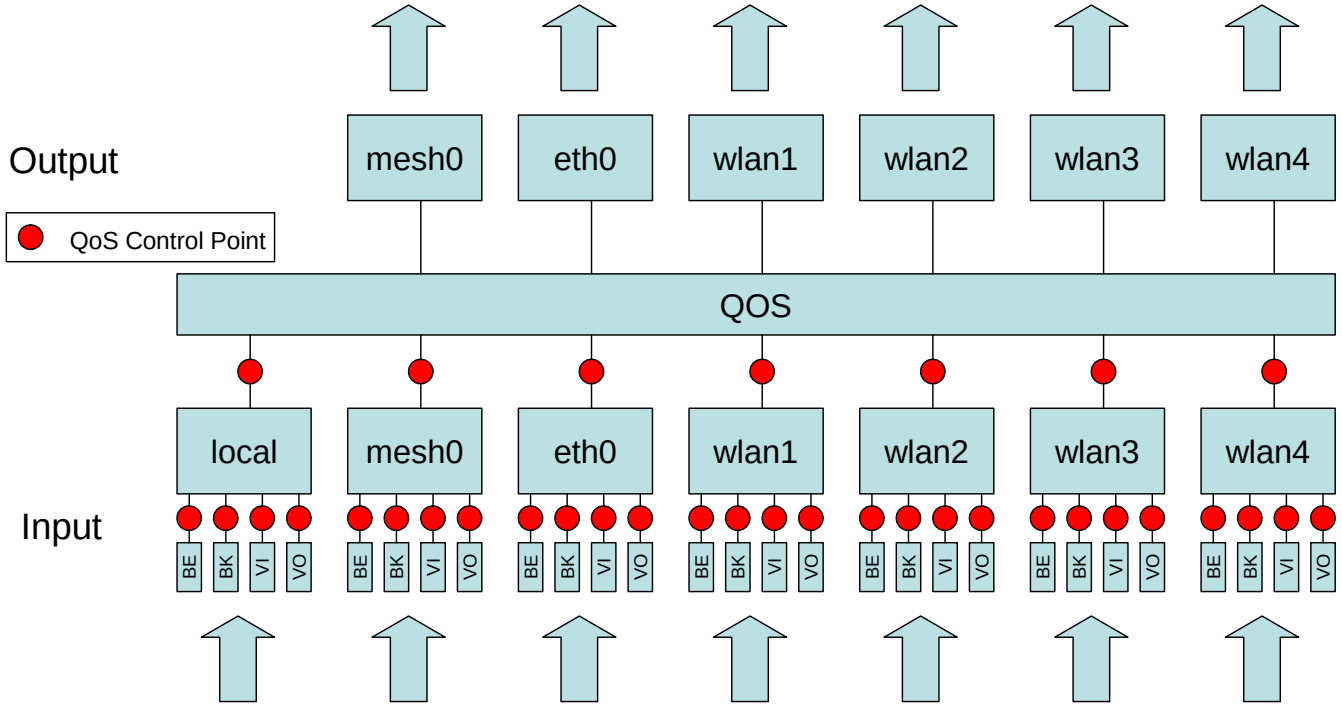

Figure 46. Quality of Service rate reservation control points

INFO

All rate reservation parameter values are in kbps. If no rate reservation parameter is set, rate reservation will be disabled for that interface or interface and traffic combination.

A rate reservation, which guarantees a certain amount of bandwidth, can be made for traffic that enters the EnRoute500 through a particular interface and exits it through another interface. Rate reservations can also be set based on traffic type through an interface. Default

value are applied to interfaces that have their bandwidth reservation parameters set to 'inherit' or are left blank.

CLI

The parameters that are used to set these rate reservations are in the 'qos' interface and are of the form 'out.<output intf>.<input intf>.reserve', where <output intf> is one of the following: default, eth0, mesh0, wlan1, wlan2, wlan3, wlan4; and <input intf> is one of the following: default, eth0, local, mesh0, wlan1, wlan2, wlan3, wlan4.

Typically, most rate reservations will involve reserving bandwidth for traffic from a particular client interface to the mesh0 interface. The example below shows how to reserve differing amount of bandwidth on mesh0 for traffic originating from the wlan1, wlan2, wlan3, and wlan4 interfaces.

```
> use qos
qos> set out.mesh0.wlan1.reserve=2048
qos> set out.mesh0.wlan2.limit=1024
qos> set out.mesh0.wlan3.limit=512
qos> set out.mesh0.wlan4.limit=256
```

A rate reservation for a certain type of traffic that enters the EnRoute500 through a particular interface and exits it through another interface can be set with the 'out.<output intf>.<input intf>.<traffic type>.reserve.' parameters in the 'qos' interface, where <output intf> is one of the following: default, eth0, mesh0, wlan1, wlan2, wlan3, wlan4; <input intf> is one of the following: default, eth0, local, mesh0, wlan1, wlan2, wlan3, wlan4; <traffic type> is one of the following: 'vo', 'vi', 'be', 'bk' (see Table 15 for description of traffic types).

The 'out.default.default.limit' value is applied to interfaces that have the 'out.<output intf>.<input intf>.reserve' parameter set to 'inherit' or is left blank.

The example below shows how to reserve bandwidth for voice, video, best effort, and background traffic from wlan1 through the mesh0 interface to 512 kbps, 1 Mbps, 256 kbps, and 128 kbps, respectively.

```
> use qos
qos> set out.mesh0.wlan1.vo.reserve=512
qos> set out.mesh0.wlan1.vi.reserve=1024
qos> set out.mesh0.wlan1.be.reserve=256
qos> set out.mesh0.wlan1.bk.reserve=128
```

Web GUI

The rate reservation parameters can be set via the web interface under the "QoS" and "Advanced QoS" tabs on the "QoS" page (see Figure 43 and Figure 44).

14 Enabling VLAN Tagging

The EnRoute500 supports VLAN tagging, with each client interface capable of supporting a different VLAN tag. If VLAN tagging is enabled for an interface, client devices that connect to the interface must be capable of receiving VLAN-tagged frames.

14.1 Client Interface Configuration

VLAN tagging can be independently controlled on each client interface (eth0, wlan1-4). The Enable VLAN parameters for the 'eth0', 'wlan1', 'wlan2', 'wlan3', and 'wlan4' interfaces controls the state of VLAN tagging.

VLAN tagging must be enabled on the backhaul Ethernet interface on a mesh cluster's gateway for VLAN tags to be included in data frames sent to the WAN. See section 14.2 for more details.

The VLAN ID value for each client interface is set with the VLAN ID parameter for each interface. The VLAN ID must be in the range from 0 to 4095. Note that 0 and 4095 are reserved values and 1 is the default VLAN ID. There are no restrictions on VLAN IDs for different interfaces or nodes having to match or be different.

CLI

The example below shows how to enable VLAN tagging on the 'wlan1' interface and set the VLAN ID to 12 using the parameters 'vlan.enable' and 'vlan.id' in the 'wlan1' interface.

```
> use wlan1
wlan1> set vlan.enable=yes
> use wlan1
wlan1> set vlan.id=12
```

Web GUI

The VLAN Enable and VLAN ID parameters can be set via the web interface under the "wlanN" tabs on the "Wireless Interfaces" page and on the "Wired/Backhaul Interface" page (see Figure 47).

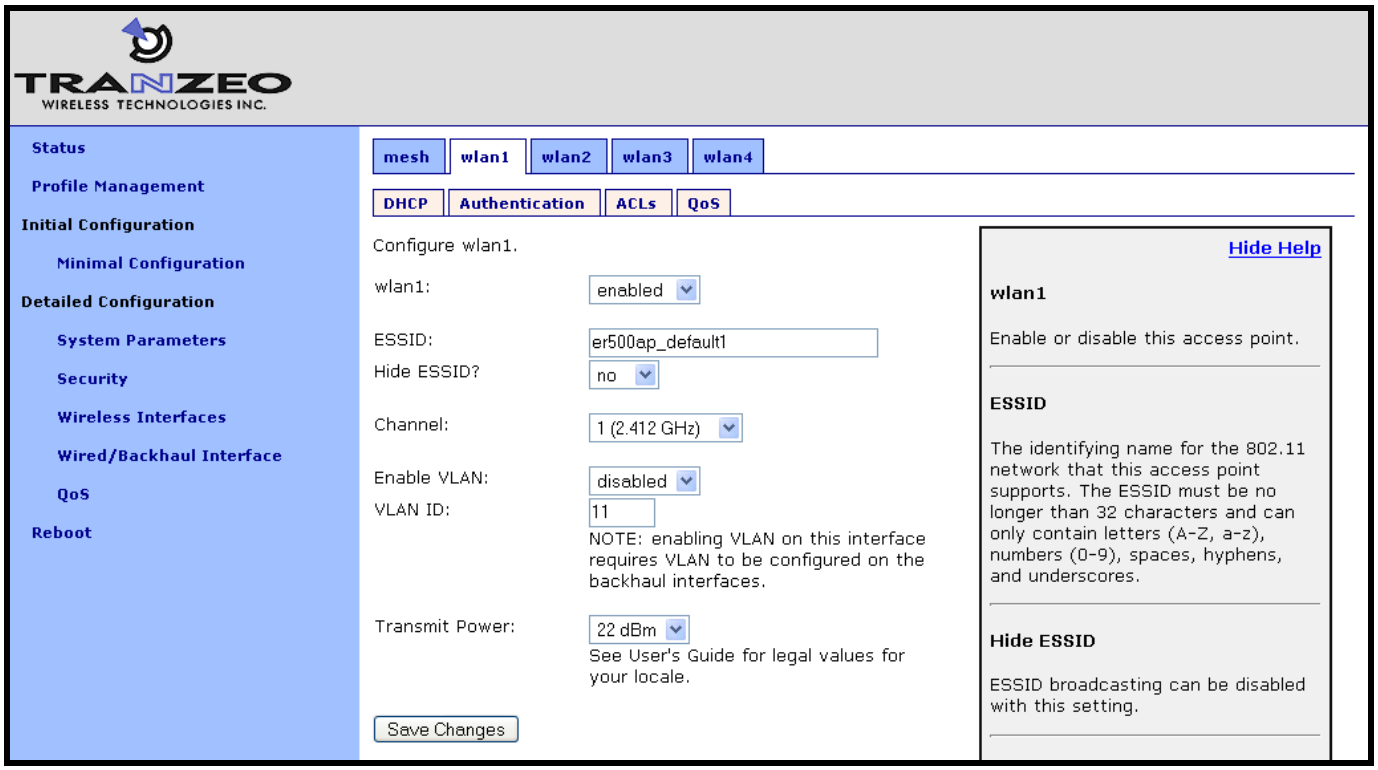

Figure 47. Configuring VLAN for access point interfaces

14.2 Gateway Configuration

For VLAN tags to be preserved on traffic that exits a mesh cluster, VLAN support must be enabled for the Ethernet interface on the mesh cluster's gateway node. The Enable VLAN parameter for the Wired/Backhaul interface controls the state of VLAN tagging. If VLAN tagging is enabled on the gateway's interface to the WAN, all outbound traffic will have its VLAN tags preserved. If VLAN tagging is disabled for the backhaul interface, all VLAN tags will be stripped from frames entering the mesh cluster.

When VLAN is enabled for the backhaul interface, data frames forwarded by the gateway to the WAN will preserve their existing VLAN tag, if they have one. Frames that do not have a tag will be tagged with the default VLAN ID for the gateway's Ethernet interface. The VLAN ID must be in the range from 0 to 4095. Note that 0 and 4095 are reserved values and 1 is the default VLAN ID.

CLI

The example below shows how to enable VLAN tagging on the backhaul interface on a gateway node using the 'vlan.enable' parameter in the 'eth0' interface.

```
> use eth0
eth0> set vlan.enable=yes
```

The example below shows how to set the VLAN ID for the backhaul Ethernet interface using the 'vlan.id' parameter in the 'eth0' interface.

```
> use eth0
eth0> set vlan.id=1
```

Web GUI

The backhaul VLAN parameters are set on the "Wired/Backhaul Interface" page as shown in Figure 48.

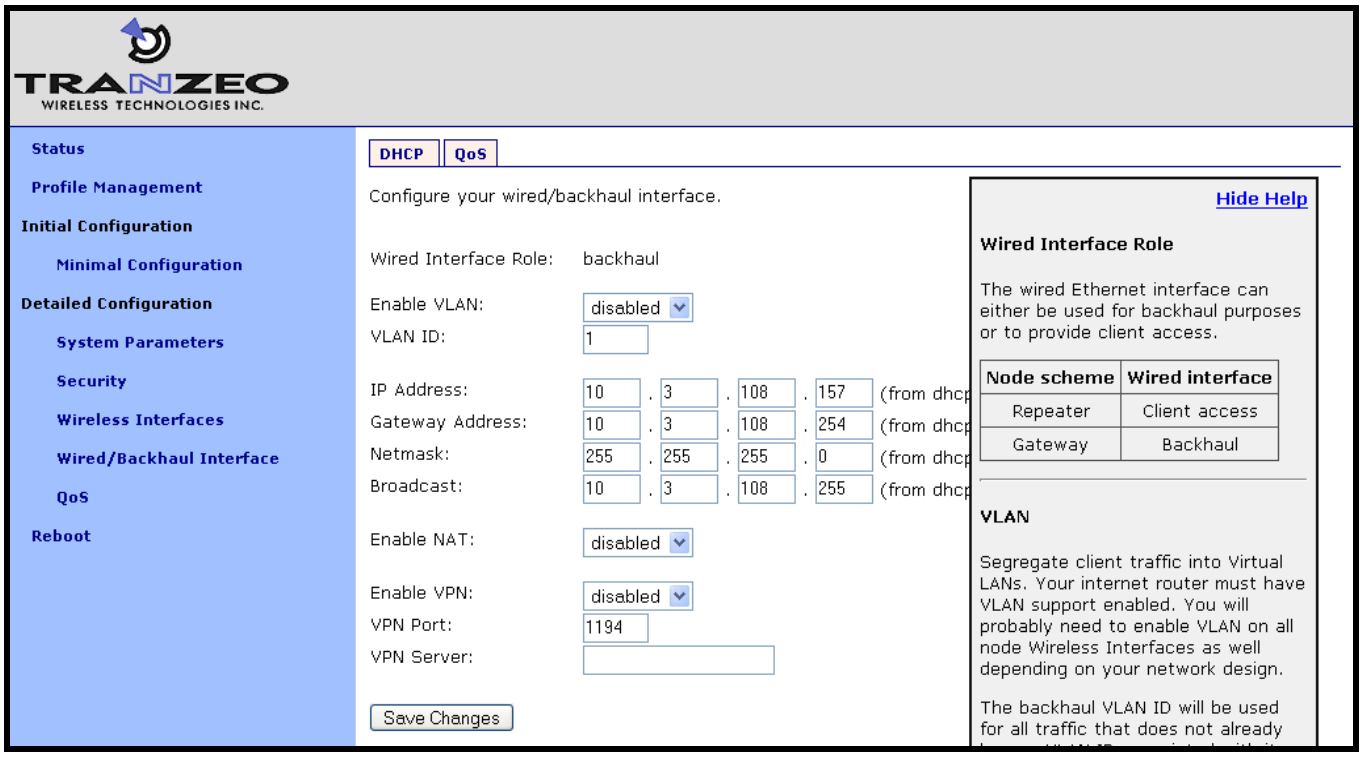

Figure 48. Configuring VLAN for backhaul interface

15 Integration with Enterprise Equipment

The EnRoute500 supports authentication, accounting, and monitoring services that easily integrate with enterprise equipment. In this section the following topics are described:

- Splash pages
- Backhaul health monitoring
- Layer 2 client emulation

15.1 Configuring Splash Pages

The EnRoute500 supports splash pages, which can be used to restrict access to the mesh network and provide information to users that connect to the mesh. When a user connects through a client interface to an EnRoute500 with splash page support enabled, the splash page for the appropriate interface will be displayed and the user will be restricted from accessing other destinations on the Internet until having logged in. The splash page can require the user to enter logon credentials or simply click a button to complete the login process.

To use splash pages, a number of URLs for login, successful login, and failed login must be specified. A RADIUS server that provides authentication services may also need to be specified.

15.1.1 Enabling Splash Pages

The enabling of splash pages can be controlled on a per-interface basis. Two splash page mode are supported – one which requires clients to login in to gain access to the network and another which requires them to simply click on a button on the web page to proceed.

CLI

Enable or disable splash pages with the 'splash.enable.wlanN' parameters in the 'sys' interface. For a splash page to be displayed on an interface, the appropriate parameter must be set to 'yes'. The example below illustrates how to set the 'splash.enable.wlan1' parameter in the 'sys' interface to enable splash pages for the wlan1 interface.

```
> use sys
sys> set splash.enable.wlan1=yes
```

Use the 'splash.auth.server.wlanN.enable' parameters in the 'sys' interface to select whether a user is required to provide login credentials for a particular interface. The example below

illustrates how to set the parameter for the wlan1 interface such that a user will be required to login to access the network.

```
> use sys
sys> set splash.auth.server.enable.wlan1=yes
```

Web GUI

Splash pages can be enabled on a per-interface basis on the "Splash Pages" sub-tab under the "AAA" tab on the "System Parameters" page of the web interface (see Figure 49). Setting whether client login is required can also be set on this page with the "Require Login" parameter.

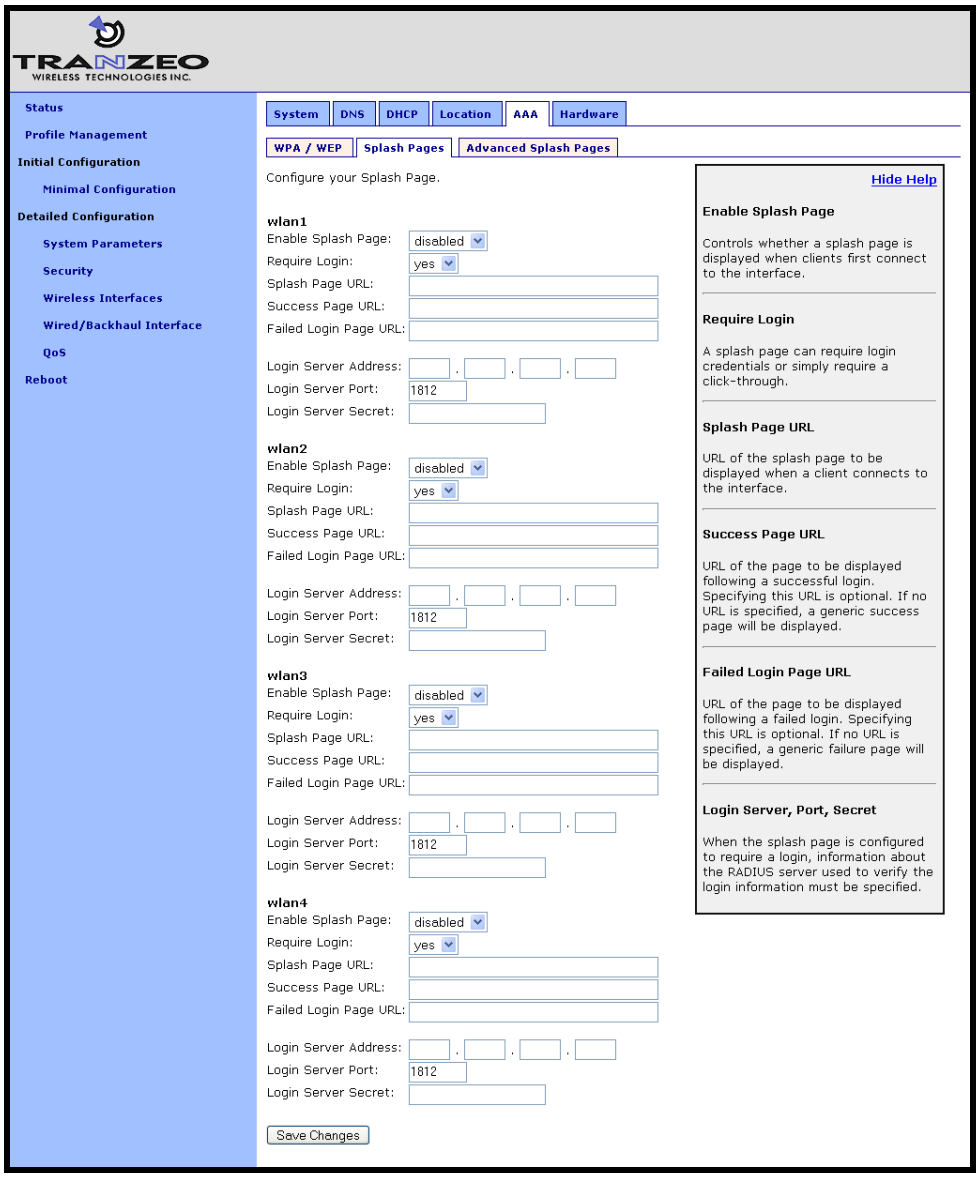

Figure 49. Splash page configuration

15.1.2 Configuring Splash URLs

The URL that a user is redirected to for login purposes can be individually configured for each client interface that supports splash pages (wlan1-4). URLs for successful login, failed login, and error conditions can also be specified for each interface.

The 'login URL' parameter sets the URL that a user is redirected to when they attach to the interface and have not yet been authenticated. This parameter should not be left blank if splash pages are enabled for the interface. No client would be able to access the network through the interface if the login URL parameter does not point to a valid URL.

The 'success URL' parameter sets the URL that a user is redirected to when they have successfully logged in. If this variable is left blank, a default page that indicates login success will be displayed.

The 'fail URL' parameter sets the URL that a user is redirected to when a login attempt fails. If this variable is left blank, a default page that indicates login failure will be displayed.

The 'error URL' parameter sets the URL that a user is redirected to when a login error has occurred. For example, this page would be displayed if a valid authentication server could not be reached. If this variable is left blank, a default page that indicates an error has occurred will be displayed.

CLI

The 'splash.url.<intf>.login' parameters in the 'sys' interface, where <intf> is either 'wlan1', 'wlan2', 'wlan3', or 'wlan4', set the login URLs. The 'splash.url.<intf>.success' parameters in the 'sys' interface, where <intf> is either 'wlan1', 'wlan2', 'wlan3', or 'wlan4', set the success URLs. The 'splash.url.<intf>.fail' parameters in the 'sys' interface, where <intf> is either 'wlan1', 'wlan2', 'wlan3', or 'wlan4', set the fail URLs. The 'splash.url.<intf>.error' parameters in the 'sys' interface, where <intf> is either 'wlan1', 'wlan2', 'wlan3', or 'wlan4', set the error URLs

The example below shows how the 'wlan1' and 'wlan2' interfaces can be set to use different URLs for the login process.

```
> use sys
sys> set splash.url.wlan1.login=http://server.domain.com/wlan1_login.htm
sys> set splash.url.wlan1.success=http://server.domain.com/wlan1_success.htm
sys> set splash.url.wlan1.fail=http://server.domain.com/wlan1_fail.htm
sys> set splash.url.wlan1.error=http://server.domain.com/wlan1_error.htm
sys> set splash.url.wlan2.login=http://server.domain.com/wlan2_login.htm
sys> set splash.url.wlan2.success=http://server.domain.com/wlan2_success.htm
sys> set splash.url.wlan2.fail=http://server.domain.com/wlan2_fail.htm
sys> set splash.url.wlan2.error=http://server.domain.com/wlan2_error.htm
```

Web GUI

All of the splash page-related URLs can be set on the "Splash Pages" sub-tab under the "AAA" tab on the "System Parameters" page of the web interface (see Figure 49).

15.1.3 Sample HTML Code for Splash Pages

The login HTML page must contain specific form information as shown in the sample code in Figure 50 and Figure 51. Figure 50 contains the code required for an interface that requires a login. Figure 51 contains code for a login page that the user just clicks through to unlock network access.

The critical lines in Figure 50 are 6, 12, 15, and 19. The 'action' value in line 6 of Figure 50 must point to a server name for which there is a DNS proxy entry on the local node and the last part of it must be '/radius/login.cgi'. The DNS proxy entry, which will be different for each node in the network, must be mapped to one of the node's IP addresses (see section 6.7 for more information on DNS proxy configuration).

The example below shows how to configure the DNS proxy assuming the login page redirects to the host 'redirect.domain.com' and the IP address of the wlan1 interface is 10.1.2.1.

```
> use sys
sys> set dnsproxy.enable=yes
sys> set dnsproxy.hosts="dns.proxy.name.here=10.1.2.1"
```

INFO

The DNS proxy setting is used in conjunction with the splash pages to ensure that a common login URL can be used on all nodes. The DNS proxy entry directs the results of the login process to the right location – that is, the EnRoute500 that the client device is connected to.

The login page must also contain the 'input' fields on lines 12, 15, and 19. These are used to allow a user logging in to provide their username and password, and to submit them. The names of these input fields, 'username', 'password', and 'login', must not be changed.

```
 1 <html>
 2 <head>
 3   <title>Test Login Page</title>
 4 </head>
 5 <body>
 6   <form method="POST" action="https://dns.proxy.name.here/radius/login.cgi">
 7   Welcoming text or 'Terms of Service' could go here. <br />
 8
 9   <table border="0">
10   <tr>
11     <td> Username: </td>
12     <td> <input name="username" type="text"><br /> </td>
13   </tr><tr>
14     <td> Password: </td>
15     <td> <input name="password" type="password"> </td>
16   </tr>
17   </table>
18
19     <input name="login" type="submit" value="Submit">
20   </form>
21 </body>
22 </html>
```

Figure 50. Sample HTML code for login web page

If the splash page is not configured to require a user to provide login credentials, the requirements for the login page are slightly different, as shown in Figure 51. The page must still contain a form definition similar to that on line 6 in Figure 51. The 'action' value must be set to point to a proxied server name, just as for the case where a user is required to provide login credentials. The last part of the 'action' value must be '/splash/nologin.cgi'. Also, a button with the name 'login' must be defined, as shown on line 8 of Figure 51.

```
 1 <html>
 2 <head>
 3   <title>Test Login Page</title>
 4 </head>
 5 <body>
 6   <form method="POST" action="https://dns.proxy.name.here/splash/nologin.cgi">
 7   Welcoming text or 'Terms of Service' could go here.<br />
 8     <input name="login" type="submit" value="Continue">
 9   </form>
10 </body>
11 </html>
```

Figure 51. Sample HTML code for web page when authentication is disabled

15.1.4 Configuring the Authentication Server

A RADIUS authentication server must be specified when the splash page is enabled for an interface and login is required. The following parameters must be specified:

- the server address – can be either a hostname or and IP address

- the port on the server that the RADIUS server is listening on
- the shared secret – must be a string of alphanumeric characters that is 32 characters or less in length.

CLI

The 'splash.auth.server.<intf>.host', 'splash.auth.server.<intf>.port', and 'splash.auth.server.<intf>.secret' parameters in the 'sys' interface, where <intf> is either 'wlan1', 'wlan2', 'wlan3', or 'wlan4', specify the authentication server to use. The example below shows how to configure the authentication server for interfaces 'wlan1' and 'wlan2'.

```
> use sys
sys> set splash.auth.server.wlan1.host=auth1.yourserverhere.com
sys> set splash.auth.server.wlan1.port=1812
sys> set splash.auth.server.wlan1.secret=authsecret
sys> set splash.auth.server.wlan2.host=auth2.yourserverhere.com
sys> set splash.auth.server.wlan2.port=1812
sys> set splash.auth.server.wlan2.secret=authsecret
```

Web GUI

The authentication server parameters can be set on the "Splash Pages" sub-tab under the "AAA" tab on the "System Parameters" page of the web interface (see Figure 49).

15.1.5 Trusted MAC Addresses

A list of trusted MAC addresses, which do not require splash page authentication, can be defined. When a device with one of these MAC addresses connects to a node, it will automatically have full access to the WAN.

CLI

The list of trusted MAC addresses is set with the 'splash.trusted_macs' parameter in the 'sys' interface. The MAC addresses are specified as a list of 48-bit addresses separated by commas. An example of setting this parameter is shown below.

```
> use sys
sys> set splash.trusted_macs="aa:bb:cc:00:00:01,aa:bb:cc:00:00:02"
```

Web GUI

The authentication server parameters can be set on the "Advanced Splash Pages" sub-tab under the "AAA" tab on the "System Parameters" page of the web interface (see Figure 52). The list of trusted MAC addresses is displayed on this page. To delete a trusted MAC from the list, click on the "Delete MAC" button next to the MAC address.

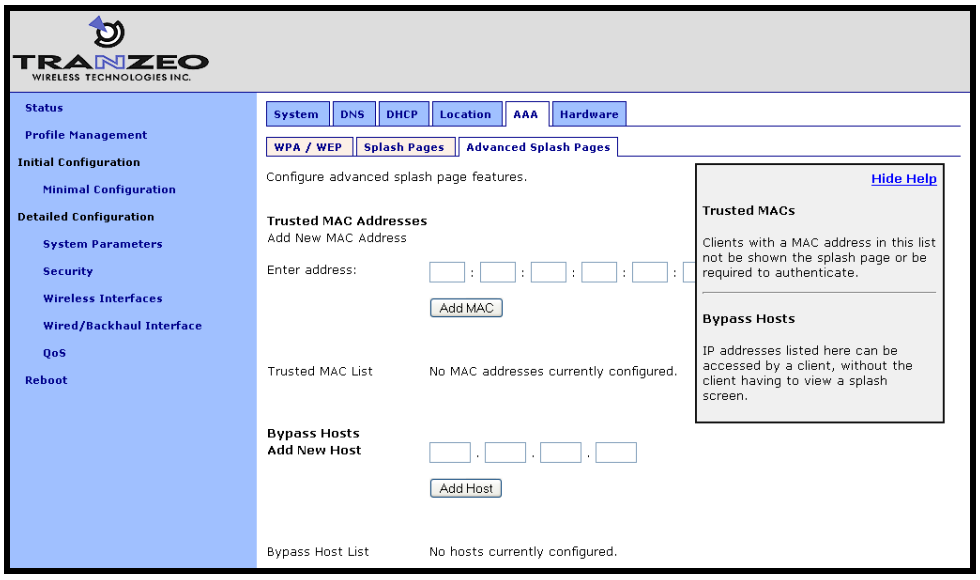

Figure 52. Adding trusted MAC addresses and accessible hosts

15.1.6 Bypass Splash Pages for Access to Specific Hosts

It is possible to specify a list of IP addresses that clients can access without the clients having to view a splash screen.

CLI

The list of hosts that can be accessed without having to view a splash screen is set with the 'splash.bypass_hosts' parameter in the 'sys' interface. The hosts are specified by their IP addresses and must be separated by commas. An example of setting this parameter is shown below.

```
> use sys
sys> set splash.bypass_hosts="1.1.1.1,2.2.2.2"
```

Web GUI

The IP addresses of hosts that can be accessed without having to view a splash screen can be set on the "Advanced Splash Pages" sub-tab under the "AAA" tab on the "System Parameters" page of the web interface (see Figure 52). The list of IP addresses of bypassed hosts is displayed on this page. To delete an IP address from the list, click on the "Delete Host" button next to the IP address.

15.2 Layer 2 Emulation

Certain back-end systems (Internet gateways) use the MAC addresses of client devices for authentication and accounting purposes. The EnRoute500 uses a layer 3 approach to mesh routing, which means that the client MAC addresses are typically not provided to the back-end servers. A layer 2 emulation mode can be enabled on the EnRoute500 to provide the client MAC address information to back-end systems.

When the layer 2 emulation mode is enabled, a mesh cluster gateway will send Ethernet (layer 2) frames to the WAN using the MAC address of the device the packet originated from as the source address. Mesh gateways will also act as proxies and forward packets with MAC destination addresses of clients that are in the mesh cluster they service.

CLI

Layer 2 emulation is enabled with the 'l2.client_mac_fwd' parameter in the 'sys' interface. This parameter should be set to the same value for all devices in a given mesh cluster. The example below shows how to enable layer 2 emulation.

```
> use sys
sys> set l2.client_mac_fwd=yes
```

16 Firmware Management

The EnRoute500 supports secure remote firmware upgrade.

16.1 Displaying the Firmware Version

CLI

Firmware version information is available in the 'version' interface. The example below shows how to display the current firmware version.

```
> use version
version> get release
 release = ENROUTE500_20060419_00_00_0133
```

Web GUI

The firmware version is also displayed at the top of the "Status" page accessible via the web interface.

16.2 Upgrading the Firmware

Contact Tranzeo for instructions on upgrading the EnRoute500's firmware.

17 Glossary

ACL	Access Control List
AP	Access Point
CLI	Command line interface
ESSID	Extended Service Set Identifier
LAN	Local-Area Network
Mesh cloud	A group of EnRoute500 nodes configured as one or more clusters
Mesh cluster	A group of two or more EnRoute500 nodes with at least one configured as a gateway
Mesh gateway	A mesh node that, in addition to relaying traffic between neighboring mesh nodes and supporting wireless clients through its built-in APs, acts as the layer 3 gateway for a mesh cluster
Mesh node	A single EnRoute500 that is part of a mesh cluster
Mesh repeater	A mesh node that relays traffic to neighboring mesh nodes and supports wireless and wired clients.
NAT	Network Address Translation
PoE	Power over Ethernet
QoS	Quality of Service
RSSI	Received signal strength indicator
VLAN	Virtual Local-Area Network
VPN	Virtual Private Network
WAN	Wide-Area Network
WLAN	Wireless Local-Area Network
WPA	Wi-Fi Protected Access
WPA-PSK	Wi-Fi Protected Access Pre-Shared Key