EL-900 Access Point
User's Guide

Rev. A1

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

Tranzeo, the Tranzeo logo and EL-900 are trademarks of Tranzeo Wireless Technologies Inc. All rights reserved.

All other company, brand, and product names are referenced for identification purposes only and may be trademarks that are the properties of their respective owners.

Copyright © 2007, Tranzeo Wireless Technologies Inc.

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

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.

INFO

The Tranzeo EL-900 Access Point 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 EL-900 8
1.1 EL-900 Variants 8
1.2 EL-900 Capabilities 8
1.3 EL-900 Interfaces 9
1.3.1 Ethernet and PoE 10
1.3.2 Antenna 11
1.4 Deployment Considerations 11
1.4.1 AP Channel Selection 12

2 Connecting to the EL-900 13
2.1 Network Interfaces 13
2.2 Connecting to an Unconfigured EL-900 14
2.3 Default Login and Password 15
2.4 Resetting the 'admin' Password 15

3 Using the Web Interface 16
3.1 Accessing the Web Interface 16
3.2 Navigating the Web Interface 18
3.3 Setting Parameters 18
3.4 Help Information 19
3.5 Rebooting 19

4 Using the Command Line Interface 21
4.1 Accessing the CLI 21
4.2 User Account 21
4.3 CLI Interfaces 22
4.4 CLI Features 22
4.4.1 Control of the Cursor 22
4.4.2 Cancel a Command 22
4.4.3 Searching the Command History 23
4.4.4 Executing a Previous Command 23
4.5 CLI Commands 23
4.5.1 '?' command 23
4.5.2 'whoami' command 23
4.5.3 'help' command 24
4.5.4 'show' command 24
4.5.5 'use' command 25
4.5.6 'set' command 25
4.5.7 'get' command 26
4.5.8 'list' command 27
4.5.9 'ping' command 27

4.5.10 'ifconfig' command 28
4.5.11 'route' command 28
4.5.12 'clear' command 28
4.5.13 'history' command 29
4.5.14 '!' command 30
4.5.15 'exit' command 31
4.5.16 'quit' command 31

5 Initial Configuration of an EL-900 32

6 Status Information 34
6.1 Configuration Overview Page 34
6.2 Interface Status 35
6.2.1 Virtual AP Interfaces 35
6.2.2 Wired Interface Status 36
6.3 Bridging 36
6.4 Routing Table 37
6.5 ARP Table 38
6.6 Event Log 39
6.7 DHCP Event Log 39

7 Configuration Profile Management 41
7.1 Saving the Current Configuration 41
7.2 Load a Configuration Profile 42
7.3 Delete a Configuration Profile 42
7.4 Downloading a Configuration Profile from an EL-900 43
7.5 Uploading a Configuration Profile to an EL-900 44

8 Mode of Operation 45

9 System Settings 47
9.1 User Password 47
9.2 Node ID 48
9.3 DNS / Domain Settings 49
9.4 DNS Proxy Configuration 50
9.5 NetBIOS Server 51
9.6 SNMP 51
9.7 Location 52
9.8 Certificate Information 54
9.9 Time Synchronization 54
9.10 Web GUI Console 56
9.11 OnRamp Configuration Access 56
9.12 CLI Timeout 58

10 Client Addressing Schemes 59
10.1 Implicit Addressing Scheme 60
10.1.1 LAN Prefix 61

10.1.2 Client Address Space Segmentation in Implicit Addressing Mode 61
10.2 Explicit Addressing Scheme 64

11 Ethernet Interface Configuration 66
11.1 DHCP 66
11.2 Manual IP Configuration 69

12 Bridge Interface Configuration 71
12.1 IP Configuration 71
12.2 Bridging Parameters 73

13 Virtual Access Point (VAP) Configuration 74
13.1 Virtual Access Point Interfaces 75
13.2 Enabling and Disabling Virtual Access Points 75
13.3 Virtual Access Point Client Device Address Space 75
13.4 Channel 77
13.5 ESSID 78
13.6 IP Configuration of Client Devices 79
13.6.1 IP Configuration of Clients Devices via DHCP 79
13.6.2 Manual IP Configuration of Client Devices 79
13.7 Client Devices 81
13.8 Encryption and Authentication 81
13.8.1 WEP Encryption 82
13.8.2 WPA Pre-Shared Key Mode (WPA-PSK) 83
13.8.3 WPA EAP Mode 84
13.9 Transmit Power Cap 85
13.10 Radio Rate 86
13.11 Preamble Length 86
13.12 Beacon Interval 87
13.13 Maximum Link Distance 87

14 Client DHCP Configuration 89
14.1 Using Local DHCP Servers 89
14.2 Using a Centralized DHCP Server 92
14.2.1 Support for Clients with Static IP Addresses 93
14.2.2 Configuring the EL-900s 93
14.2.3 Configuring the Central DHCP Server 95

15 Connecting an EL-900 to a LAN 97
15.1 Routed mode 97
15.1.1 Manual Configuration 97
15.1.2 Network Address Translation (NAT) 98
15.2 Bridge Mode 99

16 Controlling Access to the EL-900 100
16.1 Firewall 100
16.2 Gateway Firewall 101

16.3 Blocking Client-to-Client Traffic 102
16.4 Connection Tracking 103
16.4.1 Connection Tracking Table Size 104
16.4.2 Connection Tracking Timeout 104
16.4.3 Limiting Number of TCP Connections Per Client Device 105
16.5 Custom Firewall Rules 105
16.6 Access Control Lists (ACLs) 107

17 Quality of Service (QoS) Configuration 109
17.1 Priority Levels 109
17.2 Rate Limiting 112
17.3 Rate Reservation 114

18 Enabling VLAN Tagging 117
18.1 Client Access Interface Configuration 117
18.2 Ethernet Interface Configuration 118

19 Integration with Enterprise Equipment 120
19.1 Configuring Splash Pages 120
19.1.1 Enabling Splash Pages 120
19.1.2 Configuring Splash URLs 122
19.1.3 Sample HTML Code for Splash Pages 123
19.1.4 Configuring the Authentication Server 124
19.1.5 Trusted MAC Addresses 125
19.1.6 Bypass Splash Pages for Access to Specific Hosts 126
19.2 Layer 2 Emulation 127

20 Diagnostics Tools 129
20.1 Ping 129
20.2 Traceroute 129
20.3 Packet Capture 130
20.4 Centralized DHCP Testing 132
20.5 RADIUS Server Testing 133
20.6 Diagnostic Dump 133

21 Firmware Management 135
21.1 Displaying the Firmware Version 135
21.2 Upgrading the Firmware 135

Glossary 137

Abbreviations 138

1 Working with the EL-900

Thank you for choosing the Tranzeo EL-900 802.11 Access Point. The EL-900 is a full-featured access point in a ruggedized enclosure designed for outdoor installation. 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 an EL-900.

1.1 EL-900 Variants

There are two EL-900 variants available, as shown in Table 1.

Model Number	Frequency Band	802.11 standard
EL-900HG	2.4 GHz	802.11b/g
EL-900HA	5.8 GHz	802.11a

Table 1. EL-900 variants

INFO

Throughout the manual, "EL-900" will be used to collectively refer to this family of products. Where the functionality of the variants differs, the actual model number will be used.

1.2 EL-900 Capabilities

Based on the IEEE 802.11b/g and 802.11a standards and complete with FCC certification, the EL-900 family of outdoor access points are fully standards compliant. This family of outdoor access points has been designed with a multitude of network and management features for ease of installation and operation in any new or existing network. Features include:

- Multiple ESSIDs per radio
- High-powered +26dBm output in 802.11b/g mode
- High-powered +23dBm output in 802.11a mode
- Router or bridge mode operation
- DHCP server
- DHCP relay
- QoS support (IEEE 802.11e WMM)
- VLAN support (IEEE802.1q)
- Security
    - WPA
    - WPA2
    - WEP 64/128

  - Stateful packet inspection
  - Custom firewall rules
- Web GUI
- Tranzeo CLI (SSH)
- Remote upgrade
- Configuration management

1.3 EL-900 Interfaces

The interfaces available on the EL-900 are Ethernet and a radio port.

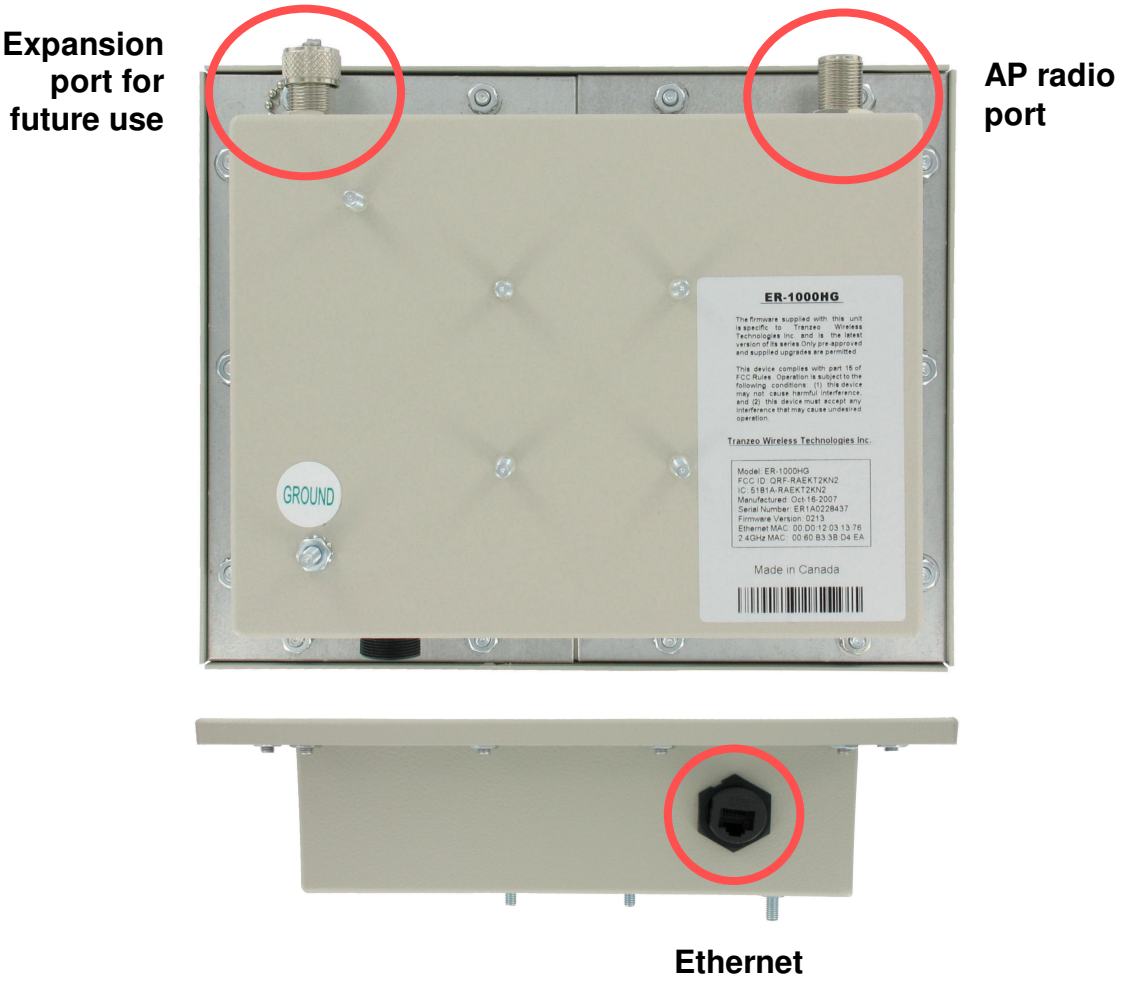

Figure 1. EL-900 interfaces.

Interface	Description
AP radio port	N-type antenna connector for access point radio
Ethernet	10/100 Mbit Ethernet interface
Passive PoE	PoE power input (9-28VDC, 12W) *Not compatible with IEEE 802.3af*

Table 2. EL-900 Interfaces

1.3.1 Ethernet and PoE

The EL-900 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 EL-900 is provided in Table 3.

INFO

The EL-900 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

To power the EL-900, connect an Ethernet cable from the Ethernet port of the EL-900 to the port labeled “CPE” on the supplied PoE injector and apply power to the PoE injector using the supplied power supply

DO NOT CONNECT ANY DEVICE OTHER THAN THE EL-900 TO THE PORT LABELED "CPE" ON THE PoE INJECTOR. NETWORK EQUIPMENT THAT DOES NOT SUPPORT PoE CAN BE PERMANENTLY DAMAGED BY CONNECTING TO A PoE SOURCE. NOTE THAT MOST ETHERNET INTERFACES ON PERSONAL COMPUTERS (PCs), LAPTOP/NOTEBOOK COMPUTERS, AND OTHER NETWORK EQUIPMENT (E.G. ETHERNET SWITCHES AND ROUTERS) DO NOT SUPPORT PoE.

1.3.2 Antenna

The EL-900 AP radio port is an N-type RF connector that can interface with a wide range of Tranzeo antennas. After purchasing the desired 2.4GHz or 5.8GHz antenna (for the EL-900HG or EL-900HA models respectively), attach the antenna to the access point (AP) radio port on the EL-900. The antenna must be chosen such that its gain combined with the output power of the radio complies with maximum radiation power regulatory requirements in the area the EL-900 is used.

The following is a list of supported accessory antennas sold with the EL-900 family, as shown in Table 2.
This device has been designed to operate with the antennas listed below, and having a maximum gain of 32 dBi. Antennas not included in this list or having a gain greater than 32 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

Tranzeo Part Number	Antenna Type
TR-OD900-12	Omni
TR-900H-120-12	Horizontal Sector
TR-900V-120-13	Vertical Sector

Table 2 Supported Accessory antennas

1.4 Deployment Considerations

The EL-900's radio operates in either the 2.4 GHz or the 5.8 GHz ISM band, depending on the model. It is possible that there will be other devices operating in these bands that will interfere with the EL-900's radio. Interference from adjacent EL-900s can also degrade performance if the EL-900s are not configured properly.

It is advisable to carry out a site survey prior to installation to determine what devices are operating in the band that your EL-900 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.

1.4.1 AP Channel Selection

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 EL-900HG's radio can be configured to use are overlapping. Only channels 1, 6, and 11 are non-overlapping.

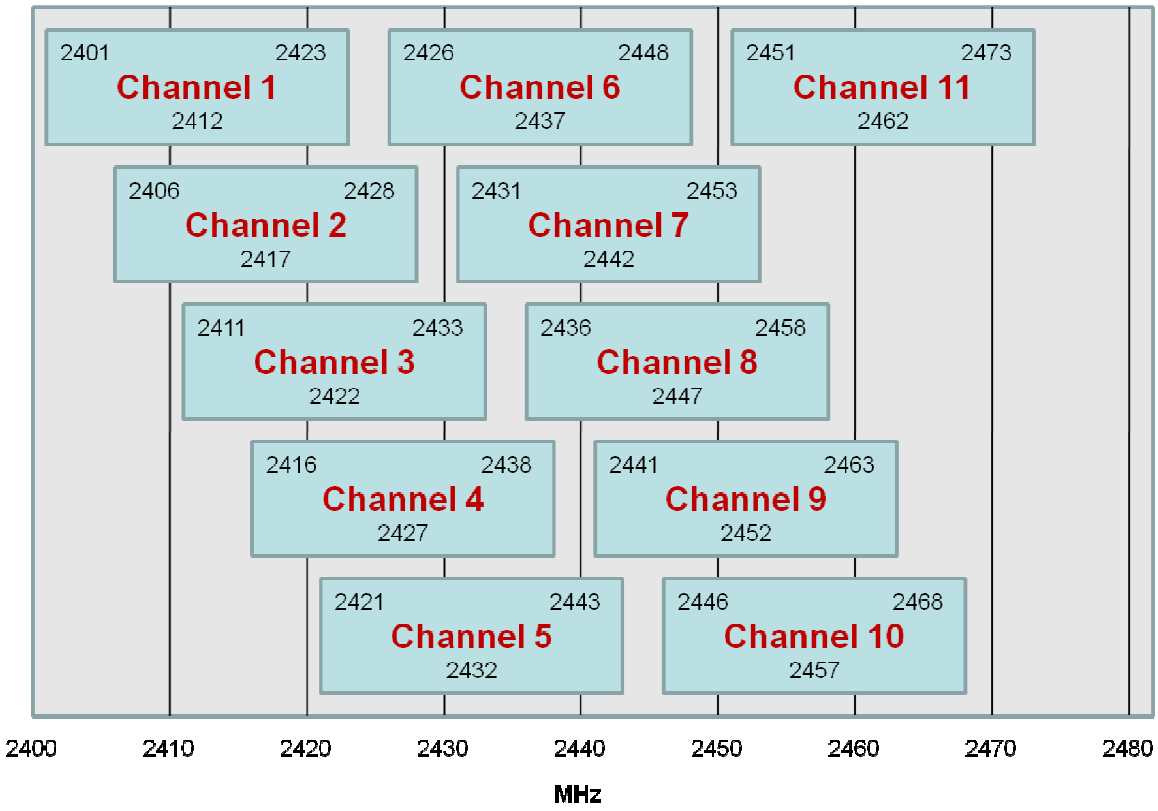

Figure 2. 802.11b/g channel chart, showing top, bottom, and center frequencies for each channel

2 Connecting to the EL-900

The EL-900 can be configured and monitored by connecting to one of its network interfaces. The wired Ethernet interface on the EL-900 should be used for initial configuration of the device, but the wireless network interface can be used to connect to the device after initial configuration has been completed.

2.1 Network Interfaces

The EL-900 has several network interfaces, as shown in Table 4.

INFO

The network interfaces listed in the table below are logical, not hardware, interfaces. Some of the interfaces listed in the table share the same hardware interface.

Interface	Hardware Interface	Primary Function	Interface Availability	Default Address	Can be altered by the user?
Wired	Ethernet	Connecting to a LAN	Enabled by default	10.253.0.1/24	No
Bridge	N/A	Access to the device when operating in bridge mode	Enabled in bridge mode	10.253.1.1/24	No
Static Configuration	Ethernet	Configuring the device before a unique Ethernet IP address has been configured	Always present	169.254.253.253/16	Yes
OnRamp Configuration	Ethernet	Configuring the device before a unique Ethernet IP address has been configured. Unlike the static configuration interface, this interface's address can be modified, allowing multiple unconfigured EL-900s to be attached to a LAN	Disabled by default	N/A	No
VAP 1 – 4	AP radio	Providing connectivity to wireless client devices	Only VAP1 enabled by default	10.253.1.1/24 10.253.2.1/24 10.253.3.1/24 10.253.4.1/24	No
Centralized DHCP	N/A	Provides a gateway for client devices when using centralized DHCP mode	All disabled by default	N/A	No

Table 4. EL-900 network interfaces

Note that the "Static Configuration" interface is the only interface that has a fixed address that cannot be changed by the user. Since this interface is known to always be present, it can be

used for initial configuration and for accessing devices whose configuration settings are unknown.

2.2 Connecting to an Unconfigured EL-900

Use the Static Configuration interface with IP address **169.254.253.253** and netmask **255.255.0.0** to establish network connectivity to an unconfigured EL-900.

The Static Configuration interface functions only with the EL-900's wired interface. Do not try to access the EL-900 over a wireless link using the address of this interface.

To connect to an EL-900 using its Static Configuration IP address, you must configure your computer's IP address to be in the 169.254.253.253/16 subnet, e.g. 169.254.253.1 and connect the computer's Ethernet cable to the "PC" port on the EL-900's PoE injector.

ENSURE THAT THE DATA CONNECTION FROM THE PC OR THE LAN IS MADE TO THE "PC" PORT. DO NOT CONNECT ANY DEVICE OTHER THAN THE EL-900 TO THE PORT LABELED "CPE" ON THE PoE INJECTOR. NETWORK EQUIPMENT THAT DOES NOT SUPPORT PoE CAN BE PERMANENTLY DAMAGED BY CONNECTING TO A PoE SOURCE. NOTE THAT MOST ETHERNET INTERFACES ON PERSONAL COMPUTERS (PCs), LAPTOP/NOTEBOOK COMPUTERS, AND OTHER NETWORK EQUIPMENT (E.G. ETHERNET SWITCHES AND ROUTERS) DO NOT SUPPORT PoE.

Since the Static Configuration IP address is the same for all EL-900s, you should not simultaneously connect multiple EL-900s to a common LAN and attempt to access them using the Static Configuration IP address.

If you are configuring multiple EL-900s with the same computer in rapid succession, it may be necessary to clear the ARP cache since the IP addresses for the EL-900s 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 EL-900 entry

Linux

```
arp –d 169.254.253.253
```

2.3 Default Login and Password

The EL-900's default login is '**admin**' and the default password is '**default**'. The login and password are the same for the web interface and the CLI. Changing the password using one of the interfaces will change it for the other interface as well.

2.4 Resetting the 'admin' Password

The EL-900 supports a password recovery feature for the 'admin' account, should the password be lost.

Completing the password recovery procedure requires that you contact Tranzeo technical support. Please check the Tranzeo website (www.tranzeo.com) for how to contact technical support and hours of operation.

For security purposes, the 'admin' password can only be reset in the first 15 minutes of operation of the device. You will be able to power the unit on and off to be able to reset the password.

3 Using the Web Interface

The EL-900 has a web interface accessible through a browser that can be used to configure the device and display status parameters.

3.1 Accessing the Web Interface

You can access the web interface by entering one of the EL-900's IP addresses in the URL field of a web browser (see section 2.2 for a description of how to access an unconfigured EL-900 using its Ethernet interface). When you enter this URL, you will be prompted for a login and password. The default login and password used for the web interface are '**admin**' and '**default**', respectively.

Figure 3. Login window for web interface

Since the certificate used in establishing the secure link to the EL-900 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.

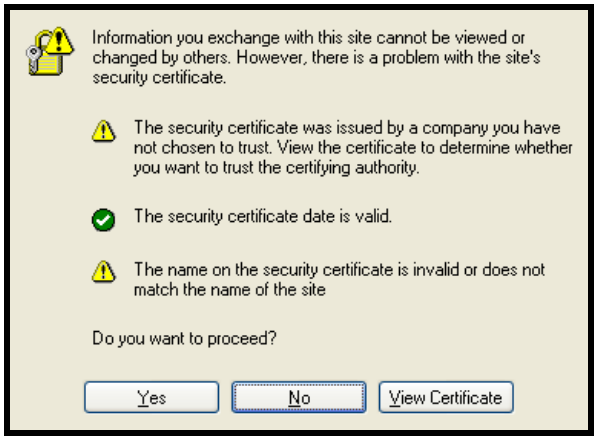

Figure 4. Certificate warning

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

- Firmware version and list of installed patches
- System uptime
- System mode of operation (router or bridge)
- Bridge information (if bridge mode is selected)
- IP addresses, netmasks, and MAC addresses for each client access interface
- Status, channel, ESSID, and encryption type for each virtual access point interface
- VLAN status and ID for all interfaces

To access the status page from any other page in the web interface, click on the “Status” link in the navigation bar that appears on the left side of the web interface.

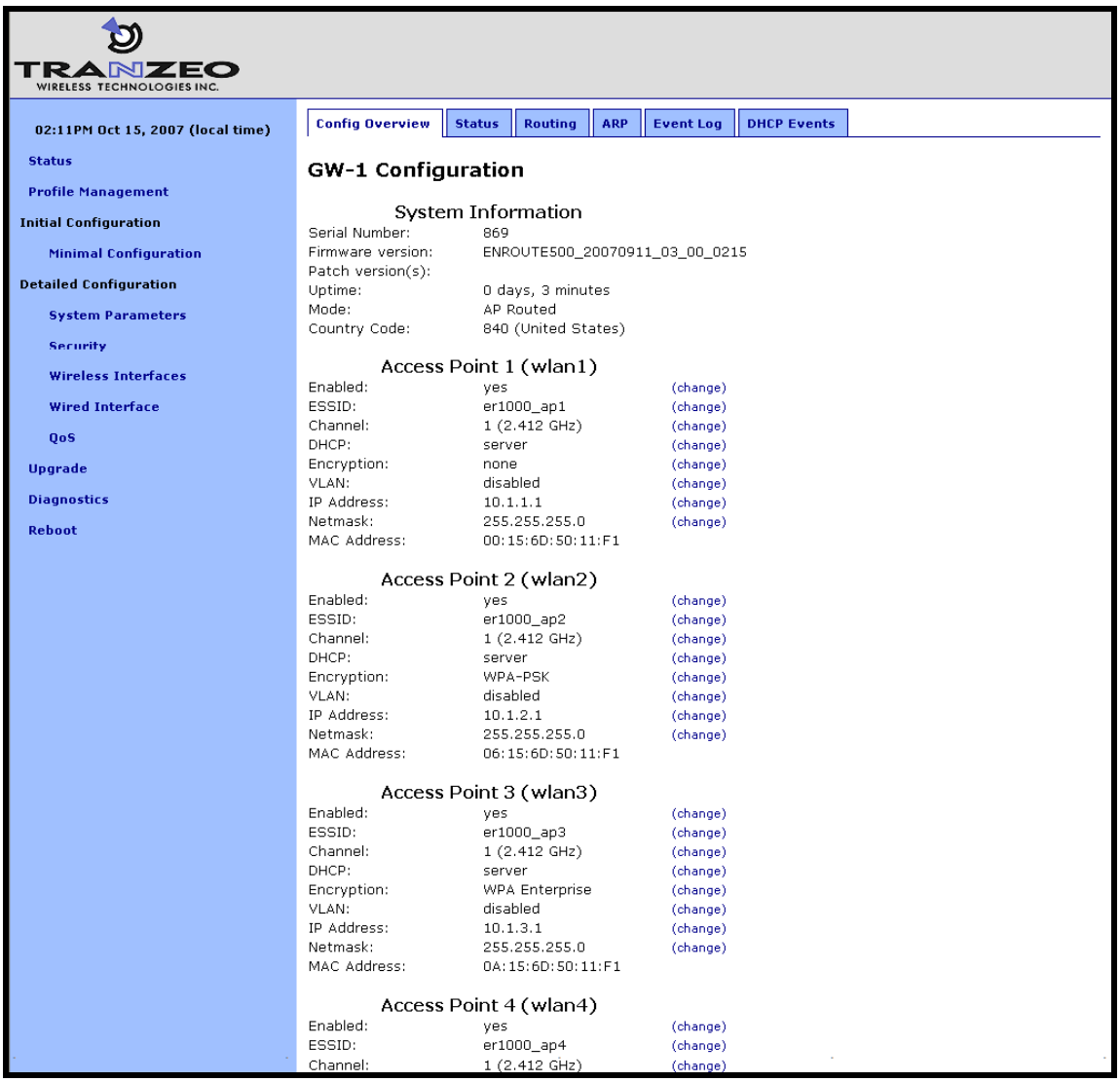

Figure 5. Configuration overview page displayed when logging in

3.2 Navigating the Web Interface

The web interface uses a three-tiered navigation scheme.

1. The first tier of navigation is the navigation bar shown on the left side of the screen. This navigation bar is displayed on all pages in the web interface and remains the same on all pages.
2. The second tier of navigation is the primary row of tabs shown across the top of the screen on many of the pages in the web interface. The labels in these tabs vary based on which page is selected on the navigation bar.
3. The third tier of navigation is the second row of tabs shown below the first row. These tabs are not present on all pages and their labels vary based on the selections made on the navigation bar and the primary row of tabs.

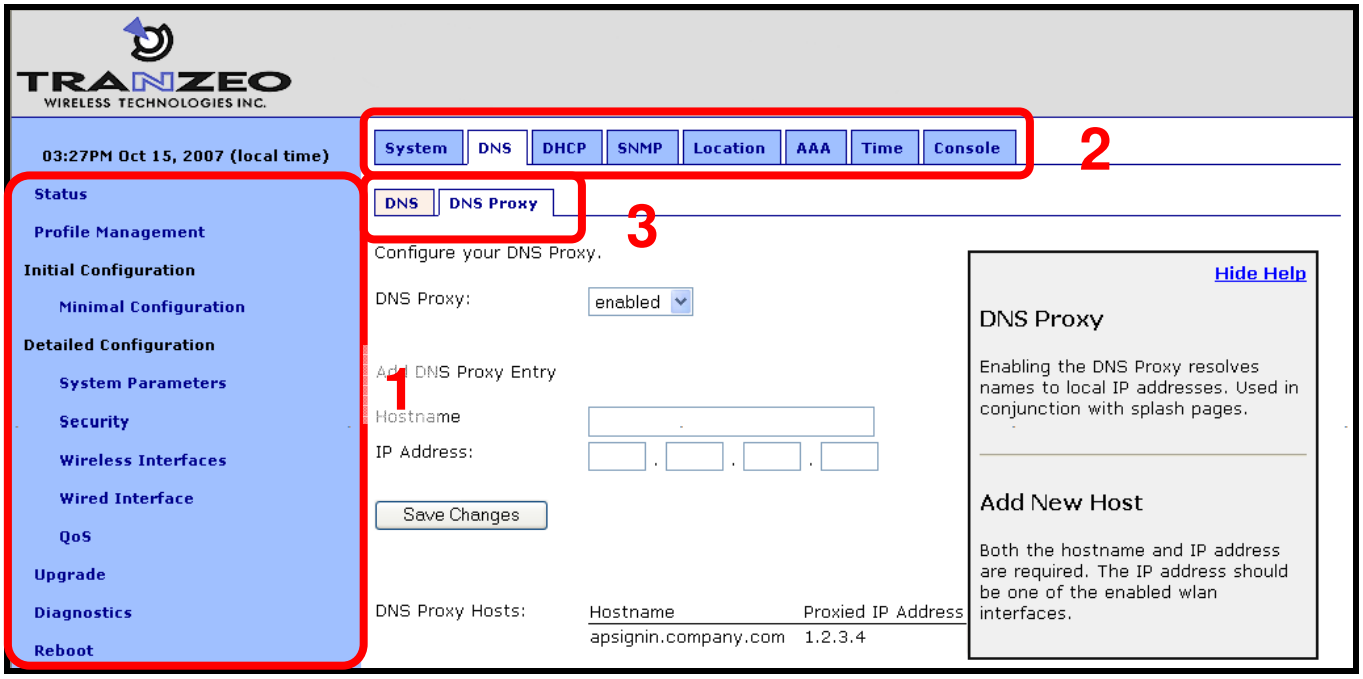

Figure 6. Web interface navigation components

The time displayed at the top of the navigation bar is the current time of the PC used to log in to the web GUI, not the time kept by the EL-900.

3.3 Setting Parameters

Many of the web interface pages allow you to set EL-900 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 EL-900 must be rebooted. After a change has been committed, a message reminding the user to reboot the EL-900 will be displayed at the top of the screen.

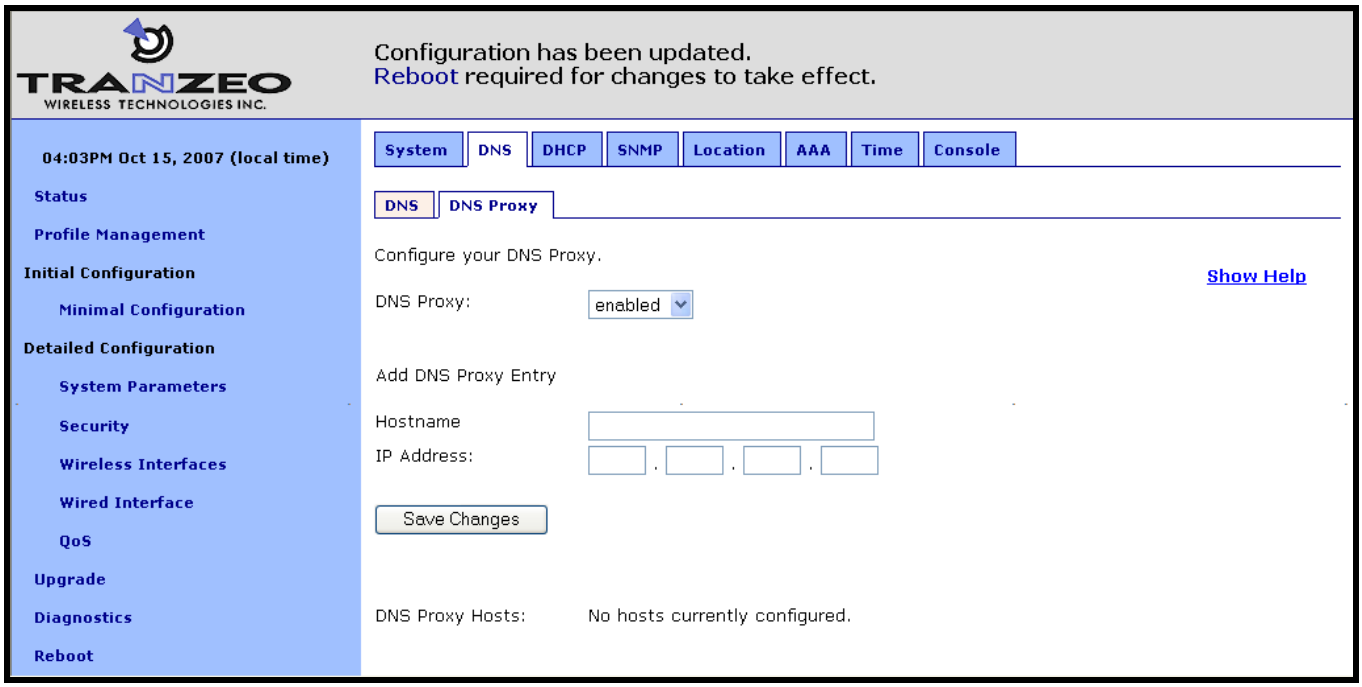

Figure 7. Page showing "Save Changes" button and message prompting the user to reboot

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 EL-900. Any changes made prior to rebooting will take effect following completion of the boot process.

It takes approximately 3 minutes for the device to reboot.

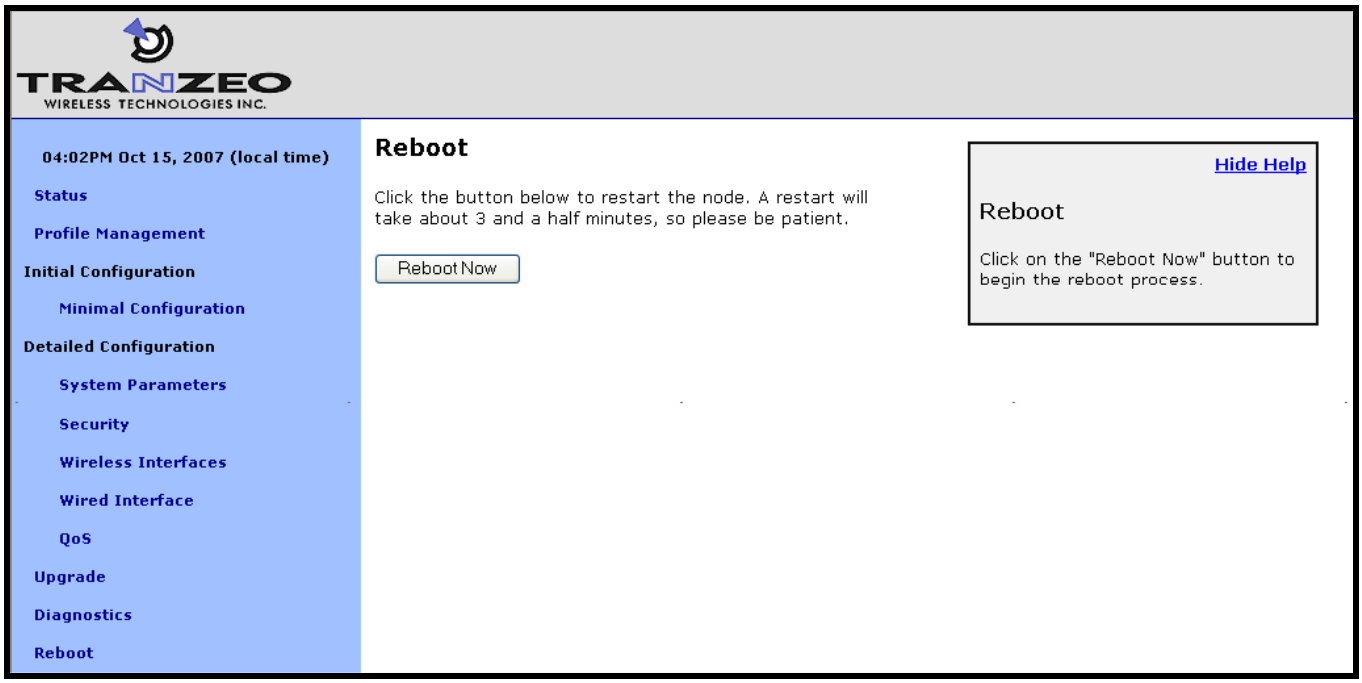

Figure 8. Rebooting the EL-900

4 Using the Command Line Interface

All configurable EL-900 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

4.1 Accessing the CLI

The EL-900's command-line interface (CLI) is accessible through its network interfaces using an SSH client. Any of the network interfaces can be used to establish the SSH connection to the EL-900. However, connecting through the Ethernet port is required for devices that have not previously been configured.

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 EL-900 using SSH.

When you log in to the EL-900, 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 9.9 describes how to change the timeout period.

```
Shell timeout: 3 minutes.

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

4.2 User Account

The user login used to access the EL-900 is 'admin'. The procedure for changing the password for this account is described in section 9.1.

4.3 CLI Interfaces

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

The available interfaces are:

- wlan1, wlan2, wlan3, wlan4 – controls for the virtual APs supported by the EL-900
- eth0 – controls for the Ethernet interface
- br0 – controls for bridge mode
- firewall – controls firewall settings
- 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 wlan1 interface is selected, the command prompt will be

```
wlan1>
```

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

4.4 CLI Features

The CLI has a number of features to simplify the configuration of the EL-900. These features are explained in the following sub-sections.

4.4.1 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.

4.4.2 Cancel a Command

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

4.4.3 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.

4.4.4 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.

4.5 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]
```

4.5.1 '?' 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 '?'.

4.5.2 'whoami' command

Syntax `whoami`

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

4.5.3 'help' command

Syntax `help [command|parameter]`

where the optional argument is either one of the CLI commands ("[command]") or a parameter in the currently selected interface ("[parameter]").

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
```

4.5.4 'show' command

Syntax `show`

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

4.5.5 'use' command

Syntax

```
use <interface>
```

where <interface> is one of the EL-900'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 wlan1
```

will select the wlan1 virtual AP interface and change the CLI prompt to

```
wlan1>
```

to reflect the interface selection.

4.5.6 '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 EL-900 to be rebooted.

Example

With the 'sys' interface selected

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

will set the node ID to 2

4.5.7 '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 'eth0' interface selected

```
get ip.address
```

will return the Ethernet interface's IP address, while

```
get ip.*
```

will return all parameters that begin with 'ip.'

```
ip.address = 10.6.0.1   [read-only]
ip.address_force =
ip.broadcast = 10.6.0.255   [read-only]
ip.broadcast_force =
ip.gateway =    [read-only]
ip.gateway_force =
ip.implicit.size.actual = 31   [read-only]
ip.implicit.size.requested = 31
ip.implicit.start.actual = 225   [read-only]
ip.implicit.start.requested = 225
ip.netmask = 255.255.255.0   [read-only]
ip.netmask_force =
```

4.5.8 'list' command

Syntax `list`

Description Lists all parameters for the selected interface

Example With the 'eth0' interface selected

```
list
```

will display

```
acl.mode          : access control list mode
dhcp.default_lease_time : default dhcp lease expiration in…
dhcp.max_lease_time : maximum requestable dhcp lease…
dhcp.relay.enable : use dhcp relay (if sys.dhcp.relay.enable=yes)
dhcp.reserve      : ip addresses to reserve at bottom of range…
dhcp.role         : interface dhcp role (none, client, server)
enable            : interface is enabled
ip.address        : IP address   [read-only]
ip.address_force  : override .ip.address (or blank)
ip.broadcast      : broadcast address   [read-only]
ip.broadcast_force : override .ip.broadcast (or blank)
ip.gateway        : gateway   [read-only]
ip.gateway_force  : override .ip.gateway (or blank)
ip.implicit.size.actual : actual size of address range
ip.implicit.size.requested : requested size of address range…
ip.implicit.start.actual : actual interface fourth octet
ip.implicit.start.requested : requested interface fourth octet…
ip.netmask        : network mask   [read-only]
ip.netmask_force  : override .ip.netmask (or blank)
routes.static     : static routes for this interface
vlan.enable       : use a vlan?
vlan.id           : vlan id (avoid 0 and 1 normally)
vpn.enable        : enable vpn on gateway node
vpn.keyfile       : base name of crt/key files
vpn.port          : port number for vpn
vpn.server        : hostname or ip address of the vpn server
```

4.5.9 '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`

4.5.10 'ifconfig' command

Syntax `ifconfig <eth0|wlan[1-4]>`

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)
```

4.5.11 'route' command

Syntax `route`

Description Displays the current route table.

4.5.12 'clear' command

Syntax `clear`

Description Clears the screen

4.5.13 'history' command

Syntax `history`

Description Shows the command history since the EL-900 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
```

4.5.14 '!' 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
```

4.5.15 'exit' command

Syntax `exit`

Description Terminates the current CLI session and logs out the user

4.5.16 'quit' command

Syntax `quit`

Description Terminates the current CLI session and logs out the user

5 Initial Configuration of an EL-900

This user's guide provides a comprehensive overview of all of the EL-900's features and configurable parameters. However, it is possible to deploy a network of EL-900s while only changing a limited number of parameters. The list below will guide you through a minimal configuration procedure that prepares a network of EL-900s for deployment.

1	**Change the 'admin' password.** The default password should be changed to prevent unauthorized access to the EL-900.	See section 9.1
2	**Set the node ID** The node ID affects the client access interface IP address spaces when the using implicit addressing scheme.	See section 9.2
3	**Set the DNS servers** Specify DNS servers to allow hostnames to be resolved.	See section 9.3

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 in the web interface navigation bar on the left side of the web interface.

In addition to setting the parameters on the "Minimal Configuration" page, OnRamp access should be disabled after initial programming. See section 9.11 for instructions on how to enable OnRamp access to the EL-900.

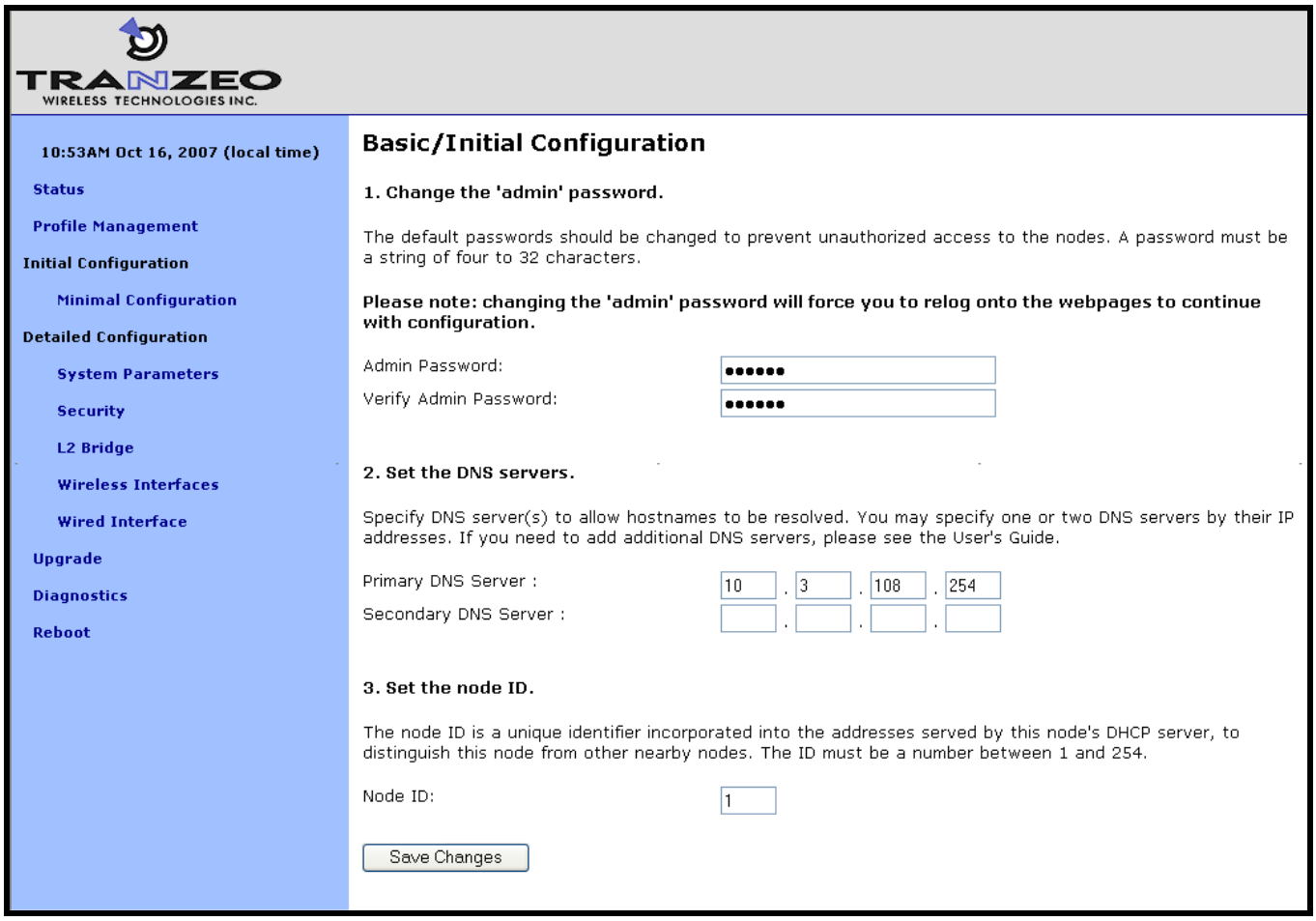

Figure 9. Initial configuration web page

6 Status Information

Multiple web interface pages that display status information about the EL-900 and client devices attached to it are available. These web pages are accessible by clicking on the "Status" link in the navigation bar and then selecting the appropriate tab shown at the top of the page.

The status information is not accessible through the CLI.

6.1 Configuration Overview Page

The main status page, which is displayed when clicking on "Status" in the navigation bar and when logging in, is the "Config Overview" page.

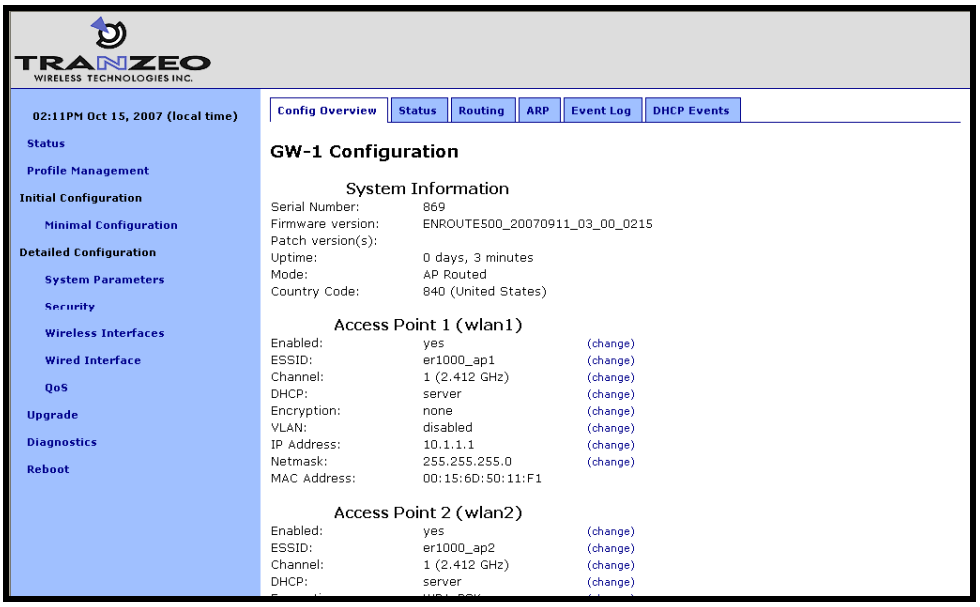

Figure 10. Partial configuration overview page

The configuration overview page shows a summary of settings for the virtual access point interfaces and the wired interface. The firmware version, uptime of the device, and its operating mode are also displayed.

Links labeled "(change)" are shown next to the settable parameters. These links take you to the appropriate page to change the setting.

6.2 Interface Status

Traffic and neighbor information for the virtual AP and wired interfaces are available on the "Status" tab of the "Status" page. Select the appropriate interface for which you wish to view information from the row of tabs below the primary tab row.

6.2.1 Virtual AP Interfaces

The sub-tabs display status information about the virtual AP interfaces. Data statistics information for the interface are displayed, showing received and transmitted data in terms of bytes and packets.

On the "wlan" sub-tabs, the client devices connected to the virtual APs are displayed. The following information is displayed for each client device:

- MAC address
- IP address
- Quantity of data received from the client device and transmitted to the client device
- Received signal strength (RSSI) in dBm and in parentheses the associated signal level based on a noise floor of -96dBm
- Time since last reception from the device
- A summary of the capabilities of the client device's radio card

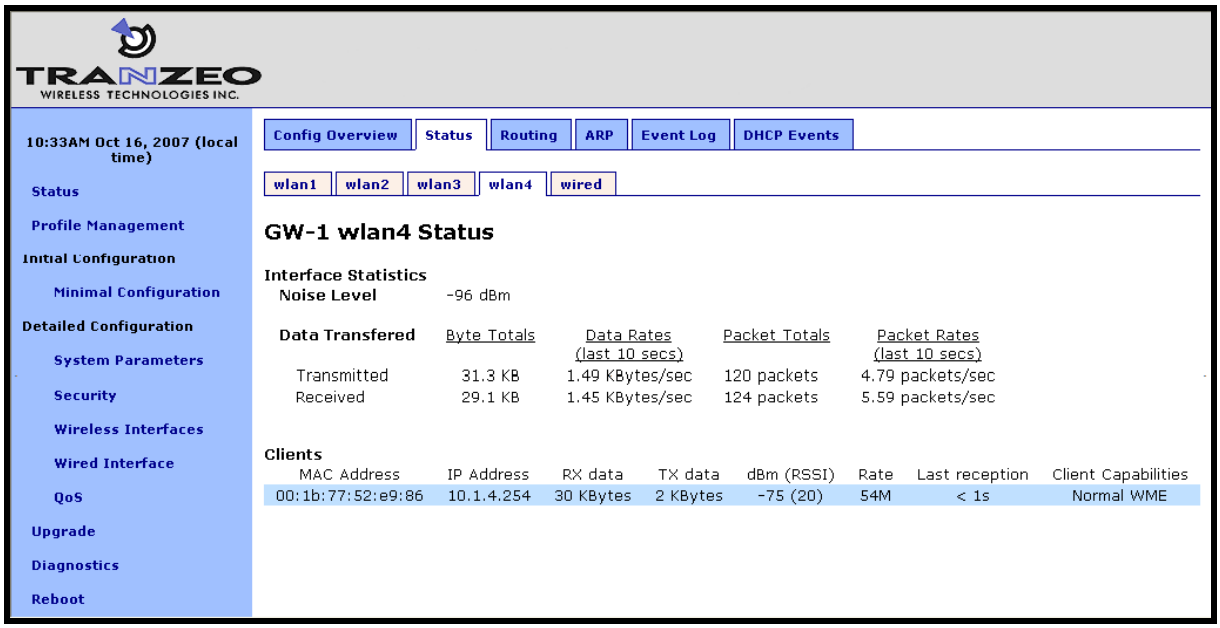

Figure 11. Status information for one of the virtual AP interfaces

6.2.2 Wired Interface Status

The wired interface status pages is similar to the wireless interface status pages, with the exception that it only displays summary information for the interface and does not break down data transferred on a per-device basis.

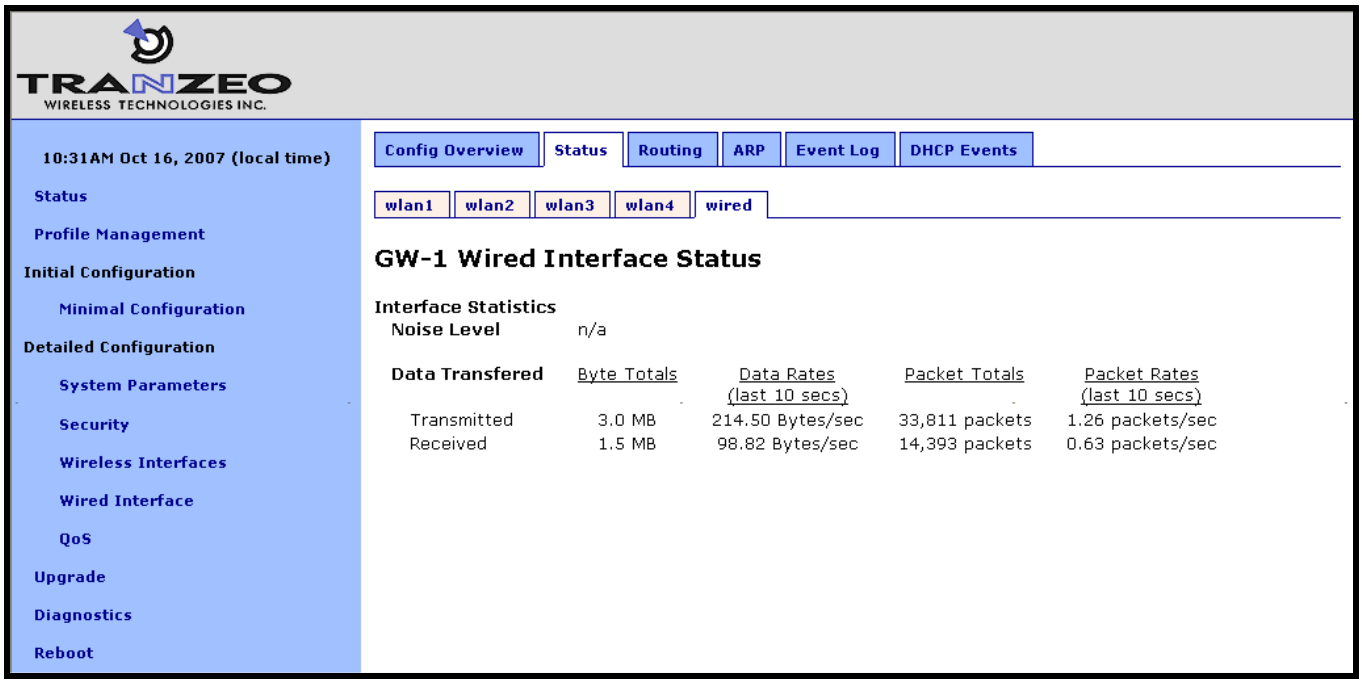

Figure 12. Wired interface status information

6.3 Bridging

The “Bridging” tab is only present when the EL-900 is in bridge mode. This page displays information about the current bridge configuration. A summary of the interfaces that are bridged is provided at the top of the page. This is followed by a list of known devices, identified by their MAC addresses.

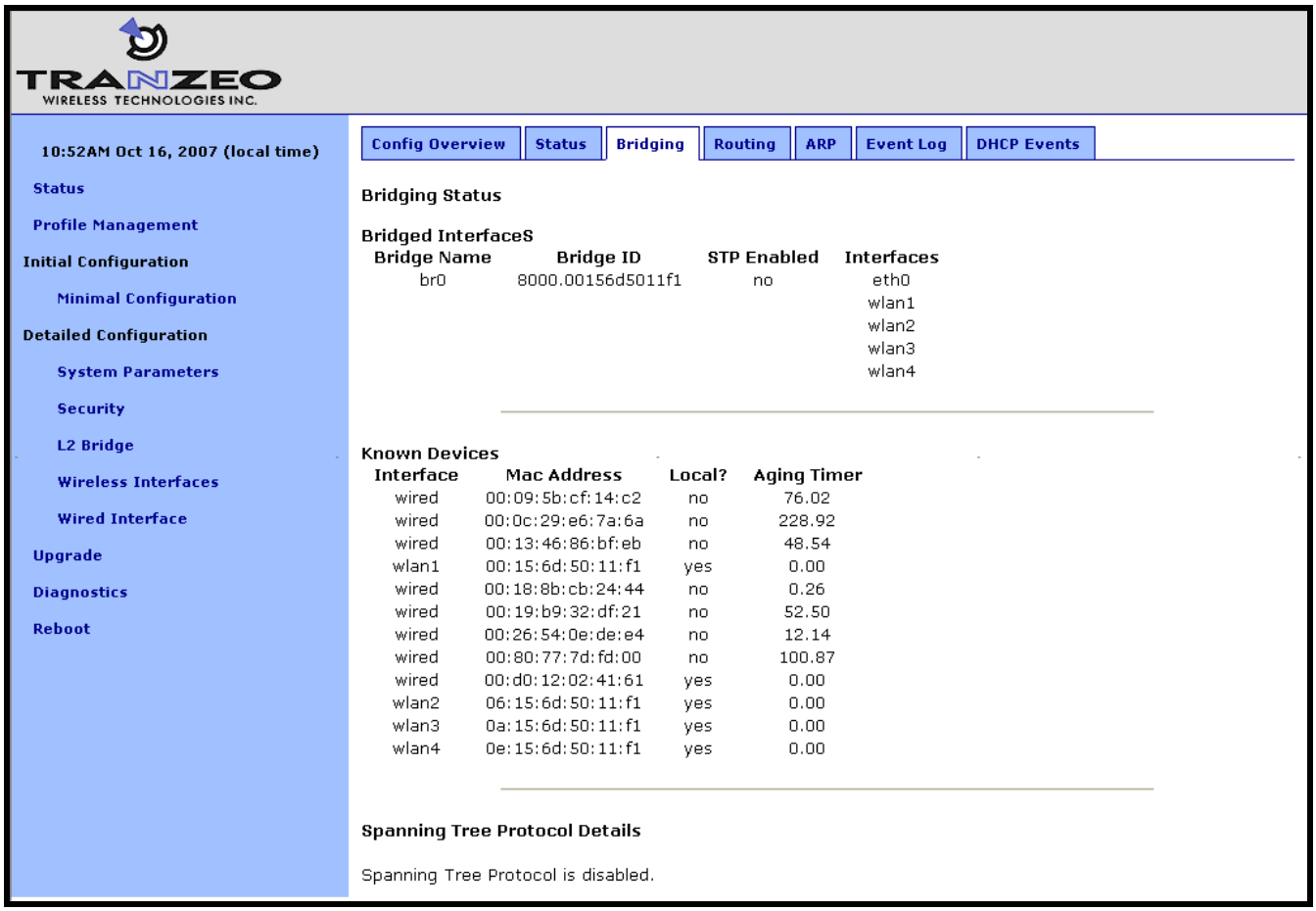

Figure 13. Bridging status information

6.4 Routing Table

The routing table used by the device can be displayed by selecting the “Routing” tab on the “Status” page.

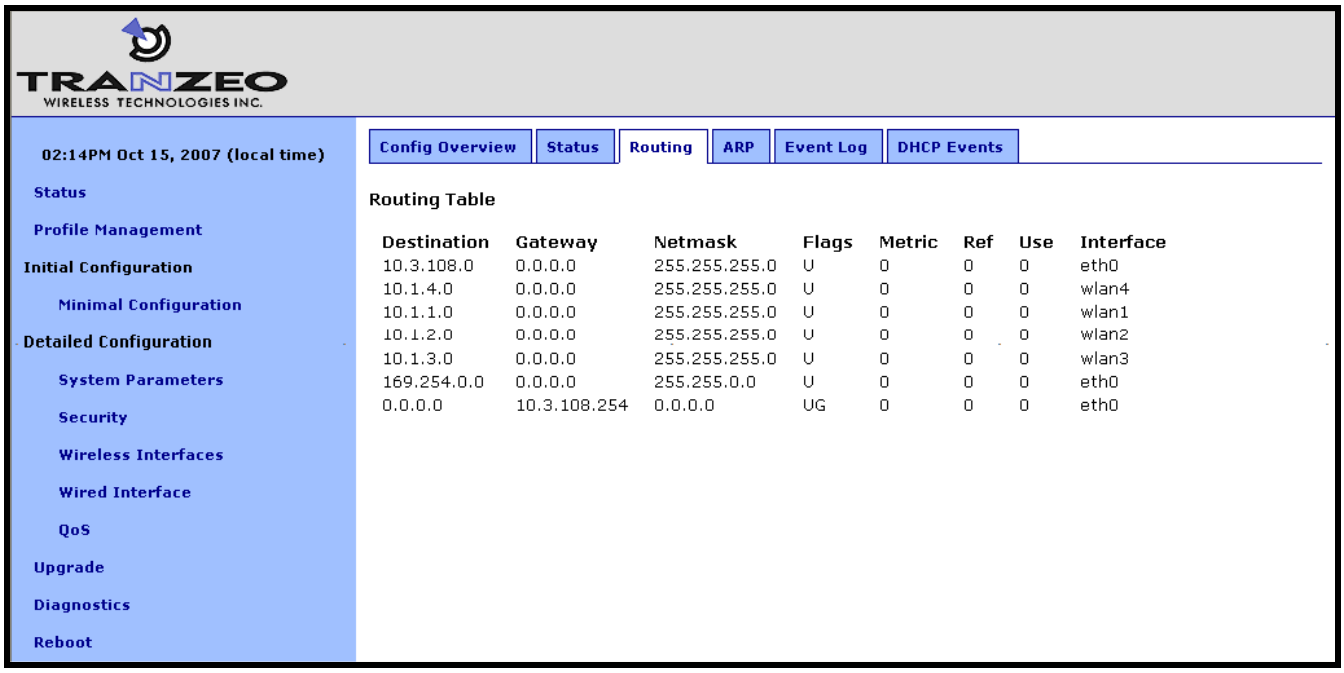

Figure 14. Routing table

6.5 ARP Table

The device's ARP table can be displayed by selecting the "ARP" tab on the "Status" page.

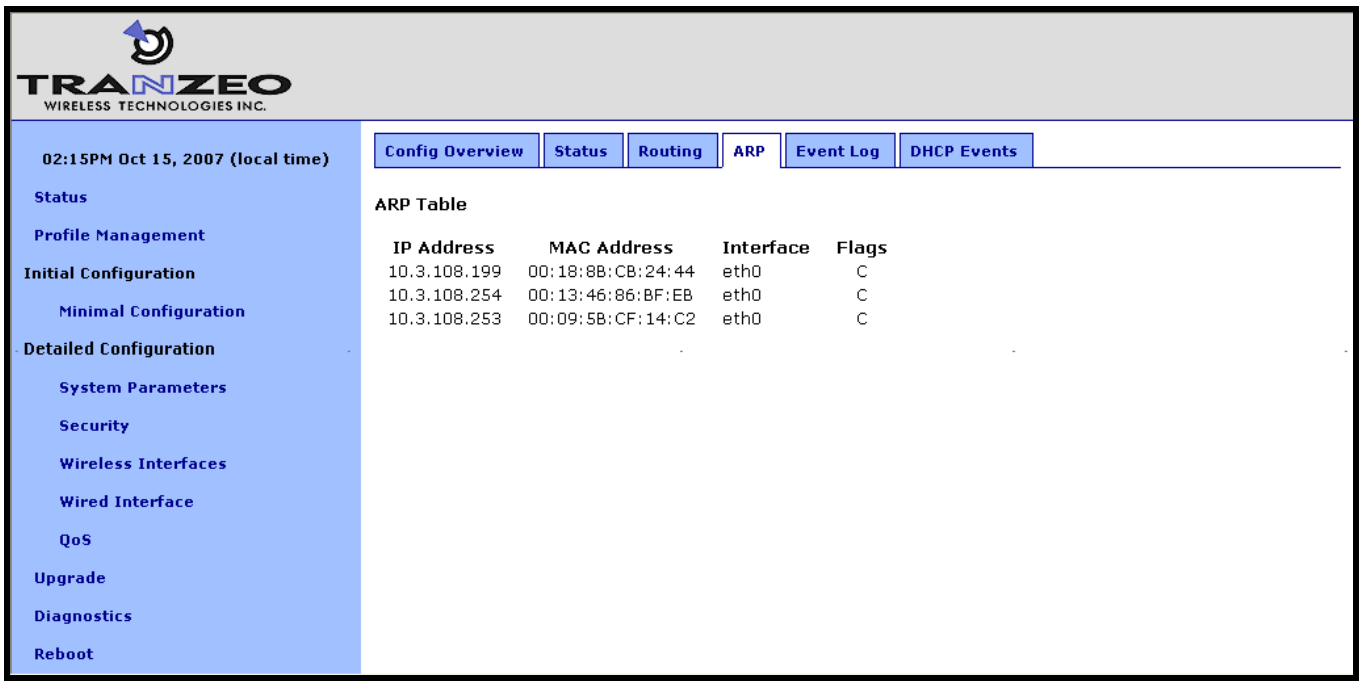

Figure 15. ARP table

6.6 Event Log

The main system log for the device is accessible by selecting “Event Log” on the “Status” page. The log is displayed in reverse chronological order, with the last recorded event appearing at the top of the page.

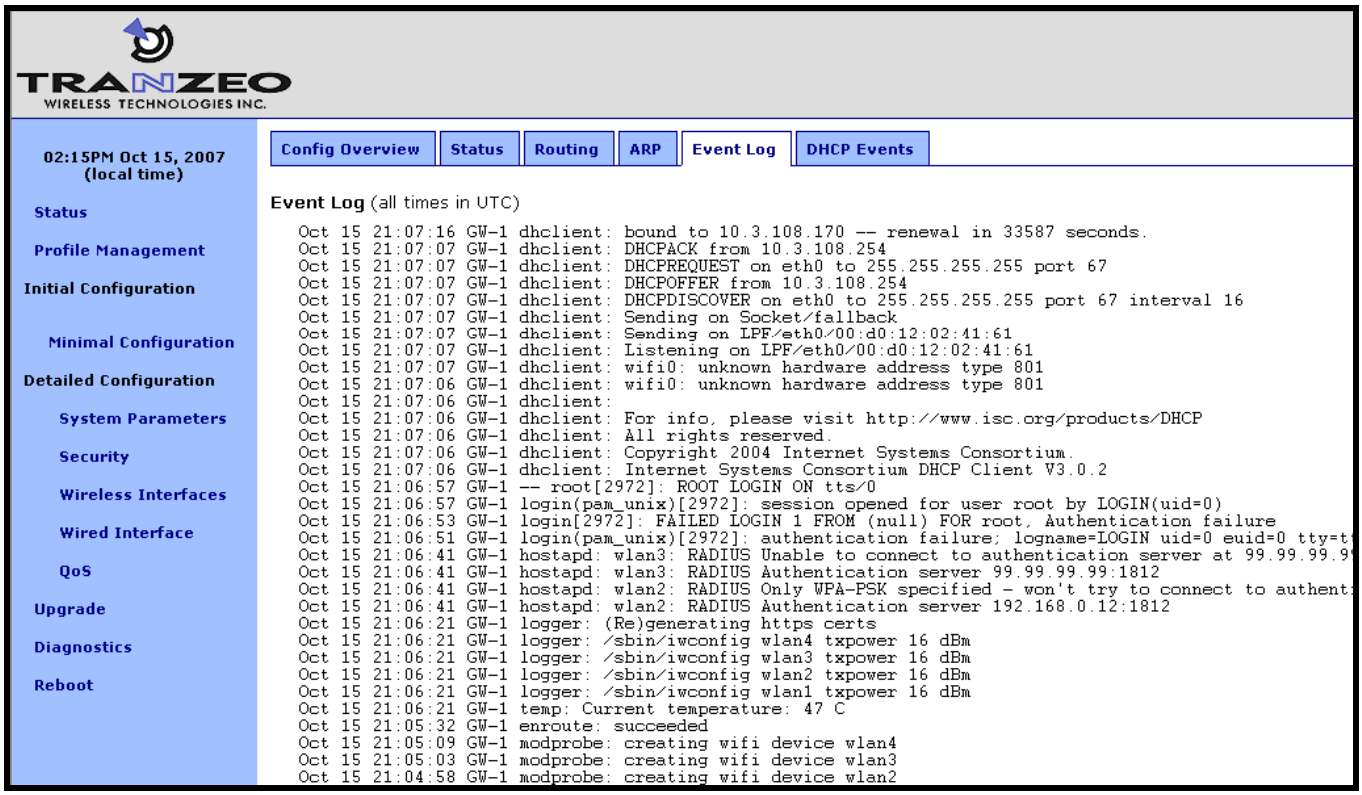

Figure 16. Event log

INFO

The time reported in the Event Log corresponds to the time maintained by the EL-900 and may not be consistent with that shown in the upper left corner of the webpage as this is the time maintained by the computer running the web browser.

6.7 DHCP Event Log

The log of DHCP-related events for the device is accessible by selecting “DHCP Events” on the “Status” page. The log is displayed in reverse chronological order, with the last recorded event appearing at the top of the page. All times in the log are in UTC time. Messages related to both local and relayed DHCP activity are displayed in the log.

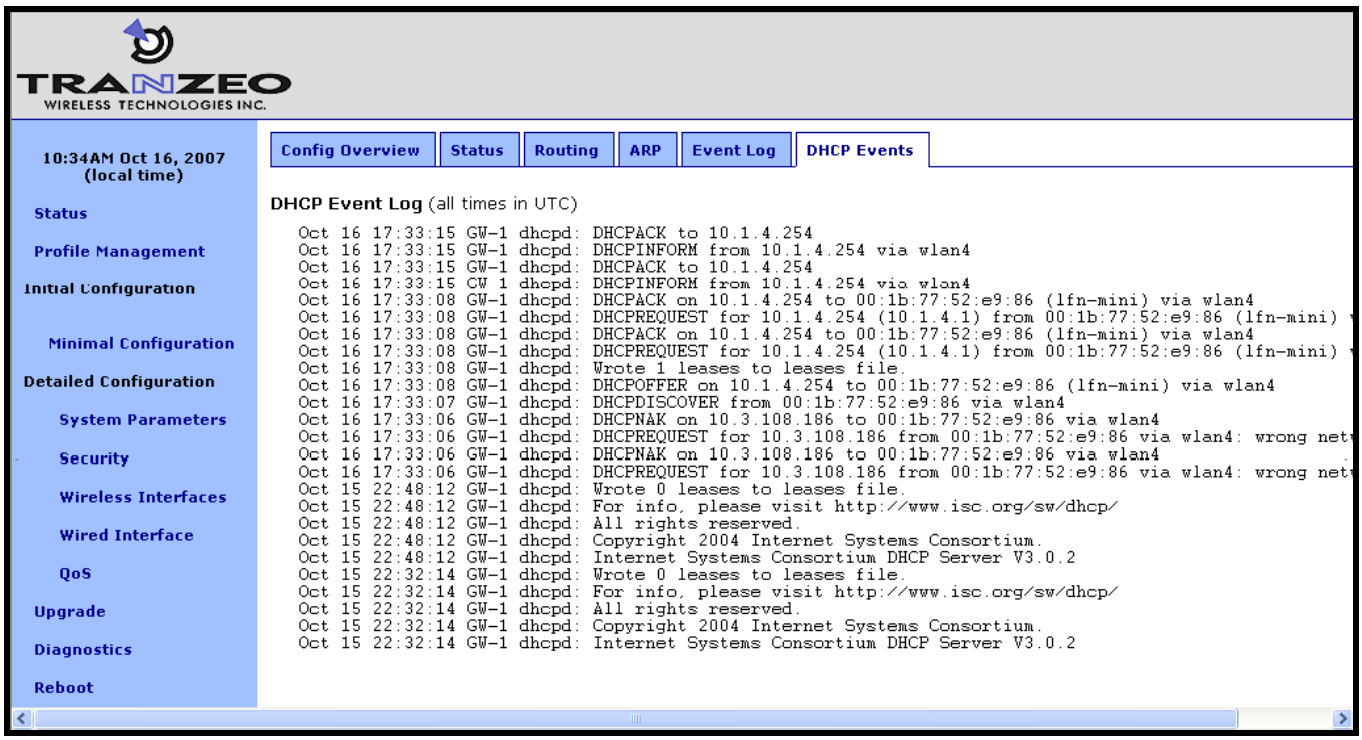

Figure 17. DHCP event log

INFO

The time reported in the DHCP Log corresponds to the time maintained by the EL-900and may not be consistent with that shown in the upper left corner of the webpage as this is the time maintained by the computer running the web browser.

7 Configuration Profile Management

Configuration profiles describe an EL-900's configuration state and can be created to simplify the provisioning and management of devices. The EL-900 supports the following configuration profile-related actions:

- Saving the current configuration as a configuration profile
- Loading, or applying, a configuration profile stored on an EL-900 to the device
- Downloading a configuration profile stored on the EL-900 to a computer
- Uploading a configuration profile from a computer to the EL-900
- Deleting a configuration profile stored on the EL-900

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

7.1 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 EL-900 and will appear in the "Existing profiles" text box. Use the "Download from Node" tab to download it to a different device.

Figure 18. Save a configuration profile

7.2 Load a Configuration Profile

A configuration stored on the EL-900 can be applied using the "Load" tab on the "Profile Management" page. This profile must either have been saved earlier or uploaded to the EL-900. Choose a profile name from the "Existing Profiles" box and then click on "Load Profile". It is necessary to reboot the EL-900 for the loaded profile settings to take effect.

INFO

A number of default configuration profiles are available on the EL-900. They are TBD.

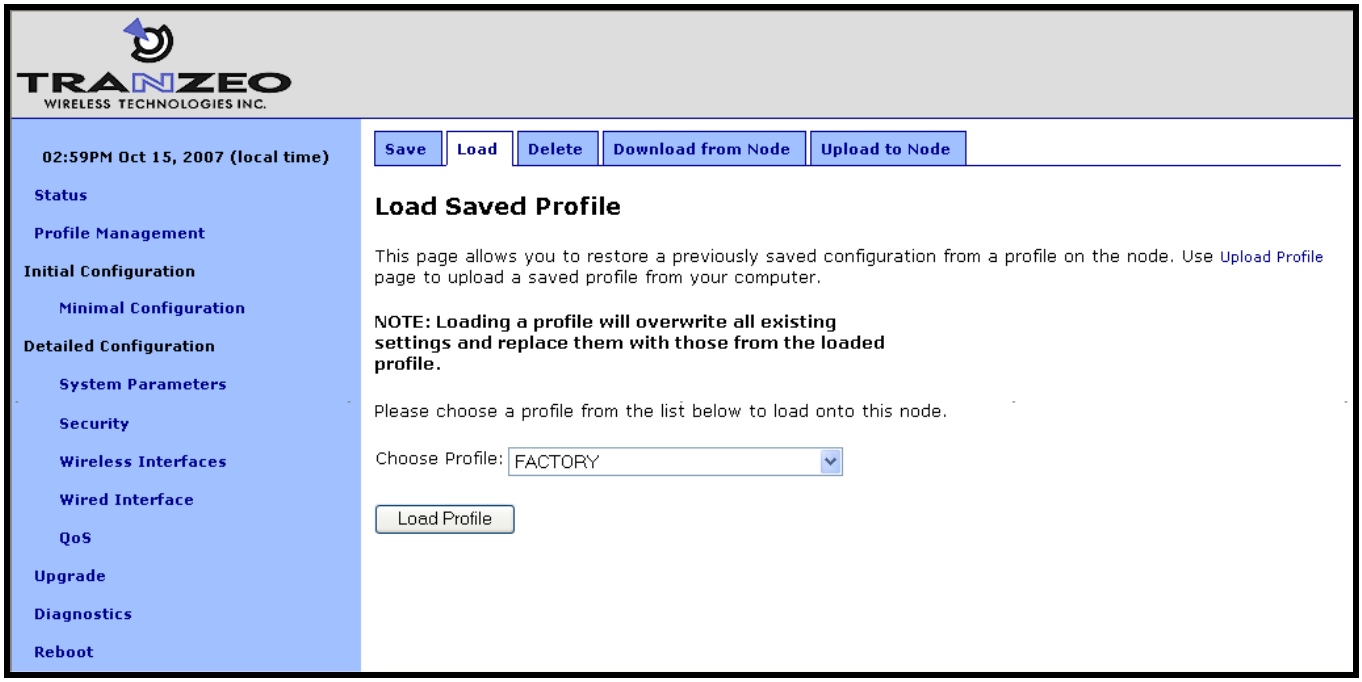

Figure 19. Load a configuration profile

7.3 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".

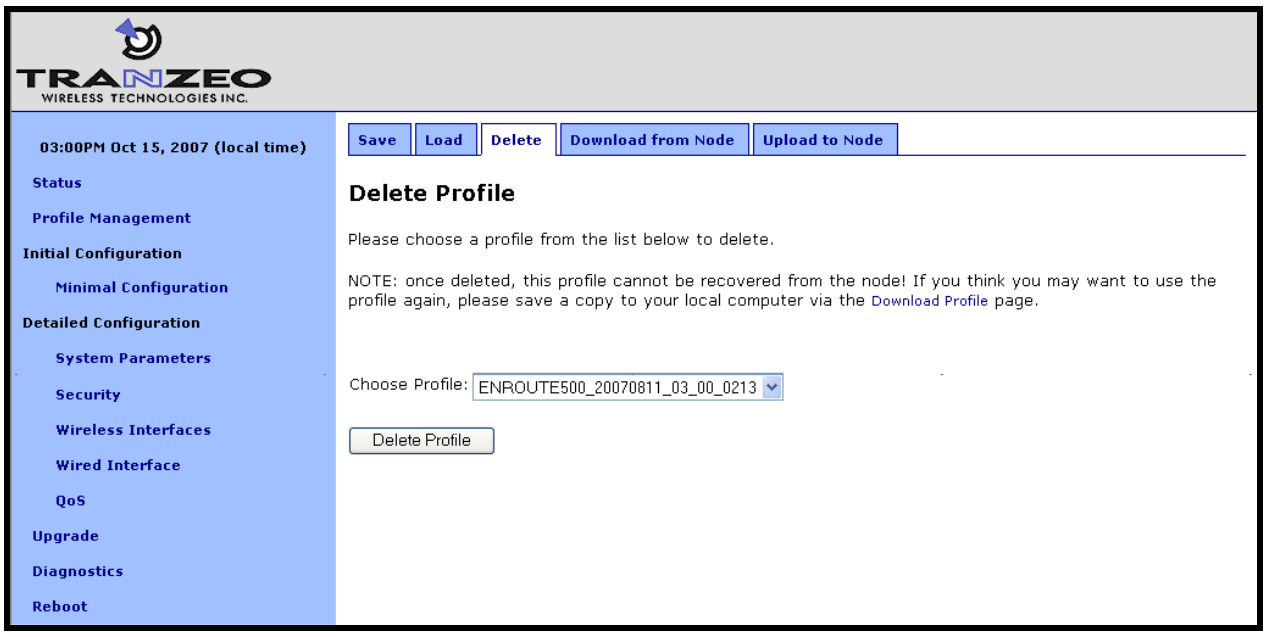

Figure 20. Deleting a configuration profile

7.4 Downloading a Configuration Profile from an EL-900

A configuration profile can be download from an EL-900 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.

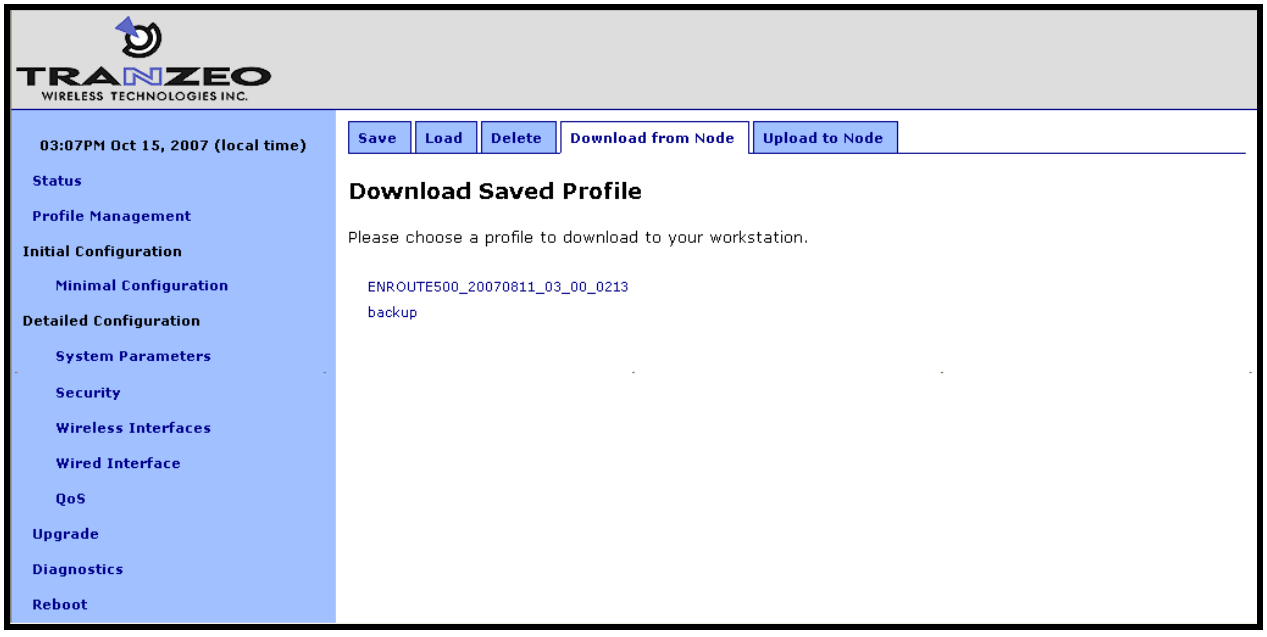

Figure 21. Downloading a configuration profile from an EL-900

7.5 Uploading a Configuration Profile to an EL-900

A configuration profile can be uploaded to an EL-900 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 EL-900. 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 EL-900.

Figure 22. Uploading a configuration profile to an EL-900

8 Mode of Operation

The EL-900 can be configured to operate in either routed or bridge mode. In routed mode, all communication is managed at the IP (layer 3) level, with the EL-900 acting as a router. In bridge mode, all communication across the EL-900 is managed at the MAC (layer 2) level, with the EL-900 acting as a switch.

The choice of the operating mode affects the availability of many of the EL-900's features, which is reflected in the web GUI options available when a particular mode is chosen. Table 5 summarizes the feature differences between the two modes

Feature	Bridge Mode	Routed mode
DHCP	• The bridge interface can be a DHCP client. • All DHCP requests from client devices attaching to the virtual APs must be handled by a separate device on the network	• The wired interface can be a DHCP client. • DHCP requests from client devices attaching to the virtual APs can be handled by a local DHCP server on the EL-900 or can be forwarded to a centralized server
Splash pages	Not available	Available
Firewall	Custom firewall rules cannot be added	Custom firewall rules can be added
Wired and virtual AP IP addresses	The interfaces do not have IP addresses	IP addresses must be assigned to the interfaces
QoS	Not available	Available
DNS proxy	Not available	Available

Table 5. Feature differences between bridge and routed mode

When switching to bridge mode, all the IP addresses for virtual access points 'wlan1 – 4' and the wired interface will be disabled. A bridge interface will be created to provide IP access to the EL-900 in bridge mode. By default the address of this interface will be set to *<LAN prefix first octet>.<node ID>*.1.1 It is recommended that an IP address is explicitly set for the bridge interface when switching to bridge mode. See section 12.1 for instructions on how to set the bridge interface parameters.

Certain web GUI pages are only available when the device is configured for bridge mode operation. These pages are:

- "L2 Bridge" in the main navigation bar
- "Bridging" tab on the "Status" page

CLI

The EL-900's operating mode is set with the 'scheme' parameter in the 'sys' interface. Valid values are 'aponly' for routed mode and 'l2bridge' for bridge mode. For example, set the operating mode to routed mode with:

```
> use sys
sys> set scheme=aponly
```

Web GUI

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

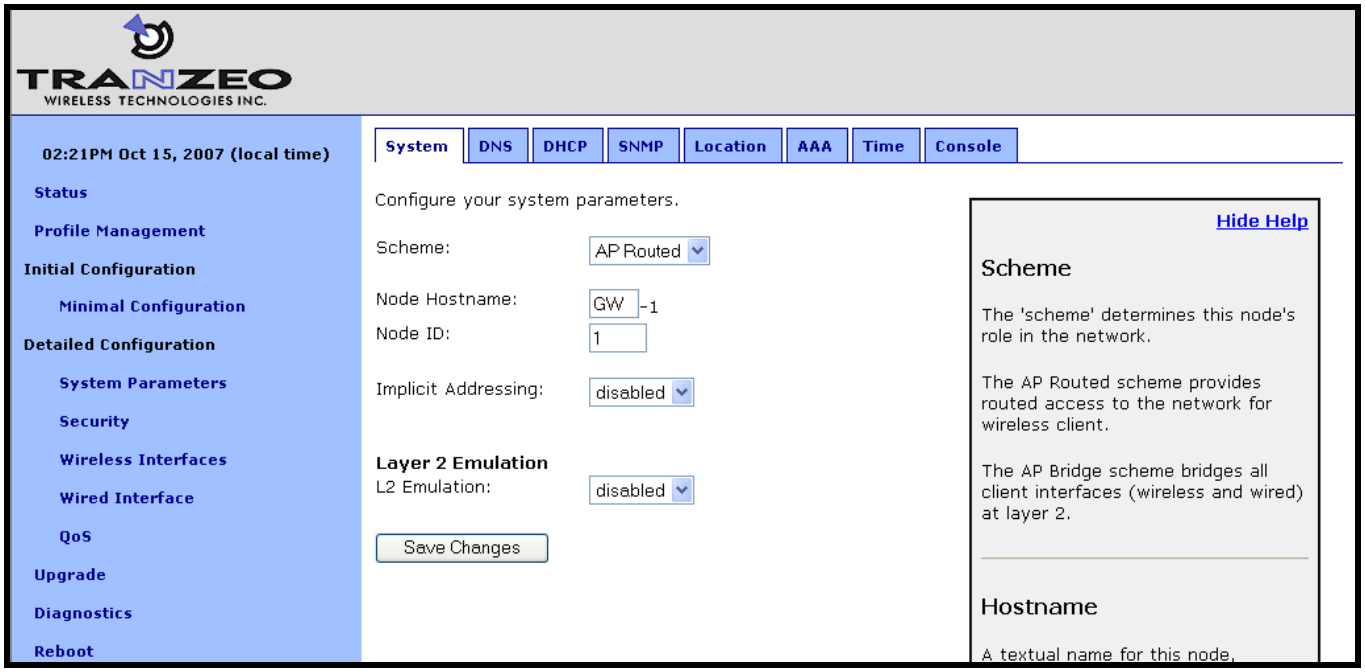

Figure 23. Setting operating mode

9 System Settings

This section describes settings that are applicable to the overall operation of the EL-900, but are not related directly to a particular interface.

9.1 User Password

The password for the ‘admin’ user is configurable. The default password is ‘default’.

See section 2.4 for instructions on resetting the ‘admin’ password if it has been lost.

CLI

The password for the ‘admin’ user can be set using the ‘password.admin’ parameter in the ‘sys’ interface. The password will not be displayed when using the ‘get’ command with these parameters. The example below shows how to set the ‘admin’ password using the CLI.

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

Web GUI

The ‘admin’ password can be changed via the web interface using the “Passwords” tab on the “System Parameters” page.

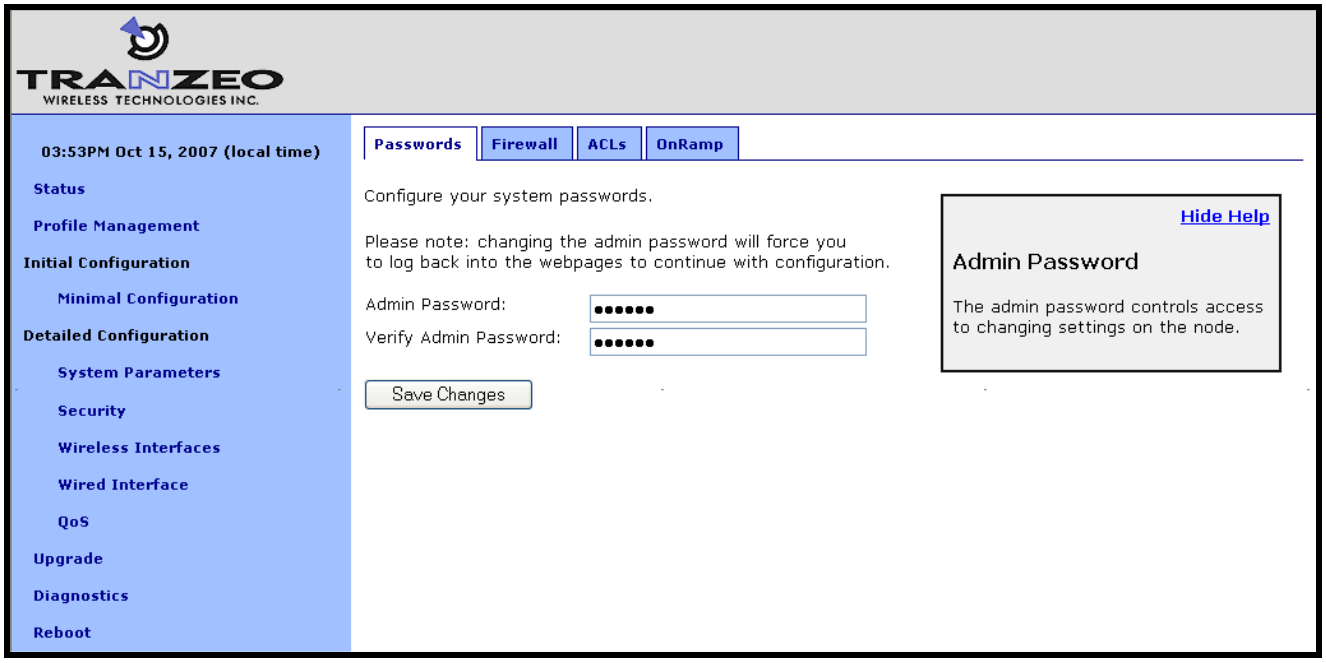

Figure 24. Passwords page

9.2 Node ID

BRIDGE

The only use of the node ID parameter when operating in bridge mode is for setting the default IP address of the bridge interface when one has not been explicitly set or acquired via DHCP.

The node ID assigned to an EL-900 affects the IP address spaces assigned to each of the EL-900's virtual AP client access interfaces when it uses implicit addressing in routed mode. If multiple EL-900s are connected to the same LAN, it is recommended that they be assigned different node IDs unless they have the NAT option enabled or use the explicit addressing scheme.

CLI

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 node ID can be set via the web interface using the "System" tab on the "System Parameters" page as shown in Figure 25.

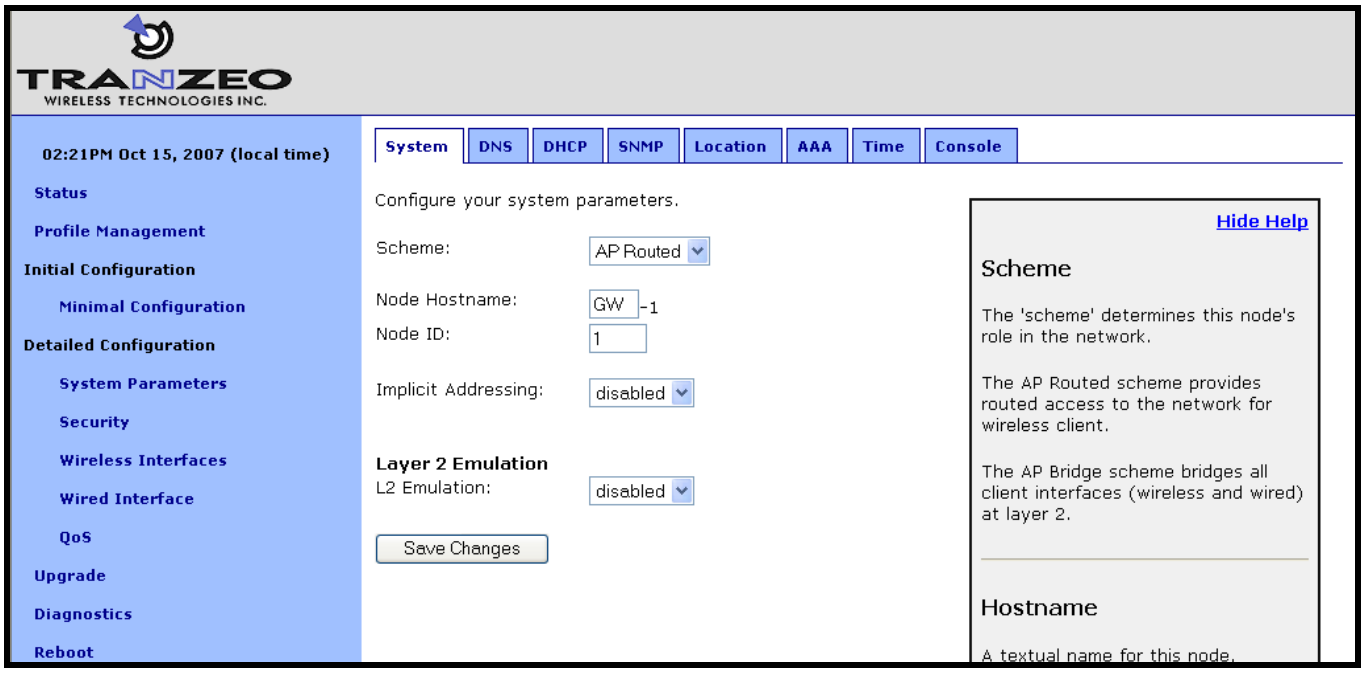

Figure 25. System settings page with EL-900 in routed mode

9.3 DNS / Domain Settings

At least one DNS server, accessible from the EL-900, must be specified for the device 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 an EL-900.

If an EL-900 acquires DNS server information through DHCP on its wired interface, this DNS server information will overwrite any manually set DNS server setting.

BRIDGE

When operating in bridge mode, the DNS settings are only used locally by the EL-900 and are not provided to any other devices on the network.

CLI

The DNS server(s) used by an EL-900 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.

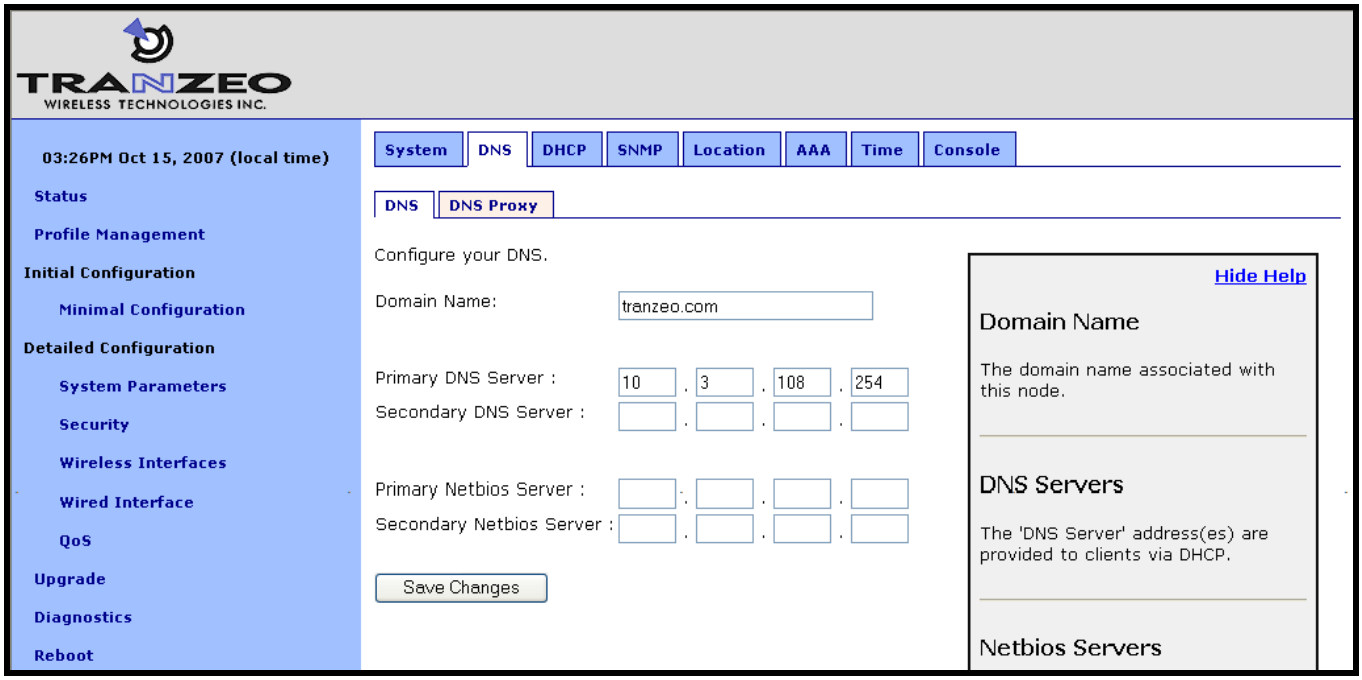

Figure 26. Setting the DNS and Netbios server(s)

9.4 DNS Proxy Configuration

DNS proxy entries can be added to an EL-900 to force local resolution of host names to IP addresses for the hosts in the proxy list. Use of a DNS proxy list on the EL-900 is a two step process, first populating the host name/IP address pairs, and then enabling DNS proxy.

BRIDGE DNS proxy is not supported when operating in bridge mode.

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

Web GUI

DNS proxy can be enabled on the "DNS Proxy" sub-tab on the "DNS" tab on the "System Parameters" page as shown in Figure 27. Hostname/IP address pairs can be added on this page as well.

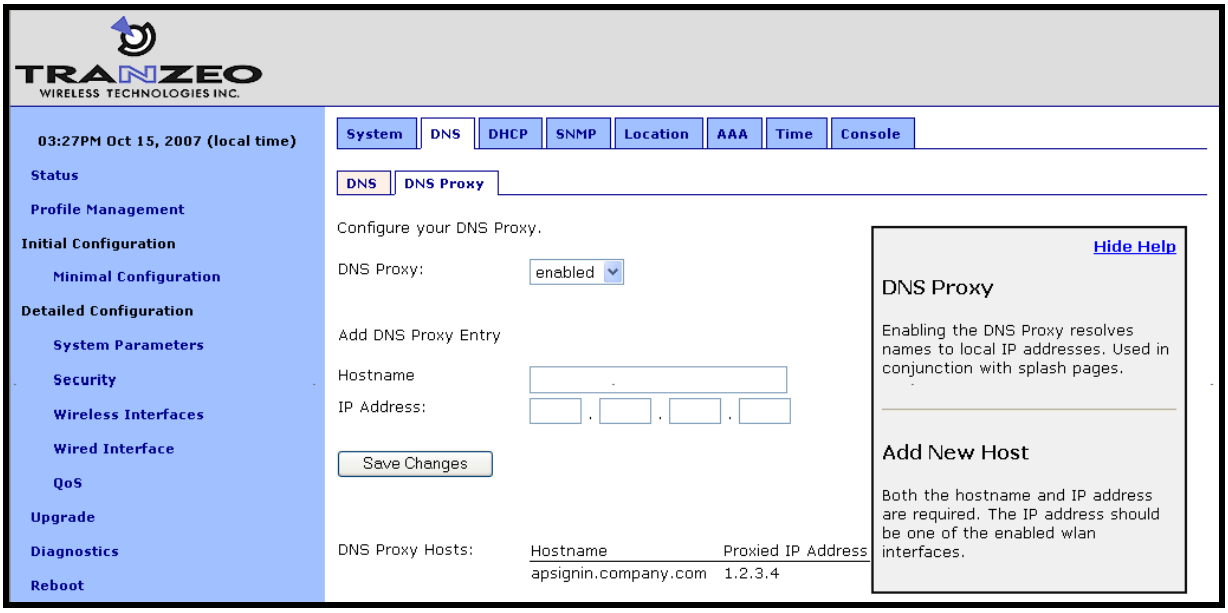

Figure 27. Configuring DNS proxy

9.5 NetBIOS Server

The NetBIOS server parameter is used to define a NetBIOS server's IP address that is provided to client devices when configured by the EL-900's local DHCP server.

BRIDGE The NetBIOS settings are not used when operating in bridge mode.

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 (see Figure 26).

9.6 SNMP

The EL-900 supports SNMP.

The read-only and read-write passwords and the port that SNMP uses can be configured. A contact person and device location can also be specified as part of the SNMP configuration.

CLI

The SNMP read-only and read/write passwords are set with the 'snmp.community.ro' and 'snmp.community.rw' parameters in the 'sys' interface. The example below shows how to set these parameters.

```
> use sys
sys> set snmp.community.ro=”read-only_password”
sys> set snmp.community.rw=”read-write_password”
```

The SNMP port is set with the 'snmp.port' parameter in the 'sys' interface as shown below. By default this parameter is set to "161".

```
> use sys
sys> set snmp.port=161
```

The contact person and location of the device located via SNMP are set with the 'snmp.contact. and 'snmp.location' parameters in the 'sys' interface as shown below.

```
> use sys
sys> set snmp.contact="Joe Smith"
sys> set snmp.location="123 Main St., Anytown, USA"
```

Web GUI

The SNMP-related parameters can be set on the "SNMP" tab on the "System" page (see Figure 28).

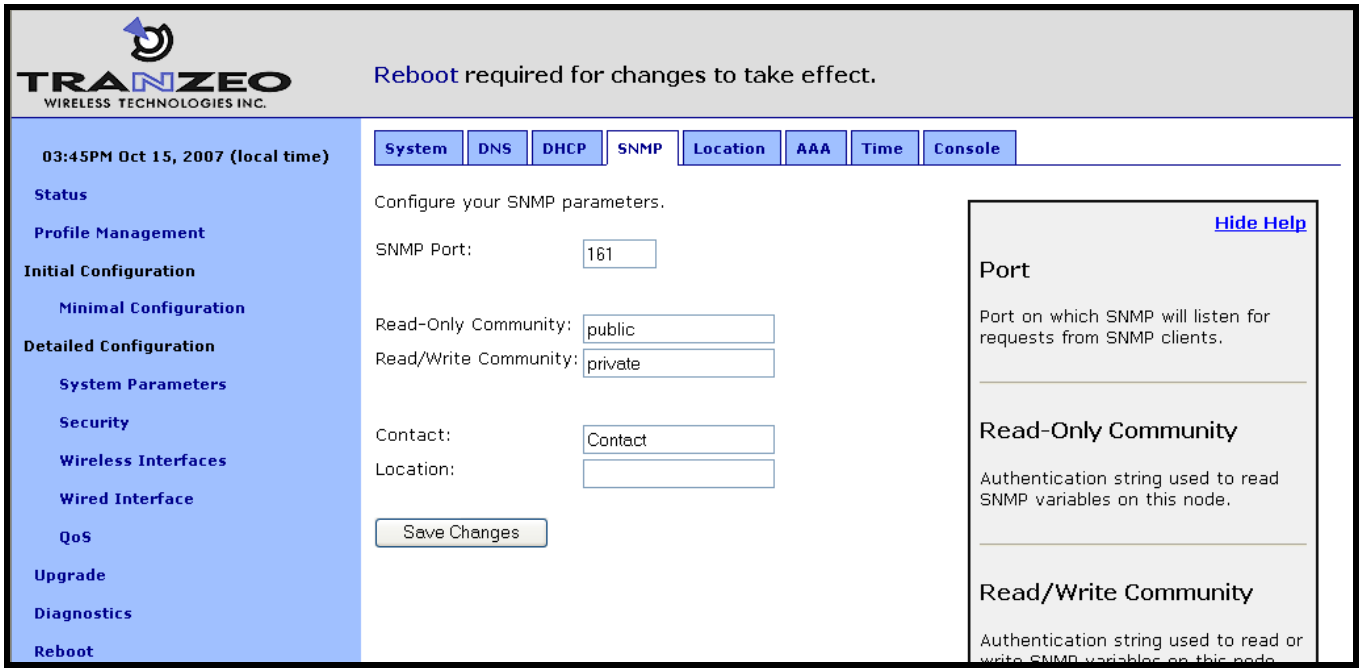

Figure 28. SNMP configuration

9.7 Location

Two types of device location information can be stored:

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

Note that these values are not automatically updated and must be entered after a device has been installed. Altitude is in meters. Latitude and longitude must be given as geographic coordinates in decimal degrees, 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 geographic location of the EL-900 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 EL-900'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.

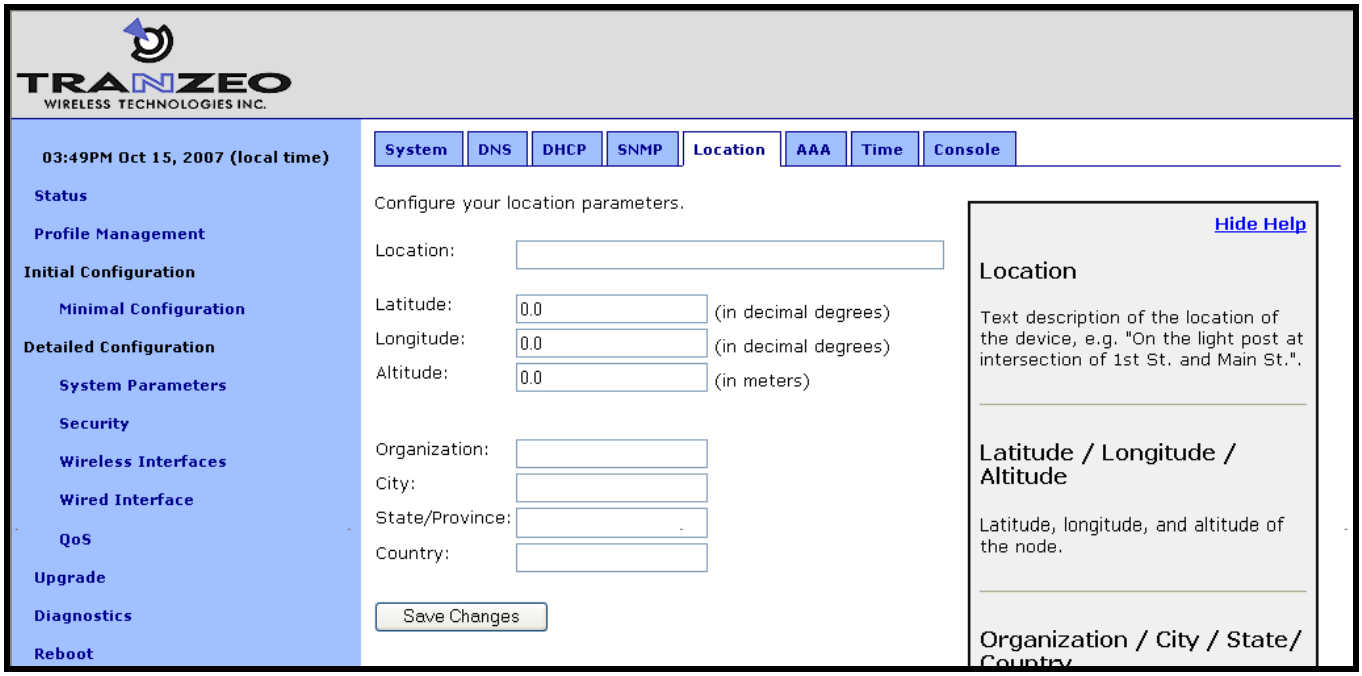

Figure 29. Setting location and certificate information

9.8 Certificate Information

A certificate for use with splash pages and the web interface is locally generated on the EL-900. The information embedded in this certificate can be defined by the user. A new certificate is automatically generated when the parameters describing the EL-900's location are changed. The specific location parameters to which the certificate is tied to are listed in the sections below.

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 (see Figure 29). Changing any of the Organization, City, State/Province, or Country parameters will cause the certificate information to be recalculated.

9.9 Time Synchronization

An EL-900 can be configured to synchronize its internal clock with an external RFC-868-compliant time server. The time synchronization will ensure that proper time stamps are displayed for entries in the event logs that are available on the web GUI's "Status" page.

CLI

The time synchronization server is set with the 'time.rfc868.server' in the 'sys' interface. The example below shows how to set the time synchronization server.

```
> use sys
sys> set time.rfc858.server="your.timeserver.here"
```

It is not possible to manually adjust the device time through the CLI. Please use the web GUI to adjust it.

Web GUI

The synchronization mode and server can be set on the “Time” tab on the “System” page (Figure 30).

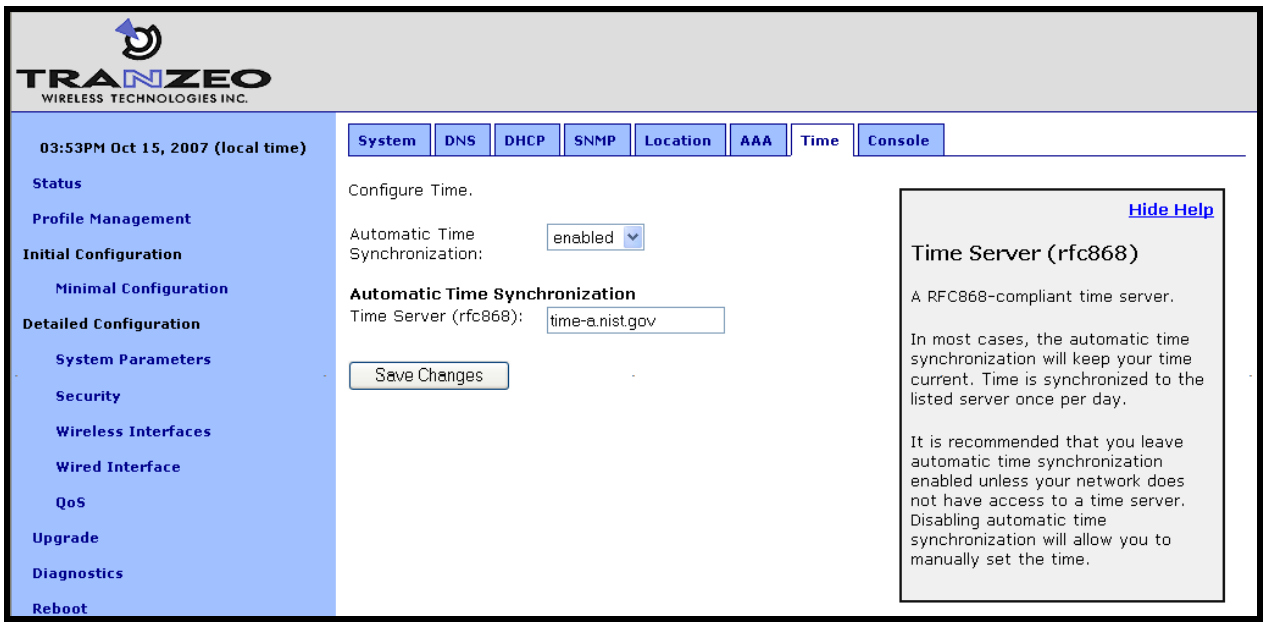

Figure 30. Automatic time synchronization

When automatic synchronization is disabled, the user can set the EL-900’s UTC time (Figure 31). Enter the time using the available drop-down menus and check the “Change Time” checkbox.

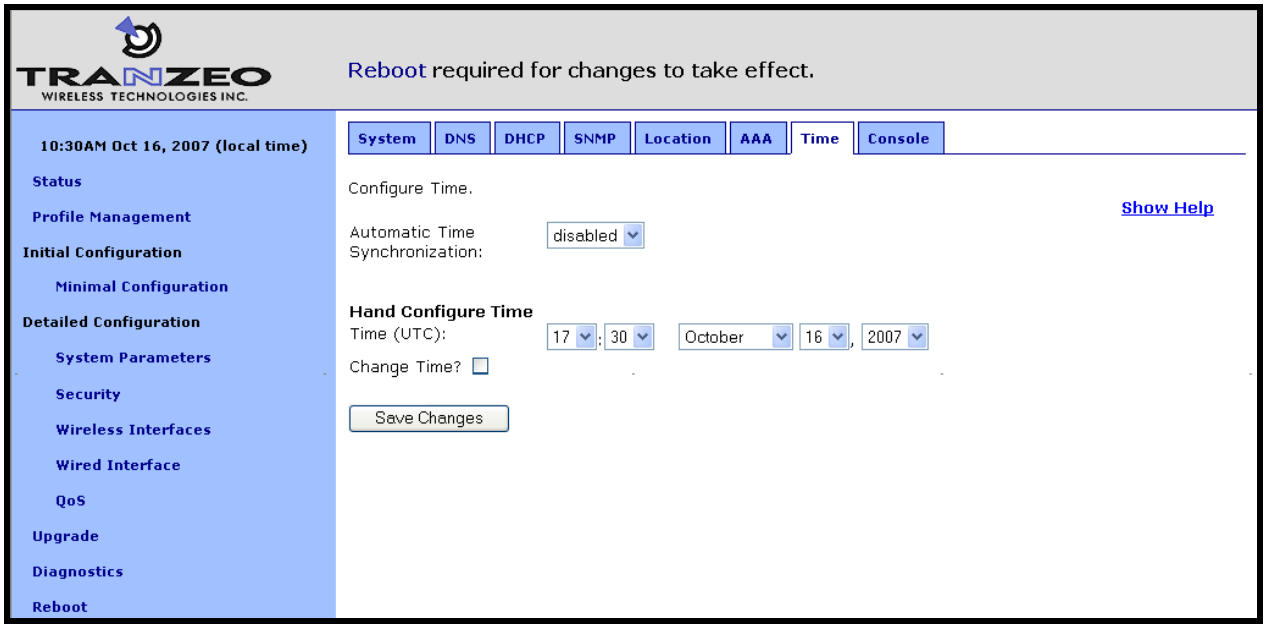

Figure 31. Setting the time manually

9.10 Web GUI Console

The web interface allows the user to set parameters that are not otherwise settable through the web interface using a console interface. The console is available on the “Console” tab on the “System” page.

CLI key/value pairs can be entered through the console. The key format used is “*<interface name>.<key>*”. For example, “wlan1.channel” is the key to set the channel used by virtual AP wlan1. To use the console, enter one or more key/value pairs in the large text box on the page, either separating each pair with a space or placing each pair on its own line. Click on the “Submit Commands” button to set the values entered in the text box.

Figure 32. Web interface console

9.11 OnRamp Configuration Access

ONRAMP IS A PC-BASED TOOL THAT WILL BECOME AVAILABLE TO SUPPORT INITIAL CONFIGURATION OF THE EL-900. IT HAS NOT BEEN RELEASED AT THE TIME OF THE WRITING OF THIS DOCUMENT. CHECK WWW.TRANZEO.COM/ONRAMP FOR STATUS.

IT IS RECOMMENDED THAT ONRAMP CONFIGURATION ACCESS IS DISABLED UNTIL THE TOOL IS MADE AVAILABLE.

The OnRamp utility provides network detection and configuration capabilities for EL-900s. The configuration capabilities are only intended for initial configuration and for security reasons, it is strongly recommended that OnRamp configuration capability is disabled after initial configuration.

You can use the CLI, the web interface, or OnRamp to determine whether a device can be configured from OnRamp. In OnRamp, the "Prog" column displays the programming capability from OnRamp. A 'Y" in this column indicates that OnRamp can configure the device, an 'N' indicates that it cannot.

CLI

The OnRamp configuration capability is controlled by the 'provisioning.enable' parameter in the 'sys' interface. Set this parameter to '0' to disable configuration through OnRamp, as shown in the example below.

```
> use sys
sys> set provisioning.enable=0
```

Web GUI

The OnRamp configuration capability is set on the "OnRamp" tab on the "Security" page (see Figure 33).

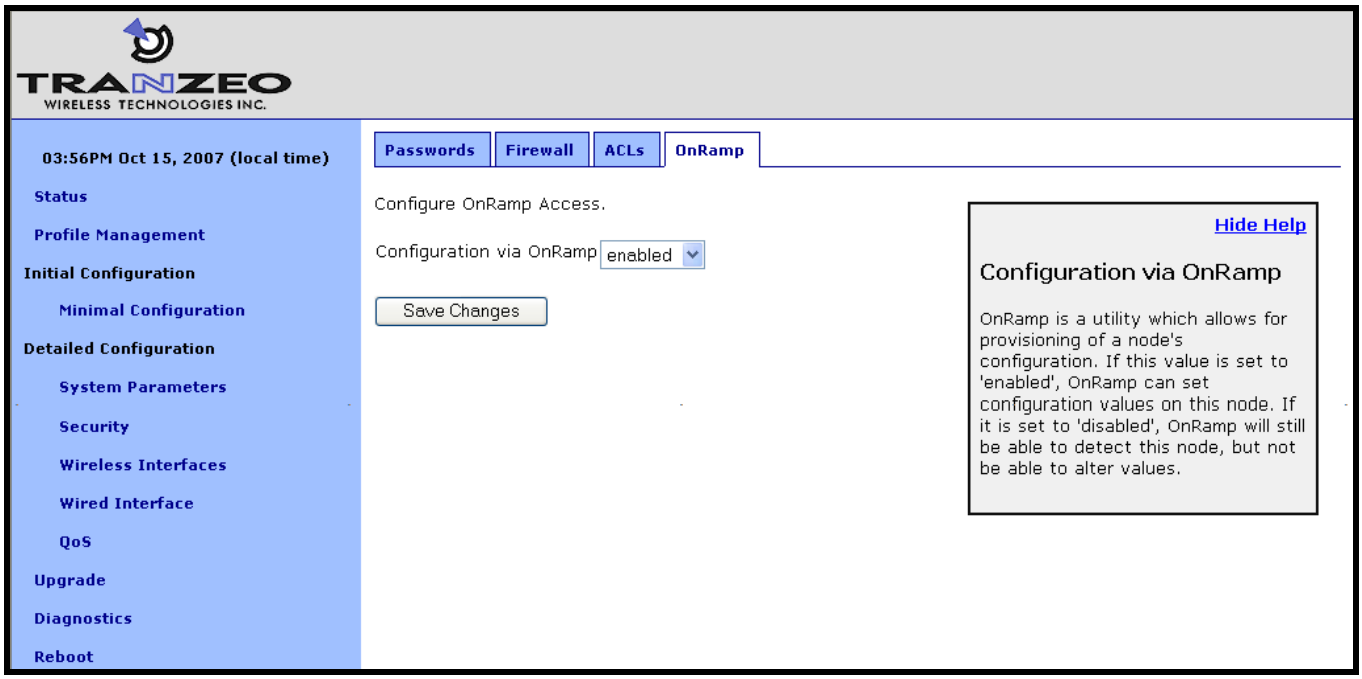

Figure 33. OnRamp configuration access

9.12 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 (6 hours).

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

10 Client Addressing Schemes

BRIDGE

The client addressing scheme setting has no effect when the EL-900 is operating in bridge mode.

The choice of client addressing scheme affects how EL-900 client access interface addresses are assigned. The EL-900 can be configured to use an implicit addressing scheme for its client access interfaces, where the address spaces assume a default size and the addresses are affected by a number of settable parameters. Alternatively, explicit address spaces can be defined for each client access interface. The addressing scheme choice also affects what the addresses of client devices will be when the EL-900 is not operating in centralized DHCP server mode.

Table 6 compares how the behavior of the EL-900 differs depending upon the addressing scheme that is chosen.

Feature	Implicit addressing scheme	Explicit addressing scheme
Client access interface addresses	Derived from node ID and LAN prefix settings. Client access interface addresses cannot be directly set.	Can be set to arbitrary values, with a few reserved address ranges that cannot be used.
Size of client address space	Each of the active client access interfaces must share a class C address space.	The address space size for each client access interface can be set independently and can be of arbitrary size.

Table 6. Differences between explicit and implicit addressing schemes

CLI

The choice of implicit or explicit addressing scheme is controlled by the 'implicit.enable' parameter in the 'mesh' interface. Set this parameter to 'yes' to select implicit addressing and to 'no' to select explicit addressing. The example below demonstrates how to select the implicit addressing scheme.

```
> use mesh0
sys> set implicit.enable=yes
```

Web GUI

The addressing scheme is set with the "Implicit Addressing" drop-down menu on the "System" tab of the "System" page. Set this to disabled to choose the explicit addressing scheme.

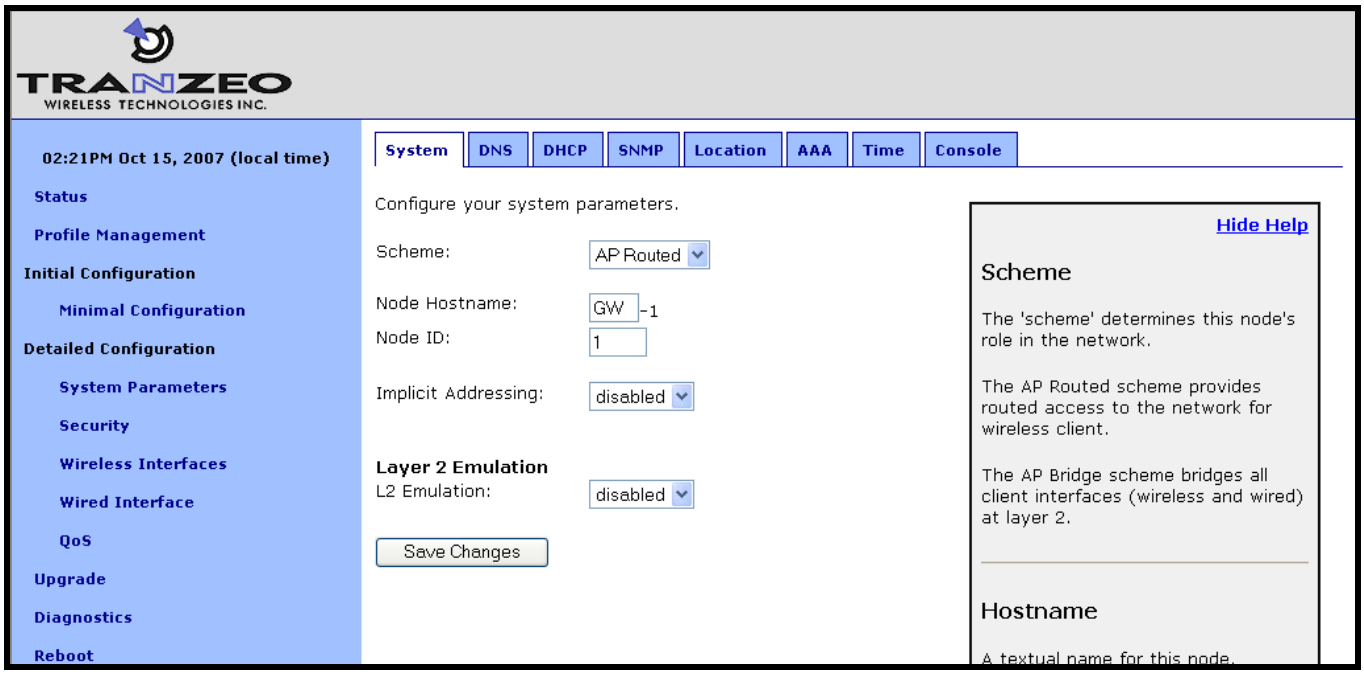

Figure 34. Setting the addressing scheme

10.1 Implicit Addressing Scheme

The implicit addressing scheme requires the sharing of a class C network between all active client access interfaces. The subnet address space is based on the node ID and the LAN prefix as shown in Figure 35.

Figure 35. Subnet address structure

INFO

If the EL-900 is operating in centralized DHCP server mode, the addresses used for the implicit addressing scheme have no bearing on the addresses that are assigned to client devices through DHCP.

The default division of the class C address space is shown in Table 7. It is possible to change this configuration, assigning larger address spaces to certain interfaces if not all interfaces are enabled.

Interface	Interface address	Broadcast address	Client device 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

subnet = <LAN prefix first octet>.<LAN prefix second octet >.<node ID>

Table 7. Default subnet segmentation between interfaces

10.1.1 LAN Prefix

The LAN prefix parameter sets the first two octets of the client access interface IP address when using the implicit addressing scheme. The suggested values for the LAN prefix are 10.x and 192.168.

The LAN prefix parameter only has an effect on an EL-900 using the explicit addressing scheme when explicit addresses have not been defined for the client access interfaces. See section 10.2 for more information on use of the LAN prefix when using the explicit addressing scheme.

CLI

The first octet of 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
```

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

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

Web GUI

The LAN prefix can be set via the web interface using the "System" tab on the "System Parameters" page (see Figure 34).

10.1.2 Client Address Space Segmentation in Implicit Addressing Mode

As mentioned above, the client access interfaces must share a class C address space when the EL-900 is using the implicit addressing scheme. The start address of each address segment and its size can be set. The following restrictions are placed on the address segment configuration:

- Each active client access interface must be assigned an address segment.
- The IP address range start address ('ip.implicit.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.implicit.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 8 lists allowed combinations.
- The address spaces for enabled interfaces must start at different addresses.
- The address spaces for enabled interfaces should not overlap.

Address range start (ip.implicit.start.requested)	IP address range size (ip.implicit.size.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 8. 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 an EL-900 is not configured such that this requirement is met, address spaces will be automatically reduced in size to prevent overlap.

CLI

The start and size of client address spaces are set with the 'ip.implicit.start.requested' and 'ip.implicit.size.requested' parameters in the 'wlan1', 'wlan2', 'wlan3', and 'wlan4' interfaces. Refer to Table 8 for allowed values for these parameters.

In the first example below, the 'wlan1' interface is set to use the entire class C address space (this requires that all the other client access interfaces, wlan2-4, are disabled). In the second example, the 'wlan1' interface is set to use the upper half of the class C address space.

```
> use wlan1
eth0> set ip.implicit.start.requested=1
eth0> set ip.implicit.size.requested=255

> use wlan1
eth0> set ip.implicit.start.requested=129
eth0> set ip.implicit.size.requested=127
```

The actual start address and size of a segment are accessible via the 'ip.implicit.start.actual' and 'ip.implicit.size.actual' parameters. These may values may differ from the requested values if the rules for setting these parameters were not abided by.

Web GUI

The address space segments' start addresses and sizes can be set via the web interface using the "DHCP" sub-tab on the "DHCP" tab on the "System Parameters" page (see Figure 36).

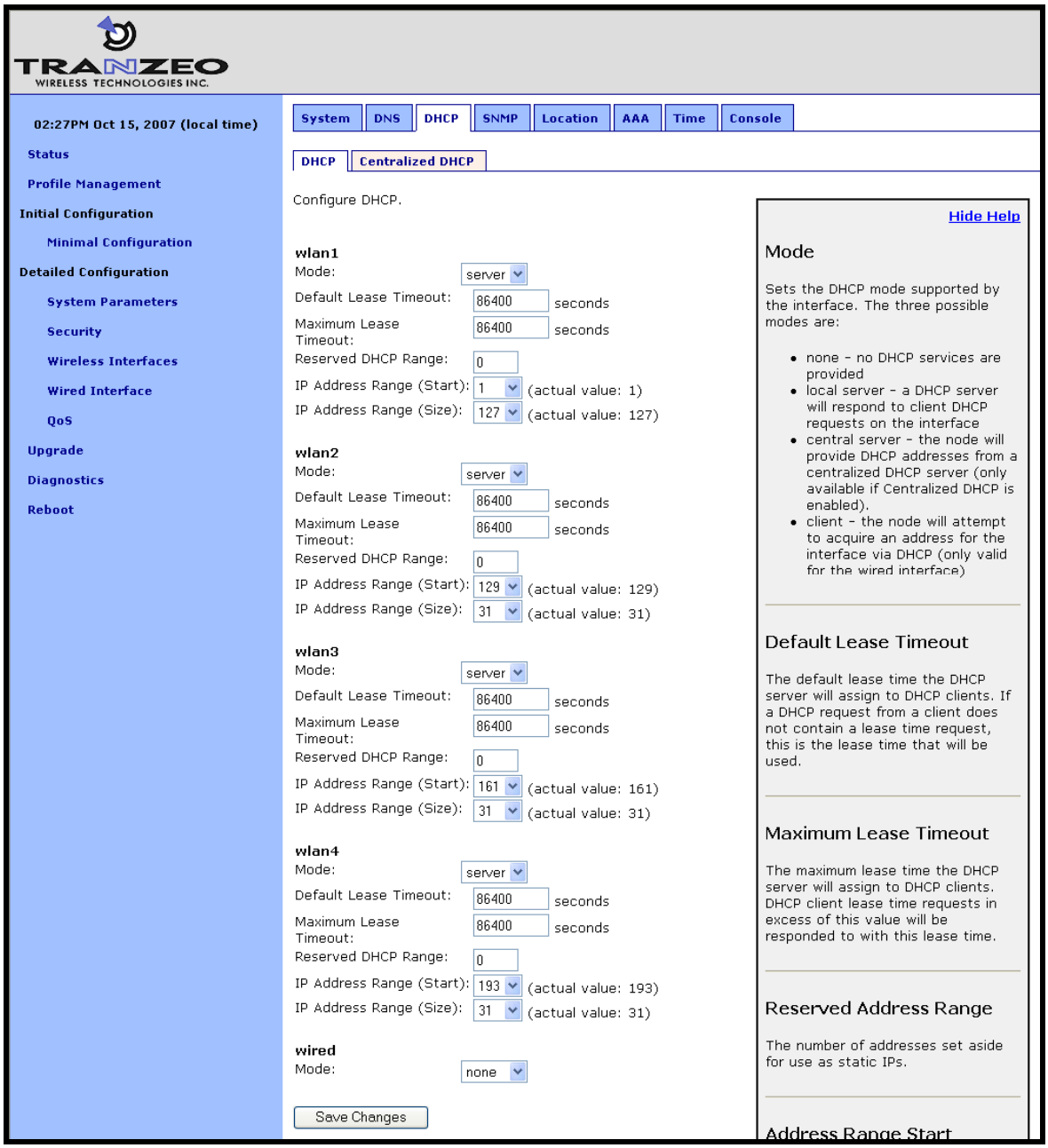

Figure 36. Address space settings in implicit addressing mode

10.2 Explicit Addressing Scheme

When using the explicit addressing scheme, the IP parameters for each interface can be specified manually on the "Wireless Interface" page.

When specifying the IP addresses and subnet sizes for the client access interfaces, the following rules should be followed:

- Specify IP address and subnet combinations that do not lead to misalignment, e.g. 10.0.0.4/24 is not a properly aligned address/subnet size combination.
- Do not specify subnets that are in the following ranges:
  - 169.254.0.0/16
  - 127.0.0.0/8
- Each subnet specified for a client access interface must not overlap with that of any other client access interface on the device.
- Do not specify any subnets for client access interfaces that overlap with subnets outside the device that you want client devices to be able to connect to.

Do not specify a gateway IP address for any of the client access interfaces when operating using the explicit addressing scheme. This field should be left blank for each interface.

If an address space is not defined for a client access interface when operating in explicit addressing mode, a default address space will be defined with the following parameters

- IP address: *<first octet of LAN prefix>.<node ID>.<virtual AP number (1-4)>.1*
- IP netmask: 255.255.255.0

CLI

Set the 'implicit.enable' parameter in the 'mesh0' to 'no' interface to select the explicit addressing scheme. The example below demonstrates this.

```
> use mesh0
sys> set implicit.enable=no
```

See section 13.3 for instructions on how to set the IP addresses for the client access interfaces when using the explicit addressing scheme.

Web GUI

The addressing scheme is set with the "Implicit Addressing" drop-down menu on the "System" tab of the "System" page (see Figure 34). Set this to "disabled" to use the explicit addressing scheme.

See section 13.3 for instructions on how to set the IP addresses for the wired and wireless client access interfaces when using the explicit addressing scheme.

11 Ethernet Interface Configuration

BRIDGE

The Ethernet interface features described in this chapter are not used in bridge mode. See section 12 for information on how to configure the bridge interface to provide IP access to the EL-900 when operating in bridge mode.

The Ethernet interface is used to connect the EL-900 to a LAN. It is also used for initial configuration of the device. The Ethernet interface IP address can either be acquired from a DHCP server on the LAN or be set manually.

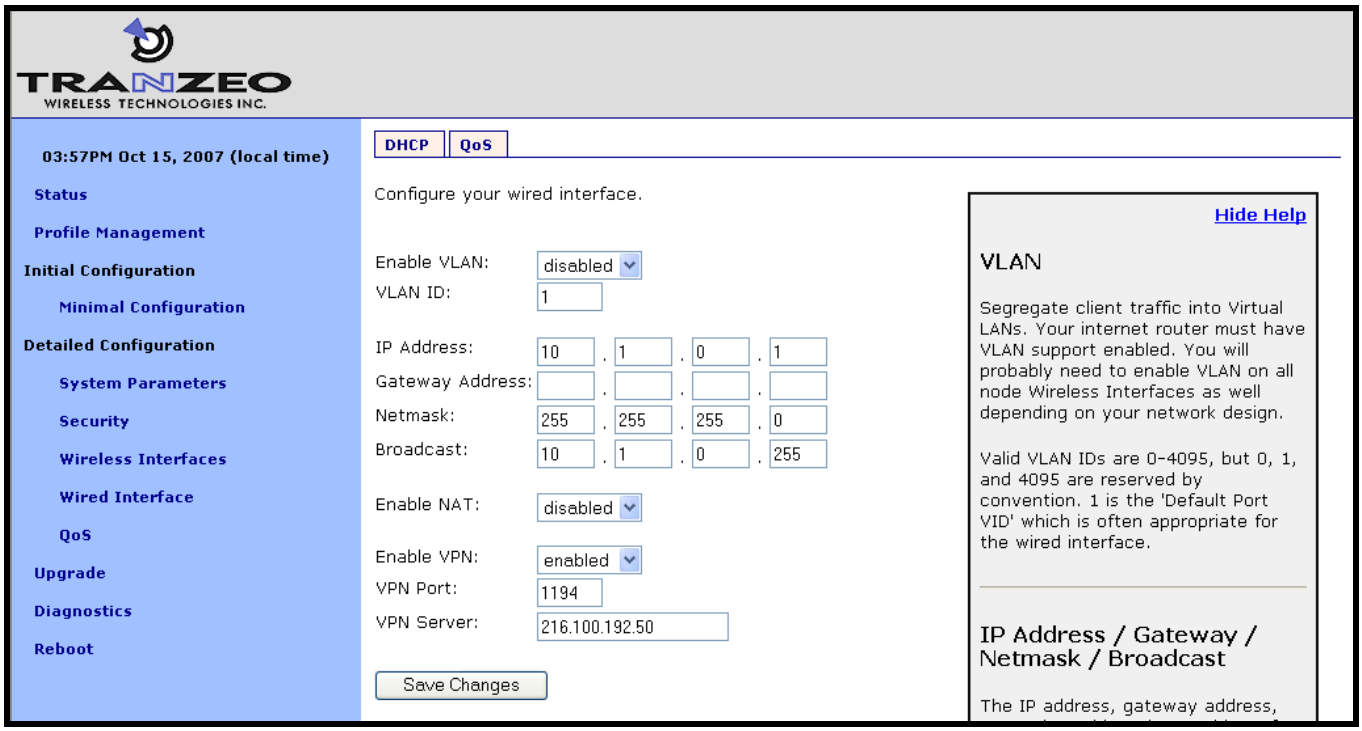

Figure 37. Wired interface parameters

11.1 DHCP

The EL-900 can be set to obtain an IP address for its Ethernet interface using DHCP. When configured as a DHCP client, the EL-900 will continually attempt to contact a DHCP server until it is successful.

If the DHCP mode is set to ‘client’, the IP configuration must be carried out manually, as described in the next section.

CLI

To set the DHCP mode to ‘client’ 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 mode parameter to ‘none’ as shown below.

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

Web GUI

The Ethernet DHCP mode value can be set via the web interface using the “DHCP” sub-tab on the “DHCP” tab on the “System Parameters” page (see Figure 38).

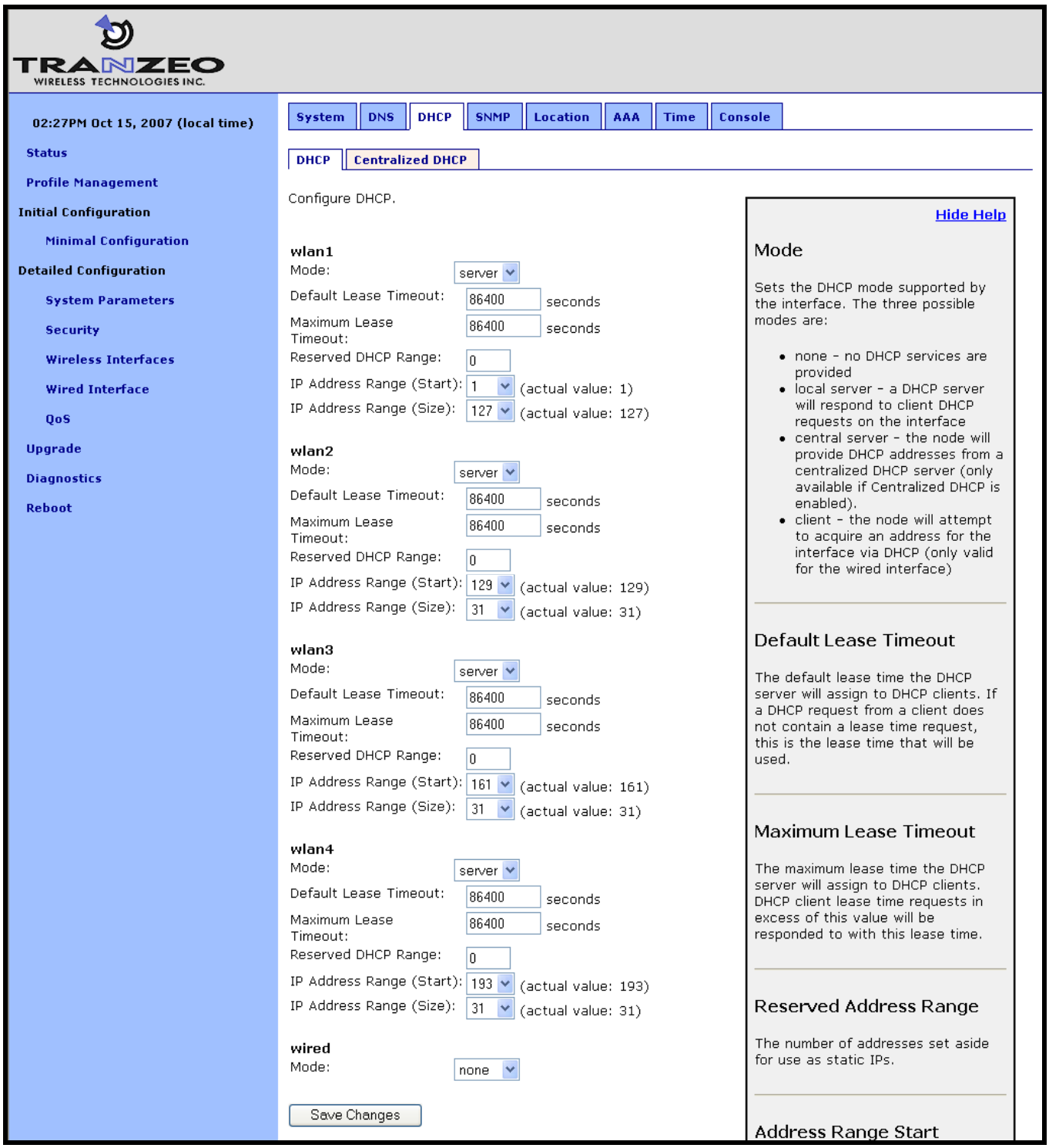

Figure 38. Wired DHCP settings

11.2 Manual IP Configuration

If the Ethernet DHCP mode 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 LAN prefix and node 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 mode setting must be set to 'none' if the EL-900 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 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 mode 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

The Ethernet IP address, gateway, netmask, and broadcast address parameters can be set via the web interface using the “Wired Interface” page (see Figure 37). The current IP values can be viewed on the “Status” page.

12 Bridge Interface Configuration

12.1 IP Configuration

The bridge interface has an IP address that can be set manually or acquired via DHCP. With the exception of the fixed configuration IP address, this is the only active IP address on the device when it is operating in bridge mode.

When not explicitly specifying an IP address or enabling DHCP client mode, the address for the bridge interface will default to *<LAN prefix first octet>.<node ID>*.1.1.

CLI

The bridge IP settings are set with the 'ip.address_force', 'ip.broadcast_force', 'ip.gateway_force', and 'ip.netmask_force' parameters in the 'br0' interface. For these settings to be used, the bridge interface DHCP mode must be disabled using the 'dhcp.role' parameter in the 'br0' interface, as shown in the example below.

The example below, shows how to manually set an IP configuration for the bridge interface

```
> use br0
br0> set dhcp.role=none
br0> set ip.address_force=10.5.1.27
br0> set ip.broadcast_force=10.5.1.255
br0> set ip.gateway_force=10.5.1.1
br0> set ip.netmask_force=255.255.255.0
```

To set the DHCP mode to 'client' for the bridge interface, set the 'dhcp.role' parameter in the 'br0' interface to 'client' as shown below.

```
> use br0
br0> set dhcp.role=client
```

Web GUI

The IP address, gateway, netmask, and broadcast address parameters can be set on the "L2 Bridge" page when the DHCP mode for the bridge interface is set to 'none' (see Figure 13). A link to the "L2 Bridge" page appears in the navigation bar when bridge mode is selected.

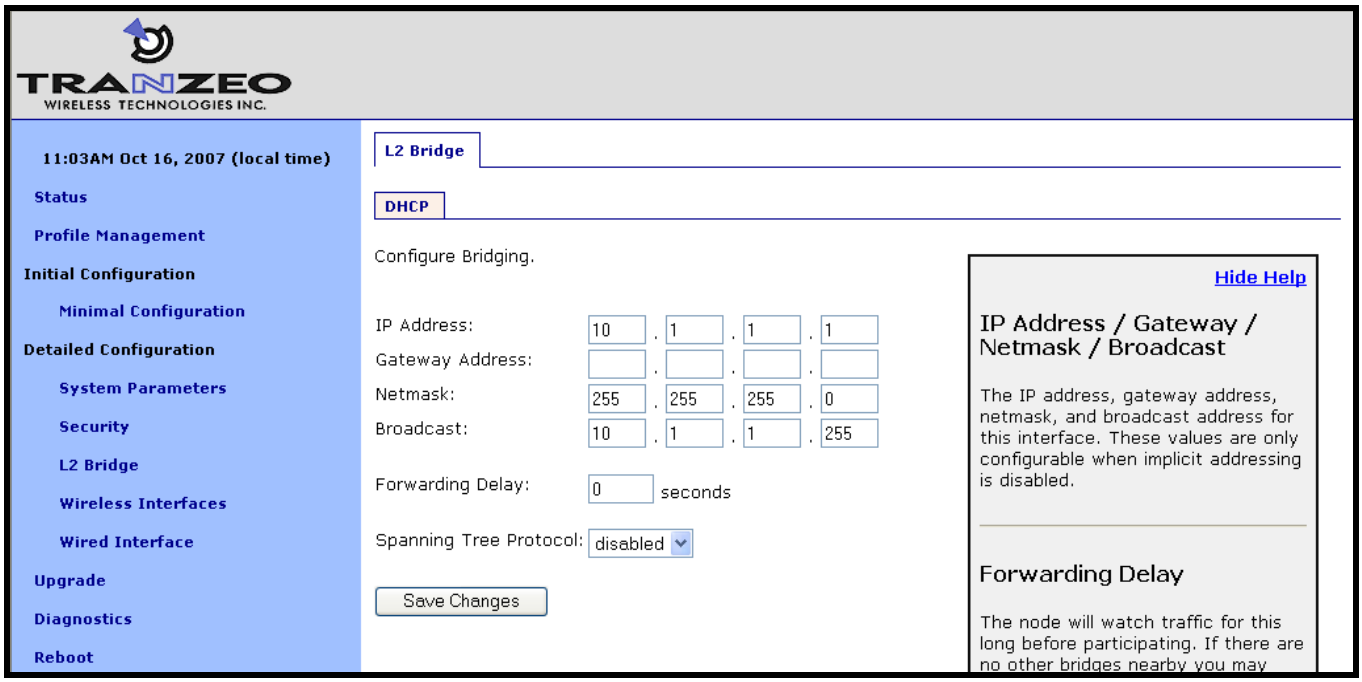

Figure 39. Bridge configuration page with DHCP client mode disabled

The DHCP mode for the bridge interface is set on the “DHCP” tab on the “System” page. When bridge mode is selected, the only setting available on this page is the bridge DHCP mode, as shown in Figure 40.

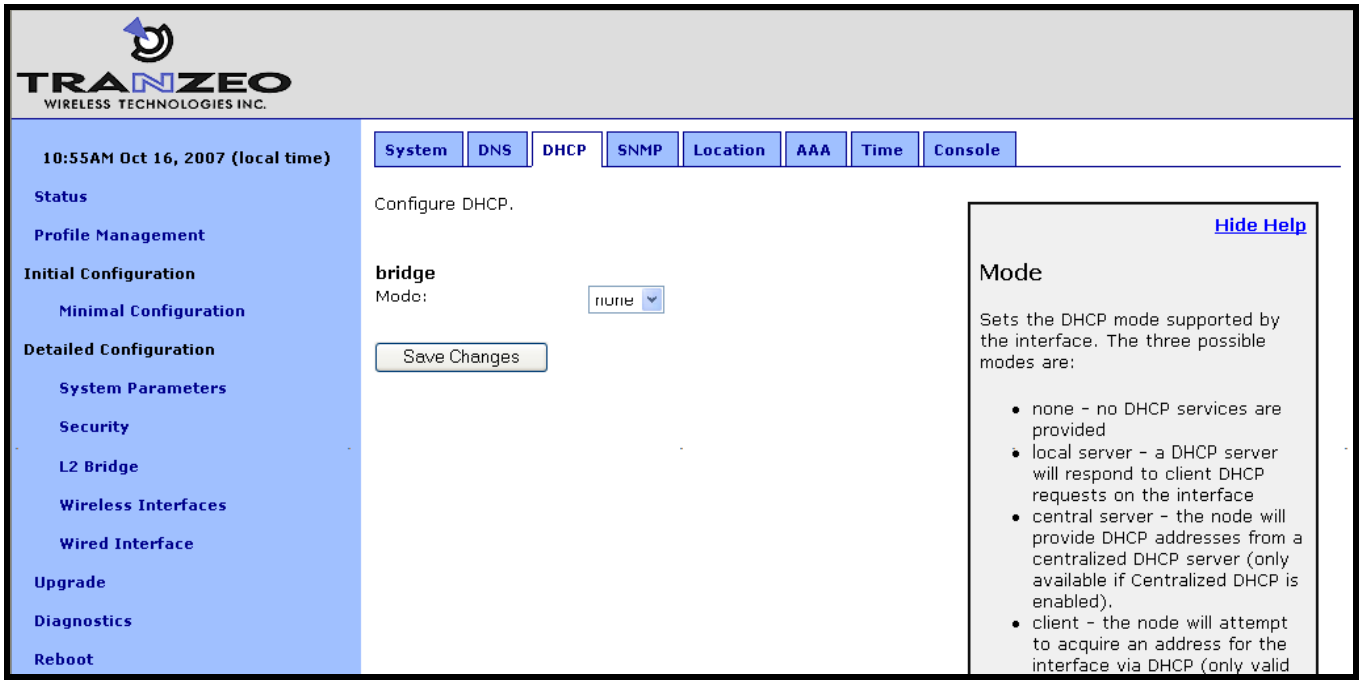

Figure 40. DHCP configuration page when operating in bridge mode

12.2 Bridging Parameters

Two parameters are available for controlling how the bridge mode operates: forwarding delay and Spanning Tree Protocol control.

The forwarding delay sets how long, in seconds, the EL-900 will watch traffic before participating. If there are no other bridges nearby the EL-900 this value can be set to 0. When the DHCP mode for the bridge interface is set to 'client', the forwarding delay will be automatically set to 15 to avoid DHCP requests timing out.

The EL-900 supports the Spanning Tree Protocol (STP), which is used to ensure a loop-free topology for any bridged LAN. STP support can be disabled or enabled.

CLI

The forwarding delay is set with the 'forwarding_delay' parameter in the 'br0' interface. The delay is specified in seconds.

```
> use br0
br0> set forwarding_delay=5
```

Spanning Tree Protocol state is set with the 'stp.enable' parameter in the 'br0' interface. Set this parameter to 'yes' to enable it and to 'no' to disable it.

```
> use br0
br0> set stp.enable=yes
```

Web GUI

The forwarding delay and Spanning Tree Protocol state can be set on the "L2 Bridge" page

13 Virtual Access Point (VAP) Configuration

An EL-900 has four virtual access points (VAPs) that can be configured to suit different application needs. These VAPs share a common radio, but, with a few exceptions noted in this chapter, can be configured independently. The availability of the four VAPs provides more flexibility in configuration and catering to different user classes than a single AP does.

INFO

The interfaces for the VAPs will be referred to as 'wlan*N*' when it applies to any of the four VAPs. 'wlan1' will be used in all examples.

Figure 41. Virtual access point interface page with EL-900 in routed mode

13.1 Virtual Access Point Interfaces

There are four interfaces that are used to configure the VAPs: wlan1, wlan2, wlan3, and wlan4. The VAPs have equivalent configuration capabilities and there is no inherent prioritization or preference for one VAP. The section on quality-of-service settings (section 17) describes how prioritization on a per-VAP basis can be configured.

13.2 Enabling and Disabling Virtual Access Points

VAPs can be individually enabled or disabled. A VAP can be configured when it is disabled and parameter settings are retained when it is disabled.

CLI

A VAP can be enabled with the 'enable' parameter in the 'wlan*N*' interface as shown below.

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

A VAP can be disabled with the following commands.

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

Web GUI

Each VAP can be enabled or disabled by setting the "State" parameter via the web interface using the appropriate "wlan*N*" tab on the "Wireless Interfaces" page (see Figure 41).

13.3 Virtual Access Point Client Device Address Space

Each VAP interface is either assigned a segment of the EL-900's class C client address space, if the device is using implicit addressing mode, or an arbitrary address space can be set for the interface when using the explicit addressing scheme . See section 10 for more information on client addressing schemes.

The EL-900 VAPs' interface IP configurations can be changed directly when it is using the explicit addressing scheme. They cannot be changed directly when the device is using the implicit addressing scheme.

When an EL-900 is configured to use the implicit addressing scheme, set the IP address to the desired value by modifying the node ID and LAN prefix parameters (see sections 9.2 and

10.1.1). Set the netmask by changing the client address space segments as described in 10.1.2.

CLI

You can view the IP settings for the VAP interfaces with the 'ip.*' parameters in the appropriate 'wlan*N*' interface as shown in the example below.

```
> use wlan1
wlan1> get ip.*
 ip.address = 10.2.4.1   [read-only]
 ip.address_force =
 ip.broadcast = 10.2.4.127   [read-only]
 ip.broadcast_force =
 ip.gateway =    [read-only]
 ip.gateway_force =
 ip.netmask = 255.255.255.0   [read-only]
 ip.netmask_force =
 ip.implicit.size.actual =    [read-only]
 ip.implicit.size.requested = 31
 ip.implicit.start.actual =    [read-only]
 ip.implicit.start.requested = 1
```

When an EL-900 is using the implicit addressing scheme, the VAP IP settings can be changed by altering the 'id.node', 'id.mesh', and 'id.lanprefix' parameters in the 'sys' interface and the 'ip.implicit.start.requested' parameter in the appropriate 'wlan*N*' interface.

When an EL-900 is using the explicit addressing scheme, the IP address, netmask, gateway address, and broadcast address can be set using the 'ip.address_force', 'ip.netmask_force', 'ip.gateway_force', and 'ip.broadcast_force' parameters in the appropriate 'wlan*N*' interface as shown in the example below.

```
> use wlan1
wlan1> set ip.address_force=10.12.8.1
wlan1> ip.broadcast_force=10.12.8.255
wlan1> ip.gateway_force=
wlan1> ip.netmask_force=255.255.255.0
```

Web GUI

The current VAP IP settings can be viewed through the web interface on the "Config Overview" tab on the "Status" page. When using the implicit addressing scheme, the VAP IP settings can be changed by altering the node ID and LAN prefix settings on the "System" parameters tab on the "System Parameters" page. In explicit addressing mode, the IP parameters can be set on the appropriate tab on the "Wireless Interface" page.

13.4 Channel

The EL-900HG has an 802.11b/g radio that can be set to operate in the channels listed in Table 9.

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 9. EL-900HG access point channels and associated center frequencies

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

The EL-900HA has an 802.11a radio that can be set to operate in the channels listed in Table 10.

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

Table 10. EL-900HA access point channels and associated center frequencies

It is not possible to configure the VAPs to use different channels. If the channel for wlan2 is changed, the channel will be changed for wlan1, wlan3, and wlan4.

CLI

The VAP channel is set with the 'channel' parameter in the 'wlan*N*' interfaces. The example below shows how to set the VAP 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 "wlan*N*" tab on the "Wireless Interfaces" page (see Figure 41).

13.5 ESSID

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

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 a VAP ESSID by restricting it from broadcasting advertisements for that ESSID. Whether it is appropriate for a VAP ESSID to be hidden depends on the application.

CLI

The VAP 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 'wlan*N*' interface. The example below shows how hiding of the ESSID can be enabled.

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

Web GUI

The VAP ESSIDs and their broadcast state can be set via the web interface using the appropriate "wlan*N*" tab on the "Wireless Interfaces" page (see Figure 41).

13.6 IP Configuration of Client Devices

The VAP interfaces allow client devices to connect to the EL-900. The client devices can be assigned their IP configuration in one of three ways when the EL-900 is operating in routed mode:

- Via DHCP from a centralized server
- Via DHCP from a local server on the EL-900 that the client device is connected to
- Be manually configured

When the EL-900 is operating in bridge mode, the client device IP address requirements will depend on the settings for the LAN that the EL-900 is connected to.

13.6.1 IP Configuration of Clients Devices via DHCP

The EL-900 can be set to serve IP addresses to client devices on the VAP interfaces using DHCP. DHCP-provided addresses can be served either from a local server on the EL-900 or from an external server. The two DHCP modes are described in detail in section 14.

13.6.2 Manual IP Configuration of Client Devices

In routed mode with centralized DHCP server mode disabled, client devices that use static IP addresses must have an IP address that is within the subnet of the VAP interface that they connect to. See section 14.2.1 for information on using static IP addresses for client devices with centralized DHCP server mode enabled.

When operating in bridge mode, the client devices IP configuration requirements will depend on the network settings for the LAN that the EL-900 is connected to.

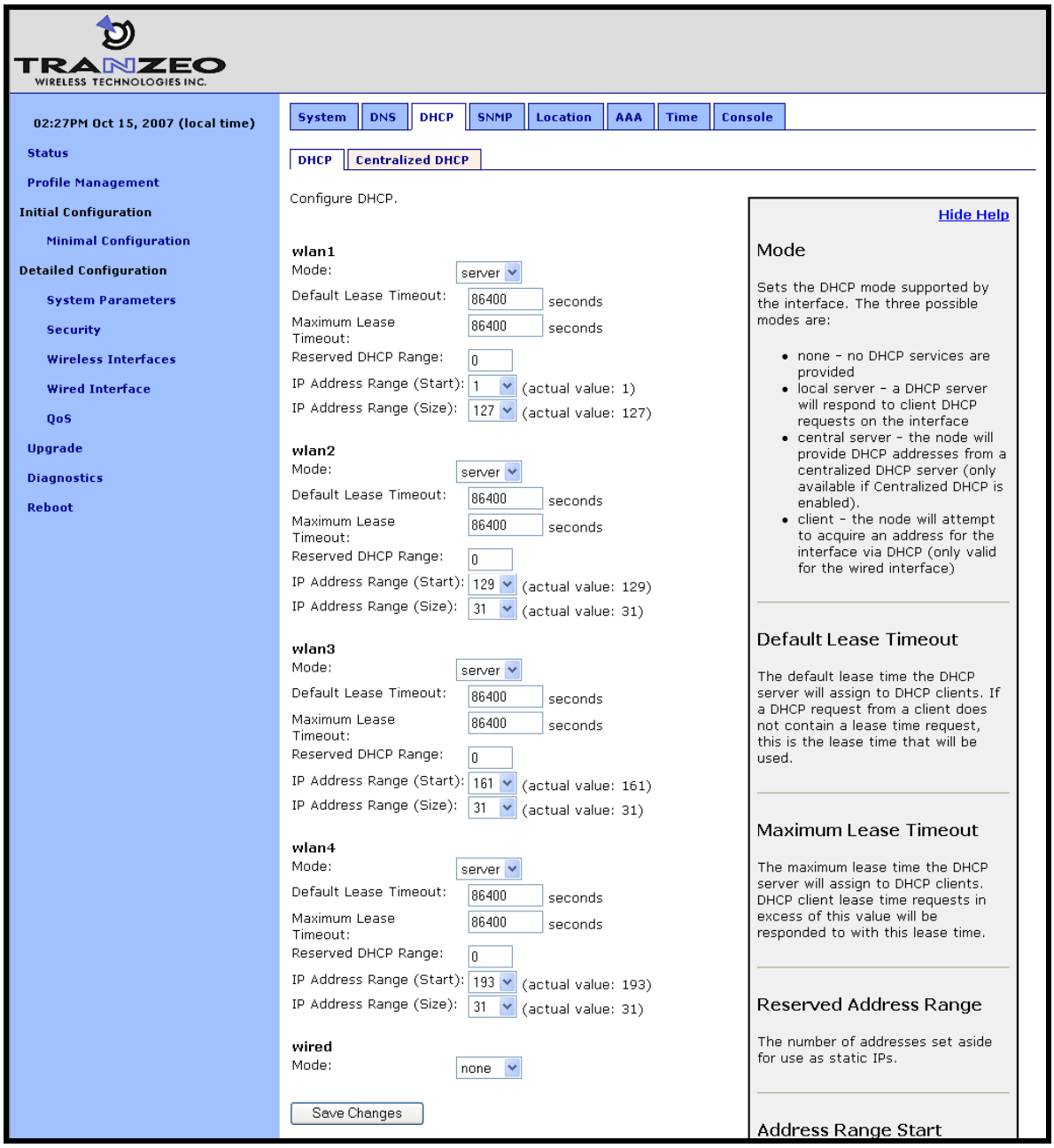

Figure 42. Virtual access point and wired interface DHCP and address space settings

If the local DHCP server is enabled for an VAP 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 interface's 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 42).

13.7 Client Devices

Each VAP has a status page that displays information about attached client devices and total throughput through the VAP. The signal strength of each client device, its 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 43.

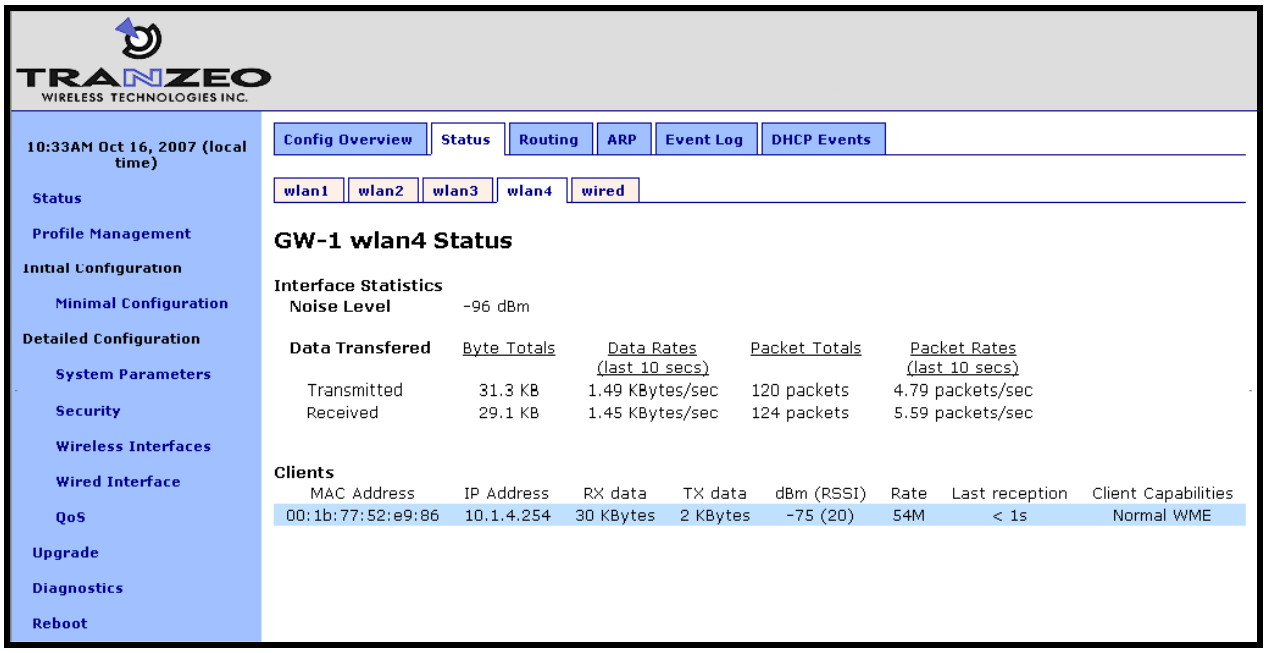

Figure 43. Virtual access point client device status information

13.8 Encryption and Authentication

The EL-900 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 VAP are independent. A VAP can only support one of the encryption/authentication modes at a time, but the VAPs in the EL-900 do not all have to use the same encryption/authentication scheme.

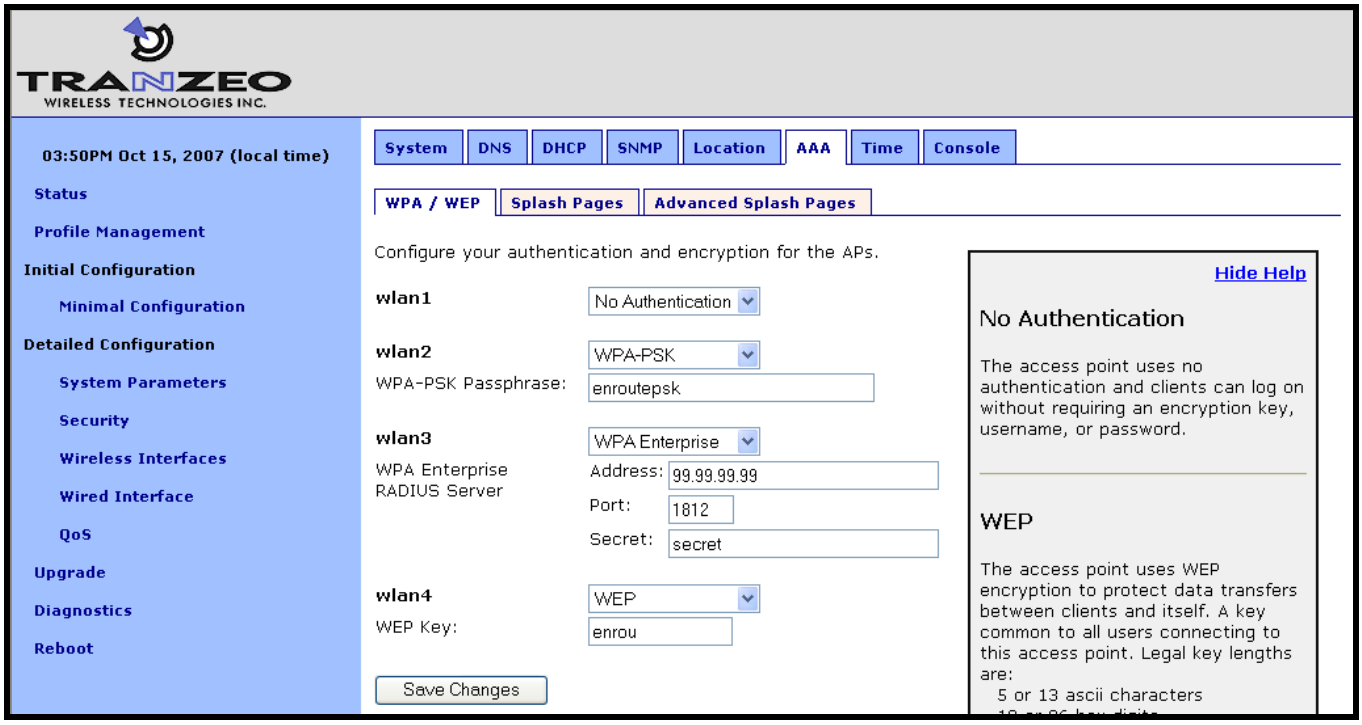

Figure 44. Virtual access point authentication and encryption settings

13.8.1 WEP Encryption

The VAPs 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 'wlan*N*' 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 'wlan*N*' 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 44). Select "WEP" as the type of encryption from the drop-down menu for the VAP you wish to configure and set the WEP key in the text box below the drop-down menu. In the example in Figure 44, 'wlan1' has been configured to use WEP.

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

In WPA pre-shared key (PSK) mode, a common passphrase is used for client devices connecting to an EL-900 VAP. 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, with at least 15 characters, is used. This will 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 44). Select "WPA-PSK" as the type of encryption/authentication from the drop-down menu for the VAP you wish to configure and enter the WPA-PSK key in the text box below the drop-down menu. In the example in Figure 44, 'wlan2' has been configured to use WPA-PSK.

13.8.3 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.

See section 20.5 for instructions on how to test the RADIUS configuration and a specific set of credentials.

CLI

To configure the EL-900 to support 802.1x authentication, the following parameters in a 'wlan*N*' 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=enroute1000_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 44). Select "WPA-EAP" as the type of encryption/authentication from the drop-down menu for the VAP 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 44, 'wlan3' has been configured to use WPA-EAP.

13.9 Transmit Power Cap

The maximum transmit power cap of the EL-900's radio is configurable. Increased output power will improve communication range, but will also extend the interference range of the radios. By default, the power cap is set to 30 dBm so as not to limit the power of the AP.

If the transmit power is set to a value in excess of what can be supported by the AP radio, the actual radio output power will be the highest power supported by the AP radio.

INFO

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

CLI

The example below shows how to set the access point radio's maximum transmit power using the CLI. The Tx power is specified in dBm, with a granularity of 0.5 dBm.

```
> use wlan1
wlan1> set txpower=20
```

Web GUI

The VAPs' maximum transmit power can be set via the web interface using the appropriate "wlan*N*" tab on the "Wireless Interfaces" page (see Figure 41). The "+" and "-" buttons can be used to increase or decrease the power setting in 0.5 dBm steps.

13.10 Radio Rate

The VAPs can be set to communicate at a specific rate or to automatically select the best rate available. For most applications, choosing automatic rate selection will be the best choice.

CLI

It is not currently possible to set this through the CLI. Please use the web GUI to set this parameter.

Web GUI

The VAPs' communication rate can be set via the web interface using the appropriate "wlan*N*" tab on the "Wireless Interfaces" page (see Figure 41). To limit communication to a specific rate, use the drop-down menu to select the appropriate rate and verify that the "Auto" checkbox is not selected. To set the device to automatically select the most appropriate rate, click on the "Auto" checkbox to select it.

13.11 Preamble Length

The VAPs can be configured to use short preambles when there are no client devices present that only support long preambles. Alternatively, the device can be forced to always use long preambles. Using short preambles reduces communication overhead, but may not be supported by older 802.11 client devices.

The preamble length setting is uniform across all VAPs. Changing it for one will automatically change it for all others as well.

CLI

The example below shows how to set the preamble type used by a VAP using the CLI. The preamble type is set with the 'iwpriv.short_preamble' parameter in the 'wlan*N*' interfaces. To enable short preambles, set this parameter to '1'. To force use of long preambles, set this parameter to '0'.

```
> use wlan1
wlan1> set iwpriv.short_preamble=1
```

Web GUI

The preamble types supported by the VAPs can be set via the web interface using the appropriate "wlan*N*" tab on the "Wireless Interfaces" page (see Figure 41). To allow support for short preambles, set the "Use Short Preamble" drop-down menu to "Yes". To limit preambles to long ones, set the drop-down menu to "No".

13.12 Beacon Interval

The VAPs' beacon intervals are configurable. The beacon interval must fall in the range from 20 to 500 ms. The beacon interval is set to 100 ms by default.

CLI

The example below shows how to set the beacon interval for a VAP using the CLI. The beacon interval is set with the 'iwpriv.beacon_interval' parameter in the 'wlan*N*' interfaces and is specified in milliseconds.

```
> use wlan1
wlan1> set iwpriv.beacon_interval=100
```

Web GUI

The beacon interval for an VAP can be set via the web interface using the appropriate "wlan*N*" tab on the "Wireless Interfaces" page (see Figure 41). Enter a value specified in milliseconds in the "Beacon Interval" field.

13.13 Maximum Link Distance

The 802.11 standard defines delay values in the communication between devices that affect the maximum communication distance that can be supported. By default, the communication distance is limited to approximately 4 km (2.5 mi). The maximum communication distance can

be increased by setting a custom maximum link distance value. This value can be specified in either metric or imperial units.

The maximum link distance setting is uniform across all VAPs. Changing it for one will automatically change it for all others as well.

CLI

The example below shows how to set the maximum link distance supported by a VAP using the CLI. The maximum link distance is set with the 'distance' parameter in the 'wlan*N*' interfaces and is specified in either kilometers or miles. The 'units' parameter in the 'sys' interface determines whether the distance units are to be entered in kilometers or miles. Set 'units' to "metric" for kilometers, and to "imperial" for miles.

Set the 'distance' parameter to "DEFAULT" or leave it blank to use the default maximum link range.

```
> use sys
sys> set units="metric"
> use wlan1
wlan1> set distance=10
```

Web GUI

The maximum link distance supported by an VAP can be set via the web interface using the appropriate "wlan*N*" tab on the "Wireless Interfaces" page (see Figure 41). Enter a value and specify whether it is in kilometers of miles using the adjacent drop-down menu.

Set the 'distance' parameter to "DEFAULT" or leave it blank to use the default maximum link range.

14 Client DHCP Configuration

When operating in routed mode, two configuration options exist for assigning IP addresses to client devices using DHCP:

- The EL-900 hosts a local DHCP server and supplies IP addresses to devices attaching to any of the client access interfaces
- A centralized DHCP server supplies IP addresses to client devices, with the EL-900s relaying DHCP messages between client devices and the centralized server.

The DHCP modes for client access interfaces on an EL-900 can be set individually to use a local server, a centralized server, or be disabled. This allows a device to support client access interfaces with a combination of centralized and localized DHCP.

BRIDGE

An EL-900 operating in bridge mode can provide access to a DHCP server on the LAN that it is bridging to, but it will not provide any local DHCP functionality for client devices when operating in this mode. Centralized DHCP server mode does not need to be configured in bridge mode since the relaying occurs implicitly by virtue of the bridging function that the EL-900 provides.

It is possible to configure the bridge interface to receive an address via DHCP (see section 12.1)

14.1 Using Local DHCP Servers

The EL-900 can be set to serve IP addresses to client devices on enabled VAP interfaces using DHCP.

The IP addresses provided by the local DHCP server will be in the subnet defined by the LAN prefix and node ID and the IP address range start address and size parameters in the appropriate client access interface. For example, for the 'wlan1' interface, the start and end of the address range are:

Start address = *<LAN prefix octet 1>.*
< LAN prefix octet 2>.
<Node ID>.
<wlan1 IP address range start address> + 1

End address = *< LAN prefix octet 1>.*
< LAN prefix octet 2>.
<Node ID>.
< wlan1 IP address range start address > -
< wlan1 IP address range size > - 2

The EL-900 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 EL-900 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 octet 1>.*
< LAN prefix octet 2>.
<Node ID>.
<wlan1 IP address range start address> + 1 - < wlan1 DHCP reserve>

CLI

The DHCP mode parameters in the 'wlan*N*' interfaces control DHCP behavior. When the mode is set to 'server', the EL-900 will respond to DHCP requests received from client devices connected to the interface.

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

```
> use wlan1
wlan1> set dhcp.role=server
wlan1> set dhcp.relay.enable=no
```

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 VAP interfaces' DHCP server state can be set via the web interface using the "DHCP" sub-tab under the "DHCP" tab on the "System Parameters" page (see Figure 45). All of the interfaces' DHCP settings can be configured on this page. Set the "Mode" field to "Server" to set the DHCP mode for a client access interface to be the local DHCP server.

The DHCP reserve setting for all VAPs 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 45).

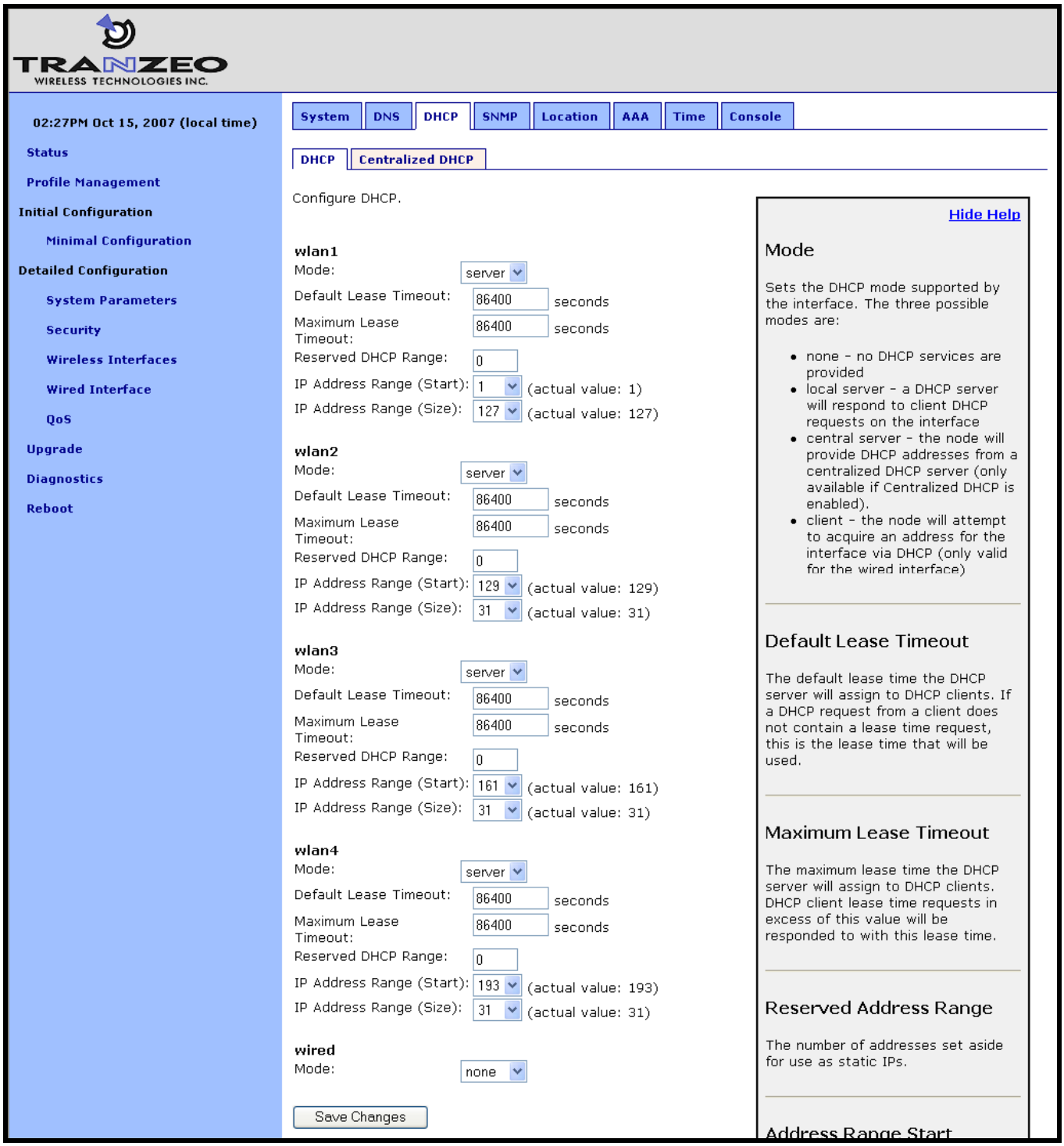

Figure 45. Virtual access point DHCP configuration

14.2 Using a Centralized DHCP Server

Centralized DHCP server mode uses DHCP relaying to enable assignment of IP addresses to wireless client devices from a common remote DHCP server. The remote DHCP server may reside either on a host connected to the LAN segment that the EL-900's Ethernet is attached to, or on a server that is beyond one or more routers. When using a common DHCP server, wireless client devices are assigned IP addresses from a single address pool, and are allowed to keep their IP address while roaming seamlessly from AP to AP.

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

1. The EL-900
2. The central DHCP server
3. Any intermediate router(s) in the path between the DHCP server and the EL-900

When using a centralized DHCP server, a Client Address Space (CAS), from which client device IP addresses are assigned, must be defined. The active VAP client access interfaces on the EL-900 (there can be up to 4 per EL-900) must also have IP addresses that fall within the CAS. This is to facilitate DHCP relay and selection of client device IP addresses from the correct DHCP scope on servers that serve hosts connected to different subnets. The VAP client access interface IP addresses must be configured statically and must be contiguous. It is recommended that a contiguous range of IP addresses at either the beginning or the end of the CAS be set aside, one for each VAPs on the EL-900.

The Client Address Space (CAS) is not equivalent to the range of addresses served by the DHCP server. The DHCP-served address range is a subset of the CAS. The CAS must also include the addresses for the client access interfaces and the address of the EL-900's Ethernet interface.

Consider the example where an EL-900 has all four of its VAPs enabled. The DHCP server resides on a host that also acts as the WAN router and is connected to the same LAN segment that the EL-900's wired interface is. We will set aside 4 IP addresses for the EL-900's VAPs. 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 EL-900's Ethernet interface, set aside 192.168.5.3 to 192.168.5.6 for the EL-900's VAP interfaces, and configure the remote DHCP server to serve IP addresses in the range of 192.168.5.7 to 192.168.5.254 to wireless client devices. We will keep 192.168.5.255 as the broadcast address.

A bridged EnRoute1000 will pass DHCP traffic through its wired interface to any client devices on its VAPs regardless of the EnRoute1000's DHCP mode settings. Centralized DHCP mode provides similar capability for an EnRoute1000 in routed mode, while adding the capability to support different subnets, a firewall, and QoS, which are not available in bridge mode.

14.2.1 Support for Clients with Static IP Addresses

When using centralized DHCP server mode for a client access interface, client devices connected to that interface can be assigned static addresses within the client address space. However, for these client devices to roam successfully across EL-900s and third party access point bridges connected to the same LAN, they must employ duplicate address detection by sending out ARP requests for their own IP address. Windows-based devices support this requirement. Please contact the client device manufacturer if you are unsure if your client device meets this requirement.

14.2.2 Configuring the EL-900s

When operating in centralized DHCP server mode, each EL-900 client access interface that is to serve DHCP addresses from the centralized server must be explicitly configured to use centralized DHCP server mode. The EL-900s with client access interfaces in centralized DHCP server mode must also 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 EL-900's Ethernet interface.

A gateway router IP address must be entered. This will be supplied to DHCP client devices as their gateway. This IP address can be the same as for the DHCP server, but need not be.

Each client access interface on the EL-900 that is to support centralized DHCP server mode must have its DHCP mode set to "server" for it to support relay of IP addresses to client devices from a central DHCP server. It is possible to disable DHCP address assignments to client devices on a per-interface basis and have them use static IP addresses instead.

The address space that is to be used for the wireless client devices is a subnet specified with the Client Address Space parameter. 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 EL-900's client access interfaces (wlan1-4) need to be manually assigned. This is done by setting the Address Base parameter, which is assigned to the first enabled client access interface. Addresses for the remaining client access interfaces are determined by successively incrementing the Base Address by one.

Layer 2 emulation must also be enabled when operating in centralized DHCP server mode. This setting is located on the "System" tab of the "System" page of the web interface. See section 19.2 for more information on layer 2 emulation mode.

CLI

Centralized DHCP 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 and next WAN router reside on the same segment to which the EL-900's Ethernet interface is connected.

```
> use sys
sys> set dhcp.relay.server=192.168.5.2
sys> set dhcp.relay.gateway=192.168.5.1
```

The example below shows how to set the DHCP mode parameters for the wlan1 and wlan2 interfaces.

```
> use wlan1
wlan1> set dhcp=server
wlan1> set wlan1.dhcp.relay.enable=yes
> use wlan2
wlan2> set dhcp=server
wlan1> set wlan2.dhcp.relay.enable=yes
```

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 access interfaces on an EL-900, is set through the 'dhcp.relay.base' parameter in the 'sys' interface.

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

Web GUI

Centralized DHCP 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 46). The external DHCP server IP address, the gateway router address, the Client Address Space parameter, and the Base Value can also be set on this page. The DHCP mode parameters for all client access interfaces can be set on the "DHCP" sub-tab under the "DHCP" tab on the "System Parameters" page. Set the DHCP mode to "central server" for all interfaces whose client devices should receive addresses from the central DHCP server.

On the “System” tab of the “System” page, set the “L2 Emulation” to “enabled”.

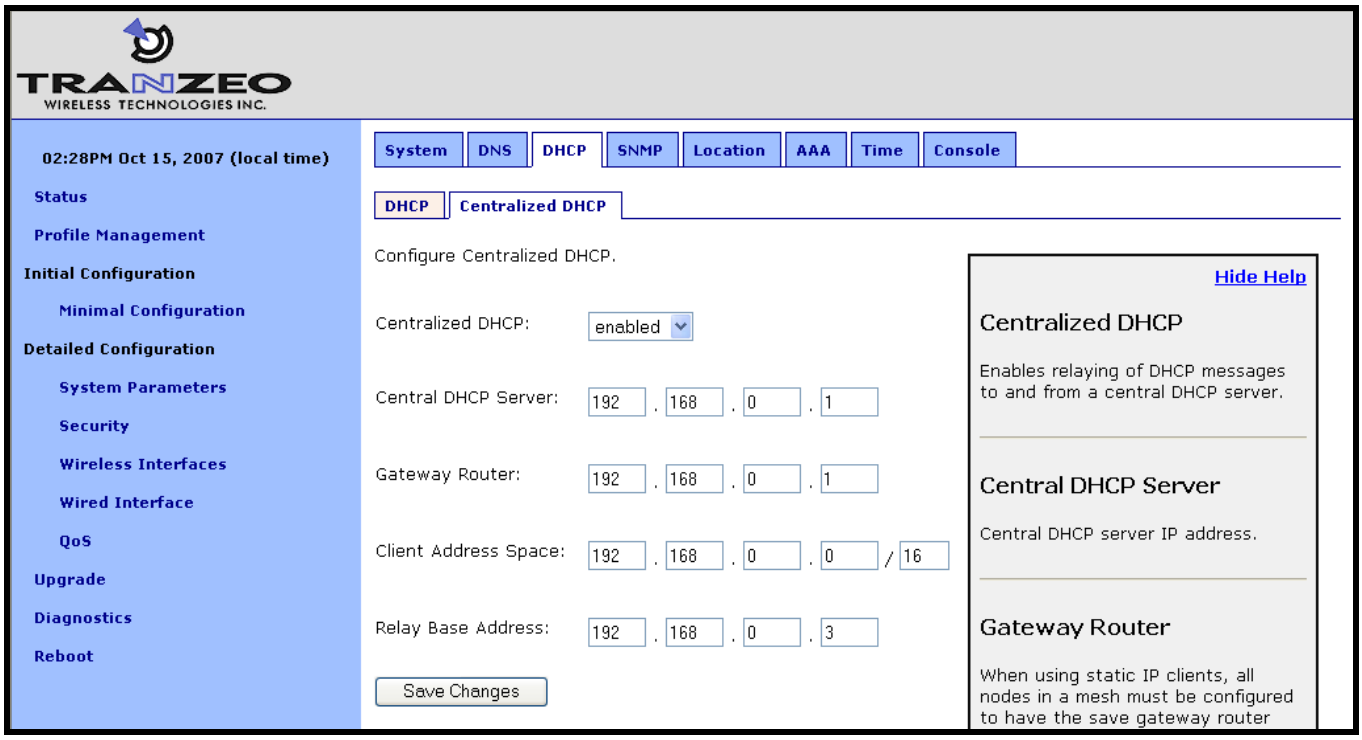

Figure 46. Centralized DHCP server mode settings

14.2.3 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 EL-900 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 client devices
4. The range of the flat IP address that is used for assigning IP addresses to client devices. The range must not include the IP addresses set aside for the client access interfaces on the EL-900.

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 part of the network pertaining to the EL-900:

```
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                           192.168.5.7 192.168.5.254;
}
```

Note that in this definition no “routers” option is needed. If a global “routers” option is defined, the EL-900 will automatically change it to an appropriate value in DHCP responses to client devices based on the centralized DHCP settings on the EL-900. In this example, two IP addresses are set aside for the DHCP server and the EL-900’s Ethernet interface and four IP addresses are set aside for the client access interfaces on the EL-900. Therefore the address pool starts from 192.168.5.7.

15 Connecting an EL-900 to a LAN

The options for connecting an EL-900 to a LAN are described below.

15.1 Routed mode

15.1.1 Manual Configuration

An EL-900 can be directly connected to a LAN without using Network Address Translation. With this configuration and with the implicit client addressing scheme in use, the router on the network that the EL-900 is attached to must be configured to forward the client access interface subnets to the EL-900s Ethernet IP address. The subnet that needs to be forwarded is:

Class C subnet: *<LAN prefix octet 1>.<LAN prefix octet 2>.<node ID>.0*

In the case where the LAN prefix is 10.12 and the node ID is 14, the subnet the router would need to forward to the EL-900 is 10.12.14.0/255.255.255.0.

If the explicit addressing scheme is used, all the individual client access interface subnets must be forwarded to the EL-900's Ethernet IP address.

The sections below describe how to acquire the parameter values that determine what subnets the router should forward to the EnRoute1000.

CLI

When using the implicit addressing scheme, 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 = 12
 sys.id.node = 4
```

This indicates the router needs to forward traffic destined for the 10.12.4.0/255.255.255.0 subnet to the EL-900.

When using the explicit addressing scheme, the subnet information has to be retrieved from the individual interfaces. The example below shows how to obtain the address information for 'wlan1'. A similar approach can be used to obtain that information for the other interfaces.

```
> use wlan1
sys> get ip.*_force
 ip.address_force = 10.5.1.1
 ip.broadcast_force = 10.5.1.255
 ip.gateway_force =
 ip.netmask_force = 255.255.255.0
```

Web GUI

The LAN prefix and node ID can be obtained by inspecting the IP addresses available on the "Status" page. The addresses of interest are the IP addresses for each of the active VAPs. When using the implicit addressing scheme, all of these addresses will fall within a single class C address space, whereas when using the explicit addressing scheme they can be of arbitrary size.

15.1.2 Network Address Translation (NAT)

Network Address Translation (NAT) shields the client access interfaces and client devices connected to the VAPs from the LAN network that the EL-900 is connected to. The EL-900 and its client devices are able to communicate with devices connected to the external network. However, devices on the external network cannot initiate communication with any devices connected to the EL-900.

The advantages of using NAT are:

- You can easily attach an EL-900 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 for the VAP interfaces and their client devices.
- The devices connected to the EL-900 are shielded from the network that the EL-900 is attached to.
- You only consume a single IP address on your existing network when connecting the EL-900 to it.

The main disadvantage of using NAT is

- You are not able to initiate connections to the client devices connected to the EL-900 from devices connected to the LAN or points beyond that..

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 Interface" page (Figure 47).

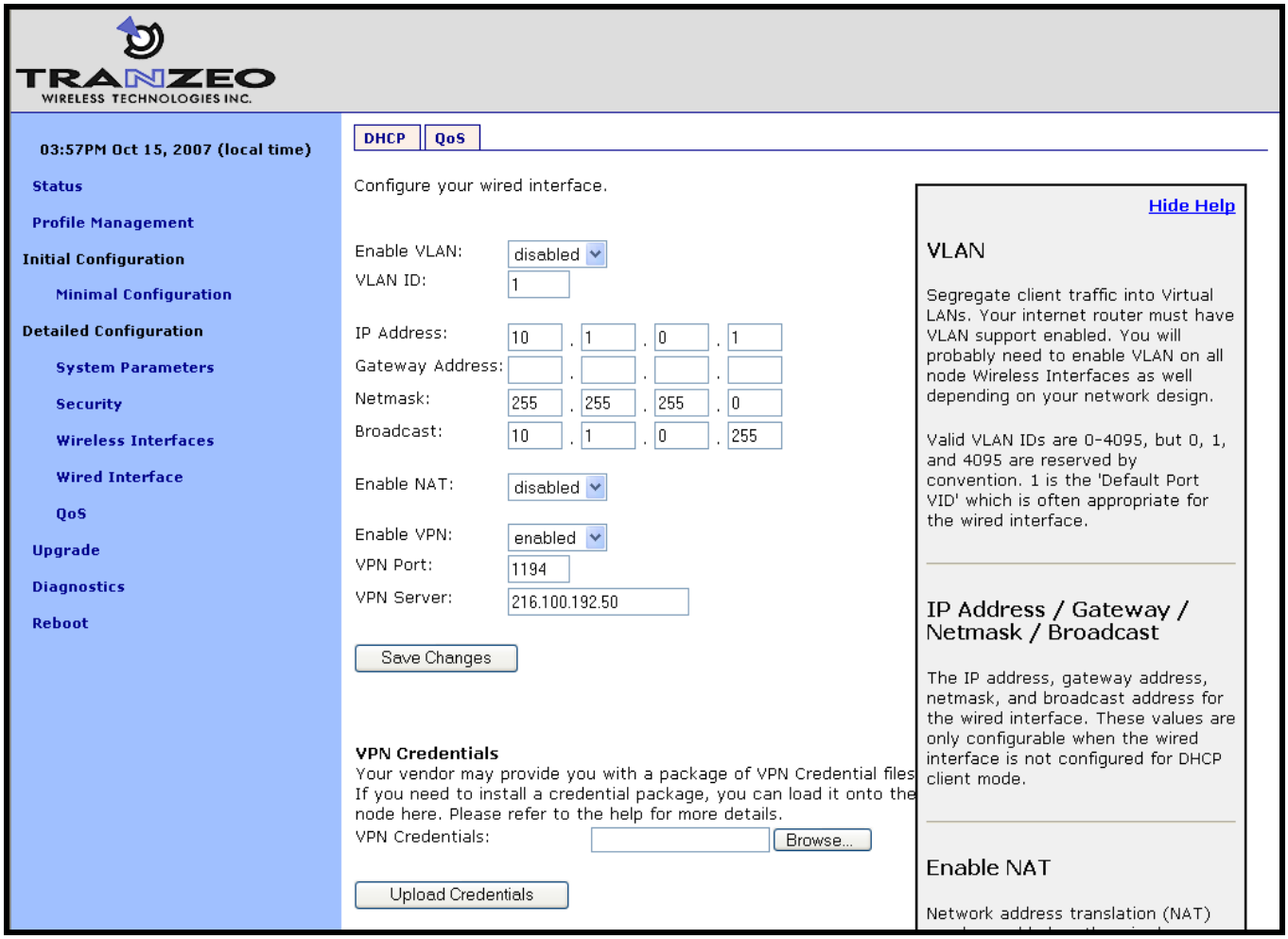

Figure 47. NAT and VPN settings

15.2 Bridge Mode

In bridge mode, the EL-900 can be connected to a LAN with minimal configuration. See section 12.2 for the parameters that are available to control bridging behavior.

16 Controlling Access to the EL-900

The EL-900 supports the following features for restricting access to it, restricting inter-client device communication, and shielding 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.

BRIDGE

The firewalls are disabled and client-to-client blocking is not possible when operating in bridge mode.

16.1 Firewall

The EL-900 has a firewall that blocks certain types of traffic destined for the EL-900. This prevents client devices attached to an EL-900 and devices on the LAN which the EL-900 is attached to from connecting to it.

INFO

The default firewall rules only affect packets destined for the EL-900, and have no effect on packets forwarded by the device. The firewall should typically be enabled on all EL-900s since it prevents undesired access them.

By default, the ports listed in Table 12 are set to be allowed for connection to the EL-900.

Function	Port(s)	Type	Protocol
SSH	22	Source & destination	TCP
DNS	53	Source & destination	UDP
DHCP	67, 68	Destination	UDP
HTTP	80	Destination	TCP
SNMP	161	Source & destination	UDP
HTTPS	443	Destination	TCP
HTTP redirect (if splash pages are enabled)	3060	Destination	TCP
Roaming support	7202 – 7205, 7207	Destination	UDP
OnRamp	20123	Source & destination	UDP

Table 12. Source and destination ports allowed by default

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"
```

Web GUI

It is not possible to configure the state of the firewall and the open firewall ports via the web interface. It is enabled by default.

16.2 Gateway Firewall

The gateway firewall blocks connections originating outside the EL-900 and its client address spaces from entering the device, protecting VAP client devices from unwanted traffic. The gateway firewall will permit return traffic for connections that originate from devices in the VAP client subnets.

If you have enabled NAT (see section 15.1.2), 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
```

Web GUI

It is not possible to configure the state of the gateway firewall via the web interface.

16.3 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 EL-900's client access interfaces, the client devices that attach to that particular interface will not be able to communicate with any client devices attached to that or any other client access interface on the EL-900. Client-to-client traffic can be controlled for interfaces wlan1, wlan2, wlan3, and wlan4.

CLI

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

- 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 client devices, set the parameter to 'yes'. The examples below illustrate how to configure these parameters.

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

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

To allow client-to-client traffic for client devices attached to wlan2:

```
> use firewall
firewall> set node.allowc2c.wlan2=yes
```

Web GUI

The client isolation parameters can be set via the web interface on the "Firewall" tab on the "Security" page (see Figure 48). By setting an interface's client isolation parameter to 'yes', client devices connecting to that interface will not be able to communicate with any other client devices connected to the EL-900.

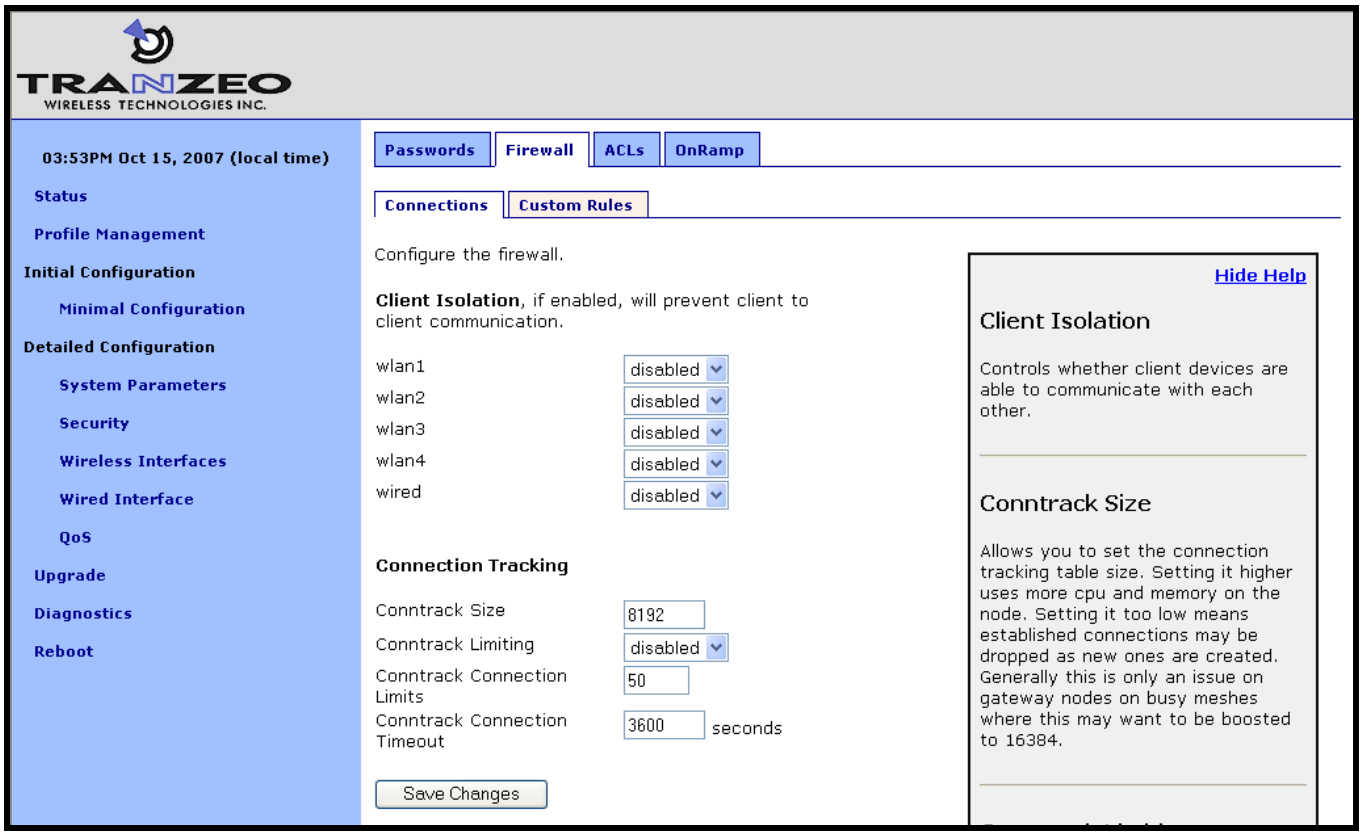

Figure 48. Connection-related firewall settings

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 EL-900 firewall (firewall.node.enable) is enabled (section 16.1).

16.4 Connection Tracking

The firewall keeps track of existing TCP connections. It is advisable to enable connection tracking for public networks that can have large numbers of users. In particular, it is important to enable connection tracking if your network is heavily loaded or if it has users running file

sharing applications. A number of parameters are available for tuning how connection tracking is handled.

16.4.1 Connection Tracking Table Size

The size of the connection tracking table can be set. Allowed values are in the range from 4096 to 16384. A larger connection tracking table allows more connections to be maintained without dropping older connections. Typically, the default size of 8192 is adequate for normal operation and the setting should only be increased on devices with high levels of traffic and many users.

CLI

The connection tracking table size is set by selecting the 'firewall' interface and setting the 'conntrack.table_size' parameter.

```
> use firewall
firewall> set conntrack.table_size=16384
```

Web GUI

The connection tracking table size is set with the "Conntrack Size" field on the "Connections" sub-tab on the "Firewall" tab of the "Security" page (see Figure 48). This field is located under the "Connection Tracking" heading.

16.4.2 Connection Tracking Timeout

The connection tracking timeout parameter allows you to flush connections that have been idle for an extended period of time from the connection tracking table. This will help limit the maximum required size of the connection tracking table. By default, this parameter is set to 3600 seconds (1 hour).

CLI

The connection tracking timeout is set by selecting the 'firewall' interface and setting the 'conntrack.tcp_timeout_established' parameter. The timeout is specified in seconds.

```
> use firewall
firewall> set conntrack.tcp_timeout_established=3600
```

Web GUI

The connection tracking timeout is set with the "Conntrack Connection Timeout" field on the "Connections" sub-tab on the "Firewall" tab of the "Security" page (see Figure 48). This field is located under the "Connection Tracking" heading. Specify the timeout limit in seconds.

16.4.3 Limiting Number of TCP Connections Per Client Device

The number of TCP connections allowed per client device can be limited. For most use cases, setting the connection limit to 30 is sufficient.

INFO

Users running file sharing applications may have difficulties establishing connections when TCP connection limiting is enabled since the file sharing application may be consuming the maximum number of TCP connections allowed.

CLI

The 'conntrack.connlimit.enable' parameter in the 'firewall' interface is used to set the state of TCP connection limiting. The 'conntrack.connlimit.connections' parameter is used to set the maximum number of connections allowed per client device.

```
> use firewall
firewall> set conntrack.connlimit.enable=yes
firewall> set conntrack.connlimit.connections=30
```

Web GUI

The TCP connection limit-related settings are set on the "Connections" sub-tab on the "Firewall" tab of the "Security" page (see Figure 48). The "Conntrack Limiting" drop-down box sets the state of TCP connection limiting and the "Conntrack Connection Limits" sets the maximum number of TCP connections allowed per client device.

16.5 Custom Firewall Rules

Custom firewall rules can be added that control how traffic forwarded by an EL-900 is handled. For example, rules can be added to:

- Block client traffic on certain ports
- Block traffic from a given client access interface to a certain subnet

The custom firewall rules can be added on the "Custom Rules" sub-tab on the "Firewall" tab on the "Security" page as shown in Figure 49. These rules are specified as you would specify

rules for iptables, with the exception of the chain that they are to be added to cannot be specified. All rules will be applied to the iptables forwarding chain.

List one rule per line in the text box on the "Custom Rules" tab and click on the "Save and Apply Changes" button when all rules have been entered. The following examples of custom rules illustrate how to use the custom firewall interface.

Blocking SMTP traffic 25

This rule will block all SMTP traffic, which uses port 25.

```
-dport 25 -j DROP
```

Limiting Access Based on Client Access Interface

Packets can be filtered based upon which interface they were received through. For example, wlan1 and wlan2 can be used to provide users with access to two different, private subnets, while wlan3 users have access to neither of these subnets. Users of all wlans would have access to the Internet though. The following rules will:

- Drop traffic from wlan1 destined for the 192.168.2.0 subnet
- Drop traffic from wlan2 destined for the 192.168.1.0 subnet
- Drop traffic from wlan3 destined for the 192.168.1.0 and 192.168.2.0 subnets

```
-i wlan1 --dst 192.168.2.0/24 -j DROP
-i wlan2 --dst 192.168.1.0/24 -j DROP
-i wlan3 --dst 192.168.1.0/24 -j DROP
-i wlan3 --dst 192.168.2.0/24 -j DROP
```

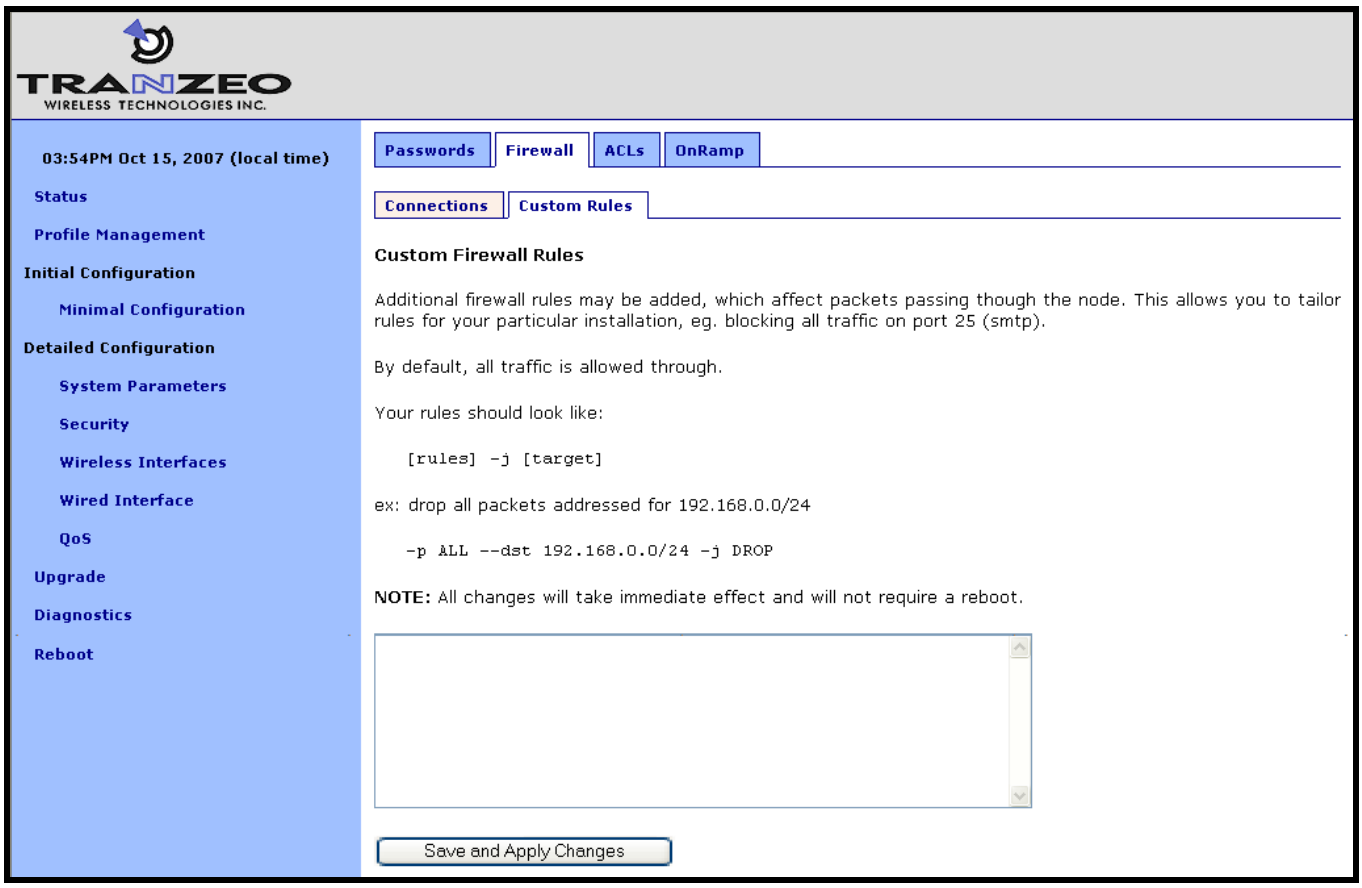

Figure 49. Custom firewall settings

16.6 Access Control Lists (ACLs)

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

Web GUI

The ACLs can be defined via the web interface on the appropriate "wlan*N*" sub-tab under the "ACL" tab on the "Security" page as shown in Figure 50. Enter a MAC address and click on the "Add MAC" button to add the address to the ACL for that VAP. 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 VAP 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.

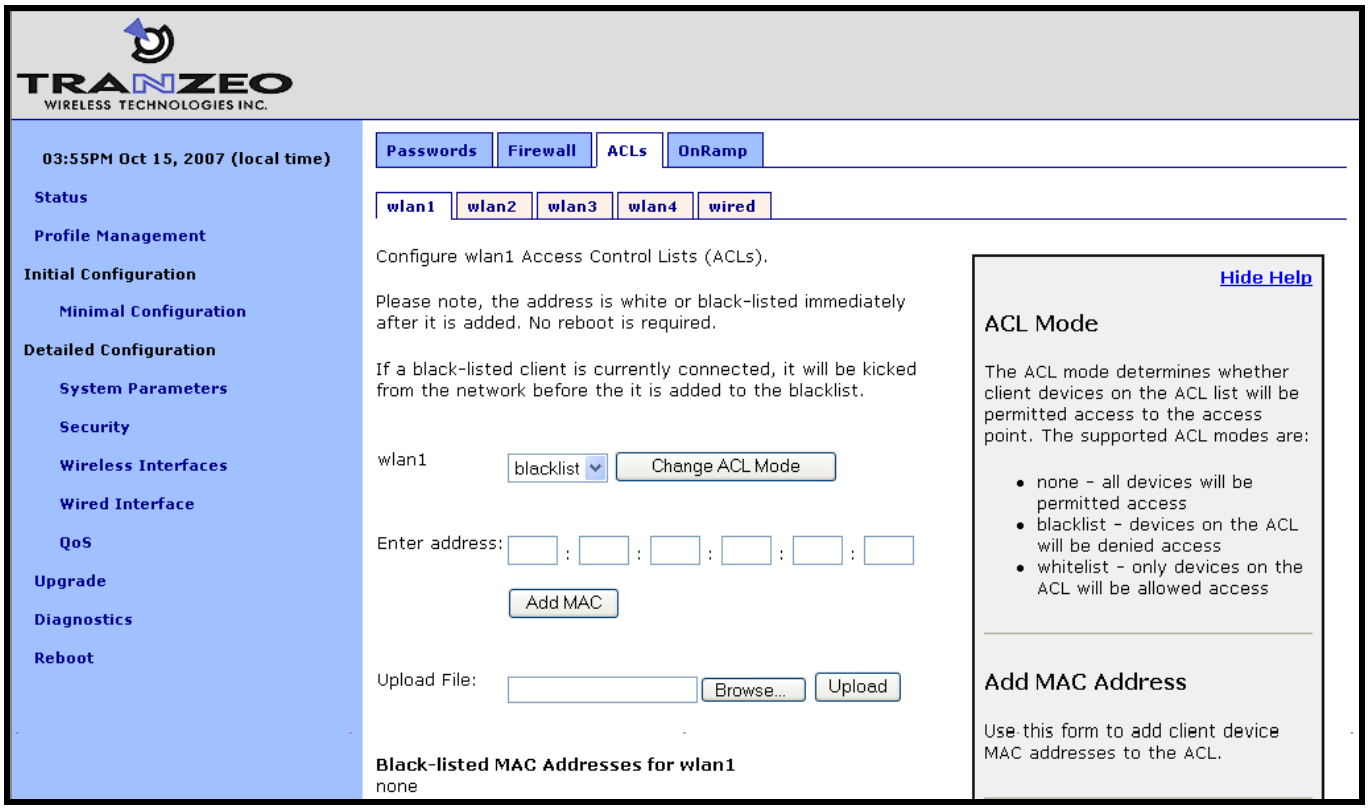

Figure 50. VAP ACL configuration

17 Quality of Service (QoS) Configuration

BRIDGE

QoS rate limiting and reservations are not supported when the EL-900 is operating in bridge mode. Priority level settings are supported in bridge mode.

The EL-900 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 EL-900 QoS scheme allows both rate limiting and rate reservation for all interfaces.

17.1 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 flow priority level parameter is set to 'inherit', the associated interface will assume the default priority level set. The default flow priority is the flow priority 'inherited' by each interface if another flow priority setting is not applied. The default flow priority is configurable.

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 Ethernet interface bandwidth.

INFO

The absolute values of the flow priority settings do not have any weighting effect. If a flow 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 13.

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

Table 13. Hardware priority levels

When sending data out through any of the wireless interfaces (wlan*N*), these hardware priorities map directly to the 802.11e hardware priority output queues on the wireless card. The default level for all traffic is Best Effort.

To increase the hardware priority of all traffic originating 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'.

INFO

Setting an interface's flow priority above that of another interface results in all traffic originating on the higher flow priority interface blocking traffic on the lower priority interface until all traffic from the prioritized interface has been sent. In comparison, elevating the Min Hardware Priority associated with an interface will prioritize, but not fully block traffic tagged with a lower hardware priority. Instead the medium access delay will be reduced (as dictated by the IEEE 802.11e standard) for the traffic with the elevated hardware priority. Thus, these two priority types provide different gradations of quality control, even when applied en mass to an interface, although further refinements can be set using the EnRoute1000 rate limiting features discussed below.

Changing hardware priorities does **not** affect the rate limiting and reservation (section 17.2), it only affects which output hardware queues that provide the required support for the 802.11e standard.

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, wlan1, wlan2, wlan3, wlan4. 'local' refers to traffic originating on the device itself, not from its client devices. 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, 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 51). The hardware priority levels can be set for each interface under the “Advanced QoS” tab on the “QoS” page (see Figure 52).

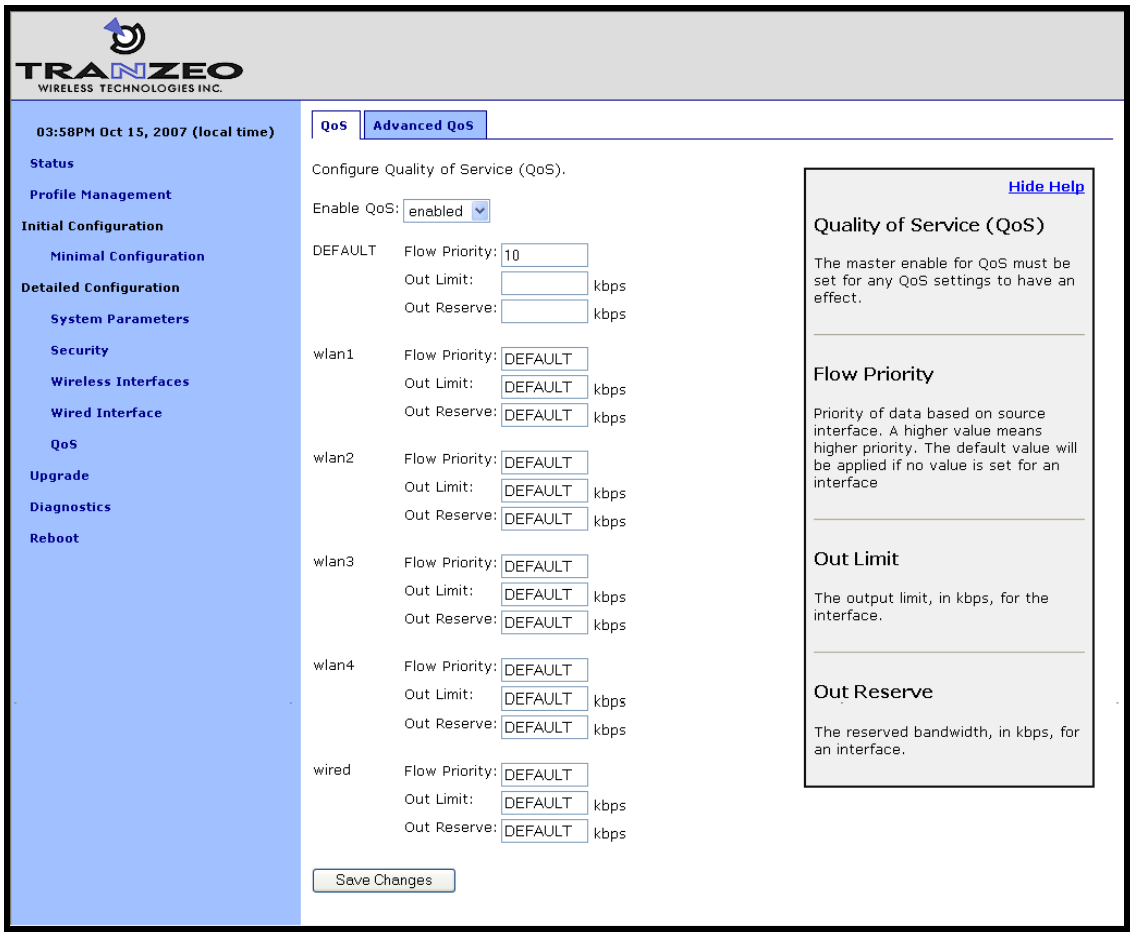

Figure 51. QoS settings

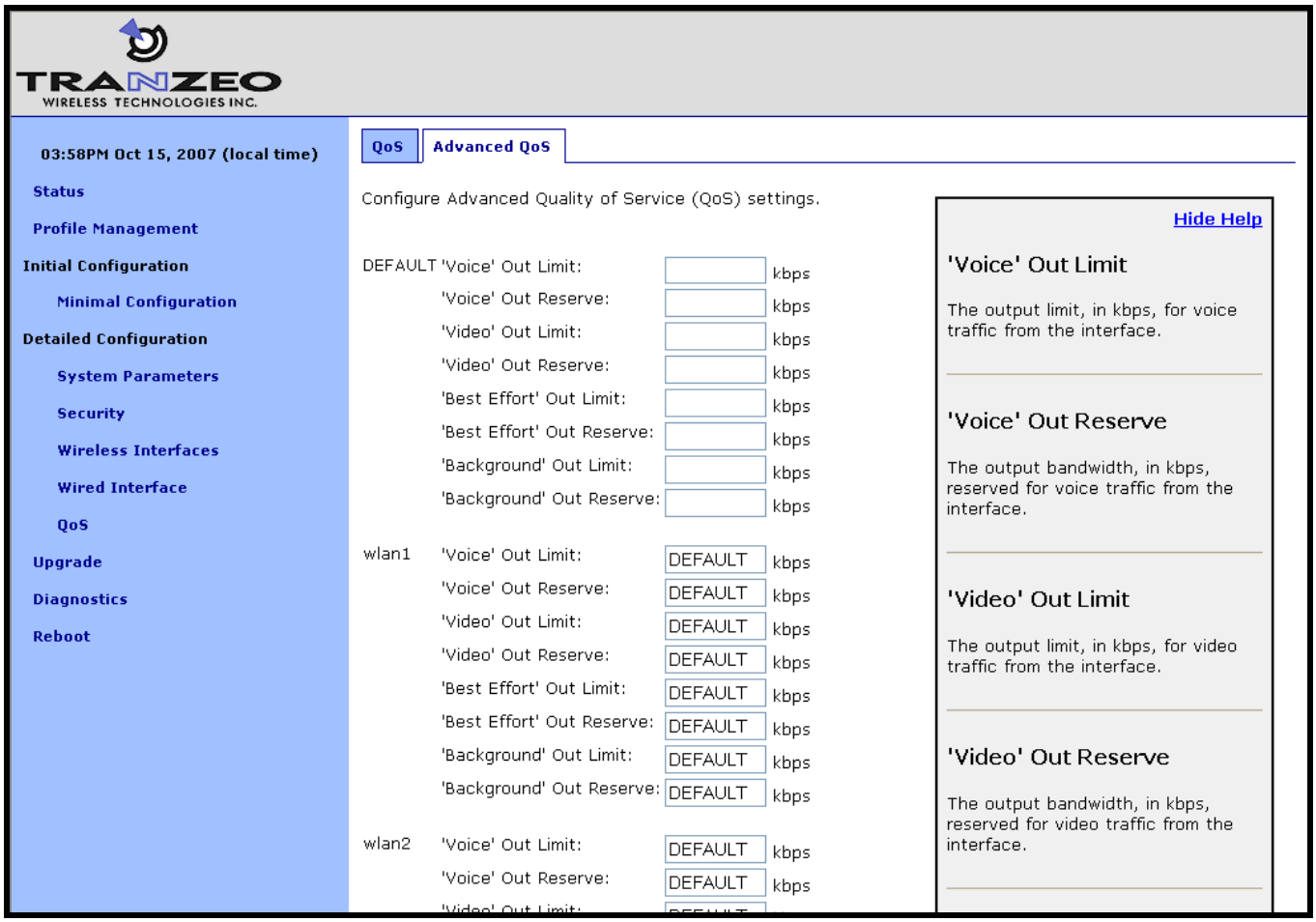

Figure 52. Advanced QoS configuration (only settings for some interfaces are shown)

17.2 Rate Limiting

A rate limit can be set at each QoS Control Point shown in Figure 53. 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 access interface. The default output limit value is applied to interfaces that have the Output Limit parameter set to 'inherit'.

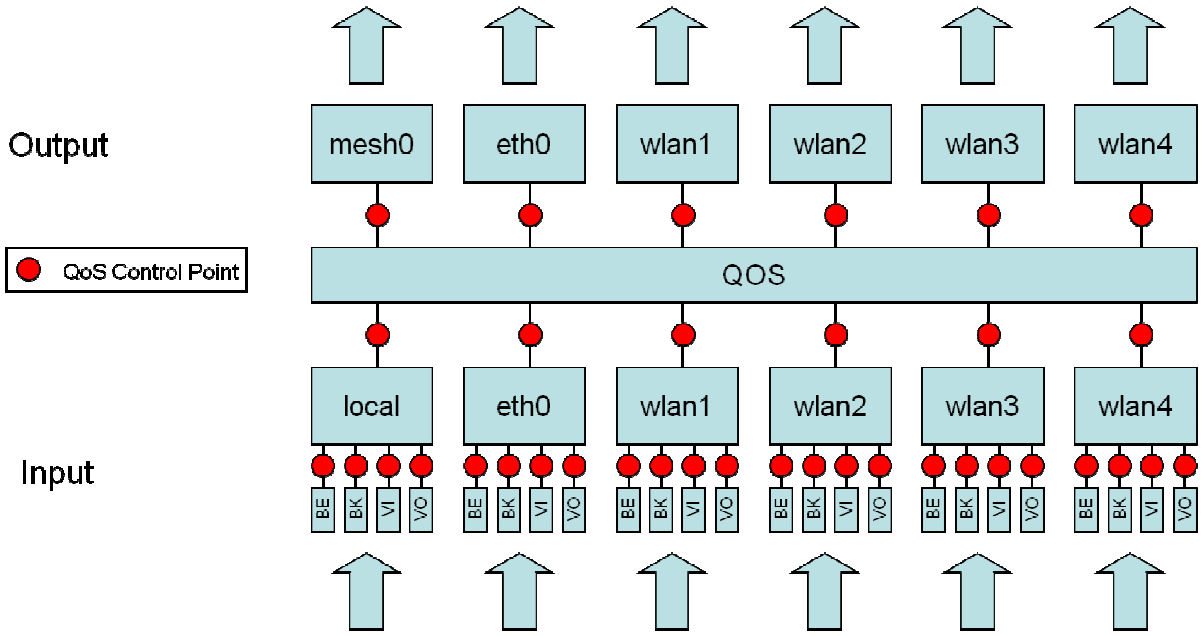

Figure 53. Quality of Service rate limit control points

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 EL-900 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 on the EL-900 only makes sense in the context of the output for another interface(s). In most cases you are concerned with eth0 as the output interface.

CLI

The example below shows how to limit the maximum output rate of the eth0 interface to 8 Mbps and the maximum output rates of all four wlan*N* interfaces to 2 Mbps each.

```
> use qos
qos> set out.eth0.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 EL-900 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,

wlan1, wlan2, wlan3, wlan4; and <input intf> is one of the following: default, eth0, local, 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 eth0 interface to 2 Mbps, 1 Mbps, 512 kbps, and 256 kbps, respectively.

```
> use qos
qos> set out.eth0.wlan1.limit=2048
qos> set out.eth0.wlan2.limit=1024
qos> set out.eth0.wlan3.limit=512
qos> set out.eth0.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, wlan1, wlan2, wlan3, wlan4; <input intf> is one of the following: default, eth0, local, wlan1, wlan2, wlan3, wlan4; <traffic type> is one of the following: 'vo', 'vi', 'be', 'bk' (see Table 13 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 eth0 interface to 256 kbps, 1 Mbps, 256 kbps, and 256 kbps, respectively.

```
> use qos
qos> set out.eth0.wlan1.vo.limit=256
qos> set out.eth0.wlan1.vi.limit=1024
qos> set out.eth0.wlan1.be.limit=256
qos> set out.eth0.wlan1.bk.limit=256
```

Web GUI

The interface- and traffic-based Output Limit parameters can be set via the web interface under the "QoS" and "Advanced QoS" tabs on the "QoS" page (see Figure 51 and Figure 52).

17.3 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 eth0 ('out.eth0.wlan1.vo.reserve'), a limit must be set with 'out.eth0.limit', 'out.eth0.wlan1.limit', or 'out.eth0.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 54. 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.

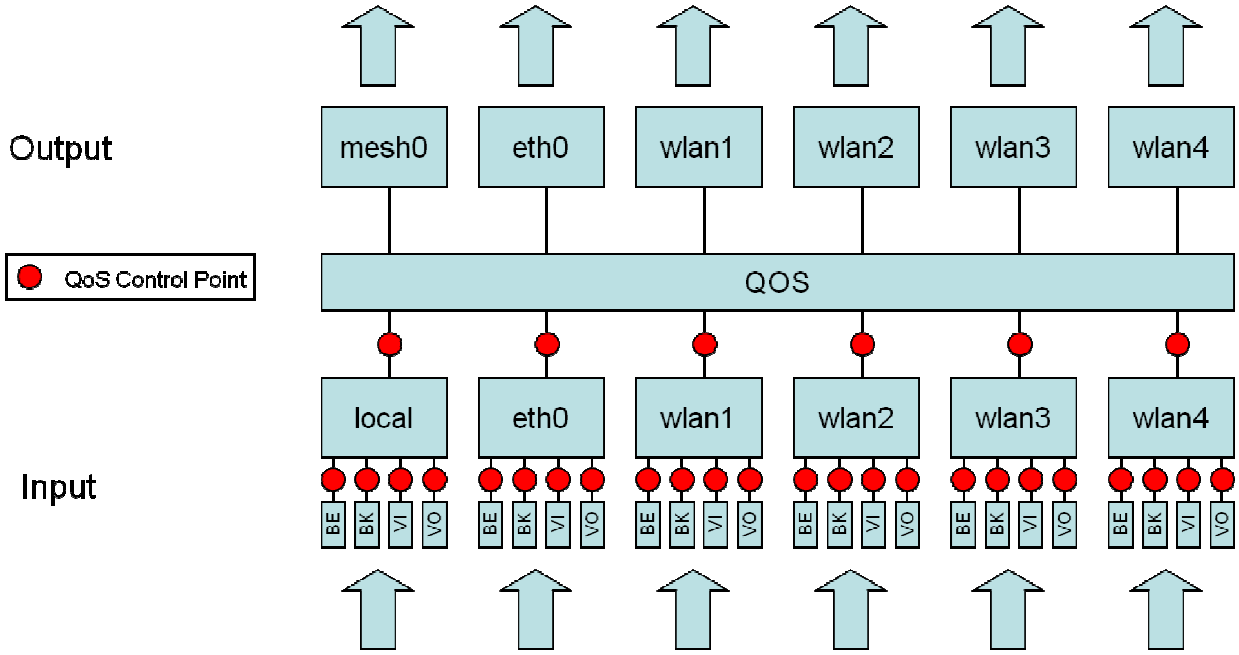

Figure 54. Quality of Service rate reservation control points

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 EL-900 through a particular interface and exits it through another interface. Rate reservations can also be set based on traffic type through an interface. The default value set for the EL-900 rate reservation is 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, wlan1, wlan2, wlan3, wlan4; and <input intf> is one of the following: default, eth0, local, wlan1, wlan2, wlan3, wlan4.

Typically, most rate reservations will involve reserving bandwidth for traffic from a particular client access interface to the eth0 interface. The example below shows how to reserve differing amount of bandwidth on eth0 for traffic originating from the wlan1, wlan2, wlan3, and wlan4 interfaces.

```
> use qos
qos> set out.eth0.wlan1.reserve=2048
qos> set out.eth0.wlan2.limit=1024
qos> set out.eth0.wlan3.limit=512
qos> set out.eth0.wlan4.limit=256
```

A rate reservation for a certain type of traffic that enters the EL-900 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, wlan1, wlan2, wlan3, wlan4; <input intf> is one of the following: default, eth0, local, wlan1, wlan2, wlan3, wlan4; <traffic type> is one of the following: 'vo', 'vi', 'be', 'bk' (see Table 13 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 eth0 interface to 512 kbps, 1 Mbps, 256 kbps, and 128 kbps, respectively.

```
> use qos
qos> set out.eth0.wlan1.vo.reserve=512
qos> set out.eth0.wlan1.vi.reserve=1024
qos> set out.eth0.wlan1.be.reserve=256
qos> set out.eth0.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 51 and Figure 52).

18 Enabling VLAN Tagging

The EL-900 supports VLAN tagging, with each client access interface capable of supporting a different VLAN tag.

18.1 Client Access Interface Configuration

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

VLAN tagging must be enabled on the Ethernet interface for VLAN tags to be included in data frames sent to the LAN. See section 18.2 for more details.

The VLAN ID value for each client access 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 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 "wlan*N*" tabs on the "Wireless Interfaces" page and on the "Wired Interface" page (see Figure 55).

Figure 55. Configuring VLAN for VAP interfaces

18.2 Ethernet Interface Configuration

For VLAN tags to be preserved on traffic that traverses the Ethernet interface, VLAN support must be enabled for the Ethernet interface. The “Enable VLAN” parameter for the wired interface controls the state of VLAN tagging. If VLAN tagging is enabled on the Ethernet interface, all outbound traffic will have its VLAN tags preserved. If VLAN tagging is disabled for the Ethernet interface, all VLAN tags will be stripped from frames received through the Ethernet interface.

When VLAN is enabled for the wired interface, data frames forwarded by the EL-900 to the LAN 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 EL-900'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 Ethernet interface 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 Ethernet interface using the 'vlan.id' parameter in the 'eth0' interface.

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

Web GUI

The Ethernet interface VLAN parameters are set on the "Wired Interface" page as shown in Figure 56.

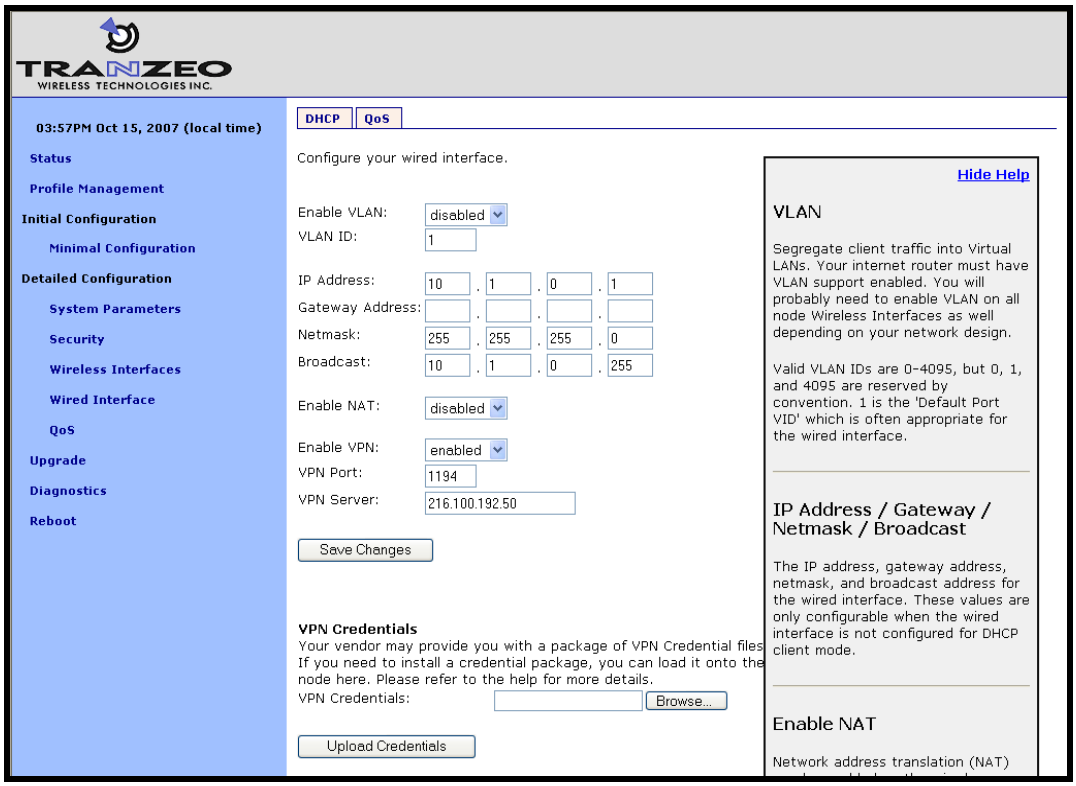

Figure 56. Configuring VLAN for Ethernet interface

19 Integration with Enterprise Equipment

The EL-900 supports authentication, accounting, and monitoring services that easily integrate with enterprise equipment. In this section the following topics are described:

- Splash pages
- Layer 2 client emulation

BRIDGE

Splash pages are not supported and Layer 2 emulation is unnecessary when operating in bridge mode.

19.1 Configuring Splash Pages

The EL-900 supports splash pages, which can be used to restrict access to the 802.11 network and provide information to users that connect to the network. When a user connects through a client access interface to an EL-900 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 they have 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.

19.1.1 Enabling Splash Pages

The enabling of splash pages can be controlled on a per-interface basis. Two splash page modes are supported – one which requires client device users 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.wlan*N*' 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.wlan*N*.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 57). Setting whether client login is required can also be set on this page with the "Require Login" parameter.

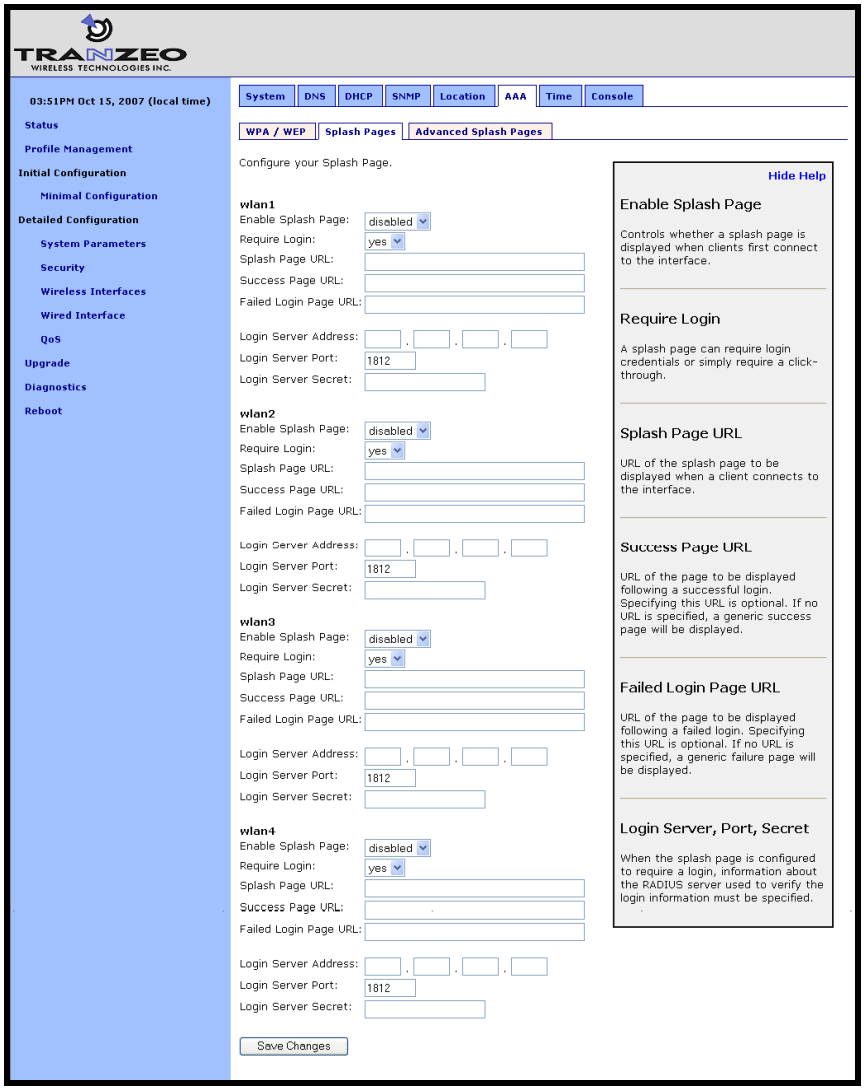

Figure 57. Splash page configuration

19.1.2 Configuring Splash URLs

The URL that a user is redirected to for login purposes can be individually configured for each client access 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 device would be able to access the network through the interface if splash pages are enabled and 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

In the examples that follow, <intf> represents any of the client access interfaces 'wlan1', 'wlan2', 'wlan3', or 'wlan4'. The 'splash.url.<intf>.login' parameters in the 'sys' interface set the login URLs. The 'splash.url.<intf>.success' parameters in the 'sys' interface set the success URLs. The 'splash.url.<intf>.fail' parameters in the 'sys' interface set the fail URLs. The 'splash.url.<intf>.error' parameters in the 'sys' interface 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 57).

19.1.3 Sample HTML Code for Splash Pages

The login HTML page must contain specific form information as shown in the sample code in Figure 58 and Figure 59. Figure 58 contains the code required for an interface that requires a login. Figure 59 contains code for a login page that the user just clicks through to unlock network access.

The critical lines in Figure 58 are 6, 12, 15, and 19. The ‘action’ value in line 6 of Figure 58 must point to a server name for which there is a DNS proxy entry on the EL-900 and the last part of it must be ‘/radius/login.cgi’. The DNS proxy entry, which will be different for each deployed EL-900, must be mapped to one of the EL-900’s IP addresses (see section 9.4 for more information on how to set 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 EL-900. The DNS proxy entry directs the results of the login process to the right location – that is, the EL-900 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 58. Sample HTML code for login web page with password authentication

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 59. The page must still contain a form definition similar to that on line 6 in Figure 59. 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 59.

```
 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 59. Sample HTML code for web page when authentication is disabled

19.1.4 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 57) using the fields for "Login Server Address", "Login Server Port", and "Login Server Secret".

19.1.5 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 an EL-900, 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 60). 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.

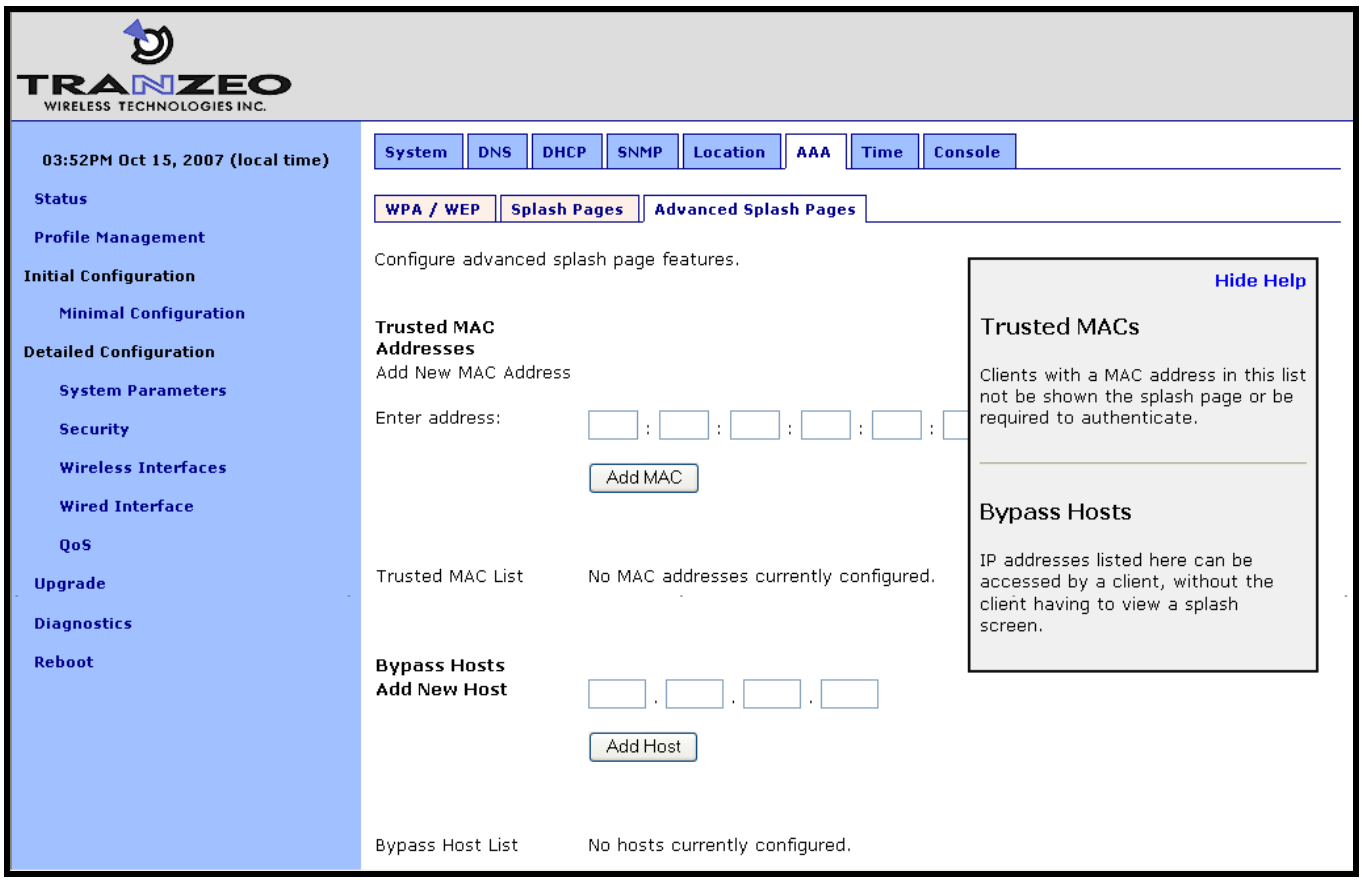

Figure 60. Adding trusted MAC addresses and accessible hosts

19.1.6 Bypass Splash Pages for Access to Specific Hosts

It is possible to specify a list of IP addresses that client devices can access without the client devices 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 60). 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.

19.2 Layer 2 Emulation

Certain back-end systems (e.g. Internet gateways) use the MAC addresses of client devices for authentication and accounting purposes. When the EL-900 is operating in routed mode client device MAC addresses are typically not provided to the back-end servers. A layer 2 emulation mode can be enabled on the EL-900 to provide the client device MAC address information to back-end systems.

When layer 2 emulation is enabled, the EL-900 will send Ethernet (layer 2) frames to the LAN using the MAC address of the device the packet originated from as the source address. The EL-900 will also act as a proxy and forward packets with MAC destination addresses of client devices that are connected to it.

In layer 2 emulation mode, an EL-900 will respond to ARP requests if it has a route to the target IP address contained in the ARP request. The list of subnets that the EL-900 has routes to includes implicit/explicit network addresses. Thus care must be taken that these subnets are not used elsewhere in the network.

Alternatively, to reduce the amount of address space consumed by the EL-900’s subnets, the ARP responses can be limited to certain parts of the EL-900’s address space. The EL-900 can be configured to disregard all ARP requests except for those with IP addresses within the client address space that it has a host or network route for.

CLI

Layer 2 emulation is enabled with the ‘l2.client_mac_fwd’ parameter in the ‘sys’ interface. The example below shows how to enable layer 2 emulation.

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

To limit the range of addresses for ARP requests that the EL-900 will respond to, set the ‘l2.hide_internal.enable’ parameter in the ‘sys’ interface to ‘yes’. Set ‘l2.hide_internal.gateway.deny.all’ in the ‘sys’ interface to ‘yes’ to disregard all ARP requests except for those with addresses within the client address subnet. The example shows how to disregard all ARP requests except for those for addresses within the client address space.

```
> use sys
sys> set l2.hide_internal.enable=yes
sys> set l2.hide_internal.gateway.deny.all=yes
```

Web GUI

The state of layer 2 emulation is set on the “System” tab of the “System” page (see Figure 61). The console interface in the web GUI must be used to configure which address ranges the EL-900 responds to ARP requests for. See the CLI section above for parameter names and set these using the console interface (see section 9.10).

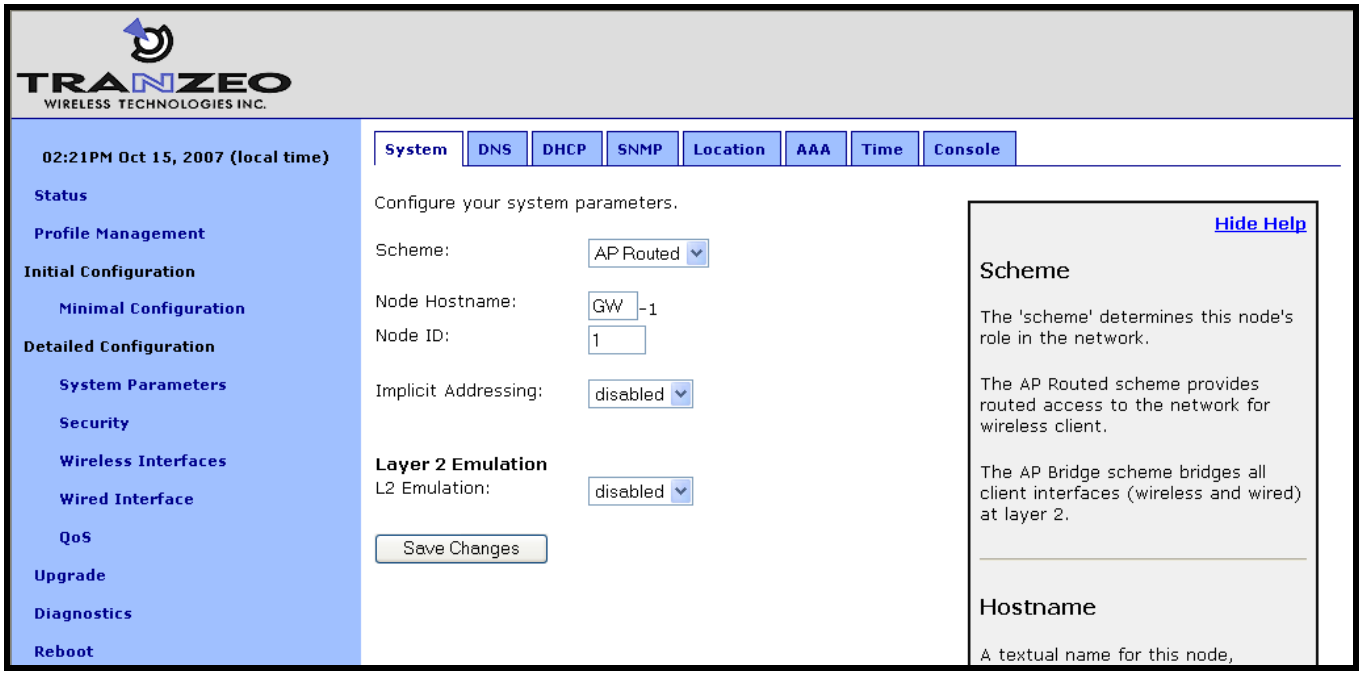

Figure 61. Enabling/disabling layer 2 emulation

20 Diagnostics Tools

The EL-900 has a number of diagnostics tools to help the user diagnose and correct configuration issues. These tools are available on the “Diagnostics” page, accessible from the navigation bar. The individual diagnostics tools are accessible from the row of tabs shown on the “Diagnostics” page.

20.1 Ping

The “Ping” tab on the “Diagnostics” page allows the user to check for network connectivity by pinging a remote device (see Figure 62). Either an IP address, e.g. 10.1.2.3, or a hostname, e.g. www.yahoo.com, can be specified. The number of pings to send can be set to 1, 10, or 100.

Click on “Ping Address” to start pinging the device. The results of the pings will appear on the bottom half of the page shortly after clicking on the button. There may be a delay of a few seconds to display the ping results if the ping destination is not responsive.

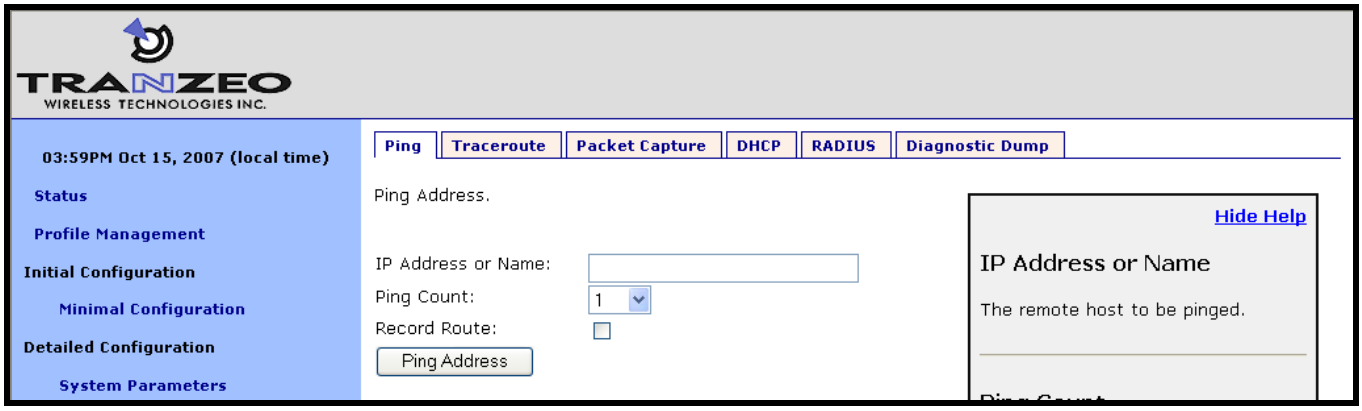

Figure 62. Pinging a remote device

20.2 Traceroute

The “Traceroute” tab on the “Diagnostics” page allows the user to determine the individual intermediary devices used to route traffic from the EL-900 to a remote device (see Figure 63).

Enter the IP address, e.g. 10.1.2.3, or hostname, e.g. www.yahoo.com, of the device you wish to find the route path to. Check the “Resolve Names” box if traceroute should show device names, when available, instead of just IP addresses. Click on the “Trace Route” button to begin tracing the route. The intermediary nodes will be displayed on the bottom half of the page. Click on “Stop Trace” to stop the tracing process.

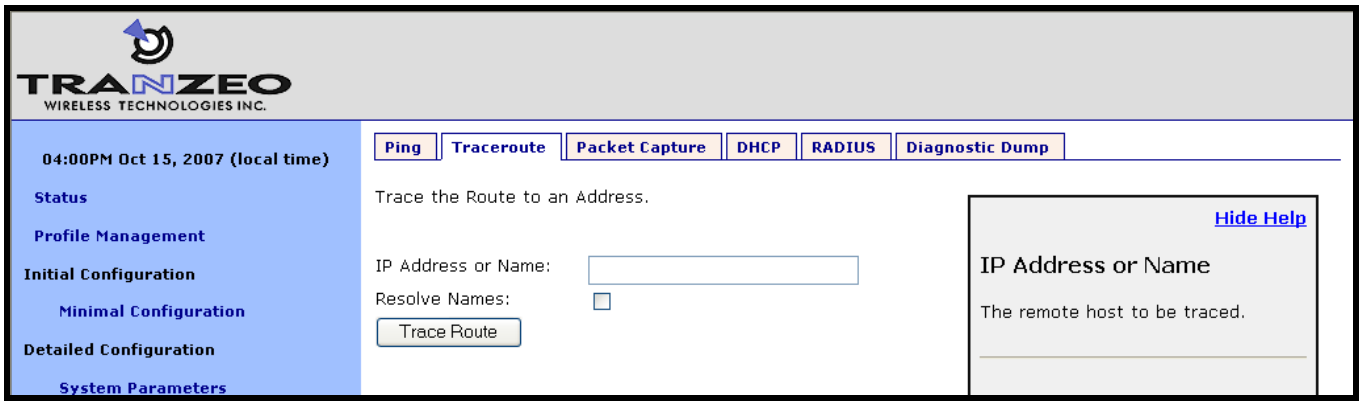

Figure 63. Determining the route from the EL-900 to a remote device using traceroute

20.3 Packet Capture

The "Packet Capture" tab on the "Diagnostics" page allows the user to capture traffic on the EL-900's network interfaces (see Figure 64). The captured data can either be displayed in the web interface or saved to a file that can be downloaded and analyzed using 3rd-party tools, such as Wireshark (http://www.wireshark.org/). At most, 10 captured files can be saved on the EL-900 at any given time.

The full array of options available for packet capture is described in Table 14. A number of examples of common packet capture scenarios are also presented below.

Capturing DHCP Traffic From Clients on wlan1

1. Set "Interface" to "wlan1"
2. Set "Protocol" to "all"
3. Set "Packet Count" to "20"
4. Set "Packet length" to 500
5. Click on "DHCP" next to "Common Protocols"
6. Set "Output" to "File"
7. Click on "Start Capture"
8. Allow the capture to complete automatically when the prescribed number of packets has been captured or click on "Stop Capture" to halt the capture
9. The captured data is accessible by clicking on the link at the bottom of the page under the heading "Available tcpdump files". The file name format used is "<file prefix>_MMDDYYY.HHMM. Click on this link to save it to your computer. The downloaded file can be parsed by packet analyzers such as Wireshark.
10. Click the checkbox next to the filename in the "Available tcpdump list" and click on the "Delete Selected" button. This will delete the file from the EL-900 and free up space for other capture files.

Capturing All Traffic From a Specific Client Device

1. Set “Interface” to the one that the client device is attached to
2. Set “Protocol” to “all”
3. Set “Packet Count” to “500”
4. Set “Packet Length” to 500
5. Set the “Optional Host” to the IP address of the client device of interest
6. Set “Output” to “File”
7. Click on “Start Capture”
8. Allow the capture to complete automatically when the prescribed number of packets has been captured or click on “Stop Capture” to halt the capture
9. The captured data is accessible by clicking on the link at the bottom of the page under the heading “Available tcpdump files”. The file name format used is “<file prefix>_MMDDYYY.HHMM. Click on this link to save it to your computer. The downloaded file can be parsed by packet analyzers such as Wireshark.
10. Click the checkbox next to the filename in the “Available tcpdump list” and click on the “Delete Selected” button. This will delete the file from the EL-900 and free up space for other capture files.

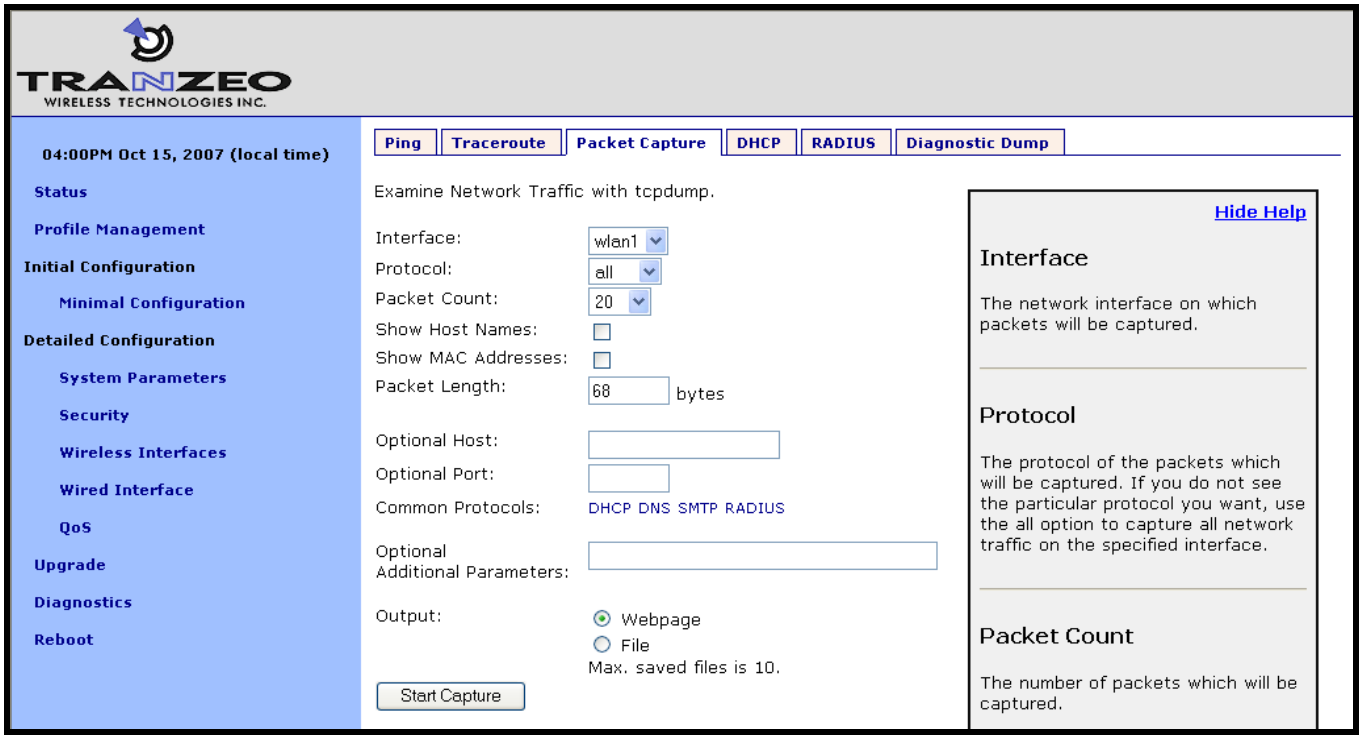

Figure 64. Capturing network traffic

Option	Description
Interface	Selects the interface from which packets are captured. Note that some packets may be available on multiple interfaces. For example, data from a client device connected to wlan1 destined for a device on the Internet will pass through wlan1 and the wired interface.
Protocol	Data can be captured for the following protocols: TCP, UDP, ICMP, and ARP. Set the value to "all" if you do not wish to filter out packets based on protocol type.
Packet Count	Sets the number of packets to capture. The provided settings are 20, 50, 100, and 500.
Show Host Names	Captured data will show resolved host names instead of IP addresses when this option is selected.
Show MAC addresses	In addition to IP address or hostnames, source and destination MAC addresses will be displayed for each packet when this option is selected.
Packet Length	Sets the length of each packet that should be captured. If you are only interested in the header contents of a packet, this value can be lowered to reduce the size of the data capture file. If it is set to too low of a value, critical data may be not be captured though.
Optional Host	Sets a host name or IP address to use for filtering purposes. All packets with this host as their source OR destination address will be captured.
Optional Port	Sets a port to use for filtering purposes. All packets with this port as their source OR destination port will be captured. NOTE: this setting only has an effect on capture of TCP or UDP packets.
Common Protocols	Click on the protocol names listed to add filtering parameters for them in the "Additional Parameters" text box. It is possible to select more than one protocol to filter on.
Optional Additional Parameters	The underlying application used to capture packets is tcpdump. Use this field to specify additional parameters to tcpdump that are not made available through the GUI.
Output	Select whether to display the data on the webpage or to save it to a file, which can be downloaded from the device. The file name format used is "<file prefix>_MMDDYYY.HHMM.
Output File Prefix	Sets an optional file prefix for saved files.

Table 14. Packet capture options

20.4 Centralized DHCP Testing

The "DHCP" tab on the "Diagnostics" page can be used to test access to an external DHCP server when the EL-900 is in centralized DHCP server mode (see Figure 65). Click on the "Test DHCP" button to initiate a test. The results of the test will be displayed at the bottom of the page.

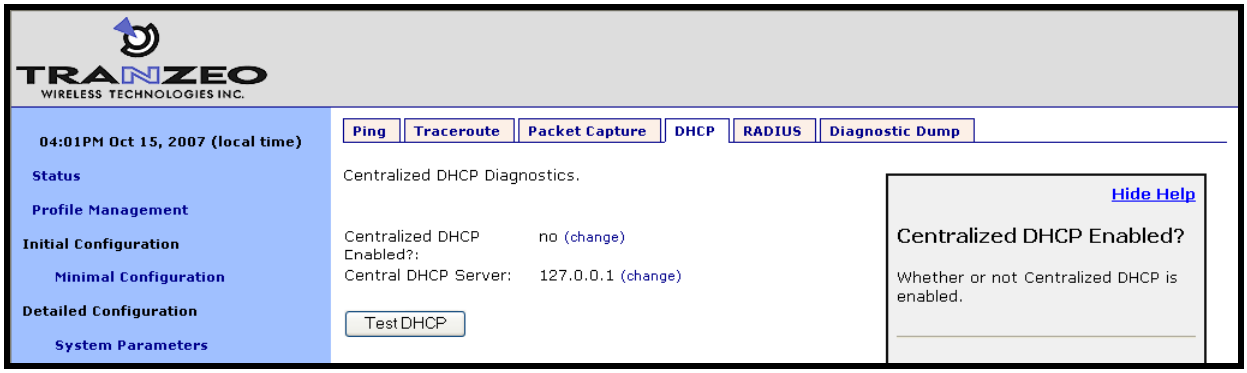

Figure 65. Testing the connection to an external DHCP server

20.5 RADIUS Server Testing

The “RADIUS” tab on the “Diagnostics” page can be used to test authentication of credentials by a RADIUS servers used for splash page or WPA authentication (see Figure 66). Use the procedure below to test the validity of credentials with a RADIUS server.

1. Select the RADIUS server you want to use for the test from the drop-down menu
2. Enter the credentials you want to test in the “Username” and “Password” fields
3. Click on the “Test User” button

The results of the test will be displayed at the bottom of the page. Three outcomes are possible:

- The credentials were authenticated by the server
- Communication was established with the server, but the credentials were not valid
- It was not possible to establish communication with the server

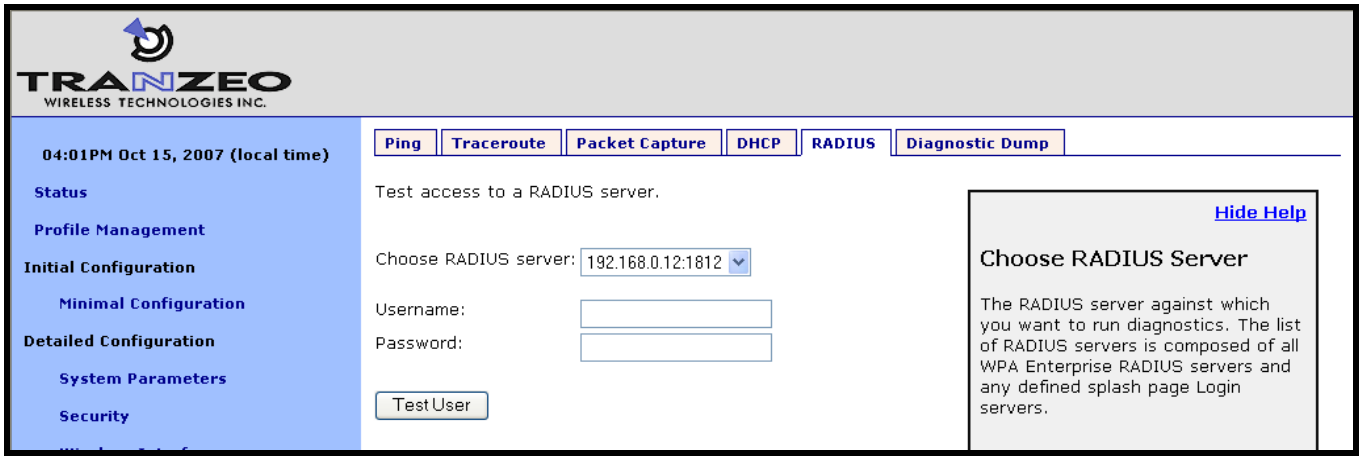

Figure 66. Testing credentials with a RADIUS server

20.6 Diagnostic Dump

The “Diagnostic Dump” tab on the “Diagnostics” page allows the user to create a snapshot of diagnostic data that can be downloaded to a PC and sent to Tranzeo technical support for analysis (see Figure 67).

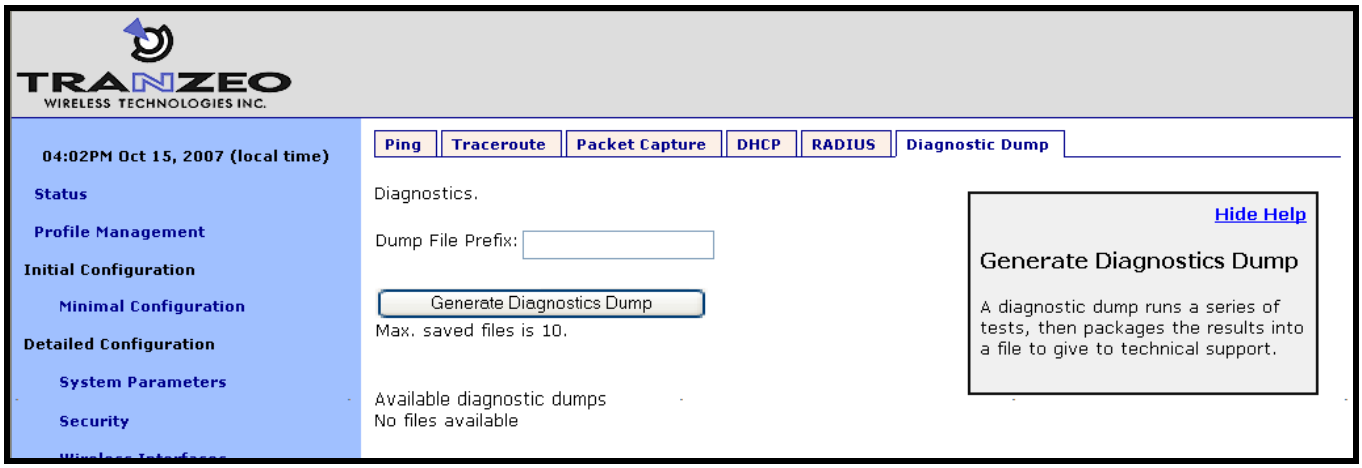

Figure 67. Generating a diagnostic dump

The list of diagnostic dumps available for download is displayed at the bottom of the page. The diagnostic dumps can be downloaded by clicking on the filenames. To delete one or more diagnostic dumps, select the check boxes next to the ones you wish to delete and then click on the “Delete Selected” button.

21 Firmware Management

21.1 Displaying the Firmware Version

The firmware version string contains the following information:

- Build date
- Major version number
- Minor version number
- Build number

These values are embedded in the version string as follows:

enroute1000_< Build date >_< Major version >_< Minor version >_< Build number>

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 = ENROUTE1000_20070911_03_00_0215
```

Web GUI

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

21.2 Upgrading the Firmware

The EL-900 supports secure remote firmware upgrade.

Prior to upgrading firmware, please contact Tranzeo technical support to find out if there are any version-specific instructions for upgrading from the firmware version you are currently using.

The EL-900 must have access to the Internet, and specifically the Tranzeo upgrade server, to complete an upgrade.

If power to the EL-900 is lost during the upgrade process, it is possible that the device will become inoperable.

The firmware can be upgraded using the “Upgrade” page. This page displays the following information:

- Firmware currently installed on the EL-900
- Firmware available on the remote upgrade server
- Firmware available in the non-volatile memory of the EL-900
- Space used/available in non-volatile memory for storing upgrade images

Follow the procedure below to upgrade the firmware on a device:

1. Select the firmware version you want to upgrade to from the “Firmware on Server” box
2. Click on the button with the arrow to the right of the “Firmware on Server” box. This will begin the download process of the firmware from the Tranzeo upgrade server to the non-volatile memory on the EL-900. While the firmware is downloading, it will be shown in blue in the “Firmware on Node” box.
3. When the download has been completed, select the firmware you wish to upgrade to from the “Firmware on Node” box.
4. Click on the “Install” button.
5. Wait for the install to complete. The EL-900 will reboot automatically when the upgrade has been completed.

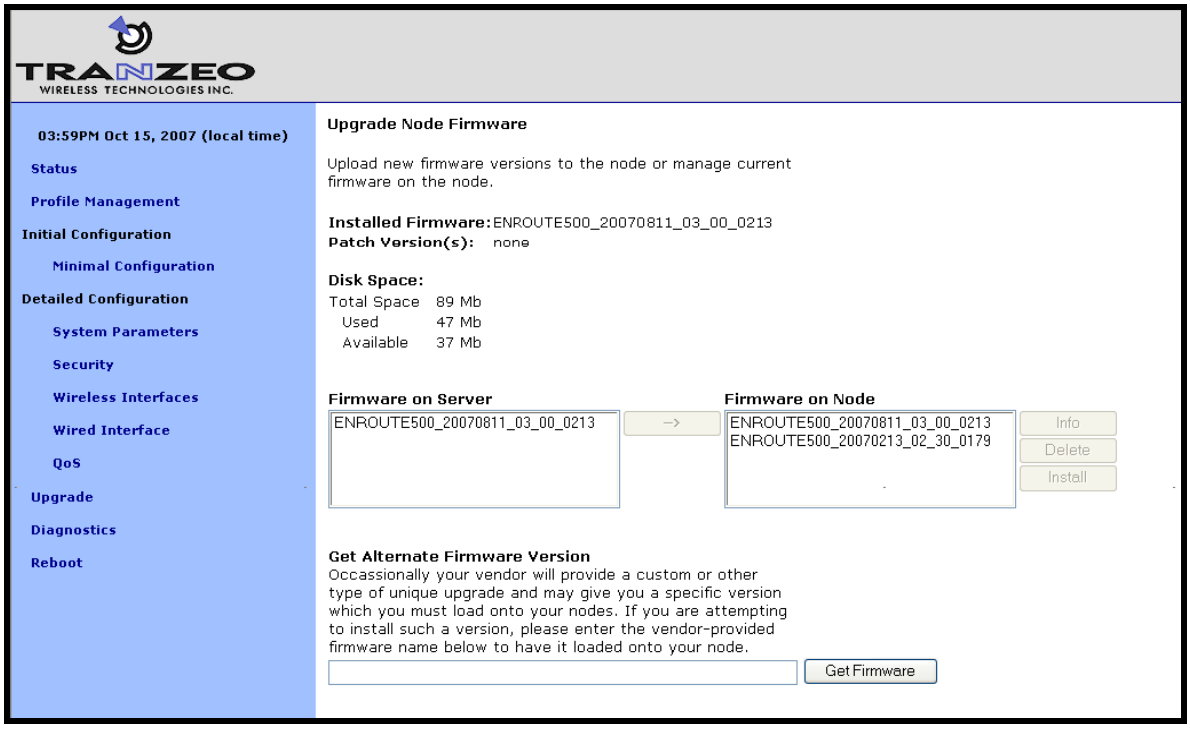

Figure 68. Updating firmware

Glossary

Client access interface	An interface on the EL-900 used by a client device, such as an 802.11-enabled laptop, to connect to the EL-900. The client access interfaces are the virtual APs wlan1 – wlan4.
Client device	A device that is connected to one of the EL-900's client access interfaces, e.g. a laptop
Client address scheme	The method used to assign address spaces to client address interfaces. The two supported client address schemes are implicit and explicit.
Operating mode	The mode that sets the method for how packets forwarding is done by the EL-900. The two supported operating modes are "bridge" and "router", with the former using layer 2-based traffic forwarding mechanisms and the latter using layer 3-based mechanisms.

Abbreviations

ACL	Access Control List
AP	Access Point
CLI	Command line interface
Client access interface	An interface on the EL-900 used by a client device, such as an 802.11-enabled laptop, to connect to the EL-900. The client access interfaces are the virtual APs wlan1 – wlan4.
ESSID	Extended Service Set Identifier
LAN	Local-Area Network
NAT	Network Address Translation
PoE	Power over Ethernet
QoS	Quality of Service
RSSI	Received signal strength indicator
STP	Spanning Tree Protocol
VAP	Virtual Access Point. An access point that uses the same radio as other access points in the system.
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