# TR-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 TR-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 © 2009, 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.

- Install the antenna so that there is a minimum of 30.7 cm (12.1 in) of distance between the antenna and people.
- 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.



The Tranzeo TR-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 TR-900	B
1.1	TR-900 Variants Error! Bookmark not defined	I.
1.2	TR-900 Capabilities	8
1.3	TR-900 Interfaces	8
1.3.1	Ethernet and PoE	9
1.3.2	Antenna10	0
1.4	Deployment Considerations1	1
1.4.1	AP Channel Selection 1	1
2	Connecting to the TR-900	3
2.1	Network Interfaces13	3
2.2	Connecting to an Unconfigured TR-90014	4
2.3	Default Login and Password1	5
2.4	Resetting the 'admin' Password1	5
3	Using the Web Interface	6
3.1	Accessing the Web Interface10	6
3.2	Navigating the Web Interface18	8
3.3	Setting Parameters18	8
3.4	Help Information19	9
3.5	Rebooting19	9
4	Using the Command Line Interface 2 <sup>-</sup>	1
4.1	Accessing the CLI	1
4.2	User Account2	1
4.3	CLI Interfaces22	2
4.4	CLI Features22	2
4.4.1	Control of the Cursor	2
4.4.2	Cancel a Command	2
4.4.3	Searching the Command History	3
4.4.4	Executing a Previous Command	3
4.5	CLI Commands	3
4.5.1	'?' command	3
4.5.2	'whoami' command	3
4.5.3	'help' command	4
4.5.4	'show' command	4
4.5.5	'use' command	5
4.5.6	'set' command	5
4.5.7	'get' command	6
4.5.8	'list' command	7
4.5.9	'ping' command	7

4.5.10	'ifconfig' command	
4.5.11	'route' command	
4.5.12	'clear' command	
4.5.13	'history' command	
4.5.14	'!' command	30
4.5.15	'exit' command	
4.5.16	'quit' command	
5	Initial Configuration of an TR-900	32
6	Status Information	24
61	Configuration Overview Page	<b></b>
6.2	Interface Status	
621	Virtual AD Interfaces	
0.2.1	Wired Interface Statue	
0.2.2	Pridaina	
0.3	Druging	
6.4 C.E	ADD Table	
0.5	ARP Table	
6.6		
6.7	DHCP Event Log	
7	Configuration Profile Management	41
71	Saving the Current Configuration	<u>4</u> 1
72	Load a Configuration Profile	42
73	Delete a Configuration Profile	42 42
7.0	Downloading a Configuration Profile from an TR-900	ב+ 12
7.4	Liploading a Configuration Profile to an TB-900	
7.0		
8	Mode of Operation	45
٩	System Settings	47
<b>3</b> Q 1	Licer Password	
9.1	Nodo ID	/4747 10
9.2	DNS / Domain Sattinga	40
9.3	DNS / Domain Sellings	
9.4	NotPLOS Server	
9.0		
9.6	SINIP	
9.7	Location.	
9.8	Certificate Information	
9.9		
9.10		
9.11	OnKamp Configuration Access	
9.12	CLI Timeout	58
10	Client Addressing Schemes	50
10.1	Implicit Addressing Scheme	03 03
10.1 1	I AN Prefix	
10.1.1		

10.1.2 10.2	Client Address Space Segmentation in Implicit Addressing Mode	61 64
<b>11</b> 11.1 11.2	Ethernet Interface Configuration DHCP Manual IP Configuration	<b>66</b> 66 69
<b>12</b> 12.1 12.2	Bridge Interface Configuration IP Configuration Bridging Parameters	<b>71</b> 71 73
<b>13</b> 13.1 13.2 13.3 13.4 13.5 13.6 13.6.1 13.6.2 13.7 13.8 13.8.1 13.8.2 13.8.3 13.9 13.10 13.11 13.12 13.13	Virtual Access Point (VAP) Configuration	<b>74</b> 75 75 75 77 77 78 78 78 78 78 78 78 79 80 81 
14 14.1 14.2 14.2.1 14.2.2 14.2.3 15 15.1 15.1.1 15.1.2 15.2	Client DHCP Configuration Using Local DHCP Servers Using a Centralized DHCP Server Support for Clients with Static IP Addresses Configuring the TR-900s Configuring the Central DHCP Server Configuring the Central DHCP Server Connecting an TR-900 to a LAN Routed mode Manual Configuration Network Address Translation (NAT) Bridge Mode	<b>88</b> 
<b>16</b> 16.1 16.2	<b>Controlling Access to the TR-900</b> Firewall Gateway Firewall	<b></b>

16.3	Blocking Client-to-Client Traffic	
16.4	Connection Tracking	
16.4.1	Connection Tracking Table Size	
16.4.2	Connection Tracking Timeout	
10.4.3	Custom Eirowell Dules	
16.5	Access Control Lists (ACLs)	104
10.0	Access Control Lists (ACLS)	
17	Quality of Service (QoS) Configuration	108
17.1	Priority Levels	108
17.2	Rate Limiting	111
17.3	Rate Reservation	113
18	Enabling VLAN Tagging	
18.1	Client Access Interface Configuration	
18.2	Ethernet Interface Configuration	
	e e e e e e e e e e e e e e e e e e e	
19	Integration with Enterprise Equipment	
19.1	Configuring Splash Pages	
19.1.1	Enabling Splash Pages	
19.1.2	Configuring Splash URLs	
19.1.3	Sample HTML Code for Splash Pages	
19.1.4	Configuring the Authentication Server	
19.1.5	I rusted MAC Addresses	
19.1.6	Bypass Splash Pages for Access to Specific Hosts	
19.2	Layer 2 Emulation	126
20	Diagnostics Tools	128
20.1	Ping	128
20.2	Traceroute	128
20.3	Packet Capture	129
20.4	Centralized DHCP Testing	131
20.5	RADIUS Server Testing	132
20.6	Diagnostic Dump	132
21	Firmware Management	
21.1	Displaying the Firmware Version	134
21.2	Upgrading the Firmware	134
Glossarv		
Abbreviatio	ons	137

## 1 Working with the TR-900

Thank you for choosing the Tranzeo TR-900 802.11 Access Point. The TR-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 TR-900.

INFO

Throughout the manual, "TR-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.

## 1.1 TR-900 Capabilities

Based on the IEEE 802.11b/g and 802.11a standards and complete with FCC certification, the TR-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
- Security
  - o WPA
  - $\circ$  WPA2
  - o WEP 64/128
- Web GUI
- Tranzeo CLI (SSH)
- Remote upgrade
- Configuration management

## 1.2 TR-900 Interfaces

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







Ethernet

Figure 1. TR-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. TR-900 Interfaces

### 1.2.1 Ethernet and PoE

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



The TR-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 TR-900, connect an Ethernet cable from the Ethernet port of the TR-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 TR-900 TO THE PORT LABELED "CPE" ON THE POE INJECTOR. NETWORK EQUIPMENT THAT DOES NOT SUPPORT POE CAN BE PERMANENTLY DAMAGED BY Α 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.

#### 1.2.2 Antenna

The TR-900 AP radio port is an N-type RF connector that can interface with a wide range of Tranzeo antennas. After purchasing the desired 900MHz antenna (for the TR-900HG or TR-900HA models respectively), attach the antenna to the access point (AP) radio port on the TR-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 TR-900 is used.

The following is a list of supported accessory antennas sold with the TR-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

## **1.3 Deployment Considerations**

The TR-900's radio operates in either the 900MHz ISM band, depending on the model. It is possible that there will be other devices operating in these bands that will interfere with the TR-900's radio. Interference from adjacent TR-900s can also degrade performance if the TR-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 TR-900 uses. To detect the presence of other 802.11 devices, a tool such as Netstumbler (<u>http://www.netstumbler.com/downloads/</u>) can be used. A spectrum analyzer can be used for further characterization of interference in the band.

#### 1.3.1 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 TR-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 TR-900

The TR-900 can be configured and monitored by connecting to one of its network interfaces. The wired Ethernet interface on the TR-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 TR-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 TR-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. TR-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 TR-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 TR-900.



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

To connect to an TR-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 TR-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 TR-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 TR-900s, you should not simultaneously connect multiple TR-900s to a common LAN and attempt to access them using the Static Configuration IP address.

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



to clear the entire cache, or

arp -d 169.254.253.253

to just clear the TR-900 entry

Linux

arp -d 169.254.253.253

## 2.3 Default Login and Password

The TR-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 TR-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 TR-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 TR-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 TR-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 TR-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.

02:11PM Oct 15, 2007 (local time)	Config Overview	Status	Routing	ARP	Event Log	DHCP Events		
Status	CM-1 Config	uuratio						
Profile Management	GW-1 Conng	Juratio						
Tritical Constitution	Syste	em Info	rmation					
	Serial Number: 869							
Minimal Configuration	Firmware version:	Firmware version: ENROUTE500_20070911_03_00_0215						
Detailed Configuration	Uptime:	0 da	ays, 3 minu	tes				
System Parameters	Mode:	AP F	Routed					
Security	Country Code:	840	(United St	ates)				
Window Tabada and	Access	Point 1	(wlan1	)				
wireless filteriates	Enabled:	yes			(change)			
Wired Interface	ESSID: Channel:	er10	00_ap1		(change) (change)			
QoS	DHCP:	serv	/er		(change)			
Upgrade	Encryption:	non	e		(change)			
Diagnostics	VLAN:	disa	bled		(change)			
	Netmask:	255	.255.255.0		(change)			
Reboot	MAC Address:	00::	15:6D:50:1	1:F1				
	4.00000	Doint	. (	、				
	Enabled:	ves	( wianz	)	(change)			
	ESSID:	, er10	)00_ap2		(change)			
	Channel:	1 (2	.412 GHz)		(change)			
	DHCP:	serv	rer		(change)			
	Encryption:	die o	A-PSK blod		(change)			
	ID Address	10 1	1 2 1		(change)			
	Netmask:	255	.255.255.0		(change)			
	MAC Address:	06:3	15:6D:50:1	1:F1	(			
	Access	Doint S	(wlan?	<u>،</u>				
	Enabled:	Ves	( wiano	,	(change)			
	ESSID:	er10	100 an3		(change)			
	Channel:	1 (2	.412 GHz)		(change)			
	DHCP:	serv	/er		(change)			
	Encryption:	WP/	A Enterprise	э	(change)			
	VLAN:	disa	bled		(change)			
	IP Address:	10.1	1.3.1		(change)			
	Netmask: 255.255.0 (change)							
	MAC AUDIESS:	UA:	13:00:50:1	1:11				
	Access	Point 4	l (wlan4	)				
	Enabled:	yes			(change)			
	ESSID:	er10	)00_ap4		(change)			
	Channel:	1 (2	.412 GHz)		(change)	-		-

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.

03:27PM Oct 15, 2007 (local time)	System DNS DHC	P SNMP Location	AAA Time Con	sole 2
Status	DNS DNS Proxy			
Profile Management	Configure your DNC Bra	J 3		
Initial Configuration	Configure your DNS Pro	xy.		Hide Help
Minimal Configuration	DNS Proxy:	enabled 🖌		DNS Provy
Detailed Configuration	2			DINS FLOXY
System Parameters	Add DNS Proxy Entry			Enabling the DNS Proxy resolves names to local IP addresses. Used in
. Security .	Hostna <b>me</b>			conjunction with splash pages.
Wireless Interfaces	IP Address:		].	
Wired Interface	Seve Changes			Add New Host
QoS	Save Changes			Both the bestrome and ID address
Upgrade				are required. The IP address should
Diagnostics	DNS Proxy Hosts:	Hostname	Proxied IP Address	be one of the enabled wlan interfaces.
Reboot		apsignin.company.com	1.2.3.4	

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 TR-900.

### **3.3 Setting Parameters**

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

	Configuration has been updated. Reboot required for changes to take effect.				
04:03PM Oct 15, 2007 (local time)	System         DNS         DHCP         SNMP         Location         AAA         Time         Console				
Status	DNS DNS Proxy				
Profile Management					
Initial Configuration	Show Help				
Minimal Configuration	DNS Proxy: enabled 💌				
Detailed Configuration					
System Parameters	Add DNS Proxy Entry				
Security	Hostname				
Wireless Interfaces	IP Address:				
Wired Interface	Sevie Changes				
QoS	Save Changes				
Upgrade					
Diagnostics	DNS Proxy Hosts: No hosts currently configured.				
Reboot					

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 TR-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.

VIRELESS TECHNOLOGIES INC.						
04:02PM Oct 15, 2007 (local time)	Reboot	Hide Help				
Status Profile Management	Click the button below to restart the node. A restart will take about 3 and a half minutes, so please be patient.	Reboot				
Initial Configuration Minimal Configuration	Reboot Now	begin the reboot process.				
System Parameters						
Security Wireless Interfaces						
Wired Interface QoS						
Upgrade						
Diagnostics Reboot						



## **4** Using the Command Line Interface

All configurable TR-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 TR-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 TR-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 3<sup>rd</sup>-party client such as SecureCRT from Van Dyke software (<u>http://www.vandyke.com/products/securecrt</u>) or the free PuTTY SSH client (<u>http://www.putty.nl/</u>) to connect to an TR-900 using SSH.

When you log in to the TR-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 TR-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 TR-900
- eth0 controls for the Ethernet interface
- br0 controls for bridge mode
- firewall controls firewall settings
- gos 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 TR-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 CtrI+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 TR-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 TR-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) : interface is enabled enable 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 (avoid 0 and 1 normally) 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 vlan.id

#### 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 if config 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 TR-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 '!' com	nand
Syntax	<pre>!<command history="" number=""/> !<string command="" matches="" of="" previously-executed="" start="" that=""> !!</string></pre>
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
	<pre>1: use wlan1 2: get essid 3: set essid=new_ap_essid1 4: use wlan2 5: set essid=new_ap_essid2</pre>
	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 TR-900

This user's guide provides a comprehensive overview of all of the TR-900's features and configurable parameters. However, it is possible to deploy a network of TR-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 TR-900s for deployment.

1	<b>Change the 'admin' password.</b> The default password should be changed to prevent unauthorized access to the TR-900.	See section 9.1
2	<b>Set the node ID</b> 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 TR-900.

10:53AM Oct 16, 2007 (local time)	Basic/Initial Configuration						
Status	1. Change the 'admin' password.						
Profile Management	The default passwords should be changed to prevent unauthorized access to the nodes. A password must be						
Initial Configuration	a string of four to 32 characters.						
Minimal Configuration	Please note: changing the 'admin' password will force you to relog onto the webpages to continue						
Detailed Configuration							
System Parameters	Admin Password:						
Security	Verify Admin Password:						
L2 Bridge							
Wireless Interfaces	2. Set the DNS servers.						
Wired Interface	Specify DNS server(s) to allow hostnames to be resolved. You may specify one or two DNS servers by their IP						
Upgrade							
Diagnostics	Primary DNS Server : 10 . 3 . 108 . 254						
Reboot	Secondary DNS Server :						
	3. Set the node ID.         The node ID is a unique identifier incorporated into the addresses served by this node's DHCP server, to distinguish this node from other nearby nodes. The ID must be a number between 1 and 254.         Node ID:       1         Save Changes						

Figure 9. Initial configuration web page

## 6 Status Information

Multiple web interface pages that display status information about the TR-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.

<b>)</b>										
02:11PM Oct 15, 2007 (local time)	Config Overview	Status	Routing	ARP	Event Log	DHCP Events				
Status	GW-1 Configuration									
Profile Management										
Initial Configuration	Syste Serial Number:	em Info 869	rmation							
Minimal Configuration	Firmware version:	ENR	OUTE500_2	007091	1_03_00_021	15				
Detailed Configuration	Patch version(s): Uptime:	0 da	ays, 3 minu	tes						
System Parameters	Mode:	de: AP Routed								
Security	Country Code:	840	(United St	ates)						
	Access	Point 1	l (wlan1	)						
Wireless Interfaces	Enabled:	ves (change)								
Wired Interface	ESSID:	er10	000_ap1		(change)					
0-0	Channel:	1 (2	.412 GHz)		(change)					
QOS	DHCP:	serv	/er		(change)					
Upgrade	Encryption:	non	e		(change)					
Disesseties	VLAN:	disa	bled		(change)					
Diagnostics	IP Address:	10.3	0.1.1		(change)					
Reboot	Netmask: MAC Address:	255	.255.255.0 15:60:50:1	1:E1	(change)					
	Access Point 2 (wlan2)									
	Enabled:	yes			(change)					
	ESSID:	er10	000_ap2		(change)					
	Channel: 1 (2.412 GHz) (change)									
	DHCP:	serv	/er		(change)					
			0.0017		2 A A					

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

<b>b</b>								
	•							
10:33AM Oct 16, 2007 (local	Config Overview S	tatus Routi	ng ARP	Event Log	DHCP Events			
Status	wlan1 wlan2 wl	an3 wlan4	wired					
Profile Management	GW-1 wlan4 S	tatus						
Initial Configuration								
Minimal Configuration	Interface Statistics Noise Level	-96 dBm						
Detailed Configuration	Data Transfered	<u>Byte Totals</u>	Data R	ates	<u>Packet Totals</u>	Pac	ket Rates	
System Parameters	Transmitted	21.2 /0	( <u>last 10</u> 1 40 KBV	<u>secs)</u> tos/soc	120 packets	( <u>las</u>	<u>t IU secs)</u> pockats/sec	
Security	Received	29.1 KB	1.45 KBy 1.45 KBy	tes/sec tes/sec	120 packets 124 packets	5.59 p	backets/sec	
Wireless Interfaces								
Wired Interface	Clients MAC Address	IP Address	RX data	TX data	dBm (RSSI)	Rate	Last reception	Client Capabilities
QoS	00:1b:77:52:e9:86	10.1.4.254	30 KBytes	2 KBytes	-75 (20)	54M	< 1s	Normal WME
Upgrade								
Diagnostics								
Reboot								

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.

10:31AM Oct 16, 2007 (local time)	Config Overview 9	Status Routing	g ARP Event Log	DHCP Events							
Status	wlan1 wlan2 w	lan3 wlan4	wired								
Profile Management											
Initial Configuration	GW-1 Wired I	nterface S	tatus								
Minimal Configuration	Interface Statistics	Interface Statistics									
Detailed Configuration	Noise Level	n/a									
System Parameters	Data Transfered	<u>Byte Totals</u>	<u>Data Rates</u> (last 10 secs)	<u>Packet Totals</u>	<u>Packet Rates</u> (last 10 secs)						
Security	Transmitted	3.0 MB	214.50 Bytes/sec	33,811 packets	1.26 packets/sec						
Wireless Interfaces	Received	1.5 MB	98.82 Bytes/sec	14,393 packets	0.63 packets/sec						
Wired Interface											
QoS											
Upgrade											
Diagnostics											
Reboot											

Figure 12. Wired interface status information

## 6.3 Bridging

The "Bridging" tab is only present when the TR-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.
10:52AH Oct 16, 2007 (local time)         Status         Profile Management         Initial Configuration         Minimal Configuration         Detailed Configuration         System Parameters         Security         L2 Bridge         Wireless Interfaces         Wireless Interfaces         Wired 00:09:5b:cf:14:c2         Wired 00:09:5b:cf:14:c2         Wired 00:09:5b:cf:14:c6         Wired 00:01:3:46:86:bf:eb <th></th>	
10:52AM Dct 16, 2007 (local time)       Config Overview       Status       Bridging       Routing       ARP       Event Log       DHCP Events         Status       Bridging Status       Bridged InterfaceS       Bridge ID       STP Enabled       Interfaces         Initial Configuration       br0       8000.00156d5011f1       no       eth0         Detailed Configuration       br0       8000.00156d5011f1       no       eth0         System Parameters       security       Known Devices       uiref face       Nana         Wireless Interface       Interface       Mac Address       Local?       Aging Timer         wired       00:09:5b:cf:14:c2       no       76.02       wired       00:01:3:46:86:bf:eb       no       48.54         Wired       00:13:46:86:bf:eb       no       48.54       wied       006	
Status       Bridging Status         Profile Management       Bridged Interfaces         Initial Configuration       Bridge Name       Bridge ID       STP Enabled       Interfaces         Minimal Configuration       br0       8000.00156d5011f1       no       eth0       wlan1         Detailed Configuration       System Parameters       Minimal Configuration       No       eth0       wlan2         Security       Interface       Mac Address       Local?       Aging Timer         Wireless Interfaces       wired       00:09:55:cf:14:c2       no       76.02         wired 100:09:55:cf:14:c2       no       76.02       No       76.02         Wireless Interface       Mac Address       Local?       Aging Timer         wired       00:09:55:cf:14:c2       no       76.02       No         Wireless Interface       Mac Address       Local?       Aging Timer         wired       00:09:55:cf:14:c2       no       76.02       No         Wired 00:09:55:cf:14:c2       no       76.02       No       90.05       No         Wired       00:09:55:cf:14:c2       no       48.54       00.05       00.05         Wired       00:15:6d:50:111:f1       yes       0.005	
Profile Management       Bridged Interfaces         Initial Configuration       Bridge Name       Bridge ID       STP Enabled       Interfaces         br0       8000.00156d5011f1       no       eth0       wlan1         br0       8000.00156d5011f1       no       eth0       wlan2         br0       wlan2       wlan3       wlan4       wlan4         Security       Ethor Devices       Enterfaces       wlan4       wlan4         Wireless Interfaces       Mac Address       Local?       Aging Timer         wired       00:09:Sb:cf:14:c2       no       76.02         wired       00:13:46:86:bf:eb       no       48.54         wired       00:13:46:86:bf:eb       no       48.54         wlan1       00:15:6d:50:11:f1       yes       0.00	
Initial Configuration     Bridge Name     Bridge ID     STP Enabled     Interfaces       Minimal Configuration     br0     8000.00156d5011f1     no     eth0       Detailed Configuration     wlan1     wlan2       System Parameters     wlan4       Security     Interfaces       Wireless Interfaces     Mired 00:09:5b:cf:14:c2     no       Wired Interface     wired       Wired Interface     wired       Wired Interface     wired       Wired Interface     wired       Wired Interface       Wired 00:13:46:86:bf:eb     no       48.54       Wian1       00:15:66:50:11:f1     yes       00:15:66:50:11:f1     yes	
Minimal Configuration       br0       8000.00156d5011f1       no       eth0         Detailed Configuration       wlan1       wlan2         System Parameters       wlan3         Security       wlan4         L2 Bridge       Known Devices         Wireless Interfaces       wired         Wired Interface       Mac Address       Local?         Wired Interface       wired         Wired       00:013:46:86:bf:eb       no         Yearde       wired       00:13:46:86:bf:eb         Wired       00:13:46:86:bf:eb       no         Wired       00:15:6d:50:11:f1       yes         Wired       00:15:6d:50:11:f1       yes	
Minimal Configuration       wlan1         Detailed Configuration       wlan2         System Parameters       wlan3         Security       wlan4         L2 Bridge       Known Devices         Wireless Interfaces       wired         Wired Interface       Wired         Upgrade       wired         Wired       00:01:31:46:86:bf;eb         No       48.54         Wian1       Wired         District Distriction       per distribution	
Detailed Configuration     Wian2 wlan3       System Parameters     wlan4       Security     Wian2       L2 Bridge     Known Devices       Wireless Interfaces     Miced       Wired Interface     Mac Address       Upgrade     wired       O0:013:46:86:bf:eb     no     48.54       Wind     O0:13:46:86:bf:eb     no     48.54       Wind     O0:15:66:50:11:f1     yes     0.00	
System Parameters       Wind         Security       Wian4         L2 Bridge       Known Devices         Wireless Interfaces       Mired       00:09:5b:cf:14:c2       no       76.02         Wired Interface       Wired       00:00:29:e6:7a:6a       no       228.92         Upgrade       Wired       00:13:46:86:bf:eb       no       48.54         Wind       00:15:66:50:11:f1       yes       0.00	
Security     Known Devices       L2 Bridge     Known Devices       Wireless Interfaces     Interface     Mac Address     Local?     Aging Timer       Wired Interface     wired     00:09:5b:cf:14:c2     no     76.02       Upgrade     wired     00:13:46:86:bf:eb     no     48.54       Wind     00:15:66:50:11:f1     yes     0.00	
L2 Bridge       Known Devices         Wireless Interfaces       Interface       Mac Address       Local?       Aging Timer         wired Interface       wired       00:09:5b:cf:14:c2       no       76.02         wired 00:00:29:e6:7a:6a       no       228.92         wired       00:13:46:86:bf:eb       no       48.54         wlan1       00:15:6d:50:11:f1       yes       0.00	
Wireless Interfaces     Micrown Devices       Wired Interface     Mac Address     Local?     Aging Timer       Wired Interface     wired     00:09:5b:cf:14:c2     no     76.02       Upgrade     wired     00:01:29:e6:7a:6a     no     228.92       Wired     00:13:46:86:bf:eb     no     48.54       Wah1     00:15:66:50:11:f1     yes     0.00	
Wireless Interfaces         wired         00:09:Sb:cf:14:c2         no         76.02           Wired Interface         wired         00:00:29:e6:7a:6a         no         228.92           Upgrade         wired         00:13:46:86:bf:eb         no         48.54           Wan1         00:15:66:50:11:f1         yes         0.00	-
Wired Interface         wired         00:0c:29:e6:7a:6a         no         228.92           Upgrade         wired         00:13:46:86:bf:eb         no         48.54           wlan1         00:15:66:50:11:f1         yes         0.00	
Upgrade         wired         00:13:46:86:bf:eb         no         48.54           wlan1         00:15:66:50:11:f1         yes         0.00	
Upgrade         wlan1         00:15:6d:50:11:f1         yes         0.00           upgrade         upgrade         upgrade         0.015:6d:50:11:f1         yes         0.00	
uired 00:10:0b;cb;04:44 no 0.05	
Diagnostics Wired 00:18:80:00:24:44 no 0.20	
wired 00:19:b9:32:df:21 no 52.50	
Reboot wired 00:26:54:0e:de:e4 no 12.14	
wired 00:80:77:7d:fd:00 no 100.87	
wired 00:d0:12:02:41:61 yes 0.00	
wlan2 06:15:6d:50:11:f1 yes 0.00	
wlan3 0a:15:6d:50:11:f1 yes 0.00	
wlan4 0e:15:6d:50:11:f1 yes 0.00	
Spanning Tree Protocol Details	
Spanning Tree Protocol is disabled.	

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.

02:14PM Oct 15, 2007 (local time)	Config Overvie	w Status	Routing	ARP	Event Log	DHCP	Events		
Status	Routing Table								
Profile Management	Destination	Gateway	Netma	ask	Flags	Metric	Ref	Use	Interface
Initial Configuration	10.3.108.0	0.0.0.0	255.25	5.255.0	U	0	0	0	eth0
Minimal Configuration	10.1.4.0 10.1.1.0	0.0.0.0 0.0.0.0	255.25 255.25	5.255.0 5.255.0	U U	0 0	0 0	0 0	wlan4 wlan1
Detailed Configuration	10.1.2.0 10.1.3.0	0.0.0.0 0.0.0.0	255.25 255.25	5.255.0 5.255.0	U U	0 0	0. 0.	0 0	wlan2 wlan3
System Parameters	169.254.0.0	0.0.0.0	255.25	5.0.0	U	0	0	0	eth0
Security	0.0.0.0	10.3.108.254	F 0.0.0.0	D	UG	0	0	0	ethO
Wireless Interfaces									
Wired Interface									
QoS									
Upgrade									
Diagnostics									
Reboot									

### 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.

<b>b</b>							
02:15PM Oct 15, 2007 (local time)	Config Overview	w Status	Routing	ARP	Eve	ent Log	DHCP Events
Status	ARP Table						
Profile Management	IP Address	MAC Ad	dress	Interf	ace	Flags	
Initial Configuration	10.3.108.199	00:18:8B:C	CB:24:44	eth0		c	
Minimal Configuration	10.3.108.254 10.3.108.253	00:13:46:8 00:09:5B:0	36:BF:EB CF:14:C2	ethO ethO		с с	
Detailed Configuration			-				
System Parameters							
Security							
Wireless Interfaces							
Wired Interface							
QoS							
Upgrade							
Diagnostics							
Reboot							

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.

	C.
02:15PM Oct 15, 2007	Config Overview         Status         Routing         ARP         Event Log         DHCP Events
(local time)	Event Lee (all times in UTC)
Status	Even Log (all times in otc)
Profile Management	Oct 15 21:07:16 GW-1 dhclient: bound to 10.3.108.170 renewal in 33587 seconds. Oct 15 21:07:07 GW-1 dhclient: DHCPACK from 10.3.108.254 Oct 15 21:07:07 GW-1 dhclient: DHCPREQUEST on eth0 to 255.255.255.255 port 67
Initial Configuration	Oct 15 21:07:07 GW-1 dhclient: DHCPOFFER from 10.3.108.254 Oct 15 21:07:07 GW-1 dhclient: DHCPOFFER on etb0 to 255 255 255 255 port 67 interval 16
	Oct 15 21:07:07 GW-1 dhclient: Sending on Socket/fallback
Minimal Configuration	Oct 15 21:07:07 GW-1 dhclient: Sending on LPF/eth/700:d0:12:02:41:61
Detailed Configuration	Oct 15 21:07:07 GW-1 dhclient: wifi0: unknown hardware address type 801 Oct 15 21:07:06 GW-1 dhclient: wifi0: unknown hardware address type 801
Contract Devenue to an	Oct 15 21:07:06 GW-1 dhclient:
System Parameters	Oct 15 21:07:06 GW-1 dhclient: For into, please visit http://WWW.isc.org/products/DBCP Oct 15 21:07:06 GW-1 dhclient: All rights reserved.
Security	Oct 15 21:07:06 GW-1 dhclient: Copyright 2004 Internet Systems Consortium.
Wireless Interfaces	Oct 15 21:06:57 GW-1 root(2972): ROOT LOGIN ON tts/0
Willess Interfaces	Oct 15 21:06:57 GW-1 login(pam_unix)[2972]: session opened for user root by LOGIN(uid=0) Oct 15 21:06:53 GW-1 login(2972): FAITED LOGIN 1 FEOM (null) FOF root Authentication failure
Wired Interface	Oct 15 21:06:51 GW-1 login(pam_unix)[2972]: authentication failure; logname-LOGIN uit=0 euid=0 tty=t
005	Oct 15 21:06:41 GW-1 hostapd: wlan3: RADIUS Unable to connect to authentication server at 99.99.99.99 Oct 15 21:06:41 GW-1 hostapd: wlan3: RADIUS Authentication server 99.99.99.99.1812
	Oct 15 21:06:41 GW-1 hostapd: wlan2: RADIUS Only WPA-PSK specified - won't try to connect to authent:
Upgrade	Oct 15 21:00:41 GW-1 hostapa: Wianz: KADIUS Authentication server 152.168.0.12:1812 Oct 15 21:06:21 GW-1 logger: (Re)generating https certs
Diagnostics	Oct 15 21:06:21 GW-1 logger: /sbin/iwconfig wlan4 txpower 16 dBm
Debest	Oct 15 21:06:21 GW-1 logger: /sbin/wconfig wlan2 txpower 16 dBm
Rebubl	Oct 15 21:06:21 GW-1 logger: /sbin/iwconfig wlan1 txpower 16 dBm
	Oct 15 21:05:32 GW-1 enroute: succeeded
	Oct 15 21:05:09 GW-1 modprobe: creating wifi device wlan4
	Oct 15 21:04:58 GW-1 modprobe: creating will device wian2

Figure 16. Event log



The time reported in the Event Log corresponds to the time maintained by the TR-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.

2	
WIRELESS TECHNOLOGIES IN	C.
	Config Overview Status Routing ARP Event Log DHCP Events
10:34AM Oct 16, 2007 (local time)	
Status	DHCP Event Log (all times in UTC)
	Oct 16 17:33:15 GW-1 dhopd: DHCPACK to 10.1.4,254
Profile Management	Oct 16 17:33:15 GW-1 dhepd: DHCFINFORN from 10.1.4.254 Via Wian4 Oct 16 17:33:15 GW-1 dhepd: DHCPACK to 10.1.4.254
Initial Configuration	Oct 16 17:33:15 CW 1 dhepd: DHCPINFORM from 10.1.4.254 via wlan4 Oct 16 17:33:08 GW-1 dhepd: DHCPACK on 10.1.4.254 to 00:1b:77:52:e9:86 (lfn-mini) via wlan4
	Oct 16 17:33:08 GW-1 dhcpd: DHCPREQUEST for 10.1.4.254 (10.1.4.1) from 00:1b:77:52:e9:86 (lfn-mini) +
Minimal Configuration	Oct 16 17:33:08 GW-1 dhcpd: DhCPREQUEST for 10.1.4.254 (0.00.10.77.52.87.08 (11h-mini) via wian4 Oct 16 17:33:08 GW-1 dhcpd: DHCPREQUEST for 10.1.4.254 (10.1.4.1) from 00:1b:77:52:e9:86 (1fn-mini)
Detailed Configuration	Oct 16 17:33:08 GW-1 dhcpd: Wrote 1 leases to leases file. Oct 16 17:33:08 GW-1 dhcpd: DHCPOFFER on 10.1.4.254 to 00:1b:77:52:e9:86 (lfn-mini) via wlan4
System Darameters	Oct 16 17:33:07 GW-1 dhepd: DHCPDISCOVER from 00:1b:77:52:e9:86 via wlan4 Oct 16 17:33:06 GW-1 dhepd: DHCPNAK on 10 3 108 186 to 00:1b:77:52:e9:86 via wlan4
system r di diffeters	Oct 16 17:33:06 GW-1 dhopd: DHCPREQUEST for 10.3.108.186 from 00:1b:77:52:e9:86 via wlan4: wrong net
<ul> <li>Security</li> </ul>	Oct 16 17:33:06 GW-1 dhcpd: DHCPNAK on 10.3.108.166 to 00:1D:77:52:e9:86 via wian4 Oct 16 17:33:06 GW-1 dhcpd: DHCPREQUEST for 10.3.108.186 from 00:1D:77:52:e9:86 via wian4: wrong net
Wireless Interfaces	Oct 15 22:48:12 GW-1 dhepd: Wrote 0 leases to leases file. Oct 15 22:48:12 GW-1 dhepd: For info, please visit http://www.isc.org/sw/dhep/
Wired Interface	Oct 15 22:48:12 GW-1 dhopd: All rights reserved.
	Oct 15 22:46:12 GW-1 ancpa: Copyright 2004 Internet Systems Consortium. Oct 15 22:48:12 GW-1 dhcpd: Internet Systems Consortium DHCP Server V3.0.2
QoS	Oct 15 22:32:14 GW-1 dhopd: Wrote 0 leases to leases file. Oct 15 22:32:14 GW-1 dhopd: For info, please visit http://www.isc.org/sw/dhop/
Upgrade	Oct 15 22:32:14 GW-1 dhopd: All rights reserved. Oct 15 22:32:14 GW-1 dhopd: Conunight 2004 Internet Sustems Consortium
Diagnostics	Oct 15 22:32:14 GW-1 dhepd: Internet Systems Consortium DHCP Server V3.0.2
Debest	
Kebuot	
5	×

Figure 17. DHCP event log



The time reported in the DHCP Log corresponds to the time maintained by the TR-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 TR-900's configuration state and can be created to simplify the provisioning and management of devices. The TR-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 TR-900 to the device
- Downloading a configuration profile stored on the TR-900 to a computer
- Uploading a configuration profile from a computer to the TR-900
- Deleting a configuration profile stored on the TR-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 TR-900 and will appear in the "Existing profiles" text box. Use the "Download from Node" tab to download it to a different device.

WIRELESS TECHNOLOGIES INC.							
02:58PM Oct 15, 2007 (local time)	Save         Load         Delete         Download from Node         Upload to Node						
Status	Save Profile						
Profile Management							
Initial Configuration	This page allows you to save a copy of the current configuration locally on the node. Once saved, you can download a copy of the profile to your local computer via the Download Profile page.						
Minimal Configuration	Enter a new profile name or choose an existing profile to be overwritten.						
Detailed Configuration							
System Parameters	Profile Name:						
Security							
Wireless Interfaces	Choose an Existing Profile: ENROUTE500_20070811_03_00_0213 Y						
Wired Interface	Save Profile						
QoS							
Upgrade							
Diagnostics							
Reboot							



## 7.2 Load a Configuration Profile

A configuration stored on the TR-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 TR-900. Choose a profile name from the "Existing Profiles" box and then click on "Load Profile". It is necessary to reboot the TR-900 for the loaded profile settings to take effect.

INFO	A number TBD.	of def	fault	configuration	profiles	are	available	on	the	TR-900.	They	are
-												



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".

03:00PM Oct 15, 2007 (local time)	Save Load Delete Download from Node Upload to Node						
Status	Delete Profile						
Profile Management	Blasse shoese a profile from the list below to delate						
Initial Configuration							
Minimal Configuration	NOTE: once deleted, this profile cannot be recovered from the node! If you think you may want to use the profile again, please save a copy to your local computer via the Download Profile page.						
Detailed Configuration							
System Parameters							
Security	Choose Profile: ENROUTE500_20070811_03_00_0213 M						
Wireless Interfaces	Delete Profile						
Wired Interface							
QoS							
Upgrade							
Diagnostics							
Reboot							

Figure 20. Deleting a configuration profile

## 7.4 Downloading a Configuration Profile from an TR-900

A configuration profile can be download from an TR-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 TR-900

# 7.5 Uploading a Configuration Profile to an TR-900

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

ີງ TRANZEO								
WIRELESS TECHNOLOGIES INC.								
02:19PM Oct 15, 2007 (local time)	Save         Load         Delete         Download from Node         Upload to Node							
Status	Upload Profile							
Profile Management								
Initial Configuration	Please choose a profile on your computer to upload to the node.							
Minimal Configuration	Note: if the profile with the same name already exists on the node, it will be overwritten.							
Detailed Configuration	Browse							
System Parameters								
Security	Upload Profile							
Wireless Interfaces								
Wired Interface								
QoS								
Upgrade								
Diagnostics								
Reboot								

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

# 8 Mode of Operation

The TR-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 TR-900 acting as a router. In bridge mode, all communication across the TR-900 is managed at the MAC (layer 2) level, with the TR-900 acting as a switch.

The choice of the operating mode affects the availability of many of the TR-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	<ul> <li>The bridge interface can be a DHCP client.</li> <li>All DHCP requests from client devices attaching to the virtual APs must be handled by a separate device on the network</li> </ul>	<ul> <li>The wired interface can be a DHCP client.</li> <li>DHCP requests from client devices attaching to the virtual APs can be handled by a local DHCP server on the TR-900 or can be forwarded to a centralized server</li> </ul>
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 TR-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 TR-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.

02:21PM Oct 15, 2007 (local time)	System         DNS         DHCP         SNMP         Location         AAA         Time         Console
Status	Configure your system parameters.
Profile Management Initial Configuration	Scheme: AP Routed  Scheme Scheme
- Minimal Configuration	Node Hostname: GW1 The 'scheme' determines this node's
Detailed Configuration	Node ID: 1 role in the network.
System Parameters	Implicit Addressing: disabled
Security	wireless client.
Wireless Interfaces	Layer 2 Emulation The AP Bridge scheme bridges all
Wired Interface	at layer 2.
QoS	Save Changes
Upgrade	Hestname
Diagnostics	Hostilane
Reboot	A textual name for this node,

Figure 23. Setting operating mode

# 9 System Settings

This section describes settings that are applicable to the overall operation of the TR-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.

<b>b</b>					
WIRELESS TECHNOLOGIES INC.					
03:53PM Oct 15, 2007 (local time)	Passwords Firewall	ACLs OnRamp			
Status	Configure your system pa	isswords.	Ltide Ltele		
Profile Management	Please note: changing th	e admin password will force you	Нае нер		
Initial Configuration	to log back into the webp	ages to continue with configuration.	Admin Password		
Minimal Configuration	Admin Password:	•••••	The admin password controls access		
Detailed Configuration	Verify Admin Password:		to changing settings on the node.		
System Parameters	Save Changes				
Security					
Wireless Interfaces					
Wired Interface					
QoS					
Upgrade					
Diagnostics					
Reboot					

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 TR-900 affects the IP address spaces assigned to each of the TR-900's virtual AP client access interfaces when it uses implicit addressing in routed mode. If multiple TR-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.

02:21PM Oct 15, 2007 (local time)	System	DNS	DHCP	SNMP	Location	AAA	Time	Consol	8
Status	Configure y	our sy	stem par	ameters.					
Profile Management	Scheme:		A	AP Bouted	*				Hide Help
Initial Configuration			Ľ	a riodica				s	cheme
Minimal Configuration	Node Hostr	name:	G	W -1				т	he 'scheme' determines this node's
Detailed Configuration	Node ID:		1					ro	le in the network.
System Parameters	Implicit Ad	dressin	g: c	lisabled N	•			т	he AP Routed scheme provides
Security								rc W	ireless client.
Wireless Interfaces	Layer 2 Er	nulatio	on					Т	he AP Bridge scheme bridges all
Wired Interface	L2 Emulatio	on:	c	disabled	*			c	ient interfaces (wireless and wired)
QoS	Save Ch	anges							
Upgrade	L								
Diagnostics								F	lostname
Reboot								A	textual name for this node.

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

### 9.3 DNS / Domain Settings

At least one DNS server, accessible from the TR-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 TR-900.

If an TR-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 TR-900 and are not provided to any other devices on the network.

CLI

The DNS server(s) used by an TR-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.

<b>D</b>							
03:26PM Oct 15, 2007 (local time)	System DNS DHCP	SNMP	Location	AAA	Time	Console	
Status	DNS DNS Proxy						
Profile Management	Configure your DNS						
Initial Configuration	configure your DNS.						Hide Help
Minimal Configuration	Domain Name:	tranzeo		omain Name			
Detailed Configuration							
System Parameters	Primary DNS Server :	10	. 3 .	108 .	254	Th th	ie domain name associated with is node.
Security	Secondary DNS Server :						
Wireless Interfaces							
Wired Interface	Primary Netbios Server :		·				NS Servers
QoS	Secondary Netbios Server	:				Tł	e 'DNS Server' address(es) are ovided to clients via DHCP.
Upgrade	Save Changes						
Diagnostics							
Reboot						N	etbios Servers

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

### 9.4 DNS Proxy Configuration

DNS proxy entries can be added to an TR-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 TR-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.

<b>b</b>		
VIRELESS TECHNOLOGIES INC.		
03:27PM Oct 15, 2007 (local time)	System DNS DHCP SNMP Location AAA Time Con	sole
Status	DNS DNS Proxy	
Profile Management	Configure your DNS Brown	
Initial Configuration		Hide Help
Minimal Configuration	DNS Proxy: enabled 💌	DNS Proxy
Detailed Configuration		
System Parameters	Add DNS Proxy Entry	Enabling the DNS Proxy resolves names to local IP addresses. Used in
. Security .	Hostname .	conjunction with splash pages.
Wireless Interfaces	IP Address:	
Wired Interface	Roup Changes	Add New Host
QoS	Save Changes	Both the bostname and ID address
Upgrade		are required. The IP address should
Diagnostics	DNS Proxy Hosts: Hostname Proxied IP Address	interfaces.
Reboot	apsignin.company.com 1.2.3.4	

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 TR-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 TR-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).

	Reboot required for changes to take effect.	
03:45PM Oct 15, 2007 (local time)	System DNS DHCP SNMP Location AAA Time Console	
Status	Configure your SNMP parameters.	1 - 1 -
Profile Management	SNMP Port: 161	<u>telp</u>
Initial Configuration	Port	
Detailed Configuration	Read-Only Community: public Port on which SNMP will listen for requests from SNMP clients.	
System Parameters	Read/Write Community: private	
Security	Contact: Contact Read-Only Community	
Wireless Interfaces	Location: Authentication string used to rea	d
Wired Interface	SNMP variables on this node.	
yos Ungrade		
Diagnostics	Read/Write Community	
Reboot	Authentication string used to real write SNMD variables on this pade	d or

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 TR-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 TR-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.

03:49PM Oct 15, 2007 (local time)	System DNS	DHCP	SNMP	Location	AAA	Time	Cons	ole
Status	Configure your l	ocation pa	rameters				Г	
Profile Management	Location:						_	Hide Help
Initial Configuration							-	Location
Minimal Configuration	Latitude:	0.0		(in decir	mal deg	rees)		Text description of the location of
Detailed Configuration	Longitude:	0.0		(in decir	mal deg	rees)		the device, e.g. "On the light post at intersection of 1st St. and Main St."
System Parameters	Altitude:	0.0		(in mete	ers)			
Security								
Wireless Interfaces	Organization:							Latitude / Longitude /
Wired Interface	City:							Altitude
	State/Province:							Latitude, longitude, and altitude of
Ungrade	Country:							the node.
opgrade								
Diagnostics	Save Change	s						Organization / City / State /
Reboot								Country

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 TR-900. The information embedded in this certificate can be defined by the user. A new certificate is automatically generated when the parameters describing the TR-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 TR-900 can be configured to synchronize its internal clock with an external RFC-868compliant 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).

03:53PM Oct 15, 2007 (local time)	System         DNS         DHCP         SNMP         Location         AAA         Time         Console
Status	Configure Time.
Profile Management	Automatic Time enabled
Initial Configuration	Synchronization:
Minimal Configuration	Automatic Time Synchronization A RFC868-compliant time server.
System Parameters	In most cases, the automatic time synchronization will keep your time
Security	listed server once per day.
Wireless Interfaces	It is recommended that you leave
Wired Interface	automatic time synchronization enabled unless your network does
QoS	not have access to a time server. Disabling automatic time
Upgrade	synchronization will allow you to
Diagnostics	mandally set the time.
Reboot	

Figure 30. Automatic time synchronization

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

	Reboot required for changes to take effect.
10:30AM Oct 16, 2007 (local time)	System         DNS         DHCP         SNMP         Location         AAA         Time         Console
Status	Configure Time.
Profile Management Initial Configuration	Automatic Time disabled  Synchronization:
Minimal Configuration	
Detailed Configuration	Hand Configure Time Time (UTC): 17 V. 30 V October V 16 V 2007 V
System Parameters	Change Time?
Security	
Wireless Interfaces	Save Changes
Wired Interface	
QoS	
Upgrade	
Diagnostics	
Reboot	

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.

03:53PM Oct 15, 2007 (local time)	System         DNS         DHCP         SNMP         Location         AAA         Time         Console						
Status	Command Console						
Profile Management	Allows you to set configuration keys directly.						
Initial Configuration	Syntax: kev=value, eq. wlan1.essid=ESSID 1						
Minimal Configuration							
Detailed Configuration	key/value pairs can be separated by either a space or a newline. Values which have spaces in them must be enclosed in double quotes.						
System Parameters							
Security							
Wireless Interfaces							
Wired Interface							
QoS							
Upgrade							
Diagnostics	Submit Commands						
Reboot							

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 TR-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.

1

The OnRamp utility provides network detection and configuration capabilities for TR-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).

3		
03:56PM Oct 15, 2007 (local time)	Passwords Firewall ACLs OnRamp	
Status	Configure OnRamp Access.	Hide Help
Profile Management	Configuration via OnRamp enabled 💌	Configuration via OnRamp
Minimal Configuration	Save Changes	OnRamp is a utility which allows for
Detailed Configuration		provisioning of a node's configuration. If this value is set to
System Parameters		'enabled', OnRamp can set configuration values on this node. If it is set to 'disabled'. OnRamp will still
Wireless Interfaces		be able to detect this node, but not be able to alter values.
Wired Interface		
QoS		
Upgrade Diagnostics		
Reboot		

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 TR-900 is operating in bridge mode.

The choice of client addressing scheme affects how TR-900 client access interface addresses are assigned. The TR-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 TR-900 is not operating in centralized DHCP server mode.

Table 6 compares how the behavior of the TR-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.

02:21PM Oct 15, 2007 (local time)	System	DNS	DHCP	SNMP	Location	AAA	Time	Console
Status	Configure	your sy	stem pa	rameters.				Lida Liala
Profile Management	Scheme:		/	AP Routec	Scheme			
Minimal Configuration	Node Host	name:	C	GW -1	The 'scheme' determines this node's			
Detailed Configuration	Node ID:		1					role in the network.
System Parameters	Implicit Ac	ldressin	g: (	disabled 🛉	*			The AP Routed scheme provides routed access to the network for
Wireless Interfaces	Laver 2 E	mulati	on					wireless client.
Wired Interface	L2 Emulati	on:		disabled 🛉	*			client interfaces (wireless and wired)
QoS	Save Cl	nanges						
Upgrade								Hestname
Diagnostics								Hostname
Reboot								A textual name for this node.

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



If the TR-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 TR-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 TR-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 address range size (ip.implicit.size.requested)			
(ip.implicit.start.requested)	31	63	127	255
1	Yes	Yes	Yes	Yes
33	Yes	No	No	No
65	Yes	Yes	No	No
97	Yes	No	No	No
129	Yes	Yes	Yes	No
161	Yes	No	No	No
193	Yes	Yes	No	No
225	Yes	No	No	No

 Table 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 TR-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).

02:27PM Oct 15, 2007 (local time)	System DNS DHCP SNMP Location AAA Time Co	nsole		
Status	DHCP Centralized DHCP			
Profile Management				
Initial Configuration	Configure DHCP. Hide Help			
Minimal Configuration	wlan1	Mode		
Detailed Configuration	Mode: server 🖌	inouc		
System Parameters	Default Lease Timeout: 86400 seconds	Sets the DHCP mode supported by the interface. The three possible		
Security	Maximum Lease 86400 seconds	modes are:		
Wireless Interfaces	Reserved DHCP Range: 0	<ul> <li>none - no DHCP services are</li> </ul>		
Wired Interface	IP Address Range (Start): 1 🝸 (actual value: 1)	provided • local server - a DHCP server		
QoS	IP Address Range (Size): 127 🗸 (actual value: 127)	will respond to client DHCP requests on the interface		
Upgrade	udan9	central server - the node will		
	Mode: server 🗸	centralized DHCP addresses from a		
Rehoot	Default Lease Timeout: 86400 seconds	available if Centralized DHCP is enabled).		
KEBUDI	Maximum Lease 86400 seconds	<ul> <li>client - the node will attempt to acquire an address for the</li> </ul>		
	Reserved DHCP Range: 0	interface via DHCP (only valid		
	IP Address Range (Start): 129 🝸 (actual value: 129)	for the wired interface)		
	IP Address Range (Size): 31 💌 (actual value: 31)			
	wlan3	Default Lease Timeout		
	Mode: server 🖌	The default lease time the DHCP		
	Default Lease Timeout: 86400 seconds	server will assign to DHCP clients. If		
	Maximum Lease 86400 seconds	not contain a lease time request,		
	Reserved DHCP Range: 0	this is the lease time that will be used.		
	IP Address Range (Start): 161 🔽 (actual value: 161)			
	IP Address Range (Size): 31 👻 (actual value: 31)			
	wlan4	Maximum Lease Timeout		
	Mode: server 🖌	The maximum lease time the DHCP		
	Default Lease Timeout: 86400 seconds	DHCP client lease time requests in		
	Maximum Lease 86400 seconds	excess of this value will be responded to with this lease time.		
	Reserved DHCP Range: 0			
	IP Address Range (Start): 193 🔽 (actual value: 193)			
	IP Address Range (Size): 31 🝸 (actual value: 31)	Reserved Address Range		
	wired	The number of addresses set aside for use as static IPs.		
	none 💌			
	Save Changes			
		Address Range Start		

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:
  - $\circ$  169.254.0.0/16
  - o **127.0.0/8**
- 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 TR-900 when operating in bridge mode.

The Ethernet interface is used to connect the TR-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.

03:57PM Oct 15, 2007 (local time)	DHCP QoS		
Status	Configure your wi	red interface.	Hide Help
Profile Management			<u>Inde heip</u>
Initial Configuration	Enable VLAN:	disabled 💌	VLAN
Minimal Configuration	VLAN ID:	1	Segregate client traffic into Virtual
Detailed Configuration	IP Address:	10 . 1 . 0 . 1	VLAN support enabled. You will
System Parameters	Gateway Address		probably need to enable VLAN on all node Wireless Interfaces as well
Security	Netmask:	255 . 255 . 255 . 0	depending on your network design.
Wireless Interfaces	Broadcast:	10 . 1 . 0 . 255	Valid VLAN IDs are 0-4095, but 0, 1, and 4095 are reserved by
Wired Interface	Enable NAT:	disabled 💙	convention. 1 is the 'Default Port
QoS			VID' which is often appropriate for the wired interface.
Upgrade	Enable VPN:	enabled 💌	
Diagnostics	VPN Port:	1194	
Reboot	VPN Server:	216.100.192.50	IP Address / Gateway / Netmask / Broadcast
	Save Changes		The IP address, gateway address,

Figure 37. Wired interface parameters

## 11.1 DHCP

The TR-900 can be set to obtain an IP address for its Ethernet interface using DHCP. When configured as a DHCP client, the TR-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).

<b>A</b> .		
VIRELESS TECHNOLOGIES INC.		
02:27PM Oct 15, 2007 (local time)	System DNS DHCP SNMP Location AAA Time Con	sole
Status	DHCP Centralized DHCP	
Profile Management	-	
Initial Configuration	Configure DHCP.	Hide Help
Minimal Configuration	wight 1	Mode
Detailed Configuration	Mode: server 💙	Mode
System Parameters	Default Lease Timeout: 86400 seconds	Sets the DHCP mode supported by the interface. The three possible
Security	Maximum Lease 86400 seconds	modes are:
Wireless Interfaces	Reserved DHCP Range: 0	<ul> <li>none - no DHCP services are</li> </ul>
Wired Interface	IP Address Range (Start):	provided • local server - a DHCP server
QoS	IP Address Range (Size): 127 🗸 (actual value: 127)	will respond to client DHCP requests on the interface
Upgrade	wlan?	central server - the node will
Diagnostics	Mode: server 💙	centralized DHCP server (only
Rehaat	Default Lease Timeout: 86400 seconds	available if Centralized DHCP is enabled).
	Maximum Lease 86400 seconds	<ul> <li>client - the node will attempt to acquire an address for the</li> </ul>
	Reserved DHCP Range: 0	interface via DHCP (only valid
	IP Address Range (Start): 129 💌 (actual value: 129)	for the wred interface)
	IP Address Range (Size): 31 💌 (actual value: 31)	
	wlan3	Default Lease Timeout
	Mode: server 💌	The default lease time the DHCP
	Default Lease Timeout: 86400 seconds	server will assign to DHCP clients. If a DHCP request from a client does
	Maximum Lease 86400 seconds Timeout:	not contain a lease time request,
	Reserved DHCP Range: 0	used.
	IP Address Range (Start): 161 💌 (actual value: 161)	
	IP Address Range (Size): 31 💌 (actual value: 31)	M
	wlan4	Maximum Lease Timeout
	Mode: server 👻	The maximum lease time the DHCP server will assign to DHCP clients
	Default Lease Timeout: 86400 seconds	DHCP client lease time requests in
	Maximum Lease 86400 seconds Timeout: Reserved DHCP Range: n	excess of this value will be responded to with this lease time.
	IP Address Range (Start): 193 🗸 (actual value: 193)	
	IP Address Range (Size): 31 🗸 (actual value: 31)	Reserved Address Range
	wired Mode:	The number of addresses set aside for use as static IPs.
	Save Changes	Address Range Start

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 TR-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=255.255.0
```

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.

11:03AM Oct 16, 2007 (local time)	L2 Bridge
Status	DHCP
Profile Management	
Initial Configuration	Hide Help
Minimal Configuration	IP Address: 10 1 1 1 III III IP Address / Gateway /
Detailed Configuration	Gateway Address: Netmask / Broadcast
System Parameters	Netmask: 255 255 0 The IP address, gateway address,
Security	Broadcast: 10 . 1 . 255 Interface. These values are only
L2 Bridge	Configurable when implicit addressing is disabled.
Wireless Interfaces	seconds
Wired Interface	Spanning Tree Protocol: disabled 💌
Upgrade	Forwarding Delay
Diagnostics	The node will watch traffic for this
Reboot	long before participating. If there are no other bridges nearby you may

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.

10:55AM Oct 16, 2007 (local time)	System         DNS         DHCP         SNMP         Location         AAA         Time         Console			
Status	Configure DHCP.			
Profile Management	Hide Help			
Initial Configuration Minimal Configuration	bridge     Mode       Mode:			
Detailed Configuration	Save Changes bits the interface. The three possible modes are:			
System Parameters Security	<ul> <li>none – no DHCP services are provided</li> </ul>			
L2 Bridge	Iocal server - a DHCP server     will respond to client DHCP			
Wireless Interfaces	requests on the interface <ul> <li>central server - the node will</li> </ul>			
Wired Interface	provide DHCP addresses from a centralized DHCP server (only			
Upgrade	available if Centralized DHCP is			
Diagnostics	<ul> <li>client - the node will attempt</li> </ul>			
Reboot	to acquire an address for the interface via DHCP (only valid			

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 TR-900 will watch traffic before participating. If there are no other bridges nearby the TR-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 TR-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 TR-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 'wlanN' when it applies to any of the four VAPs. 'wlan1' will be used in all examples.

A			
3			
03:56PM Oct 15, 2007 (local time)	wlan1 wlan2 wla	ın3 wlan4	
Status			
Profile Management	DHCP Authenticatio	n    ACLS    QOS	
Initial Configuration	Configure wlan1.		Hide Heln
- Minimal Configuration	wlan1 State:	enabled 💌	uden 1
Detailed Configuration	wlan1 Mode:	802 11 B/C	wiani
System Parameters			Enable or disable this access point.
Security	IP Address:	10 . 1 . 1 . 1	
Wireless Interfaces	Gateway Address:		IP Address / Gateway /
Wired Interface	Broadcast:		Netmask / Broadcast
QoS			The IP address, gateway address,
Upgrade	ESSID:	er1000_ap1	the wlan1 interface. These values
Diagnostics	Hide ESSID?	no 💌	are only configurable when implicit addressing is disabled.
Reboot	Channel:	1 (2.412 GHz) 💌	
	VLAN State:	disabled V	ESSID
	VLAN ID:	11	23312
		NOTE: enabling VLAN on this interface	The identifying name for the 802.11 network that this access point
		wired interface.	supports. The ESSID must be no longer than 32 characters and can
	Transmit Power Cap:	30.0 dBm	only contain letters (A-Z, a-z), numbers (0-9), spaces, hyphens,
		- +	and underscores.
	Radio Rate:	54 V Mbps V Auto	
			Hide ESSID
	Use Short Preamble?	yes 🗸	ESSID broadcasting can be disabled
			with this setting.
	Beacon Interval:	100 milliseconds	
	Distance:		Channel
			The access point's operating
	Save Changes		channel. NOTE: All access points on

Figure 41. Virtual access point interface page with TR-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 'wlanN' 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 TR-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 TR-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 TR-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 'wlanN' 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 TR-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 'wlanN' interface.

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

Channel	Center Frequency (MHz)
1/5MHz	908
2/5MHz	913
3/5MHz	918
4/56Hz	923
1/10MHz	910
2/10MHz	920
1/20MHz	915

Table 9. TR-900HG 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 'wlanN' 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 "wlanN" 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 TR-900. The client devices can be assigned their IP configuration in one of three ways when the TR-900 is operating in routed mode:

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

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

## 13.6.1 IP Configuration of Clients Devices via DHCP

The TR-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 TR-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 TR-900 is connected to.

02:27PM Oct 15, 2007 (local time) Status	System         DNS         DHCP         SNMP         Location         AAA         Time         Corr           DHCP         Centralized DHCP	nsole
Profile Management Initial Configuration	Configure DHCP.	Hide Help
Minimal Configuration Detailed Configuration	wlan1 Mode: server 💌	Mode
System Parameters Security	Default Lease Timeout: 86400 seconds Maximum Lease 86400 seconds Timeout	the interface. The three possible modes are:
Wireless Interfaces Wired Interface	Reserved DHCP Range: 0 IP Address Range (Start): 1 ¥ (actual value: 1)	<ul> <li>none - no DHCP services are provided</li> <li>local server - a DHCP server</li> </ul>
QoS Ungrade	IP Address Range (Size): 127 🖌 (actual value: 127)	will respond to client DHCP requests on the interface • central server - the node will
Diagnostics	Mode: server 🕶 Default Lease Timeout: 86400 seconds	provide DHCP addresses from a centralized DHCP server (only available if Centralized DHCP is enabled).
Renout	Maximum Lease 86400 seconds Timeout: Reserved DHCP Range: 0 IP Address Range (Start): 129 v (actual value: 129)	<ul> <li>client - the node will attempt to acquire an address for the interface via DHCP (only valid for the wired interface)</li> </ul>
	IP Address Range (Size): 31 ♥ (actual value: 31) wlan3 Mode: server ♥ Default Lease Timeout: 86400 seconds Maximum Lease 866400 seconds Timeout: Reserved DHCP Range: 0 IP Address Range (Start): 161 ♥ (actual value: 161)	Default Lease Timeout The default lease time the DHCP server will assign to DHCP clients. If a DHCP request from a client does not contain a lease time request, this is the lease time that will be used.
	IP Address Range (Size): 31 v (actual value: 31) wlan4 Mode: server v Default Lease Timeout: 86400 seconds Maximum Lease 866400 seconds Timeout: Reserved DHCP Range: 0 IP Address Range (Start): 193 v (actual value: 193) IP Address Range (Size): 31 v (actual value: 31)	Maximum Lease Timeout The maximum lease time the DHCP server will assign to DHCP clients. DHCP client lease time requests in excess of this value will be responded to with this lease time. Reserved Address Range
	wired Mode: none	The number of addresses set aside for use as static IPs.
	Save Changes	Address Range Start

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 TR-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 TR-900 do not all have to use the same encryption/authentication scheme.

03:50PM Oct 15, 2007 (local time)	System DNS DHC	P SNMP Location AAA Time Con	sole
Status	WPA / WEP Splash I	Pages Advanced Splash Pages	
Profile Management	0		
Initial Configuration	Configure your authent	ication and encryption for the APS.	Hide Help
Minimal Configuration	wlan1	No Authentication 🖌	No Authentication
Detailed Configuration	wlan2	WPA-PSK	<b>-</b> 1
System Parameters	WPA-PSK Passphrase:	enroutepsk	authentication and clients can log on
Security	wlan?		without requiring an encryption key, username, or password.
Wireless Interfaces	WPA Enternrise		
Wired Interface	RADIUS Server	Port: 1812	
QoS		Secret: secret	WEP
Upgrade			The access point uses WEP
Diagnostics	wlan4	WEP	between clients and itself. A key
Reboot	WEP Key:	enrou	common to all users connecting to this access point. Legal key lengths are
	Save Changes		5 or 13 ascii characters

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 'wlanN' interface. The length of the encryption key is determined by the format used to specify the 'key' value. Valid key formats and the corresponding encryption type and key length are listed in Table 11.



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

Key format	Encryption format	Encryption key length
s:<5 ASCII characters> <10 hex values>	WEP	40 bits
s:<13 ASCII characters> <26 hex values>	WEP	104 bits
<blank></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 TR-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.



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 TR-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 dropdown 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 TR-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.



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 "wlanN" 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 "wlanN" 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 'wlanN' 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 "wlanN" 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 TR-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 TR-900s relaying DHCP messages between client devices and the centralized server.

The DHCP modes for client access interfaces on an TR-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 TR-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 TR-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 TR-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 1="" octet="" prefix="">.</lan>
	< LAN prefix octet 2>.
	<node id="">.</node>
	<wlan1 address="" ip="" range="" start=""> + 1</wlan1>
End address =	< LAN prefix octet 1>.
	< LAN prefix octet 2>.
	<node id="">.</node>
	< wlan1 IP address range start address > -
	< wlan1 IP address range size > - 2

The TR-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 TR-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 TR-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).

ື TRANZEO		
02:27PM Oct 15, 2007 (local time) Status	System     DNS     DHCP     SNMP     Location     AAA     Time       DHCP     Centralized DHCP	Console
Profile Management Initial Configuration	Configure DHCP.	Hide Help
Detailed Configuration System Parameters	wlan1 Mode: server 💙 Default Lease Timeout: 86400 seconds	Mode Sets the DHCP mode supported by the interface. The three possible
Security Wireless Interfaces	Maximum Lease 86400 seconds Timeout: Reserved DHCP Range: 0	<ul> <li>none - no DHCP services are</li> </ul>
Wired Interface QoS	IP Address Range (Start): 1 ▼ (actual value: 1) IP Address Range (Size): 127 ▼ (actual value: 127)	<ul> <li>local server - a DHCP server will respond to client DHCP requests on the interface</li> <li>control convert the node will</li> </ul>
Upgrade Diagnostics	wlan2 Mode: server v Default Lease Timeout: 86400 seconds	<ul> <li>central server - the node with provide DHCP addresses from a centralized DHCP server (only available if Centralized DHCP is expelled)</li> </ul>
Reboot	Maximum Lease 86400 seconds Timeout: Reserved DHCP Range: 0 IP Address Range (Start): 129 v (actual value: 129) IP Address Range (Size): 31 v (actual value: 31)	<ul> <li>client - the node will attempt to acquire an address for the interface via DHCP (only valid for the wired interface)</li> </ul>
	wlan3         Mode:       server v         Default Lease Timeout:       86400         Maximum Lease       86400         Timeout:       86400         Reserved DHCP Range:       0         IP Address Range (Start):       161 v	Default Lease Timeout The default lease time the DHCP server will assign to DHCP clients. If a DHCP request from a client does not contain a lease time request, this is the lease time that will be used.
	IP Address Range (Size): 31 v (actual value: 31) wlan4 Mode: server v Default Lease Timeout: 86400 seconds Timeout: 86400 seconds Timeout: 0 IP Address Range (Start): 193 v (actual value: 193) IP Address Range (Size): 31 v (actual value: 31) wired	Maximum Lease Timeout The maximum lease time the DHCP server will assign to DHCP clients. DHCP client lease time requests in excess of this value will be responded to with this lease time. Reserved Address Range The number of addresses set aside for use as static IPs.
	Save Changes	Address Range Start

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 TR-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 TR-900
- 2. The central DHCP server
- 3. Any intermediate router(s) in the path between the DHCP server and the TR-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 TR-900 (there can be up to 4 per TR-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 TR-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 TR-900's Ethernet interface.

Consider the example where an TR-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 TR-900's wired interface is. We will set aside 4 IP addresses for the TR-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 TR-900's Ethernet interface, set aside 192.168.5.3 to 192.168.5.6 for the TR-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 TR-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 TR-900s

When operating in centralized DHCP server mode, each TR-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 TR-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 TR-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 TR-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 TR-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 TR-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 TR-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".

02:28PM Oct 15, 2007 (local time)	System DNS DH0	CP SNMP Locatio	n AAA	Time	Console
Status	DHCP Centralized D	НСР			
Profile Management	Configure Centralized F				
Initial Configuration	Configure Centralized E	incr.			Hide Help
Minimal Configuration	Centralized DHCP:	enabled 🔽			Centralized DHCP
Detailed Configuration					Enables relaying of DHCB messages
System Parameters	Central DHCP Server:	192 . 168 . 0	. 1		to and from a central DHCP server.
Security					
Wireless Interfaces	Gateway Router:	192 168 (	1		Control DUCD Comion
Wired Interface			] · [:		Central DHCP Server
QoS	Client Address Space:	192 168 (	Π	/ 16	Central DHCP server IP address.
Upgrade			] · [ <u>°</u>		
Diagnostics	Relay Base Address:	192 168 0	3		Gateway Router
Reboot			· Lº		Mileon using static ID clients all
	Save Changes				nodes in a mesh must be configured to have the save gateway router

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 TR-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 TR-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 TR-900:

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

# 15 Connecting an TR-900 to a LAN

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

# 15.1 Routed mode

## 15.1.1 Manual Configuration

An TR-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 TR-900 is attached to must be configured to forward the client access interface subnets to the TR-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 TR-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 TR-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 TR-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 TR-900 is connected to. The TR-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 TR-900.

The advantages of using NAT are:

- You can easily attach an TR-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 TR-900 are shielded from the network that the TR-900 is attached to.
- You only consume a single IP address on your existing network when connecting the TR-900 to it.

The main disadvantage of using NAT is

 You are not able to initiate connections to the client devices connected to the TR-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 car	n be set via the web	interface on the	"Wired Interface"	page (Figure 47).
-------------------	----------------------	------------------	-------------------	-------------------

WIRELESS TECHNOLOGIES INC.		
03:57PM Oct 15, 2007 (local time)	DHCP Qos	
Status	Configure your wired interface.	
Profile Management		Hide Heip
Initial Configuration	Enable VLAN: disabled 💙	VLAN
Minimal Configuration	VLAN ID: 1	Segregate client traffic into Virtual
Detailed Configuration	IP Address: 10 . 1 . 0 . 1	LANs. Your internet router must have VLAN support enabled. You will
System Parameters	Gateway Address:	probably need to enable VLAN on all node Wireless Interfaces as well
Security	Netmask: 255 . 255 . 255 . 0	depending on your network design.
Wireless Interfaces	Broadcast: 10 . 1 . 0 . 255	Valid VLAN IDs are 0-4095, but 0, 1,
Wired Interface	Enable NAT: disabled 🗸	and 4095 are reserved by convention. 1 is the 'Default Port
QoS		VID' which is often appropriate for the wired interface.
Upgrade	Enable VPN: enabled V	
Diagnostics	VPN Port: 1194	
Reboot	216.100.192.50	IP Address / Gateway /
	Save Changes	Nethiasky broadcast
	<b>VPN Credentials</b> Your vendor may provide you with a package of VPN Credential files If you need to install a credential package, you can load it onto the node here. Please refer to the help for more details.	The IP address, gateway address, netmask, and broadcast address for the wired interface. These values are only configurable when the wired interface is not configured for DHCP client mode.
	VPN Credentials: Browse	Enable NAT
	Opidad Gredentials	Network address translation (NAT)

Figure 47. NAT and VPN settings

# 15.2 Bridge Mode

In bridge mode, the TR-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 TR-900

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



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

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

Function	Port(s)	Туре	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	ТСР
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 TR-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.

```
INFO
```

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 clientto-client traffic blocking for one or more of an TR-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 TR-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 TR-900.

03:53PM Oct 15, 2007 (local time)	Passwords Firewall i	ACLs OnRamp	
Status	Connections Custom Ru	les	
Profile Management	Configure the frequel		
Initial Configuration	configure the firewall.		Hide Help
Minimal Configuration	Client Isolation, if enable client communication.	d, will prevent client to	Client Isolation
Detailed Configuration	and an effective of the second s		
System Parameters	wlan1 wlan2	disabled 💙 disabled 💙	Controls whether client devices are able to communicate with each other
Security	wlan3	disabled 😽	other.
Wireless Interfaces	wlan4	disabled 🖌	
Wired Interface	wired	disabled 💙	Conntrack Size
QoS			Allows you to set the connection
Upgrade	Connection Tracking		tracking table size. Setting it higher
Diagnostics	Conntrack Size	8192	node. Setting it too low means
Reboot	Conntrack Limiting	disabled 💌	established connections may be dropped as new ones are created.
	Conntrack Connection Limits Conntrack Connection Timeout	50 3600 seconds	Generally this is only an issue on gateway nodes on busy meshes where this may want to be boosted to 16384.
	Save Changes		

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.



# 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 TR-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

<b>A</b> .			
2			
TRANZEO			
WIRELESS TECHNOLOGIES INC.			
03:54PM Oct 15, 2007 (local time)	Passwords         Firewall         ACLs         OnRamp		
Status	Connections Custom Rules		
Profile Management			
Initial Configuration	Custom Firewall Rules		
Minimal Configuration	Additional firewall rules may be added, which affect packets passing though the node. This allows you to tailor rules for your particular installation, eg. blocking all traffic on port 25 (smtp).		
Detailed Configuration	By default, all traffic is allowed through.		
System Parameters			
Security	Your rules should look like:		
Wireless Interfaces	[rules] -j [target]		
Wired Interface	ex: drop all packets addressed for 192.168.0.0/24		
QoS	-p &LLdst 192.168.0.0/24 -j DROP		
Upgrade	NOTE: All changes will take immediate effect and will not require a reboot.		
Diagnostics			
Reboot			
	Save and Apply Changes		

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.

03:55PM Oct 15, 2007 (local time)	Passwords         Firewall         ACLs         OnRamp	
Status	wlan1 wlan2 wlan3 wlan4 wired	
Profile Management	Configure wight Access Control Lists (ACLs)	
Initial Configuration	configure wiant Access control Lists (Accis).	Hide Help
Minimal Configuration	Please note, the address is white or black-listed immediately after it is added. No reboot is required.	ACL Mode
Detailed Configuration	If a black-listed client is currently connected, it will be kicked	The ACL mode determines whether
System Parameters	from the network before the it is added to the blacklist.	client devices on the ACL list will be
Security		permitted access to the access point. The supported ACL modes are:
Wireless Interfaces	wlan1 blacklist 💙 Change ACL Mode	<ul> <li>none - all devices will be</li> </ul>
Wired Interface		permitted access
QoS	Enter address:	blacklist - devices on the ACL     will be denied access
Upgrade		<ul> <li>whitelist - only devices on the ACL will be allowed access</li> </ul>
Diagnostics	Add MAC	
Reboot		
	Upload File: Browse Upload	Add MAC Address
· · · ·		Use this form to add client device
	Black-listed MAC Addresses for wlan1 none	MAC addresses to the ACL.

Figure 50. VAP ACL configuration

# **17** Quality of Service (QoS) Configuration

BRIDGE

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

The TR-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 TR-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.



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	<b>Priority level</b>
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'.

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.

INFO

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).

WIRELESS TECHNOLOGIES INC.	QoS Advanced QoS	
Status	Configure Quality of Service (QoS).	
Profile Management	Fashla OaG	Hide Help
Initial Configuration	Enable QUS: enabled	Quality of Service (QoS)
Minimal Configuration	DEFAULT Flow Priority: 10	The master enable for QoS must be
Detailed Configuration	Out Limit: kbps	set for any QoS settings to have an effect
System Parameters	Out Reserve: kbps	
Security	wlan1 Flow Priority: DEFAULT	
Wireless Interfaces	Out Limit: DEFAULT khns	Flow Priority
Wired Interface	Out Reserve: DEFAULT kbps	Priority of data based on source
QoS		interface. A higher value means higher priority. The default value will
Upgrade	wian2 Flow Priority: DEFAULT	be applied if no value is set for an interface
Diagnostics	Out Peserve: DEFAULT kbps	
Reboot	Cut Reserve. DEFAULT kbps	
	wlan3 Flow Priority: DEFAULT	Out Limit
	Out Limit: DEFAULT kbps	The output limit, in kbps, for the
	Out Reserve: DEFAULT kbps	interface.
	wlan4 Elow Priority: DEEAUUT	
	Out Limit: DEFAULT kbps	Out Reserve
	Out Reserve: DEFAULT khns	The reserved bandwidth in khos for
		an interface.
	wired Flow Priority: DEFAULT	
	Out Limit: DEFAULT kbps	
	Out Reserve. DEFAULT kbps	
	Save Changes	

Figure 51. QoS settings

03:58PM Oct 15, 2007 (local time)	QoS Advanced QoS	
Status	Configure Advanced Quality of Service (QoS) settings.	
Profile Management		Hide Help
Initial Configuration	DEFAULT 'Voice' Out Limit: kbps	'Voice' Out Limit
Minimal Configuration	'Voice' Out Reserve: kbps	The output limit, in kbps, for voice
Detailed Configuration	'Video' Out Limit: kbps	traffic from the interface.
System Parameters	'Video' Out Reserve: kbps	
Security	'Best Effort' Out Limit: kbps	'Voice' Out Reserve
Wireless Interfaces	'Best Effort' Out Reserve: kbps	voice outricitie
Wired Interface	'Background' Out Limit: kbps	The output bandwidth, in kbps, reserved for voice traffic from the
QoS	Background Out Reserve: kbps	interface.
Upgrade	wlan1 'Voice' Out Limit: DEFAULT kbps	
Diagnostics	'Voice' Out Reserve: DEFAULT kbps	'Video' Out Limit
Rehaat	'Video' Out Limit: DEFAULT kbps	Theorem Contentine
Rebut	'Video' Out Reserve: DEFAULT kbps	The output limit, in kbps, for video traffic from the interface.
	'Best Effort' Out Limit: DEFAULT kbps	
	'Best Effort' Out Reserve: DEFAULT kbps	
	'Background' Out Limit: DEFAULT kbps	'Video' Out Reserve
	'Background' Out Reserve: DEFAULT kbps	The output bandwidth, in kbps,
	wlan2 'Voice' Out Limit: DEFALIET where	reserved for video traffic from the interface.
	Voice' Out Reserve: DEFAULT kbps	
	Video! Out Limit:	

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



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 TR-900 through a particular interface and exits it through another interface can be limited.



There is no standalone input rate limiting. Limiting the input rate of an interface on the TR-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 TR-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 TR-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 TR-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 TR-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 TR-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).

03:56PM Oct 15, 2007 (local time)	wlan1 wlan2 wla	an3 wlan4	
Status Profile Management	DHCP Authenticatio	ACLs QoS	
Initial Configuration Minimal Configuration	wlan1 State:	enabled 💌	<u>Hide Help</u>
Detailed Configuration	wlan1 Mode:	802.11 B/G 💌	WIANI Enable or disable this access point.
System Parameters Security	IP Address:	10 . 1 . 1 . 1	
Wireless Interfaces	Netmask:	.         .         .         .           255         .         255         .         0	IP Address / Gateway / Netmask / Broadcast
Qos	Broadcast:	10 . 1 . 1 . 255	The IP address, gateway address, netmask, and broadcast address for
Upgrade Diagnostics	Hide ESSID?	er1000_ap1	the wlan1 interface. These values are only configurable when implicit addressing is disabled.
Reboot	Channel:	1 (2.412 GHz)	
	VLAN State: VLAN ID:	disabled 11 NOTE: enabling VLAN on this interface requires VLAN to be configured on the wired interface.	ESSID The identifying name for the 802.11 network that this access point supports. The ESSID must be no longer than 32 characters and can
	Transmit Power Cap:	30.0 dBm - +	only contain letters (A-Z, a-z), numbers (0-9), spaces, hyphens, and underscores.
	Radio Rate:	54 🕶 Mbps 🗹 Auto	Hide ESSID
	Use Short Preamble?	yes 💌	ESSID broadcasting can be disabled with this setting.
	Beacon Interval:	100 milliseconds	
	Distance:	DEFAULT kilometers	Channel
	Save Changes		channel. NOTE: All access points on a node must use the same channel.

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 TR-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 TR-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

03:57PM Oct 15, 2007 (local time)	DHCP QoS	
Status	Configure your wired interface.	
Profile Management		Hide Heit
initial Configuration	Enable VLAN: disabled 🗸	VLAN
Minimal Configuration	VLAN ID: 1	Segregate client traffic into Virtual
Detailed Configuration	IP Address: 10 . 1 . 0 . 1	VLAN support enabled. You will
System Parameters	Gateway Address:	probably need to enable VLAN on all node Wireless Interfaces as well
Security	Netmask: 255 . 255 . 0	depending on your network design.
Wireless Interfaces	Broadcast: 10 . 1 . 0 . 255	Valid VLAN IDs are 0-4095, but 0, 1,
Wired Interface	Enable NAT: disabled 💌	convention. 1 is the 'Default Port
QoS	Enable VPN:	the wired interface.
Upgrade	VPN Port: 1194	
Diagnostics	VPN Server: 216 100 192 50	
Reboot	210.100.102.00	Netmask / Broadcast
	Save Changes	
		The IP address, gateway address, netmask, and broadcast address for
		the wired interface. These values are
	VPN Credentials	interface is not configured for DHCP
	If you need to install a credential package, you can load it onto the	client mode.
	node here. Please refer to the help for more details.	
	Browse	Enable NAT
	Upload Credentials	
		Network address translation (NAT)

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

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

Use the 'splash.auth.server.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.

03:51PM Oct 15, 2007 (local time)	System DNS	DHCP	SNMP	Location	AAA	Time	Console	
Status	WPA / WEP SI	alash P.	ages Ad	vanced Sola	sh Page	5		
Profile Management			-9 []					
itial Configuration	Configure your Sp	olash Pa	age.					Hide He
Minimal Configuration								-hl- O-lh D
tailed Configuration	Enable Splash Pa	ge:	disabled 🗸				En	able Splash Page
System Parameters	Require Login:		/es 💙				Con	trols whether a splash page is layed when clients first connect
Security	Splash Page URL:	Ē					to t	he interface.
Wireless Interfaces	Success Page UR	L: [					]	
Wined Intenfaces	Failed Login Page	URL:						
wired Interface	Login Server Add	nee: [				_	Re	quire Login
Qos	Login Server Rud			· · ·	·		A s	olash page can require login
pgrade	Login Server Sec	· [] ret: [	812				thro	dentials or simply require a click- ough.
iagnostics	Login contor coo							
eboot	wian2							
	Enable Splash Par Require Login:	ge: c	disabled 🎽				Sp	lash Page URL
	Solash Page URI :	2	/es 🎽				URL	of the splash page to be
	Success Page UR	L: [					disp the	layed when a client connects to interface.
	Failed Login Page	URL:					1	
	Login Server Add	ress:			].		Su	ccess Page URL
	Login Server Port	: 1	812				URL	of the page to be displayed
	Login Server Seci	ret:					follo	wing a successful login. cifving this URL is optional. If n
	wlan3						URL	is specified, a generic success
	Enable Splash Pa	ge: 🛛	disabled 🚩				pag	e will be displayed.
	Require Login:	2	/es 🚩					
	Splasn Page URL:	Ļ					Fai	led Login Page URL
	Success Page OR							of the name to be displayed
	ralieu Login Page	ORL.					follo	wing a failed login. Specifying
	Login Server Add	ress:			].		spe	ORL is optional. If no ORL is cified, a generic failure page wil
	Login Server Port	: 1	812				be	displayed.
	Login Server Seci	ret:						
	wlan4						10	ain Server, Port, Secret
	Enable Splash Pa	ge: o	disabled 🔽					
	Require Login:	2	/es 🔽				to r	en the splash page is configured equire a login, information about
	Splash Page URL:						the	RADIUS server used to verify the information must be specified.
	Success Page UR	L: [					]	
	Failed Login Page	URL:						
	Login Server Add	ress: [				-		
	Login Server Port	: 6	812	· L	J • [			
	Login Server Seci	ret: 🗆	0.2					

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>.fail' parameters in the 'sys' interface set the fail URLs. The 'splash.url.<intf>.fail' parameters in the 'sys' interface set the fail URLs. The 'splash.url.<intf>.fail' parameters in the 'sys' interface set the fail URLs. The 'splash.url.<intf>.fail' parameters in the 'sys' interface set the fail URLs. The 'splash.url.<intf>.fail' parameters in the 'sys' interface set the fail URLs. The 'splash.url.<intf>.fail' parameters in the 'sys' interface set the fail URLs. The 'splash.url.<intf>.fail' parameters in the 'sys' interface set the fail URLs. The 'splash.url.</id>

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.fail=http://server.domain.com/wlan2_fail.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 TR-900 and the last part of it must be '/radius/login.cgi'. The DNS proxy entry, which will be different for each deployed TR-900, must be mapped to one of the TR-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"
```



The DNS proxy setting is used in conjunction with the splash pages to ensure that a common login URL can be used on all TR-900. The DNS proxy entry directs the results of the login process to the right location – that is, the TR-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">
    Welcoming text or 'Terms of Service' could go here. <br />
7
8
9
    10
    11
       Username: 
       <input name="username" type="text"><br /> 
12
13
     Password: 
14
15
       <input name="password" type="password"> 
16
    17
    18
19
      <input name="login" type="submit" value="Submit">
20
    </form>
21
  </body>
22 </html>
```



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



#### **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 TR-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.

Q			
WIRELESS TECHNOLOGIES INC.			
03:52PM Oct 15, 2007 (local time)	System DNS DHC	P SNMP Location AAA Time Con	sole
Status	WPA / WEP Splash	Pages Advanced Splash Pages	
Profile Management	Configure advanced on		
Initial Configuration	connigure advanced sp	lasii page leatures.	Hide Help
Minimal Configuration	Trusted MAC		Trusted MACs
Detailed Configuration	Addresses		Clients with a MAC address in this list
System Parameters			not be shown the splash page or be
Security	Enter address:		required to authenticate.
Wireless Interfaces		Add MAC	
Wired Interface			Bypass Hosts
QoS			IP addresses listed here can be
Upgrade	Trusted MAC List	No MAC addresses currently configured.	accessed by a client, without the
Diagnostics			screen.
Reboot	Bypass Hosts		
	Add New Host		
		Add Host	
	Bypass Host List	No hosts currently configured.	

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 TR-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 TR-900 to provide the client device MAC address information to back-end systems.

When layer 2 emulation is enabled, the TR-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 TR-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 TR-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 TR-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 TR-900's subnets, the ARP responses can be limited to certain parts of the TR-900's address space. The TR-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 TR-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 TR-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 TR-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.

03:59PM Oct 15, 2007 (local time)	Ping         Traceroute         Packet Capture         DHCP         RADIUS         Diagnostic Dump
Status	Ping Address.
Profile Management	нае нер
Initial Configuration	IP Address or Name: IP Address or Name
Minimal Configuration	Ping Count: 1
Detailed Configuration	Record Route:
System Parameters	

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 TR-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.

04:00PM Oct 15, 2007 (local time)	Ping         Traceroute         Packet Capture         DHCP         RADIUS         Diagno	stic Dump
Status	Trace the Route to an Address.	Hide Hole
Profile Management		<u>ride riep</u>
Initial Configuration	IP Address or Name:	IP Address or Name
Minimal Configuration	Resolve Names:	The remote host to be traced.
Detailed Configuration	Trace Route	
System Parameters		

Figure 63. Determining the route from the TR-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 TR-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 3<sup>rd</sup>-party tools, such as Wireshark (<u>http://www.wireshark.org/</u>). At most, 10 captured files can be saved on the TR-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 TR-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 TR-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	In addition to IP address or hostnames, source and destination MAC addresses will be
addresses	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.</file>
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 TR-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

04:01PM Oct 15, 2007 (local time)	Ping Traceroute Packet Capture DHCP RADIUS Diagno	stic Dump
Status	Test access to a RADIUS server.	Hide Hele
Profile Management		<u>niue neip</u>
Initial Configuration	Choose RADIUS server: 192.168.0.12:1812 💌	Choose RADIUS Server
Minimal Configuration	Username:	The RADIUS server against which
Detailed Configuration	Password:	of RADIUS servers is composed of all
System Parameters		WPA Enterprise RADIUS servers and any defined splash page Login
Security	TestUser	servers.

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).

04:02PM Oct 15, 2007 (local time)	Ping Traceroute Packet Capture DHCP RADIUS	Diagnostic Dump
Status	Diagnostics.	
Profile Management	Dump File Prefix:	Hide Help
Initial Configuration		Generate Diagnostics Dump
Minimal Configuration	Generate Diagnostics Dump	A diagnostic dump runs a series of
Detailed Configuration	Max. saved files is 10.	tests, then packages the results into a file to give to technical support.
System Parameters	Available diagnostic dumos	
Security	No files available	
Wingloss Totoufaces		

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



# If power to the TR-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 TR-900
- Firmware available on the remote upgrade server
- Firmware available in the non-volatile memory of the TR-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 TR-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 TR-900 will reboot automatically when the upgrade has been completed.

WIRELESS TECHNOLOGIES INC.						
03:59PM Oct 15, 2007 (local time)	Upgrade Node Firmware					
Status	Upload new firmware versions to the n firmware on the node.	ode or mana <u>c</u>	ge current			
Profile Management						
Initial Configuration	Installed Firmware:ENROUTE500_20 Patch Version(s): none	070811_03_0	0_0213			
Minimal Configuration	Dick Snaco					
Detailed Configuration	Total Space 89 Mb	Disk Space: Total Space - 89 Mb				
System Parameters	Used 47 Mb Available 37 Mb					
Security						
Wireless Interfaces	Firmware on Server		Firmware on Node			
Wired Interface	ENROUTE500_20070811_03_00_0213	$\rightarrow$	ENROUTE500_20070811_03_00_0213 ENROUTE500_20070213_02_30_0179	Info		
QoS				Delete		
Upgrade				Install		
Diagnostics						
Reboot	Get Alternate Firmware Version Occassionally your vendor will provide type of unique upgrade and may give which you must load onto your nodes. to install such a version, please enter firmware name below to have it loaded	a custom or o you a specific If you are at the vendor-p d onto your no	other 5 version ttempting irovided ode. Get Firmware			

Figure 68. Updating firmware

# Glossary

Client access interface	An interface on the TR-900 used by a client device, such as an 802.11-enabled laptop, to connect to the TR-900. The client access interfaces are the virtual APs wlan1 – wlan4.
Client device	A device that is connected to one of the TR-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 TR-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 TR-900 used by a client device, such as an 802.11-enabled laptop, to connect to the TR-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