



QUICK START GUIDE FOR THE TRANZEO WIRELESS TR-49

REVISION 2.0a
JANUARY 2ND, 2006

FCC Information

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a Residential environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communication.

Operation in the 4940-4990 MHz band is restricted to the U.S. Operation in this range is restricted to the Public safety bands. Use of these bands is restricted to entities that meet the requirements listed the FCC Part 90.20 Public Safety Pool and are properly licensed to operate a transmitter in the Public Safety band in accordance with Part 90Y of the technical rules can operate in the 4940-4990 MHz band. FCC regulations state in Part 90, operation in the 4.9-GHz band requires frequency coordination before the system can be operated.

Operation of this equipment in residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his or her own expense.

The user should not modify or change this equipment without written approval from Tranzeo Wireless. Modification could void authority to use this equipment.

For the safety reasons, people should not work in a situation which RF Exposure limits be exceeded. To prevent the situation happening, people who work with the antenna should be aware of the following rules

1. Install the antenna in a location where a distance of 65 cm from the antenna may be maintained.
2. While installing the antenna, do not turn on power to the unit.
3. Do not connect the antenna while the device is in operation.
4. The antenna used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Safety Notices

Safety Precautions:

YOU MUST READ AND UNDERSTAND THE FOLLOWING SAFETY INSTRUCTIONS BEFORE INSTALLING THE DEVICE:

- This antenna's grounding system must be installed according to Article 810-15, 810-20, 810-21 of the National Electric Code, ANSI/NFPA No. 70-1993. If you have any questions or doubts about your antenna grounding system, contact a local licensed electrician.
- Never attach the Grounding Wire while the device is powered.
- If the ground is to be attached to an existing electrical circuit, turn off the circuit before attaching the wire.
- Use the Tranzeo POE only with approved Tranzeo models.
- Never install Radio Equipment, surge suppressors, or lightning protection during a storm.

A BRIEF WORD ON LIGHTNING PROTECTION

The key to a Lightning Protection is providing a harmless route for lightning to reach ground. The system should not be designed to attract lightning, nor can it repel lightning. National, State and local codes are designed to protect life, limb and property, and must always be obeyed.

When in doubt, consult contact an electrician or professional trained in the design of grounding systems.

Introduction

This next-generation wireless LAN device – the TRANZEO TR-49, brings Ethernet-like performance to the wireless realm. The TRANZEO TR-49 also provides powerful features such as the Internet-based configuration utility as well as WEP and WPA security. Maximize network efficiency while minimizing your network investment and maintenance costs.

Hardware Installation

Product Kit

Before installation, make sure that you have the following items:

- The TR-49 x 1
- DC Power Adapter x 1
- Power over Ethernet Adapter x 1
- Ethernet Boot x 1
- Mounting Bracket x 1
- Kept Nuts (With Washer Attached) x 8
- U-Bolt w/ 2 Nuts x 1
- RJ-45 Patch Cable x 1
- Ethernet Boot Gasket x 1
- Ethernet Cable Lock x 1

If any of the above items is not included or damaged, please contact your local dealer for support.

In this Manual, the symbol **②** will be used to indicate changes that were introduced in Version 2.0.

Mechanical Description

LED panel of the Wireless LAN Smart Access Point

The following table provides an overview of each LED activity:

Label	Color	Indicators
POWER	Red	On: Powered On Off: No Power
LAN	Green	On: Ethernet Link Flashing : Ethernet Traffic Off: No Ethernet Link
Radio	Amber	On: Radio Link Flashing Radio Activity Off: No Radio Link
Signal	Red/Amber/Green	In CPE mode, light up in sequence to indicate signal strength

In AP mode the signal lights indicate the following:

Color	Indicators
Red	On: WEP/128 Enabled Flashing: WEP/64 Enabled Off: WEP Off
Amber	On: WPA/AES Enabled Flashing : WPA/TKIP Enabled Off: WPA Off
Amber	No Function in 4.9
Green	On: ACL Enabled Off: ACL Off
Green	On: WDS Enabled Off: WDS Off

Power Supply

ONLY use the power adapter supplied with the TR-49. Otherwise, the product may be damaged.

Hardware Installation

Take the following steps to set up your TR-49.

Site Selection: Before installation, determine the TR-49 unit's location. Proper placement of the unit is critical to ensure optimum radio range and performance. You should perform a Site Survey to determine the optimal location. Ensure the CPE is within line-of-sight of the Access Point. Obstructions may impede performance of the unit.

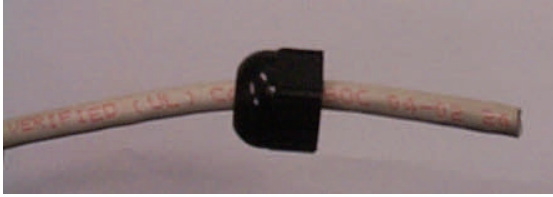
Tools Required to Install

- One 3/8 wrench
- One 3/4 wrench
- One RJ-45 crimper
- A suitable length of Cat 5 cable to bring the signal from the unit to the Power over Ethernet Adaptor
- 2 RJ-45 Jacks

Before installing, you must determine if the unit will be in the horizontal or vertical orientation. The TR-49 model can be mounted in either orientation. The Ethernet boot should always be placed so that the cable runs toward the ground for maximum environmental protection.

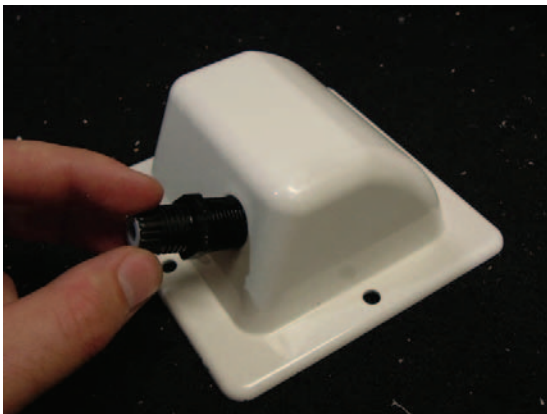
Connecting the Ethernet Cable

Step 1



Place the Ethernet Boot Cover over the end of your Cat 5 cable.

Step 2



Attach Ethernet Cable Lock on side of the Ethernet Boot. This is easiest to do before you attach the RJ-45 Jack.

Step 3



Tighten using a $\frac{3}{4}$ " wrench or socket. Tighten until the Cable Lock touches the Boot as shown in Step 3.

Step 4



Repeat steps 2 & 3 to attach the second Ethernet Cable Lock if you purchased the optional dual port boot.

Step 5



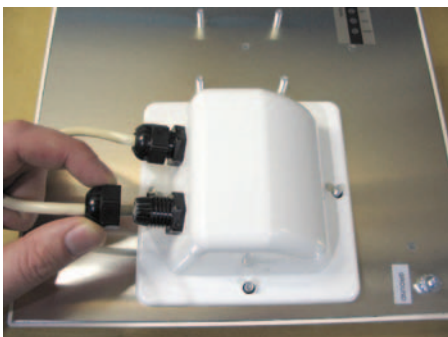
Place Sealing Gasket over screws.

Step 6



Remove gasket backing and place boot cover on radio. This will ensure that you attach the sticky side of the gasket to the underside of the Ethernet Boot. Make sure the Gasket is free of gaps.

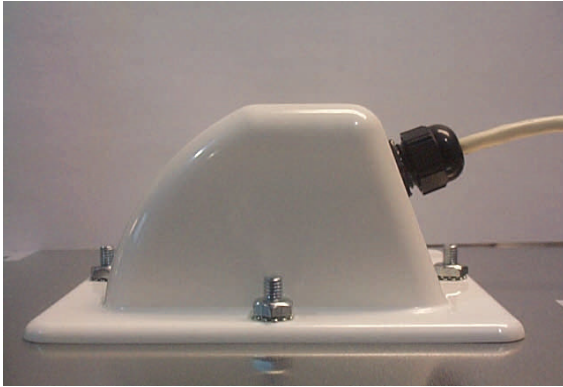
Step 7



Insert the Cat 5 Cable and tighten the Boot Cover. Be sure to pull enough cable through to reach the RJ-45 connector with an RJ-45 jack attached. The Gasket must be attached to the Boot so that it sits between the radio and the boot.

Hand tighten only. **DO NOT OVERTIGHTEN** as you may damage the environment seal.

Step 8



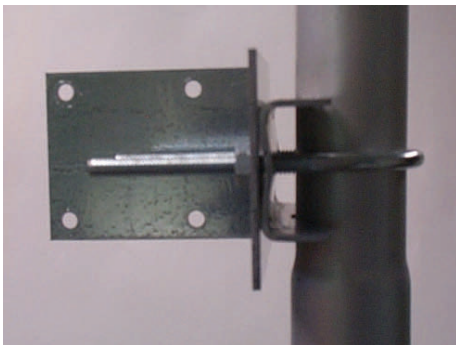
Place the Ethernet boot over the 4 Screw Posts. Apply 4 Kept nuts to the screw posts and tighten until the gasket makes full contact with the Ethernet boot. The gasket should be at least 50% compressed.



Optional dual port boot specific note.

If you are not going to be using the second port make sure that it is tightened down to ensure a weather-tight seal.

Attaching the Mounting Bracket



As shown below, the U-Bolt is designed to mount around a pole. Tighten bolts sufficiently to prevent any movement.

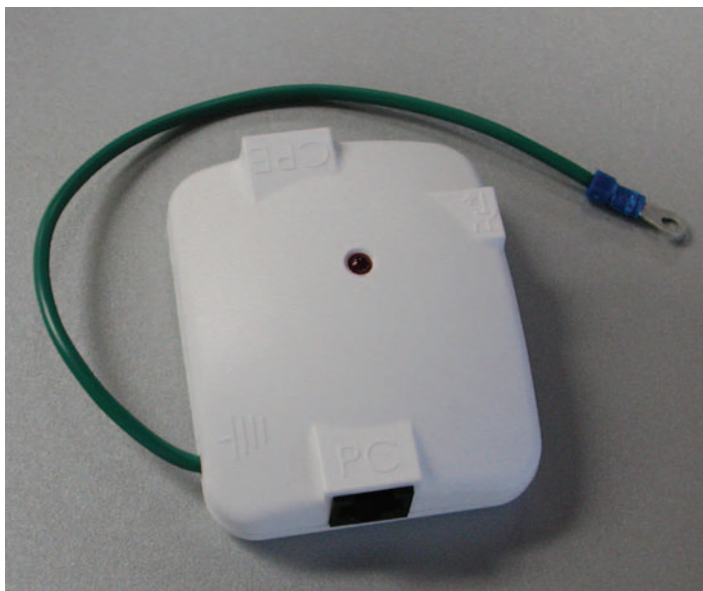


Down or up tilt can be adjusted by swinging the unit before tightening the U-Bolt.

Grounding the Antenna

Using a #6 Green grounding wire, connect the Grounding Lug on the radio to a proper ground. See APPENDIX A Lighting Information for more information.

Connect the Power Cable



Connect the power adapter to the power socket on the Power over Ethernet Adaptor (POE), and plug the other end of the power into an electrical outlet. Plug the RJ-45 Cable from the unit into the POE. The Station Adaptor will be powered on and the power indicator on the top panel will turn on.

NOTE: ONLY use the power adapter supplied with the Access Point. Otherwise, the product may be damaged.

This unit must be grounded. Connect the Green Grounding Cable to a known good earth ground, as outlined in the National Electrical Code.

Dual Ethernet Ports

The TR-49 has two Ethernet port available. **Port A** is used to connect to the radio in the radio in the case. **Port B** is used to power and provide Ethernet connectivity to additional devices. This allows for the daisy chaining of multiple devices together.



HTML Interface

NOTE: The default IP address is **192.168.1.100**
The default User Name is **admin**
The default Password is **default**

Passwords

Password Set/Reset

Use this screen to set or reset the passwords to your device if they've been lost or inadvertently changed. For security reasons, you must set both the normal administration password and the recovery passwords before accessing the administration interface.

The recovery password is available for 5 minutes after powering the device on. After 5 minutes the device must be power-cycled to reactivate the recovery password; this helps prevent abuse of the recovery password by users without physical access to the device.

Note: You must set both the normal administration and recovery passwords before using the administration interface.

Administration Password

Username: This is the normal account used to administer the device.

Password: This password is currently set to the factory default. You must set this password before using the administration interface.

Confirm:

Recovery Password


Username: This is a special account used to recover the administration password if it has been lost or inadvertently changed.

Password: This password is currently set to the factory default. You must set this password before using the administration interface.

Confirm:

When you first enter the Web Interface, you will be required to enter a new recovery password. This password is intended to allow the ISP to change the password of the device if they forget it. This password must be different than the operator password. Neither password can be left at **default**. These passwords must be changed to access the device. If you do not enter new passwords, you will return to this webpage.

Information

**TRANZEEO**
802.11a (5GHz)
Tr6 Router with
Integrated 21 dB Antenna
[AP Setup Menu](#)
[Wireless Settings](#)
[Administrative Settings](#)
[WDS](#)
[Security](#)
 [Basic](#)
 [Advanced](#)
 [Access Control](#)
[Status](#)
[Stations List](#)
[Network Configuration](#)
[Log Off](#)
Copyright © 2004,2005 Tranzeeo Wireless Technologies, Inc.

Information Page

Wireless Settings	
DFS/TPC Enabled	No
Link Status	No Link
SSID	TR6Rt
Device Name	TR6Rt
Network Settings	
IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Accessed From	192.168.1.50
Security	
Encryption	Off
Authentication	None
Radio	
Country / Regulatory	US: United States (FCC1_FCCA)
MAC Address	0060B3E29014
Channel	149
Board	
OS	6.3.34P (1019)
Software	1.10 (TR6Rt-82R)
Event Log	
Hardware Events	(none)

In the frame on the left, select the option you wish to configure.

Wireless Settings

Wireless Settings

☐ Infrastructure Station
☒ Access Point

SSID: trenzo

☒ Visible ☐ Invisible

CH3-2.422GHz

Best (automatic)

RTS Threshold (0-3000): 3000

Fragmentation Threshold (256-2346): 256

Link Distance: 0 km

ACK Timeout Tuning (-100 - 100 μ s): 100

Beacon Interval (ms): 100

DTIM Interval: 1

Burst Time: 0

☐ 802.11d Enabled

☐ PXP Mode Enabled

PXP MAC Address: 000000000000

☐ Block Inter-client Traffic

Power Cap (dBm): 30.0

Select Country: US: United States

Antenna Gain (0 - 100 dBi): 9.0

Preamble: LONG

Apply Back Auto Next Page

SSID

The SSID is a unique ID given to an Access Point.

Wireless clients associating to the Access Point must have the same SSID. The SSID can have up to 32 characters.

Visibility Status

Makes the AP visible or invisible to clients.

Channel

Sets the channel that the AP and clients will use

TX Rate

The rate at which the radio will communicate with the clients.

NOTE: Setting this rate below the maximum possible does not limit bandwidth, and often has a negative impact on the operation of your network.

RTS Threshold (0-3000)

Select RTS that works best in your location. A general rule of thumb is the more clients you have, the lower the value should be set.

Fragmentation Threshold

Select Fragmentation that works best in your location. The lower the Fragmentation, the smaller the packets.

Link Distance

Sets the distance of the link for correct ACK timing.

ACK Timeout Tuning (μ s)

For fine tuning the ACK timing if required.

Beacon Interval

Sets the rate at which the AP will broadcast its beacons.

DTIM Interval

Sets the DTIM (Delivery Traffic Indication Message) Interval. Helps to keep marginal clients connected by sending wake up frames.

Burst Time

Sets the Burst Time in ms. which will be used to send data without stopping. Note that other wireless devices in that network will not be able to transmit data for this number of microseconds.

802.11d Enabled

Enable 802.11d mode. Not used in operation in the United States or Canada.

Block Inter-Client Traffic

Select to block wireless communications between clients on the AP.

Power Cap (dBm)

Sets the output power of the radio.

2 Preamble

You can now set the preamble type: Long or Auto. Auto tries Short first, then Long. Long uses Long only. This feature was added to workaround some competitive AP's that did not support Auto Preamble.



PXP How to:

To operate the radio in PXP mode, one radio needs to be set to Access Point and the other set to Infrastructure.

- ◆ Set the SSID to be the same on both radios
- ◆ Channel is set by the AP
- ◆ Enter in the opposite radios' MAC address into the PXP Mac address field on both radios (no colons)
- ◆ Check off "PXP Mode Enabled"

Note: The LEDs on the radios will operate the same as in Infrastructure mode, with LEDs proportional to signal strength.

Administrative Settings

The screenshot shows the 'Administrative Settings' page. At the top, it says 'Please type path to targeting Image File Name or click "Browse" button.' Below this is a text field for 'Image File Name:' and a 'Browse...' button. A 'Upgrade Software' button is centered below. The next section contains instructions: 'To restore all settings to the factory defaults, please click "Defaults" button. To reboot system without resetting, click "Reboot" button. To get back to "Information Page", click "Back to Information Page" button.' Below these are 'Defaults' and 'Reboot' buttons. The form then has several input fields: 'Device Name' (Tr-AP-5a), 'User Name' (admin), 'Password' (masked with dots), and 'Confirm Password' (masked with dots). There are checkboxes for 'Extended Wireless Information' and 'Signal/Status LEDs', both of which are checked. A section titled 'SNMP Parameters' contains three input fields: 'Read Community' (public), 'SysContact' (Contact), and 'SysLocation' (Location). At the bottom are 'Apply' and 'Back to Information Page' buttons.

Image File Name

Enter the location of the Firmware update file, or use Browse to locate the file in your PC, and then press “Upgrade Software”

Defaults

Returns all settings to factory defaults.

Device Name

The network name of the device.

User Name

The access user name.

Password/Confirm Password

Enter the password for accessing the device

Ext. Info Enabled

Enable extended information. Extended information is only displayed with Tranzeo Wireless Technologies Access Points.

Signal / Status LEDs

Un-select to turn off the LEDs on the unit.

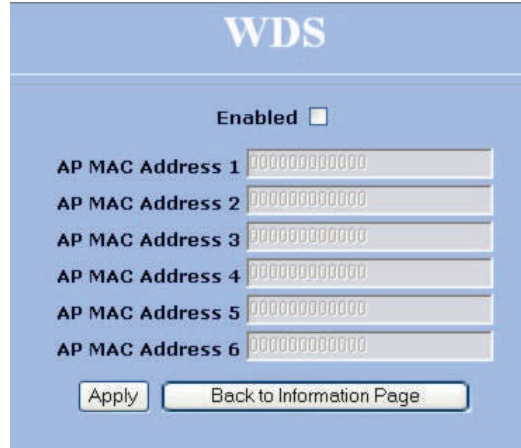
2 SNMP Parameters

Here you set the Read Community string and Contact / Location data. It is highly recommended that you change the SNMP Read Community string immediately to prevent unauthorized scanning of your network.

Version 2.0 supports MIB-II and the 80211 mib.

Note: The in and out values are in 64 bit values to accommodate the high amount of traffic that could pass through a backhaul link. This should not impact any monitoring program.

WDS



WDS (**Wireless Distribution System**) is a modification to the 802.11 spec that allows AP to communicate directly with each other. WDS allows users to spread out coverage to a larger area without the need for a backhaul link. The tradeoff is that overall throughput is greatly affected for all users of the AP's linked. WDS is not recommended for use with large numbers of clients, or in cases where throughput needs to be maximized. In cases where large numbers of users are involved, or maximum throughput is needed a dedicated PxP link should be used. However, in areas of low density WDS can allow an ISP to extend coverage into an area at very low cost.

Enabled

Select this box to enable WDS



HOW TO SET UP WDS

- ◆ Default the Unit to factory settings.
- ◆ Check the **Wireless Settings** of the APs.
- ◆ SSIDs can be different but the Channels **MUST** be the same
- ◆ Under the **WDS** settings add in the MAC address of the PEER. Unit A gets Unit B's address, Unit B gets Unit A's address. Do not insert colons or commas.
- ◆ Click 'Apply'
- ◆ Ping a station connected to the opposite end. It should reply.

Considerations for the Use of WDS

- 1) WDS Links do not appear in the station list or the performance tab. If you need to be able to monitor the link's strength and performance you should use PxP mode.
- 2) Throughput is cut by 50% per link.
- 3) WDS does not support WPA encryption.
- 4) All links need to be on the same channel.

Security Settings—Basic



The screenshot shows the 'Basic Security Settings' window with the 'WEP' tab selected. The 'Enabled' checkbox is unchecked. The 'Authentication' dropdown is set to 'Open'. The 'Key Length' dropdown is set to '64 bit'. The 'Default Key' dropdown is set to 'WEP Key 1'. There are four text input fields for keys, each containing the hexadecimal value '1234567890'. At the bottom are 'Apply' and 'Back to Information Page' buttons.

Enabled

Turn On WEP

Authentication

Select Open or Shared Key Authentication

Key Length

Level of Encryption. **NOTE:** 64 bit is referred to as 40 bit on some systems

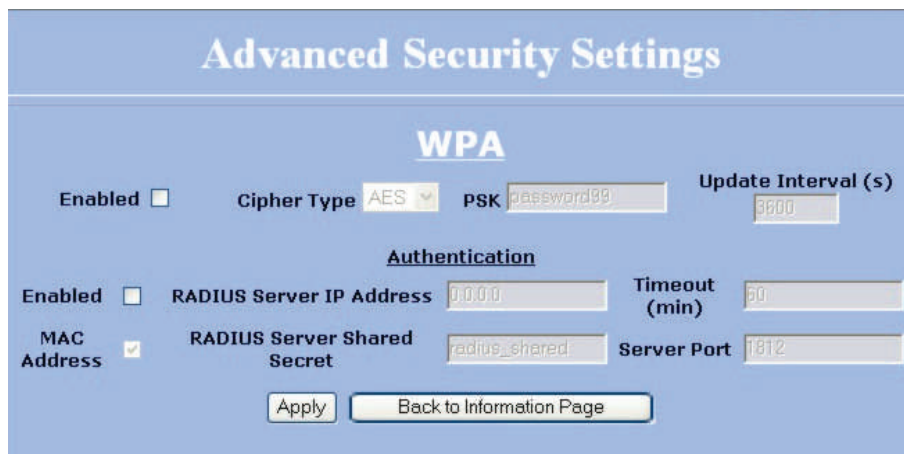
Default Key

Choose the default WEP key

Activate Keys

Enter your WEP keys. **NOTE:** Keys must be entered in HEX only.

Security Settings—Advanced



The screenshot shows the 'Advanced Security Settings' window with the 'WPA' tab selected. The 'Enabled' checkbox is unchecked. The 'Cipher Type' dropdown is set to 'AES'. The 'PSK' text field contains 'password99'. The 'Update Interval (s)' text field contains '3600'. Below this is the 'Authentication' section. The 'Enabled' checkbox is unchecked. The 'RADIUS Server IP Address' text field contains '0.0.0.0'. The 'Timeout (min)' text field contains '60'. The 'MAC Address' checkbox is checked. The 'RADIUS Server Shared Secret' text field contains 'radius_shared'. The 'Server Port' text field contains '1812'. At the bottom are 'Apply' and 'Back to Information Page' buttons.

Enabled

Turn On WPA

Cipher Type

Select the Level of Encryption. TKIP or AES

PSK

Enter your password

Update Interval

Enter the update interval

Enabled

Turn on 802.1x RADIUS Server Authentication

RADIUS Server IP Address

Enter the server IP

Timeout (min)

Enter the timeout period

RADIUS Server Shared Secret

Enter the name of the server

Server Port

Enter the port of the server

Access Control



Enable Access Control

Select this box to enable access control.

Associated Wireless Devices

Click any devices to disassociate them

Wireless Devices Available

Click any wireless device that should be associated with the AP

Associate With This Station Manually

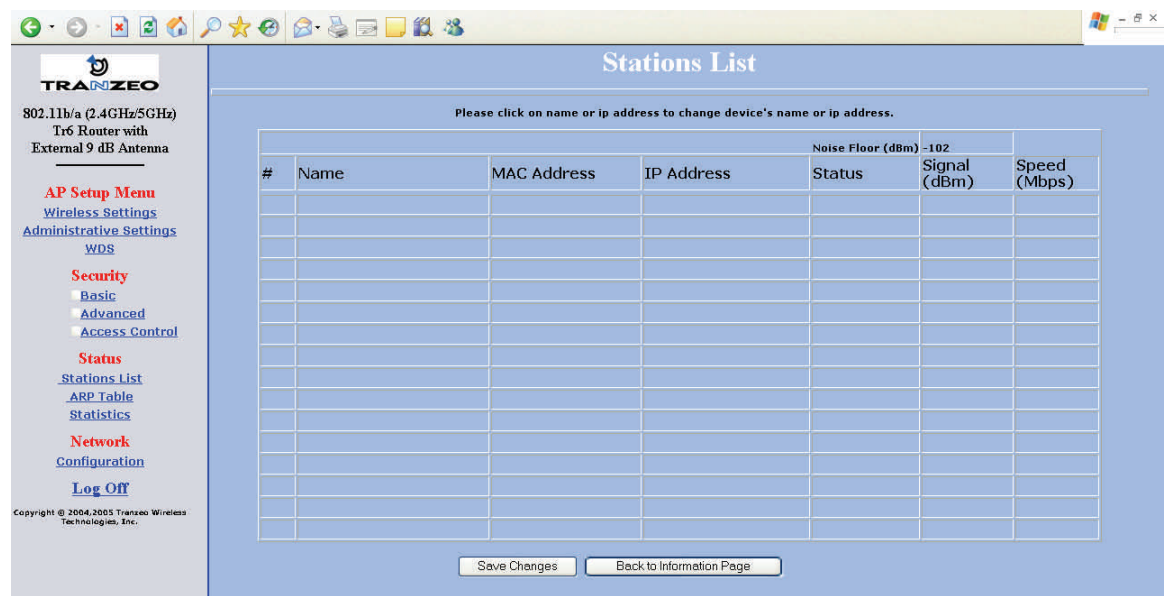
Enter the MAC address of a client and then click "add" to associate with it.

② Changes to Access Control

NOTE: If you are working via a radio link, the first MAC you should add is the address of the station you are connecting from. Otherwise, you will lock yourself out of the radio.

1. The Manually Authorize Stations section allows you to enter a long list of MAC address.
2. You can also select specific station that are already authorized and copy them to the Manually Authorize Stations box.
3. Data in the Manually Authorize Stations box can be copied to the clipboard to be pasted into another unit or a text file.
4. The Move button moves the MAC Address from Manually Authorize Stations to the Unauthorized list and vice versa.

Stations List (AP Mode Only)



This page displays a list of the stations associated with the AP and their connection statistics.

The first column is simply the order in which the stations are stored in the Station Table.

The second column is the name field. If the device is a Tranzeo 49, and it has the Extended Info option turned on in the Administrative Settings Window, then the device name will appear here. Otherwise, the field will be blank.

You can enter a name into the field by left clicking onto the field and typing the name in. This name will be retained. However, if the Extended Info is turned on at the client, the name will be overwritten with the name on the client.

The third column is the IP address. As with the name, if the client supplies it via the Extended Info option, it will appear. Otherwise you can manually enter it.

The fourth column in is the Status field.

The fifth column is the RF power in dBm as detected at the AP. This is one element of a strong link, the signal of the client end being another. Links should also be at least 10 dB higher than the receive sensitivity of the weakest element or the noise floor, whichever is higher, on both sides.

The sixth columns shows the radio speed of the link. Speed is based on both signal strength and the quality of the link. If the link is losing a lot of packets due to poor Fresnel zones or interference, the speed will be lower than the strength can support.

ARP Table

The screenshot shows a web browser window displaying the ARP Table configuration page of a Tranzeo Tr6 Router. The browser's address bar shows the URL `http://192.168.1.1`. The page has a blue header with the title "ARP Table". On the left side, there is a navigation menu with the following items: "AP Setup Menu", "Wireless Settings", "Administrative Settings", "WDS", "Security" (with sub-items "Basic", "Advanced", and "Access Control"), "Status" (with sub-items "Stations List", "ARP Table", and "Statistics"), "Network", "Configuration", and "Log Off". The main content area contains a table with three columns: "#", "MAC Address", and "IP Address". The table has 15 rows, with the first row containing the values "1", "00C09F668F0E", and "10.10.0.101". Below the table, there is a button labeled "Back to Information Page". The footer of the page contains the copyright notice: "Copyright © 2004-2005 Tranzeo Wireless Technologies, Inc."

#	MAC Address	IP Address
1	00C09F668F0E	10.10.0.101

② This feature was added as a troubleshooting screen. It shows the devices which have sent either a broadcast or directly tried to communicate with the device. Under normal circumstances, there should be a limited number of entries in this table, especially if you have interstation blocking turned on at the AP.

Network Configuration – Bridge Mode

Network Configuration

☒ Bridge ☐ Router

MTU(Kb) ☒ Default or 1.5

☒ Pinging

Allow ☒ Access to Web Server Port 80 Timeout 60

WAN

☒ Static ☐ DHCP Client ☐ IP Mode ☒ LAN DHCP Server

Copy DHCP parameters Release Probe

status

192.168.1.100 0.0.0.0 IP Address 192.168.100.1

255.255.255.0 0.0.0.0 Subnet Mask 255.255.255.0

192.168.1.1 0.0.0.0 gateway

0.0.0.0 0.0.0.0 DNS1

0.0.0.0 0.0.0.0 DNS2

Domain Name

Routing

☒ NAT ☐ QoS [Static Routes](#)

Ethernet (wired) Port A Speed (Mbs), Duplex AUTO

B AUTO

Apply Back to Information Page

This page allows you to control the network configuration of the device.

You can choose Static or DHCP Client IP configuration for the device.

Note: If you select DHCP, and a DHCP server is not present, the device will try to get an IP for up to 5 minutes. At the end on 5 minutes, it will fall back to a static IP. You can then locate it using the Locator Program and change it back to static.

You can also set the Ethernet Speed on this page.

Note: Many Ethernet devices do not auto-negotiate properly. If you see large numbers of dropped pings, you may be have collisions. Try locking the device at 10 / Half as a troubleshooting step. If the packet losses stop, step up to 100 / Half. If the device the radio is connecting can not support 100 / Half, you should replace the device or place a switch in line.

Network Configuration – Router Mode

Network Configuration

☐ Bridge ☒ Router

MTU(bytes) ☒ Default or 1500 (500-3000)

Allow ☒ Pinging

☒ Access to Web Server Port 80 Timeout 60

MAC Address ☐ Cloning into

WAN

☒ IP Mode ☐ Static ☐ DHCP Client ☐ PPPoE ☒ LAN DHCP Server

10.10.0.100 0.0.0.0 IP Address 192.168.100.1

255.0.0.0 0.0.0.0 Subnet Mask 255.255.255.0

10.0.0.2 0.0.0.0 gateway

0.0.0.0 0.0.0.0 DNS1

0.0.0.0 0.0.0.0 DNS2

Domain Name

Routing

☒ NAT ☐ QoS [Static Routes](#)

Port Management

☐ Port Filter ☐ Port Forwarding

Ethernet (wired) Port A Speed (Mbs), Duplex AUTO

B AUTO

Apply Back to Information Page

Please apply all changes first in order to visit the linked features.

You can choose Static, DHCP or PPPoE Client IP configuration for the device. Each of these options are explained on the following pages.

Note: If you select DHCP, and a DHCP server is not present, the device will try to get an IP for up to 5 minutes. At the end on 5 minutes, it will fall back to a static IP. You can then locate it using the Locator Program and change it back to static.

If you select a PPPoE client, and no PPPoE server can be found, you may be not be able to access the device from the WAN side. You will still be able to access it from the non-PPPoE interface.

You can also set the Ethernet Speed on this page.

Note: Many Ethernet devices do not auto-negotiate properly. If you see large numbers of dropped pings, you may be have collisions. Try locking the device at 10 / Half as a troubleshooting step. If the packet losses stop, step up to 100 / Half. If the device the radio is connecting can not support 100 / Half, you should replace the device or place a switch in line.

DHCP Server Configuration

DHCP Configuration

IP Parameters

Subnet Mask

255.255.255.0

Address Range

Starting Address

192.168.100.100

Number of Addresses

100

Gateway

☒ This Unit

☐ Other:

192.168.100.1

Lease Time

24

minutes

DNS

Server IP Address(s)

☒ WAN-Assigned

☐ Static: Primary

0.0.0.0

Secondary

0.0.0.0

Domain Name

☒ WAN-Assigned

☐ Static:

localdomain

WINS

☒ WAN-Assigned

☐ Static: Primary

0.0.0.0

Secondary

0.0.0.0

DHCP Clients

Apply

Back to Information Page

Subnet Mask	Subnet mask for the DHCP pool.		
Address Range			
Starting Address	The starting address of the DHCP pool.	The addresses are sequential starting with the Starting Address .	
Number of Addresses	The number of addresses you want to have in the DHCP pool		
Gateway	Select <i>This Unit</i> to use the gateway set on the WAN interface of the radio or select <i>Other</i> to set a different gateway address.		
DNS			
WAN-Assigned	Select to use the DNS server addresses as assigned on the WAN side.		
Static	Select to set DNS servers if different than those on the WAN side.	Note: If you select this option but leave the field blank or set to 0.0.0.0 the client will not get a DNS server value of 0.0.0.0. You must enter a value into this field to use a static DNS.	
Domain Name and WINS operate the same as DNS.			

Static Routing Setup Screen

IP Routing

System Routes

Interface	IP Address	Subnet Mask	Gateway	Metric
WAN	192.168.1.255	255.255.255.255	0.0.0.0	1
WAN	192.168.1.100	255.255.255.255	0.0.0.0	1
WAN	192.168.1.0	255.255.255.0	0.0.0.0	1

User Routes

Interface	IP Address	Subnet Mask	Gateway	Metric
Off	0.0.0.0	0.0.0.0	0.0.0.0	0
Off	0.0.0.0	0.0.0.0	0.0.0.0	0
Off	0.0.0.0	0.0.0.0	0.0.0.0	0
Off	0.0.0.0	0.0.0.0	0.0.0.0	0
Off	0.0.0.0	0.0.0.0	0.0.0.0	0
Off	0.0.0.0	0.0.0.0	0.0.0.0	0
Off	0.0.0.0	0.0.0.0	0.0.0.0	0
Off	0.0.0.0	0.0.0.0	0.0.0.0	0

Default Route

Select

Interface

Gateway

☒ System WAN

192.168.1.1

☐ User

WAN

0.0.0.0

Apply

Back to Information Page

Routing is an incredibly complex topic that is way beyond the scope of a QuickStart or Manual. This screen is intended for those users who have a strong understanding of IP Routing. Misconfiguration on this screen could result in serious network problems or even the loss of functionality.

Menu Options

Static Routes—Adds a new route to the IP routing table.

System Routes—This section shows the current routing table entries.

Interface—Specifies whether the entry will be enabled or disabled, and what interface it should use to transmit the packet.

IP Address—The IP address or network that the packets will be attempting to access

Subnet Mask—Used to specify which portion of the Destination IP signifies the network trying to be accessed and which part signifies the host that the packets will be routed to.

Note: 255.255.255.255 is used to signify only the host that was entered in the Destination IP field.

Gateway—Specifies the next hop to be taken if this route is used. A gateway of 0.0.0.0 implies there is no next hop, and the IP address matched is directly connected to the router on the interface specified:

Metric—The number of hops it will take to reach the Destination IP or network. A hop is considered to be traffic passing through a router from one network to another. If there is only one router between your network and the Destination network, then the Metric value would be 1.

Default Route—Allows the user to change the default route of the radio. **This option should be used with extreme caution.**

QOS

Quality of Service Configuration

Uplink Speed (Mbps):

Dynamic Fragmentation: ☒ Automatic Classification: ☒

Rules

#	enabled	Name	Protocol	Range	IP To	Range	Port To	Range	IP To	Range	Port To
0	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
1	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Menu Options

Uplink Speed (Mbps)

Sets the maximum total pipe size for this client. The order and traffic size is determined based on this value.

Dynamic Fragmentation Reduce delay for high-priority traffic and adaptive fragmentation where the fragmentation is determined by the uplink speed. This feature greatly improves the gaming and VOIP experience.

Automatic Classification

In vast majority of cases, this is all you need to select for best results. Applications such as VOIP, Gaming, etc are automatically given priority.



QOS RULES

If you chose to add you own rules, here are the various options:

Enabled	You must select enabled to turn the rule on
Priority	The lower the number, the higher it priority. 0 is the highest priority and 255 in lowest.
Name	The name here is for your reference only.
Protocol	Enter the IP Protocol Number Common options are: 0 for ANY, 1 for ICMP, 6 for TCP, and 17 for UDP. See Appendix A – IP Protocol numbers.
Source IP Range	Enter the range of the IP Addresses on the LAN side that the rule should apply to Enter 0.0.0.0 to apply the rule to all LAN IPs, otherwise enter the highest and lowest IP. For a single IP enter the same IP in both boxes
Source Port Range	Enter the range of the Ports on the LAN side that the rule should apply to. Enter 0 to apply the rule to all Ports. For a single port enter the same port in both boxes
Destination IP Range	Enter the range of the IP Addresses on the WAN side that the rule should apply to.
Destination Port Range	Enter the range of the Ports that on the WAN side the rule should apply To.

Cloning MAC

② This is a new feature. It allows the CPE to clone the MAC of the device behind it. This feature can be useful when dealing with some PPPoE and Radius Implementations. When the device is in Cloning MAC mode, it can only be managed from the LAN side of the device.

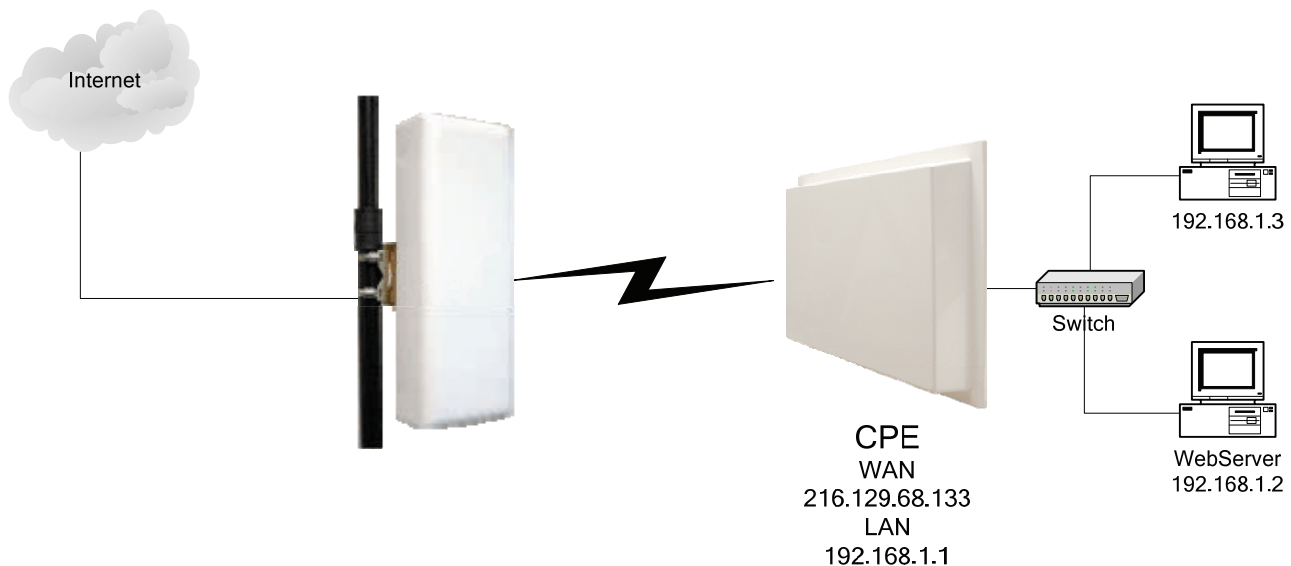
Port Management

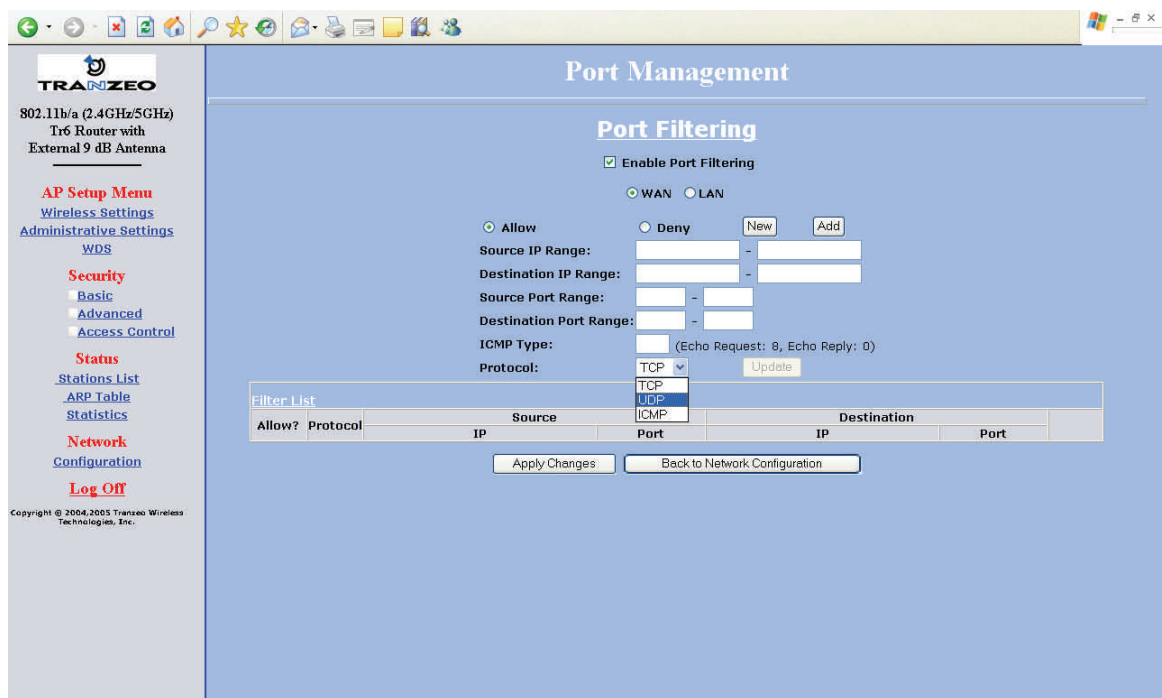
The screenshot shows a web-based configuration interface titled "Port Management". Under the "Port Forwarding" section, the "Enable Port Forwarding" checkbox is checked. There are two radio buttons for "Enabled" (selected) and "Disabled". Below these are input fields for "External Port:", "Internal Port:", and "Internal Address:". A "Protocol:" dropdown menu is set to "TCP". At the bottom, there is a table titled "Port Forwarding Rules" with columns: "Enabled?", "Protocol", "External Port", "Internal Port", and "Internal IP Address". The table contains one rule with "Enabled?" checked, "Protocol" as "TCP", "External Port" as "80", "Internal Port" as "80", and "Internal IP Address" as "192.168.1.2". There are "New" and "Update" buttons above the table. At the bottom of the interface are "Apply Changes" and "Back to Network Configuration" buttons.

② Port Forwarding

This is a new feature. It allows the radio to forward requests for certain ports to devices behind the router. For example, the customer has a webserver behind the Radio on a Private Ip that they want to have accessible to the world, then you can port forward all requests on Port 80 to 192.168.1.2.

Note: In order for this example to work, the management port of the radio would have to be changed from port 80 on the **Network Configuration** screen.





② Port Filtering

This is a new feature. It allows the radio to block requests for certain IP's or ports to and from devices behind the router. For example, if a customer wishes to block access to FTP from this network to the outside world, you would

1. Click **Add**
2. Select **Deny**
3. Select **Source IP Range**. Assuming that the clients are on 192.168.1.0/24, then the source IP would be 192.168.1.1 to 192.168.1.254
4. Select **Destination IP Range**. Assuming that the entire outside world was to be blocked, then 0.0.0.0 should be entered. 0.0.0.0 indicates all IP's
5. Select **Source Port Range**. In this case, enter 0 for all Ports
6. Ignore **ICMP type**. This field allows you to block certain types of ICMP as a prevention against port scanning and some viruses
7. Select the **Protocol**. In this case it would be TCP
8. You must click **Apply Changes** to save the rule

System Performance (CPE and PxP Modes only)

Performance

Associated Access Point Features

Name	IP Address	SSID	Channel	Status
TR6-Rt-2b	192.168.100.1	port	1	Associated

Link Details

Select Refresh Rate (seconds)

☐ Off ☒ 0.5 ☐ 1 ☐ 3 ☐ 5 ☐ 10 Sample

Receiving

	Noise (dBm)	Signal (dBm)
Lowest Level	-104	-81
Highest Level	-102	-75
Average Level	-103	-79

Transmission

Rate (Mbps/s)	Total	Packets Good (%)	Retried (%)
11			
5.5			
2			
1			
Total			

System

Select Refresh Rate (seconds)

☐ Off ☒ 0.5 ☐ 1 ☐ 3 ☐ 5 ☐ 10 Sample

	Net Pages	Memory (Bytes)	Stack (Bytes)
Total	502	34904	4096
Free	381 (75.9%)	13240 (37.9%)	3368 (82.2%)

Back to Information Page

Back to AP List Page

Select Refresh Rate

Each radio button represents a Refresh Rate. Many browsers do not allow infinite refreshes of a page through scripts, so this page may stop updating. If it does, simply change the Refresh rate to another value to restart the process.

Associated Access Point

Information about the access point is displayed here. Some items will only be displayed if the Access Point is a Tranzeo TR-49 series AP with the Extended Info turned on in the Administrative Settings Window.

2 Receiving

This box displays the current signal and the Lowest and Highest values. For the most accurate readings, data must be transmitted through the unit.

2 Transmission

This box displays the current signal traffic breakdown. For the most accurate readings, data must be transmitted through the unit. Beacons are always transmitted at the lowest possible rate. This screen only shows the values during the refresh rate. For more detailed statistics see the **Statistics** screen

2 System

This box displays the current Memory usage. It will fluctuate during normal usage. This data is mainly for the use of Tranzeo Wireless Technical Support.

Statistics

The Statistics Screen is divided into 3 main areas, UMAC*, LMAC* and Ethernet. For Radio Troubleshooting, the UMAC statistics are likely the most useful. The UMAC breaks down the statistics into Good and Bad Packets, whereas LMAC defines why the packets are bad.

The statistics are further divided into TX, RX and INT. TX and RX values are useful to ISPs and other users. The INT (Internal) stats are intended for use by Tranzeo Wireless Technical Support.

* Technical Info:

UMAC or Upper MAC functions occur in the Unit's Processor.

LMAC or Lower MAC functions occur in the Radio Chipset.

LMAC Statistics

Select Refresh Rate (s) ☒ 30 ☐ 45 ☐ 60

RX TX INT

Rate	Total	Good	Bad	Tries	RSSI
1 Mbps	1	1	0	1	0
2 Mbps	0	0	0	0	0
5 Mbps	0	0	0	0	0
11 Mbps	0	0	0	0	0
6 Mbps	0	0	0	0	0
9 Mbps	0	0	0	0	0
12 Mbps	0	0	0	0	0
18 Mbps	0	0	0	0	0
24 Mbps	0	0	0	0	0
36 Mbps	0	0	0	0	0
48 Mbps	0	0	0	0	0
54 Mbps	0	0	0	0	0
Tx Beacon	293	293	0	293	N/A

Rate	Bad Tries	Bad Underrun	Bad filtered	Beacon Rates
	Good at Series 1	Good at Series 2	Good at Series 3	Good at Series 4
	Tries at Series 1	Tries at Series 2	Tries at Series 3	Tries at Series 4

Please click on a rate to check the detailed statistics.

Back to Information Page

Back to Statistics Summary Page

You can click onto each speed level and see how the traffic breaks down. In the TX statistics, there should little to no **Tries at Series 2, 3 or 4**. The radio will try to send a packet 4 times at **Series 1**, and then tries the next series 4 times. In the RX stats, you should look for Bad CRC's and Bad Decrypts for signs of RF interference or Fresnel interference links.

Bad PHY's generally are caused when the radio is unable to decode the packets due to noise.

Note: Communication between APs and Stations always occurs at the lowest rate. In a normal link you should see a fair number of transactions at the lowest rate.

UMAC Statistics

Select Refresh Rate
(s)

☒ 10 ☐ 15 ☐ 20

		Previous Statistics	Life Statistics
Sample Period (in sec)		10.000	688.101
RX	Bytes	80	43.333 KB
	Packets	2	1108
	Clean Packets	2 (100.0%)	1035 (93.4%)
	Failed Packets	0 (0.0%)	73 (6.6%)
TX	Bytes	10154	685.875 KB
	Packets	99	6813
	Clean Packets	99 (100.0%)	6813 (100.0%)
	Retransmit Series 0	0 (0.0%)	0 (0.0%)
	Retransmit Series 1	0 (0.0%)	0 (0.0%)
	Retransmit Series 2	0 (0.0%)	0 (0.0%)
	Retransmit Series 3	0 (0.0%)	0 (0.0%)
	Total Failed Packets	0 (0.0%)	0 (0.0%)

[Back to Information Page](#)

[Back to Statistics Summary Page](#)

The failed packets should be 1% or less in a normal operating environment. In the TX statistics, there should little to no **Retransmits at Series 2, 3 or 4**. Life Statistics are reset on each reboot.

Ethernet Statistics

Select Refresh Rate (s)

☒ 30 ☐ 45 ☐ 60

		Ethernet 1	Ethernet 2
TX	Total	5	1
	Dropped by Software	0	0
	Dropped by Link	0	1
	Collision	0	0
	Late Collision	0	0
	Excessive Collision	0	0
RX	Total	7	0
	Dropped by HRT	0	0
	Dropped by DSR	0	0
	Dropped by Software	0	0
	Frames over 2048 bytes	0	0
	Frames over 1518 and less than 2048 bytes	0	0
	FCS Error	0	0
	Length Error	0	0
	Alignment Error	0	0

[Back to Information Page](#)

[Back to Statistics Summary Page](#)

In the Ethernet Statistics screen, excessive collisions are usually a sign that the radio and the device it is linked to are not on the same Duplex options. One is at full while the other is at half. Try locking both to the same values. Collisions do normally occur on an Ethernet network and are generally handled by the Carrier Sense Multiple Access with Collision Detect (CSMA/CD) mechanism.

Alignment, Length and Excessive FCS errors could the result of a Bad Radio Link, or a bad Ethernet cable.

APPENDIX A: Lightning Information

What is a proper Ground?

This antenna must be grounded to a proper Earth Ground.

According to the National Electrical Code Sections 810-15s and 810-21, the grounding conductor shall be connected to the NEAREST accessible locations of the following:

- a) The building / structure grounding electrode
- b) The grounded interior metal water piping system
- c) The power service accessible means external to enclosure
- d) The metallic power service raceway
- e) The service equipment enclosure
- f) The grounding electrode conductor

The important thing is to connect to ground at the nearest point.

Why is coiling the LMR or CAT5 bad?

The myth is that lightning follows the path of least resistance. It actually follows the path of least impedance. Coiling cables creates an air-wound transformer, which lowers the impedance. This means you are in fact making your radios a more appealing target for surges.

What standard does Tranzeo Wireless equipment meet?

This radio exceeds International Standard IEC 61000-4-5 when properly grounded. For a copy of the full testing report, see *Report Number TRL090904 - Tranzeo Surge Protection board* located on the Tranzeo website.

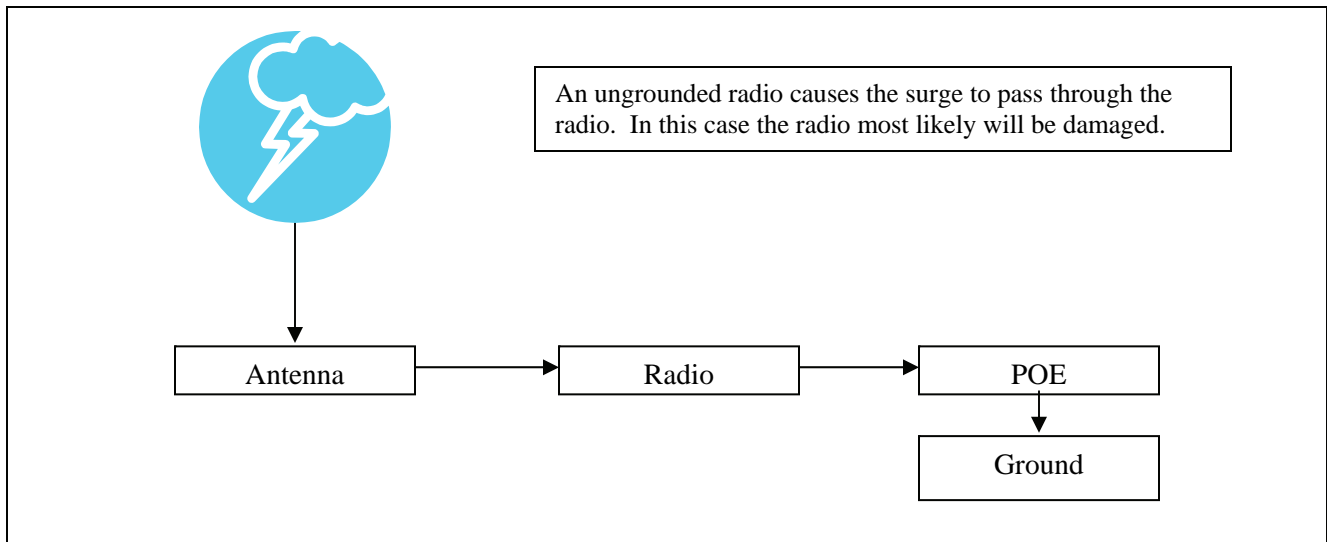
Is lightning damaged covered by the Warranty?

No. Lightning is not covered by the warranty. If you follow the instructions, your chances of lightning damage are greatly reduced, but nothing can protect a radio from a direct lightning strike.

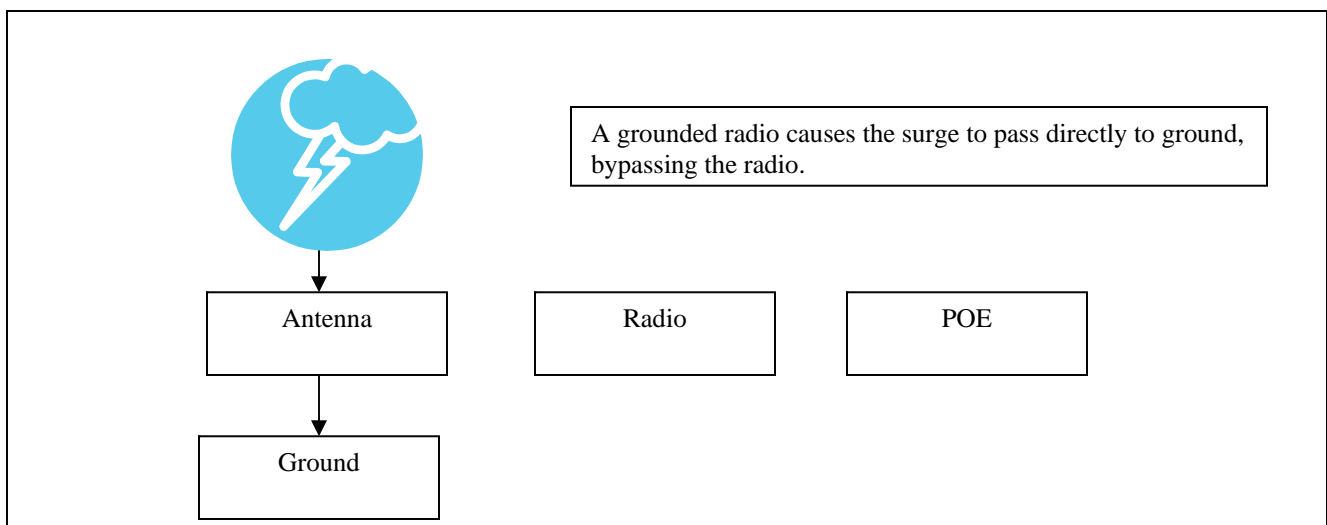
Where to Ground the device

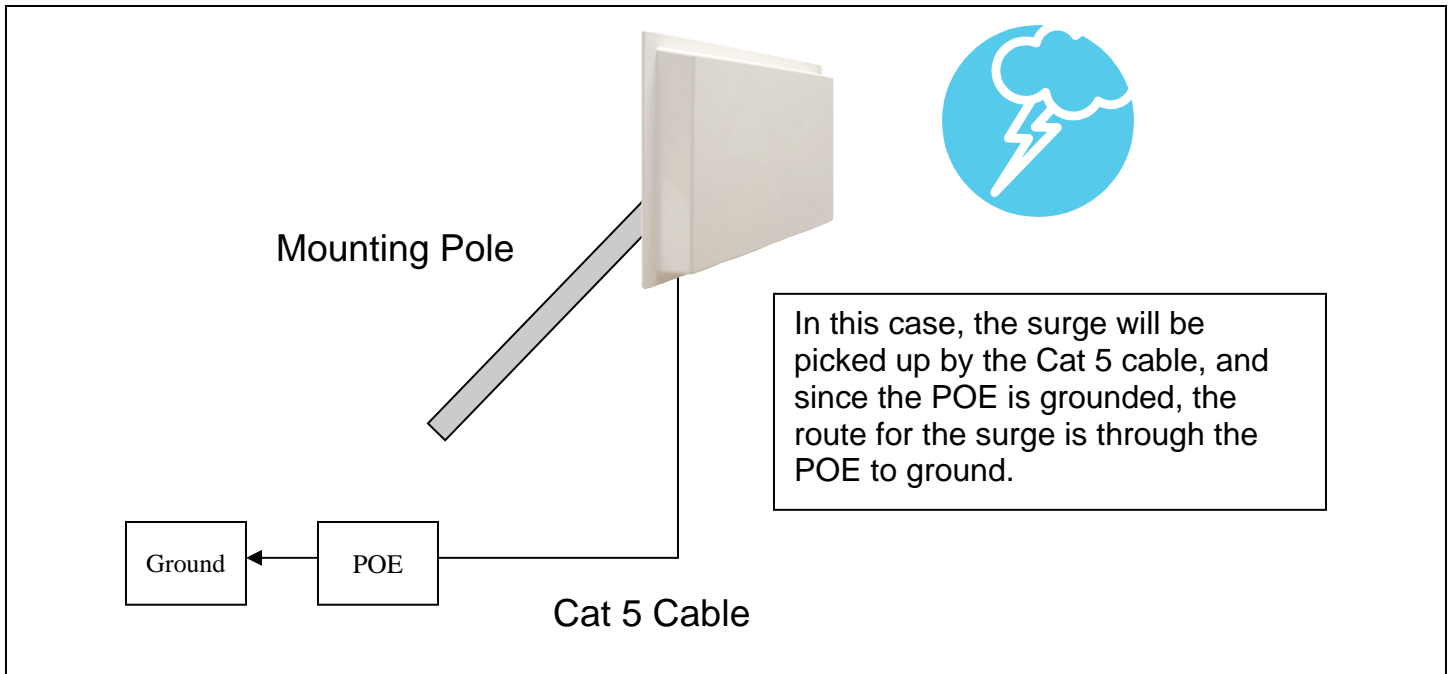
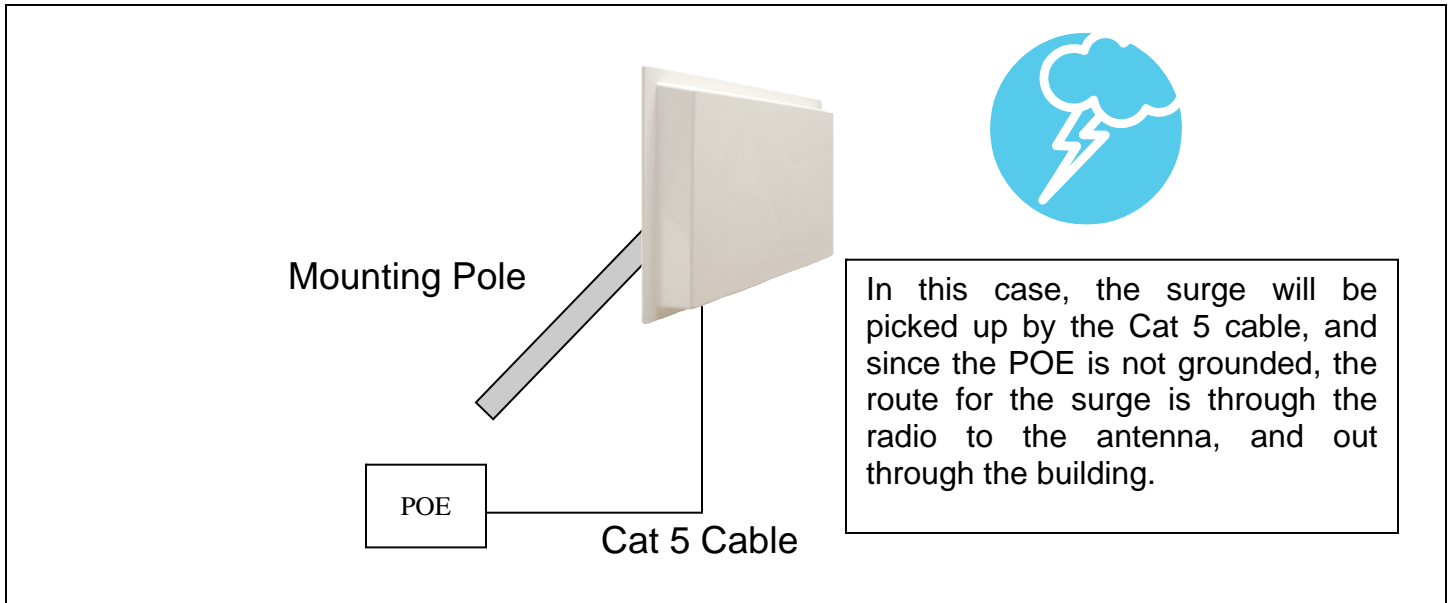
This radio must be grounded at the Pole **AND** at the POE. This is because the radio is between the Exterior Antenna and the POE ground. See the examples below

Ungrounded Radio



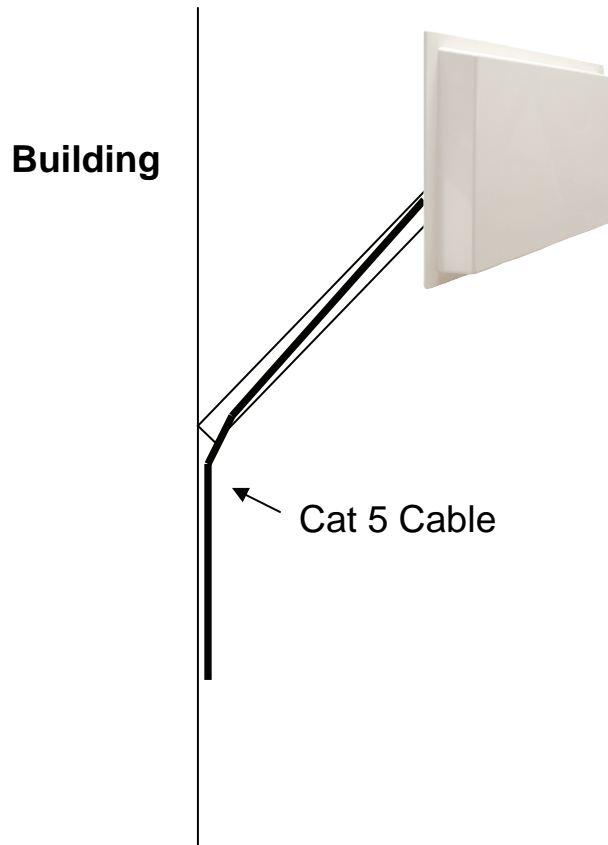
Grounded Radio





Best Practices

- 1) Always try to run the Cat5 and LMR inside of the mounting pole wherever possible. This helps to insulate the cable from any air surges.



- 2) Keep all runs as straight as possible. Never put a loop into the cables.
- 3) Test all grounds to ensure that you are using a proper Ground. If using a electrical socket for Ground, use a socket tester, such as Radio Shack 22-141
- 4) Buy a copy of the National Electrical Code Guide and follow it.
- 5) If you are in doubt about the grounding at the location, drive your own rod and bond it to the house ground. At least you will know that one rod is correct in the system.

APPENDIX B: QoS

QoS

Tranzeo Wireless Technologies' software takes full advantage of technology to ensure a consistently high quality on-line experience through the use of powerful Quality of Service (QoS) mechanisms. The key to making this applicable in a WISP environment is the Intelligent Stream Handling, a patent-pending algorithm which autonomously manages the flow of traffic going to the Internet, without the need for user configuration. As a result, real-time, interactive traffic, such as gaming, VoIP and video teleconferencing, are automatically given the appropriate priority when other users and applications use the connection. In addition, Intelligent Stream Handling minimizes the impact of large packet, lower priority traffic on latency-sensitive traffic and eliminates delays. Tranzeo Wireless Technologies' software effectively eliminates the lag and breakup problem in online gaming and other voice/video applications.

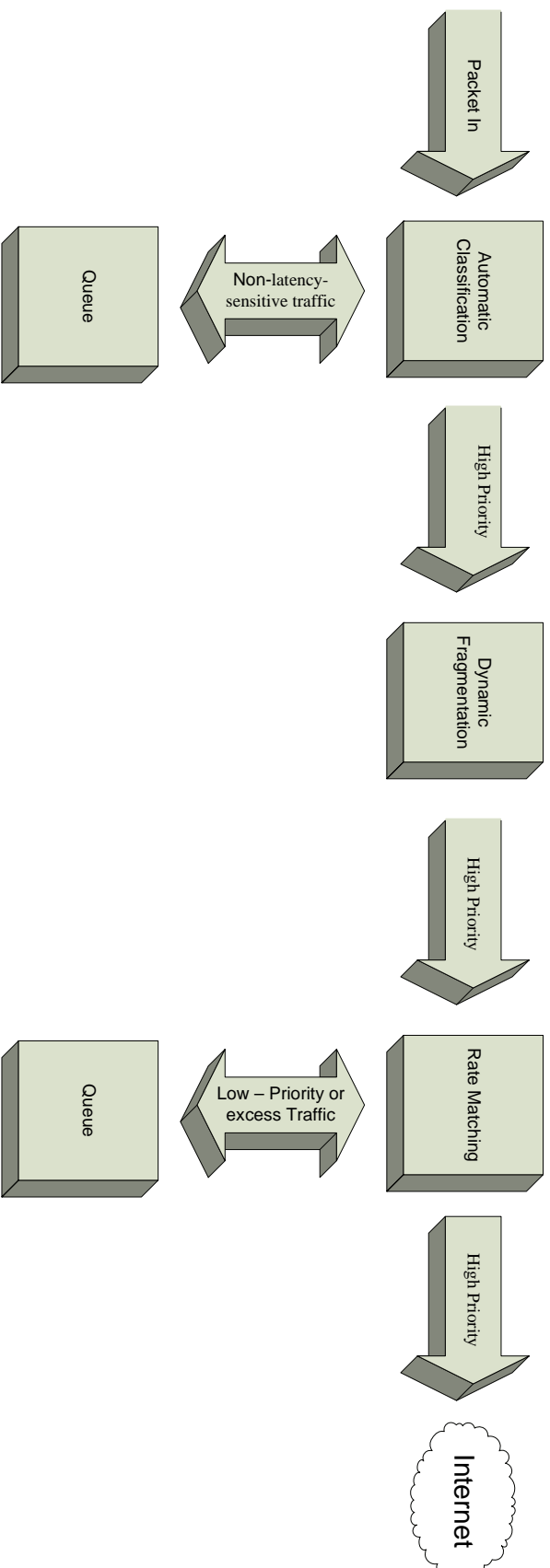
In today's broadband environment the impact of just one data stream running in parallel with a real-time application can be quite dramatic. Using NetIQ's Chariot VoIP test measurement over a connection, it can be demonstrated that introducing a single FTP transfer in the upstream direction will reduce the Mean Opinion Score (MOS) for a G.729 VoIP codec from a very good 4.4 to a completely unacceptable level of 1 immediately. Using the same scenario with Tranzeo Wireless Technologies' QoS enabled, the voice quality remains consistently high with an MOS of 4.4, and maintains that level even with multiple FTP streams.

- ◆ **Automatic Traffic Classification:** Tranzeo Wireless Technologies' software has the capability of continually monitoring and classifying traffic on the Internet connection, and dynamically adjusting the way individual streams are handled at any point in time. This enables latency-sensitive traffic, such as voice, games or even web page requests, to be given a relatively high priority. As a result, these packets are sent to their destination first, reducing delay and jitter. Less time-sensitive traffic such as email or file transfers are sent at lower priority. Since Intelligent Stream Handling operates automatically without the need for user configuration, it is able to effectively make use of 255 priority levels for fine-grained control of the packet streams.
- ◆ **Rate Matching:** A process called "rate matching" determines the bandwidth of the broadband uplink automatically so that it can shape the traffic to smooth the flow between the router and the Internet. This eliminates the potential bottlenecks and delays that can be caused by "bursty" data traffic.
- ◆ **Dynamic and Adaptive Link Fragmentation:** Low priority traffic is also fragmented to reduce the latency and jitter that can be introduced by long packets. Intelligent Stream Handling adjusts the fragment size based on the uplink speed and also stops fragmenting long packets when no latency-sensitive traffic is waiting to be sent, to improve the overall efficiency of the broadband link and ensure voice can sustain a high MOS rating.

Tranzeo's software has the capability of continually monitoring and classifying traffic on the Internet connection, and dynamically adjusting the way individual streams are handled at any point in time. This enables latency-sensitive traffic, such as voice, games or even web page requests, to be given a relatively high priority. As a result, they are sent to their destination first, reducing delay and jitter. Less time-sensitive traffic such as email or file transfers are de-prioritized.

Intelligent Stream Handling adjusts the fragment size based on the uplink speed and also stops fragmenting long packets when no latency-sensitive traffic is waiting to be sent, to improve the overall efficiency of the broadband link and ensure voice can sustain a high MOS* rating.

A process called "rate matching" determines the bandwidth of the broadband uplink automatically so that it can shape the traffic to smooth the flow between the router and the Internet. This eliminates the potential bottlenecks and delays that can be caused by "bursty" data traffic.



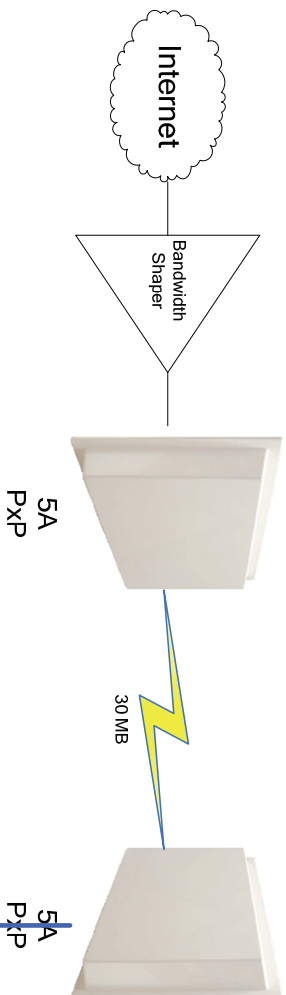
Tranzeo Wireless Technologies

QoS Block Diagram

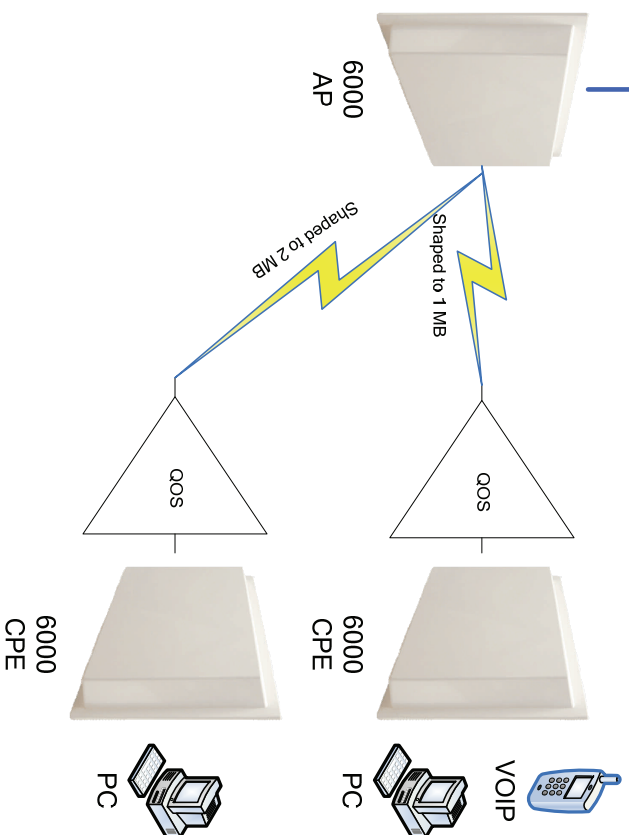
1/13/2006

*Mean Opinion Score (MOS)

In this case, the head end shaper is limiting the incoming demand based on the end user to ensure no one user is taking the entire downstream.



In this case, no one user is ever able to draw more than their fair share of the available up stream bandwidth, even if the communication is between two stations on the same AP.



Decimal	Keyword	Protocol
=====	=====	=====
0	HOPOPT	IPv6 Hop-by-Hop Option
1	ICMP	Internet Control Message
2	IGMP	Internet Group Management
3	GGP	Gateway-to-Gateway
4	IP	IP in IP (encapsulation)
5	ST	Stream
6	TCP	Transmission Control
7	CBT	CBT
8	EGP	Exterior Gateway Protocol
9	IGP	private interior gateway
10	BRM	BBN RCC Monitoring
11	NVP-II	Network Voice Protocol
12	PUP	PUP
13	ARGUS	ARGUS
14	EMCON	EMCON
15	XNET	Cross Net Debugger
16	CHAOS	Chaos
17	UDP	User Datagram
18	MUX	Multiplexing
19	DCN-MEAS	DCN Measurement
20	HMP	Host Monitoring
21	PRM	Packet Radio Measurement
22	XNS-IDP	XEROX NS IDP
23	TRUNK-1	Trunk-1
24	TRUNK-2	Trunk-2
25	LEAF-1	Leaf-1
26	LEAF-2	Leaf-2
27	RDP	Reliable Data Protocol
28	IRTP	Internet Reliable Transaction
29	ISO-TP4	ISO Transport Class 4
30	NETBLT	Bulk Data Transfer
31	MFE-NSP	MFE Network Services
32	MERIT-INP	MERIT Internodal Protocol
33	SEP	Sequential Exchange
34	3PC	Third Party Connect
35	IDPR	Inter-Domain Policy Routing Protocol
36	XTP	XTP
37	DDP	Datagram Delivery
38	IDPR-CMTP	IDPR Control Message Transport Proto
39	TP++	TP++ Transport Protocol
40	IL	IL Transport Protocol
41	IPv6	Ipv6
42	SDRP	Source Demand Routing
43	IPv6-Route	Routing Header for IPv6
44	IPv6-Frag	Fragment Header for IPv6
45	IDRP	Inter-Domain Routing
46	RSVP	Reservation Protocol
47	GRE	General Routing Encapsulation
62	MHRP	Mobile Host Routing Protocol
49	BNA	BNA
50	ESP	Encap Security Payload for IPv6
51	AH	Authentication Header for IPv6
52	I-NLSP	Integrated Net Layer Security
53	SWIPE	IP with Encryption
54	NARP	NBMA Address Resolution
55	MOBILE	IP Mobility

Decimal	Keyword	Protocol
=====	=====	=====
56	TLSP	Transport Layer Security using Kryptonet key management
57	SKIP	SKIP
58	IPv6-ICMP	ICMP for IPv6
59	IPv6-NoNxt	No Next Header for IPv6
60	IPv6-Opts	Destination Options for IPv6
61		any host internal protocol
62	CFTP	CFTP
63		any local network
64	SAT-EXPAK	SATNET and Backroom EXPAK
65	KRYPTOLAN	Kryptolan
66	RVD	MIT Remote Virtual Disk
67	IPPC	Internet Pluribus Packet Core
68		any distributed file system
69	SAT-MON	SATNET Monitoring
70	VISA	VISA Protocol
71	IPCV	Internet Packet Core Utility
72	CPNX	Computer Protocol Network Executive
73	CPHB	Computer Protocol Heart Beat
74	WSN	Wang Span Network
75	PVP	Packet Video Protocol
76	BR-SAT-MON	Backroom SATNET Monitoring
77	SUN-ND	SUN ND PROTOCOL-Temporary
78	WB-MON	WIDEBAND Monitoring
79	WB-EXPAK	WIDEBAND EXPAK
80	ISO-IP	ISO Internet Protocol
81	VMTP	VMTP
82	SECURE-VMTP	SECURE-VMTP
83	VINES	VINES
84	TTP	TTPord Protocol
85	NSFNET-IGP	NSFNET-IGP
86	DGP	Dissimilar Gateway Protocol
87	TCF	TCF
88	EIGRP	EIGRP
89	OSPFIGP	OSPFIGP
90	Sprite-RPC	Sprite RPC Protocol
91	LARP	Locus Address Resolution
92	MTP	Multicast Transport Protocol
93	AX.25	AX.25 Frames
94	IPIP	P-within-IP Encapsulation
95	MICP	Mobile Internetworking Control
96	SCC-SP	Semaphore Communications Sec.
97	ETHERIP	Ethernet-within-IP Encapsulation
98	ENCAP	Encapsulation Header
99		any private encryption scheme
100	GMTP	GMTP
101	IFMP	Ipsilon Flow Management
102	PNNI	PNNI over IP
103	PIM	Protocol Independent Multicast
104	ARIS	ARIS
105	SCPS	SCPS
106	QNX	QNX
107	A/N	Active Networks
108	IPComp	IP Payload Compression
109	SNP	Sitara Networks Protocol

108	IPComp	IP Payload Compression
109	SNP	Sitara Networks Protocol
110	Compaq-Peer	Compaq Peer Protocol
112	VRRP	Virtual Router Redundancy
113	PGM	PGM Reliable Transport
114		any 0-hop protocol
115	L2TP	Layer Two Tunneling Protocol
116	DDX	D-II Data Exchange (DDX)
117	IATP	Interactive Agent Transfer
118	STP	Schedule Transfer Protocol
119	SRP	SpectraLink Radio Protocol
120	UTI	UTI
121	SMP	Simple Message Protocol
122	SM	SM
123	PTP	Performance Transparency
124	ISIS	ISIS over IPv4
125	FIRE	
126	CRTP	Combat Radio Transport
127	CRUDP	Combat Radio User Datagram
128	SSCOPMCE	
129	IPLT	
130	SPS	Secure Packet Shield
131	PIPE	Private IP Encapsulation within IP
132	SCTP	Stream Control Transmission
133	FC	Fibre Channel
134-254		Unassigned
255		Reserved

APPENDIX D: Common TCP Ports

See <http://www.iana.org/assignments/port-numbers> for a full list of Well Known Port Numbers.

Keyword	Port	Description
=====	=====	=====
ECHO	7	Echo
SYSTAT	11	Active Users
QOTD	17	Quote of the day
MSP	18	Message Send Protocol
FTP-DATA	20	File Transfer (Data Channel)
FTP	21	File Transfer (Control)
TELNET	23	Telnet
SMTP	25	Simple Mail Transfer
NAME	42	TCP Nameserver
BOOTPS	67	Bootstrap Protocol Server
BOOTPC	68	Bootstrap Protocol Client
TFTP	69	Trivial File Transfer
WWW	80	World Wide Web
KERBEROS	88	Kerberos
POP3	110	TCP post office
NNTP	119	USENET
NFS	2049	Network File System
SIP	5060, 5061	SIP