TRANZEO TR-900

TRANZEO
WIRELESS TECHNOLOGIES INC.

# Tranzeo TR-900 Series
# User Guide

Revision: 1.1
Firmware: 2.0.18
Date: 16/04/07

## Document Revisions:

| | |
|---|---|
| Version 1.0 | August 31, 2006 |
| Version 1.1 | April 16, 2007 |


## Tranzeo Wireless Technologies Inc.

19473 Fraser Way
Pitt Meadows, BC
Canada V3Y 2V4

Toll Free Number: 1.866.872.6936
Technical Support: 1.888.460.6366
Local Number: 1.604.460.6002
Fax Number: 1.604.460.6005

General Inquiries: info@tranzeo.com
Sales: sales@tranzeo.com
Technical Support: support@tranzeo.com

# Safety Information

## FCC Compliance

This device 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 device is operated in a residential environment. This device generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the user guide, may cause harmful interference to radio communication. In case of harmful interference, the users will be required to correct the interference at their own expense.

The users should not modify or change this device without written approval from Tranzeo Wireless. Modification will void warranty and authority to use the device.

For safety reasons, people should not work in a situation where RF exposure limits could be exceeded. To prevent this situation, the users should consider the following rules:

- Install the antenna so that there is a minimum of 33.5 cm (13.19 in) of distance between the antenna and people.
- Do not turn on power to the device while installing the antenna.
- Do not connect the antenna while the device is in operation.
- Do not collocate or operate the antenna used with the device in conjunction with any other antenna or transmitter.
- Use this product only with the following Tranzeo antennas of the same or lower gain:

  12 dBi Omni – TR-OD900-12
  14 dBi Sector – TR-900V-90-14

- In order to ensure compliance with local regulations, the installer MUST enter the antenna gain at the time of installation. See *Chapter 3: Wireless Settings*, for details.

## Industry Canada Compliance

Operation of this device is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

## Safety Instructions

You must read and understand the following safety instructions before installing the device:

- This antenna's grounding system must be installed according to Articles 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's 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 Power over Ethernet (POE) adapter only with approved Tranzeo models.
- Never install radio equipment, surge suppressors or lightning protection during a storm.

## Lightning Protection

The key to lightning protection is to provide 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 local and national electrical codes or contact an electrician or professional trained in the design of grounding systems.

## Professional Installation Required

The product requires professional installation. Professional installers ensure that the equipment is installed following local regulations and safety codes.

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

# Table of Contents

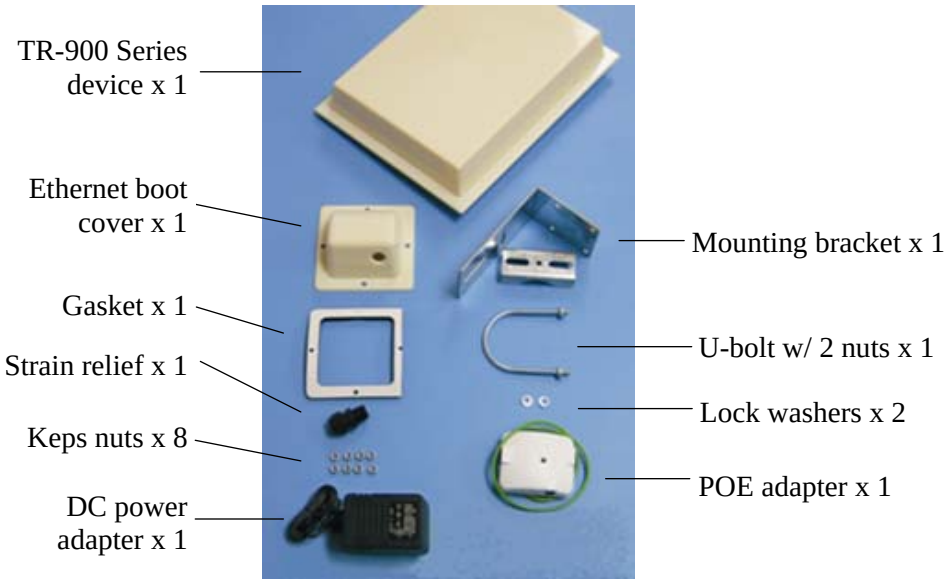
# Chapter 1: Overview

## Introduction

This next-generation wireless LAN device–the Tranzeo TR-900 series– brings Ethernet-like performance to the wireless realm. Fully compliant with the IEEE802.11a standard, the TR-900 series also provides powerful features such as the Internet-based configuration utility as well as WEP and WPA security.

## Product Kit

The TR-900 Series product kit contains the items shown below. If any item is missing or damaged, contact your local dealer for support.




## Product Description

The LEDs, ports and product information are located at the back of the TR-900 Series radio, as shown in the picture.

## LED Panel Indicators

| Label | Color | Indicators |
|---|---|---|
| **Power** | Red | **On:** Powered on<br>**Off:** No power |
| **LAN** | Green | **On:** Ethernet link<br>**Flashing:** Ethernet traffic<br>**Off:** No Ethernet link |
| **Radio** | Amber | **On:** Radio link<br>**Flashing:** Radio activity<br>**Off:** No radio link |
| **Signal (CPE Mode)** | Red | In CPE mode (Client Premises Equipment), light up in sequence to indicate signal strength. |
| | Amber | |
| | Green | |

| Label | Color | Indicators |
|---|---|---|
| **Signal (AP Mode)** | Red | **On:** WEP/128 enabled<br>**Flashing:** WEP/64 enabled<br>**Off:** WEP off |
| | Amber | **On:** WPA/AES enabled<br>**Flashing:** WPA/TKIP enabled<br>**Off:** WPA off |
| | Amber | **Flashing:** AP Mode |
| | Green | **On:** ACL enabled<br>**Off:** ACL off |
| | Green | **On:** WDS enabled<br>**Off:** WDS off |

# Chapter 2: Hardware Installation

The TR-900 Series radios are easy to install, as you'll see in this chapter. Before starting, you will need to get the tools listed below and decide about the site and orientation of the device. Once ready, follow the instructions about how to install the Ethernet cable, mount the device, ground the antenna, and make the connections in order to get a proper installation.

## Getting Ready

### Tools Required

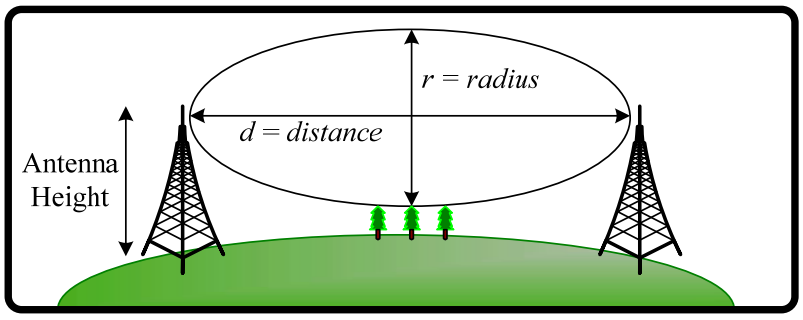
To install your TR-900 Series radio you will need the following tools:

- 1/2" wrench x 1
- 3/8" wrench x 1
- Cat 5 cable stripper x 1
- Cat 5 cable (to connect the radio to the POE adapter)
- RJ-45 patch cable
- RJ-45 crimper x 1
- RJ-45 connectors x 4
- #6 green grounding wire

### Site Selection

Determine the location of the radio before installation. Proper placement of the device 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. The line-of-sight is an ellipse, called Fresnel zone. This zone should be clear of obstacles since obstructions will impede performance of the device.




Fresnel zone

### Polarity

Determine if the antenna's polarization will be horizontal or vertical before installation. The TR-900 radios can be used in either polarity. The Ethernet boot cover should always be placed so that the cable runs toward the ground for maximum environmental protection.

### Power Supply

Only use a power adapter approved for use with the TR-900 Series radio. Otherwise, the product may be damaged and will not be covered by the Tranzeo warranty.

## Installing the Ethernet Cable

*Step 1:*

Insert the strain reliefinto the port opening of the boot cover.

*Step 2:*

Using a 3/4” wrench, tighten the strain relief until it touches the boot cover**.**

IMPORTANT! Use hand tools only. Do not over tighten.

*Step 3:*

Put the cap nut back over the strain relief and insert the Cat 5 cable through it. Wire the cable following the EIA/TIA T568B standard, and attach the RJ-45 connectors to each end of the cable. (See *Appendix F: Wiring Standard*).

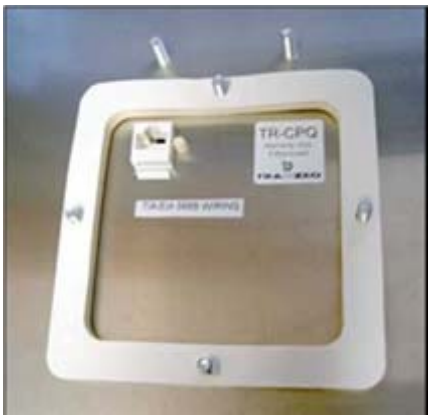
*Step 4:*

If you purchased the device with a dual port cover, repeat steps 1, 2, and 3 for the second port.

IMPORTANT! If you are not going to use the second port, insert the strain relief into the boot cover and tighten the cap nut to ensure a weather-tight seal, as shown in the picture.

*Step 5:*

Place the gasket—with the adhesive side facing up—over the 4 studs around the port of the radio. Flatten the gasket ensuring there are no gaps. Remove the backing.



*Step 6:*

Plug the Cat 5 cable inserted in the boot cover into the port. Remember to place the boot cover according to the desired polarization, so that the strain relief faces the ground.

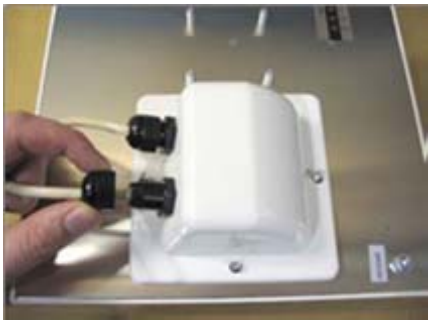
*Step 7:*

Fit the boot cover over the 4 studs and the gasket. Secure with 4 keps nuts. Tighten with a 3/8” wrench until the gasket is at least 50% compressed.

*Step 8:*

Make sure the cap nut of the strain relief is tightened properly to ensure a weather-proof seal.

IMPORTANT! Hand tighten only. Do not over tighten as you may damage the weather-tight seal of the strain relief.



## Mounting the Radio

*Step 9:*

Attach the mounting bracket to the pole using the U-bolt. Secure the U-bolt with the lock washers and the nuts. Align if necessary, and then tighten the nuts enough to prevent any movement.

*Step 10:*

Fit the radio to the mounting bracket. Secure the radio with keps nuts.

IMPORTANT! The strain relief must be always facing the ground.

## Grounding the Antenna

*Step 11:*

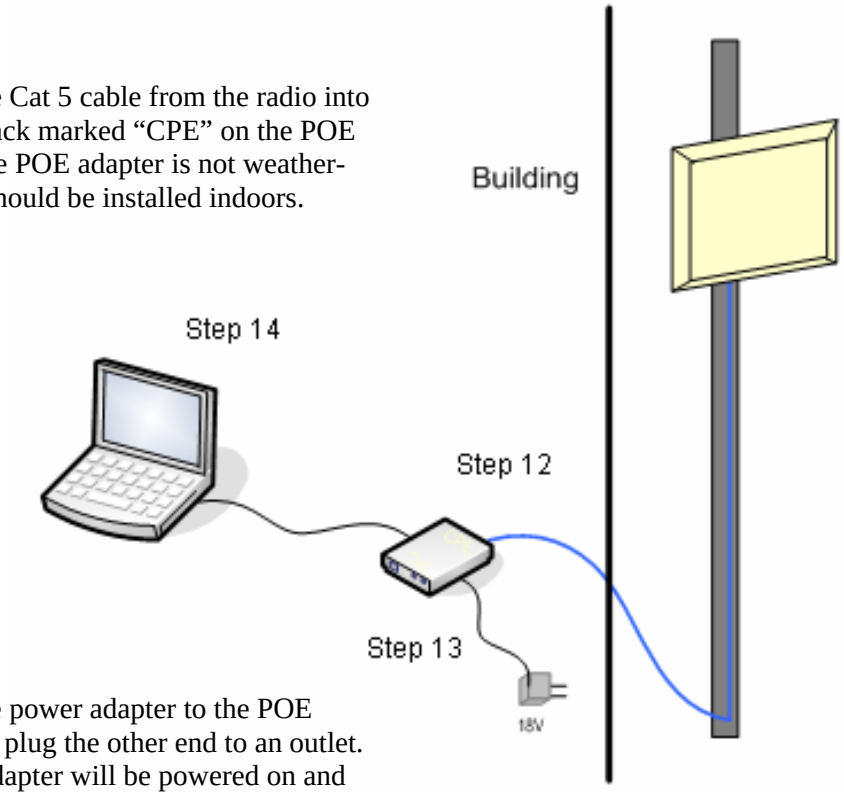
Using a #6 green grounding wire, connect the grounding lug on the radio to a proper ground. See Appendix A: Grounding and Lighting Protection Information.

IMPORTANT: This device must be grounded. Connect the green grounding wire to a known good earth ground, as outlined in the National Electrical Code. See *Appendix A: Grounding and Lightning Protection Information* for details.

## Connecting the Radio

*Step 12:*

Connect the Cat 5 cable from the radio into the RJ-45 jack marked “CPE” on the POE adapter. The POE adapter is not weather-proof and should be installed indoors.




*Step 13:*

Connect the power adapter to the POE adapter and plug the other end to an outlet. The POE adapter will be powered on and the power indicator on the top panel will turn on. We recommend to connect the power adapter to an outlet with surge suppression capability with an uninterrupted power supply (UPS) for reduced outages.

IMPORTANT! Use the power adapter supplied with the radio. Otherwise, it may be damaged.

*Step 14:*

To configure the TR-900 Series radio, connect the Ethernet cable to the POE adapter and to a computer. Ensure that the distance between the computer and the radio does not exceed 300 ft (90 m).

Note: If connecting to a hub or switch, a crossover cable may be required.

## Best Practices

Follow these practices to ensure a correct installation and grounding.

- Always try to run long Cat 5 and LMR cables inside of the mounting pole. This helps to insulate the cable from any air surges.
- Keep all runs as straight as possible. Never put a loop into the cables.
- Test all grounds to ensure that you are using a proper ground. If using an electrical socket for ground, use a socket tester, such as Radio Shack 22-141.
- Keep a copy of the National Electrical Code Guide at hand and follow its recommendations.
- 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.

# Chapter 3: Configuration

The TR-900 Series radios can be configured through an HTML configuration interface, accessible using any Internet browser. The configuration interface allows you to define and change settings, and also shows information about the performance of the device.

In this chapter we'll cover how to access the configuration interface, configure the TR-900 Series radio, and interpret the information displayed in the interface.

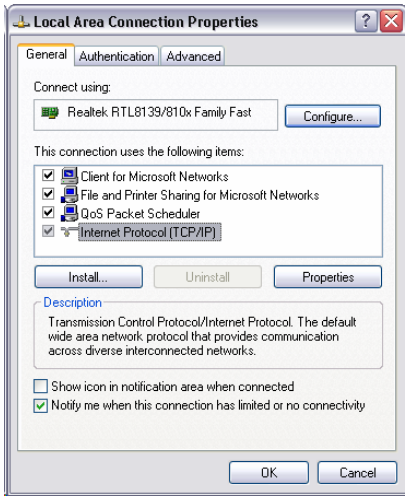
Depending on whether the device is defined as an AP or CPE (infrastructure station), some menu options, windows, and fields in the interface may vary or may not appear at all. We'll indicate so when describing each window.

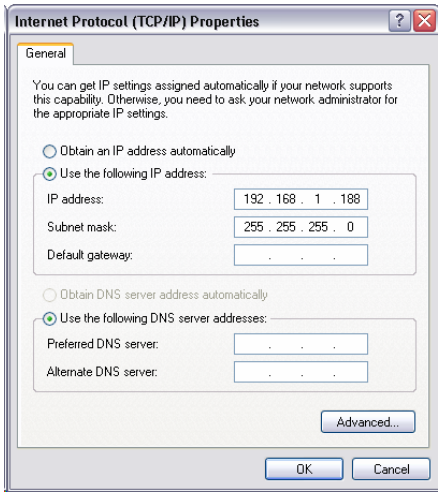
## Connecting to the Radio

Before accessing the configuration interface, you have to change the network connection settings in your computer to be on the same subnet as the radio.

### Changing the IP Address - Windows XP

1. In your computer, open Control Panel > Network Connections > Local Area Connection.
2. In Local Area Connection Status > General, click **Properties**.
3. In Local Area Connection Properties > General, select **Internet Protocol (TCP/IP)** and click **Properties**.
4. In Internet Protocol (TCP/IP) Properties > General, select **Use the following IP address**.
5. Enter your **IP address** and **Subnet Mask**. The default IP address of the radio is **192.168.1.100**, which cannot be used here.
6. Click **OK** and **Close**.

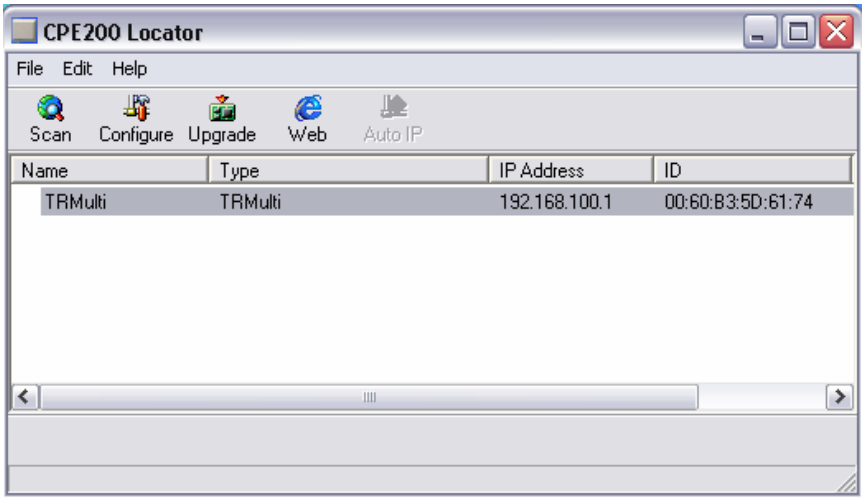


### Changing the IP Address Using the Tranzeo Locator

The Tranzeo Locator is a utility that allows users to quickly change the IP address of the Tranzeo radios. It sends out a broadcast on the network and displays a list of other Tranzeo radios connected, from which you can configure the IP address for your device.

Note: The Locator cannot locate radios through routers.




The Tranzeo Locator displays the following options:

| | |
|---|---|
| **Scan:** | Locates Tranzeo radios connected to the network. A yellow icon appears before the name when the radio is not in the same subnet. |
| **Configure:** | Used to set a static IP address or set the radio into DHCP mode. |
| **Upgrade:** | Under development. |
| **Web:** | Opens a browser to access the configuration interface. |
| **Auto IP:** | To automatically set the radio to an IP address one number higher than the IP address of the computer. |

Find the latest version of the Tranzeo Locator at www.tranzeo.com, under Tranzeo Support > Support Files > Radio Utilities.

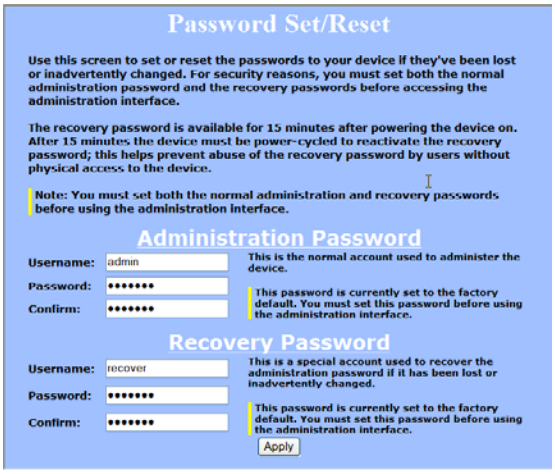
## Login into the Configuration Interface

After defining the network settings, follow these steps to login into the Tranzeo Configuration Interface.

1. Open your Internet browser (Internet Explorer, Netscape, or Firefox).
2. In the address bar, type your IP address (default IP: **http://192.168.1.100**).
3. In the login dialog, enter your **Username** and **Password** (if you're a first-time user, follow the instructions below).
4. Click **OK**. You will then access the configuration interface.


If you're a first-time user:

1. Enter the default username **admin** and the default password **default**.
2. In the Password Set/Reset window, change the **Administration** and **Recovery*** **passwords**. They cannot be left as default and must be different from each other. You can change the usernames too.
3. Click **Apply** to save the changes.
4. You will be prompted to enter your new username and password in the login dialog. You will then access the configuration interface.




* The recovery username and password are used to access the Password Set/Reset window if the administration password is lost.

## Information Page

This is the first window of the configuration interface. It shows the main menu and information about the device settings, like wireless, network, and security settings.

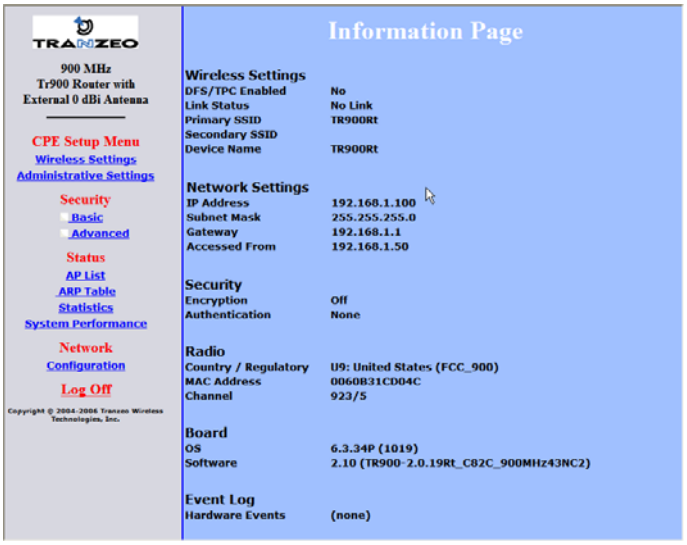
The menu is divided in four sections:

- Setup Menu
- Security
- Status
- Network

Each section contains navigation links to the configuration windows, some of which may be different for access points and CPEs.

Information Page - AP


Information Page - CPE

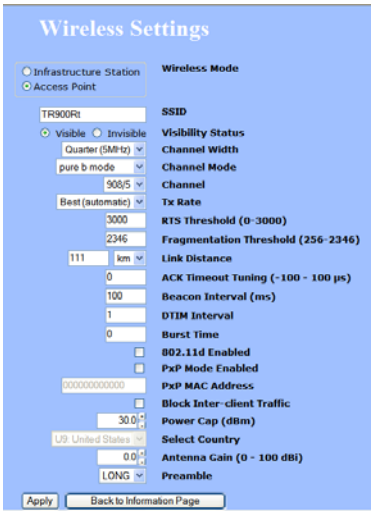


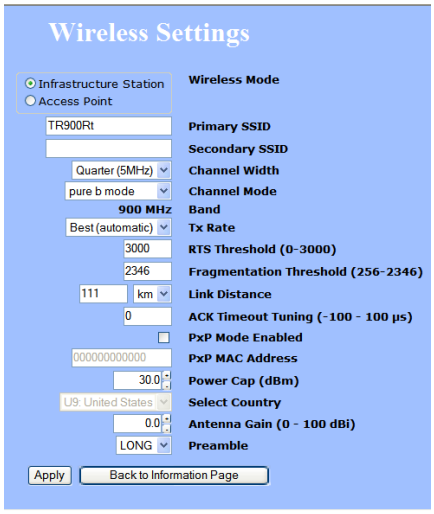
## Setup Menu

In this section you would be able to configure wireless and administrative settings for the TR-900 Series radio.

### Wireless Settings

This window displays the wireless configuration of the device. The contents are slightly different for access point and CPE.




| | |
|---|---|
| **Wireless Mode:** | Define if your device will operate as **Infrastructure Station** (CPE) or **Access Point**. |
| **SSID:** | The Service Set Identifier (SSID) is the name that identifies a specific wireless LAN. Devices must have the same SSID to communicate with each other. In Infrastructure Station mode (CPE), you can enter primary and secondary SSIDs when using two access points in the network. Clients will connect to the secondary access point when the primary is unavailable or goes down. |
| **Visibility Status*:** | You can set your access point to be **Visible** or **Invisible** to clients. |
| **Channel Width:** | Select the Channel Width you will be using |
| **Channel Mode:** | Select the mode that the channel will use. **Pure b mode, pure g mode,** or **mixed b/g mode**. |
| **Channel*:** | Select the channel that the access point and clients use. |
| **TX Rate:** | The transmission speed at which the radio and access point communicate with each other.<br>Note: Setting this rate below the maximum possible does not limit bandwidth and often has a negative impact on the operation of your network. |

* Feature available only in access point wireless mode.

| | |
|---|---|
| **RTS Threshold:** | This is the maximum size for a packet to be sent automatically. When it exceeds the RTS threshold, the CPE sends first a 'request to send' (RTS) to the access point before sending the packet.<br>Note: The more clients you have, the lower the value should be set. |
| **Fragmentation Threshold:** | This is the size at which packets are fragmented in order to be transmitted. Setting this value too low decreases the amount sent on each transmission. In noisy areas, this can improve performance. However, in quiet areas, this will decrease throughput. |
| **Link Distance:** | This is the distance between the CPE and access point. This setting is necessary to define the correct ACK timing. Setting this value too low or too high will result in low throughput and high retries. |
| **ACK Timeout Tuning:** | The time that the radio waits for an acknowledgment (ACK) from the access point accepting transmission before re-attempting to send the data. This is an offset from the ACK timing set by the link distance. |
| **Beacon Interval*:** | This is the rate at which the access point broadcasts its beacons. |
| **DTIM Interval*:** | The DTIM interval (Delivery Traffic Indication Message) helps to keep marginal clients connected by sending wake up frames. |
| **Burst Time*:** | This allows to send data without stopping. Note that other wireless devices in the network will not be able to transmit data for this number of microseconds. |
| **802.11d Enabled*:** | Check to operate in 802.11d mode. This mode is not used in USA or Canada. |
| **PxP Mode:** | Follow the instructions in next page. |
| **PxP Mac Address:** | Follow the instructions in next page. |
| **Block Inter-Client Traffic*:** | Check to block wireless communications between clients on the access point. |
| **Power Cap:** | It is the maximum output power of the radio. |
| **Country:** | Select the country where the device is located. Setting an incorrect country may be considered a violation of the applicable law, as rules differ in each country. |
| **Antenna Gain:** | Select the gain of the antenna. This information must be set by the installer at the time of installation. |
| **Preamble:** | Select type: **Long** uses long preamble only, **Auto** (recommended) tries short preamble first, then long. |

* Feature available only in access point wireless mode.

*To operate the radio in PxP mode:*

1. Set one radio to **Access Point** and the other to **Infrastructure Station**.
2. Enter the same **SSID** on both radios.
3. Set the **Channel** on the access point.
4. On both radios, enter the Mac address of the opposite radio in the **PxP Mac Address** field (no colons).
5. Check off **PxP Mode Enabled**.

Note:

> In PxP mode, the LEDs on the radios will operate the same as in Infrastructure Station mode, with LEDs proportional to signal strength.

## Administrative Settings

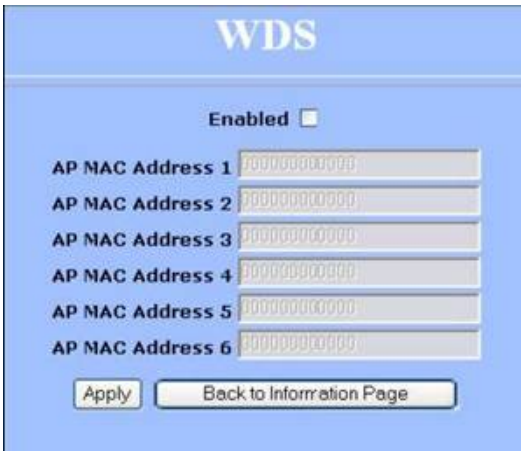
Use this window to upgrade the software, change your password, and define SNMP parameters.


| | |
|---|---|
| **Upgrade Software:** | Enter the location of the software update file or **Browse** to locate it in your computer. Click **Upgrade Software**. If the radio does not refresh the Information Page after 1 minute, press **Refresh**, **Reload** or **F5**. Verify the new firmware is installed correctly. |
| **Defaults:** | Returns all settings to factory defaults, including passwords. |
| **Reboot:** | Restarts the system without changing settings. |
| **Rollback:** | To undo the most recent change. |
| **Device Name:** | It is the network name of the device. This name appears in the Locator and on the Tranzeo stations list. |
| **User Name:** | This is the login username. |
| **Password:** | Enter a new password if you want to change it. |
| **Confirm Password:** | Re-type the new password. |
| **Extended Wireless Information:** | Enables extended information (name and IP address), which is only displayed with Tranzeo access points. |
| **Signal/Status LEDs:** | Un-check to turn off the LED panel indicators. |
| **SNMP Parameters:** | Here you set the **Read Community** string and Contact/Location information. It's highly recommended that you change the **Read Community** string immediately to prevent unauthorized scanning of your network. |

### WDS (AP only)

The Wireless Distribution System (WDS) is a modification to the 802.11 standards that allows access points 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 access points linked.

WDS is not recommended for use with large numbers of clients or when throughput needs to be maximized. In both cases, 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.




To set up WDS:

1. Select **Enabled** to activate WDS and click **Apply**.
2. Go to the Administrative Settings window and change the settings to **Defaults**.
3. Go to the Wireless Settings window and set the same **Channels** for both access points.
4. In the WDS settings window, enter the **Mac address** of the peer. Do not insert colons or commas.
5. Click **Apply**.

Note:

> WDS links don't appear in the Station List or Performance windows. To monitor the link's strength and performance, use PxP mode.

> Throughput is cut by 50% per link.

> WDS does not support WPA encryption.

> All links need to be on the same channel.

## Security

In this section you can configure both basic and advanced security settings for your device.

### Basic Security Settings

In this window you can define WEP parameters. WEP provides security by encrypting data so that it's protected when transmitted from one point to another.


| | |
|---|---|
| **Enabled:** | Check to turn on WEP security protocol. |
| **Authentication:** | Select your system to be open or shared. **Open** is always recommended. |
| **Key Length:** | This is the level of encryption. Note that 64 bit is referred to as 40 bit on some systems. |
| **Default Key:** | Select the default WEP key from the list. |
| **Activate Keys:** | Enter the four WEP keys you want to activate. Keys must be entered in HEX only. |

## Advanced Security Settings

In this window you can enter WPA parameters. WPA provides a higher level of security, enhancing the security features of WEP.


| | |
|---|---|
| **Enabled:** | Check to turn on WPA. |
| **Cipher Type:** | Select the level of encryption. |
| **PSK:** | Enter your PSK password. |
| **Update Interval:** | This is the interval at which the PSK password will be updated. |
| **Authentication:** | Ensures that only authorized network users can access the network. Enter the information about the RADIUS server from your Internet Service Provider. |

## Access Control (AP only)

This feature allows you to control the accessibility from wireless devices, in other words, to allow or deny access from other radios. It applies only to devices working as access points.

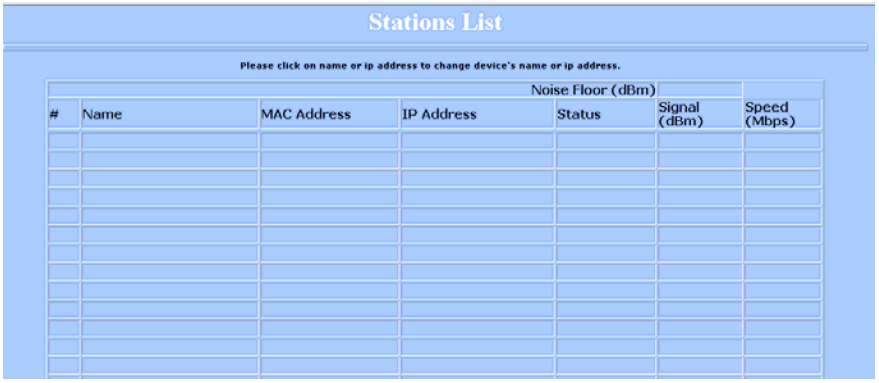

| | |
|---|---|
| **Enable Access Control:** | Enable to control accessibility from wireless devices. |
| **Edit Mode:** | Check to make changes in access control settings. |
| **Authorized Station Devices:** | This is the list of the authorized devices. To change current settings, check the devices and click **Copy All** or **Copy Selected**. The devices will appear in the **Mac Address** box on the right.<br>Note: If you are working via a radio link, add first the address of the station you are connecting from. Otherwise, you will be locked out of the radio. |
| **Available Station Devices:** | This list contains the devices available but not authorized. To authorize them, check the devices and click **Copy All** or **Copy Selected**. The devices will appear in the **Mac Address** box on the right. |
| **Manually Authorize Stations:** | In this box you can perform different actions like authorize, deauthorize and delete devices listed here. |

## Status

This section displays information about the status and performance of your radio. Most options and information cannot be modified in this section.

### Stations List (AP only)

This window displays a list of the stations associated with the access point and their connection statistics.




**Name:** This information appears here when the device is a Tranzeo 6000 and the **Extended Wireless Information** option in the Administrative Settings window is checked. Otherwise, the field will be blank. You can manually enter a name by left clicking on the field and typing in. However, if the **Extended Wireless Information** option is turned on at the client, the name you entered will be overwritten with the name on the client.

**Mac Address:** The Mac addresses of the associated stations.

**IP Address:** Works as with the **Name**. It appears when the **Extended Wireless Information** option in the Administrative Settings window is checked.

**Status:** Indicates if the station is associated or WDS BSSID.

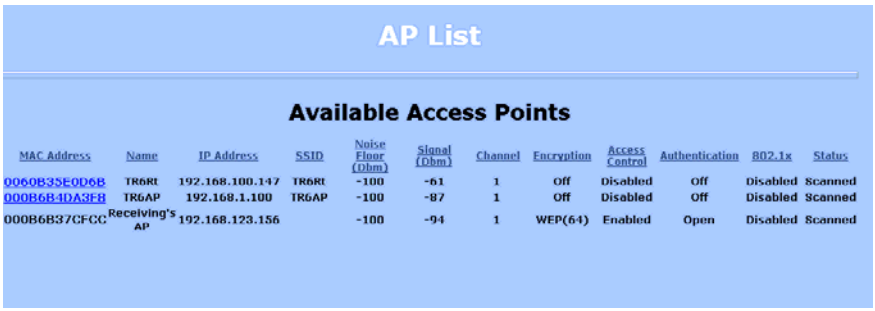
**Signal:** This is the radio frequency power in dBm as detected at the access point. A strong link is defined by both the AP signal and the client signal. Links should also be at least 10 dB higher than the receive sensitivity of the weakest element or the noise floor, whichever is higher, on both sides.

**Speed:** This is 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.

### AP List (CPE only)

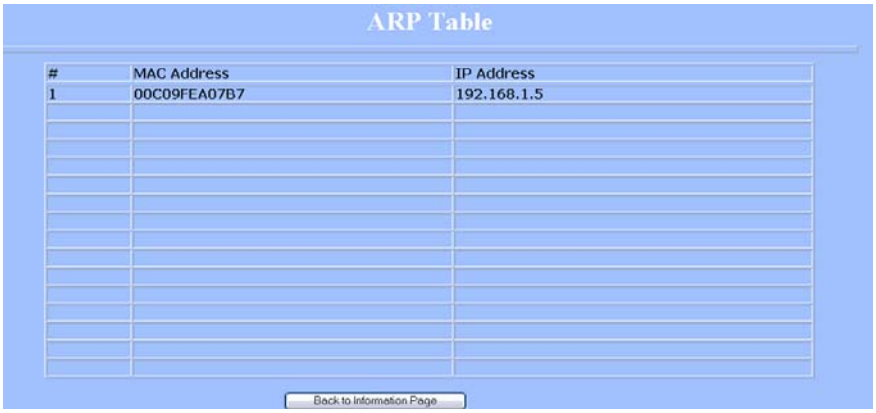
This window displays information about the access points associated with the CPE and the connection statistics.

You can set an access point's SSID as your primary SSID by clicking on the MAC address when it's displayed as a link. This will automatically reboot the radio.



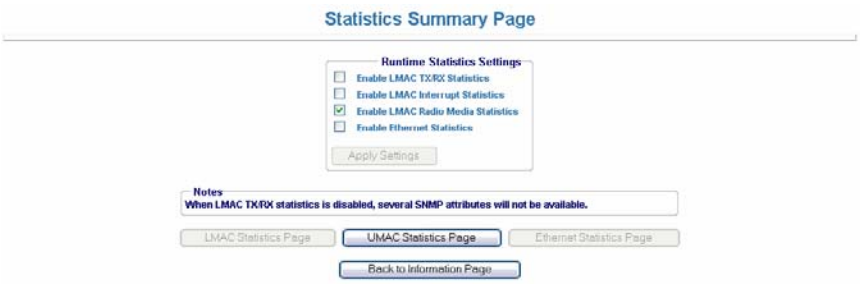

### ARP Table

This table lists the devices that have communicated with your device via TCP. There should be a limited number of entries in this table, especially if the interstation blocking is turned on at the access point.



## Statistics

This section is divided in 3 windows: LMAC (Lower Mac), UMAC (Upper Mac), and Ethernet, which can be accessed from the Statistic Summary Page.

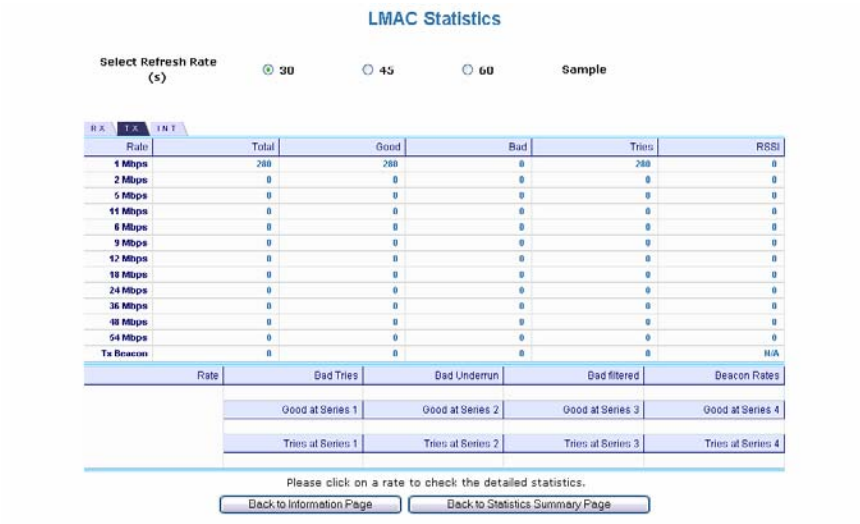



### *LMAC Statistics*

The LMAC functions occur in the radio chipset. While the UMAC divides the statistics into clean and failed packets, LMAC defines why packets failed.

This window contains three tabs: TX, RX and INT. TX and RX values are useful to ISPs and other users. The INT (internal) statistics are intended for use by Tranzeo Wireless Technical Support.

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 will try the next series 4 times. In the RX statistics, you should look for bad CRCs and bad decrypts for signs of RF interference or Fresnel interference links. Bad PHYs generally are caused when the radio is unable to decode the packets due to noise.

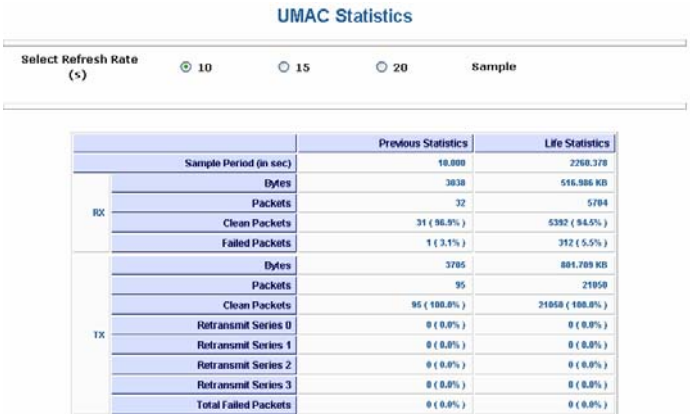



Note:
Communication between access points and CPEs always occurs at the lowest rate. In a normal link, you should see a fair number of transactions at the lowest rate.

### *UMAC Statistics*

The UMAC functions occur in the unit's processor. The UMAC statistics are likely the most useful for radio troubleshooting. This window breaks down the statistics into clean and failed packets.

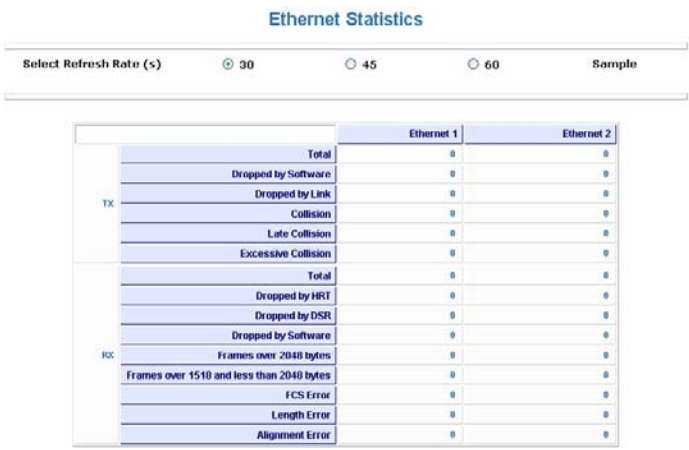
The failed packets should be less than 10% in a normal operating environment. In the TX statistics, there should be little to no Retransmits at Series 2, 3 or 4. Life Statistics are reset on each reboot.




### *Ethernet Statistics*

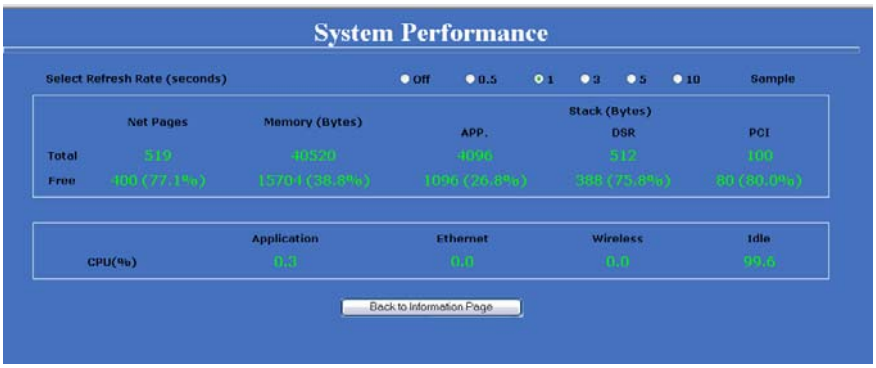
In this window, excessive collisions are usually a sign that the radio and the device it is linked to are not on the same duplex settings. One is at full while the other is at half. Try locking both to the same values.

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.



## System Performance

This window shows information about the memory usage and the CPU. Many browsers do not allow infinite refreshes of a page through scripts, so this window may stop updating. If it does, simply change the refresh rate to another value to restart the process.



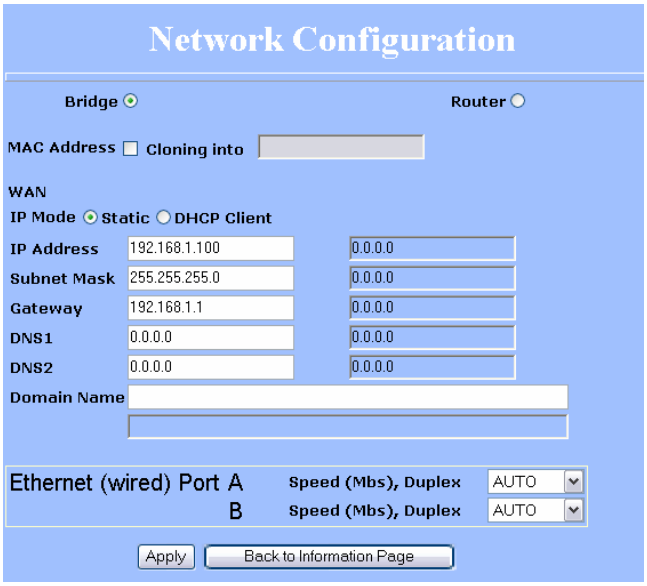

| | |
|---|---|
| **Select Refresh Rate:** | Set the time for automatic refreshes. |
| **Net Pages:** | This is the memory used for data transmission |
| **Memory:** | This is the total memory of the system. |
| **Stack:** | This section displays the memory used and available for each stack: App. (applications), DSR, and PCI. This information is relevant for programmers. |

## Network Configuration

In this window you can control the network configuration of the device. First, you must define if your radio will operate as a bridge or router. The content of the window varies depending on your selection.

When changing modes, the radio may need to reboot before certain features become available.

### Bridge Mode




**Cloning MAC Address:** This feature allows the radio to copy the MAC address of the device you have connected to the network. This is useful when you change your device and don't want to register a new MAC address, or when dealing with some PPPoE and Radius implementations. When the device is cloning a MAC address, it can only be managed from the LAN side. To clone a MAC address, check the **MAC Address** box and enter the MAC address in the field **Cloning into**. Uncheck to restore the original MAC address.

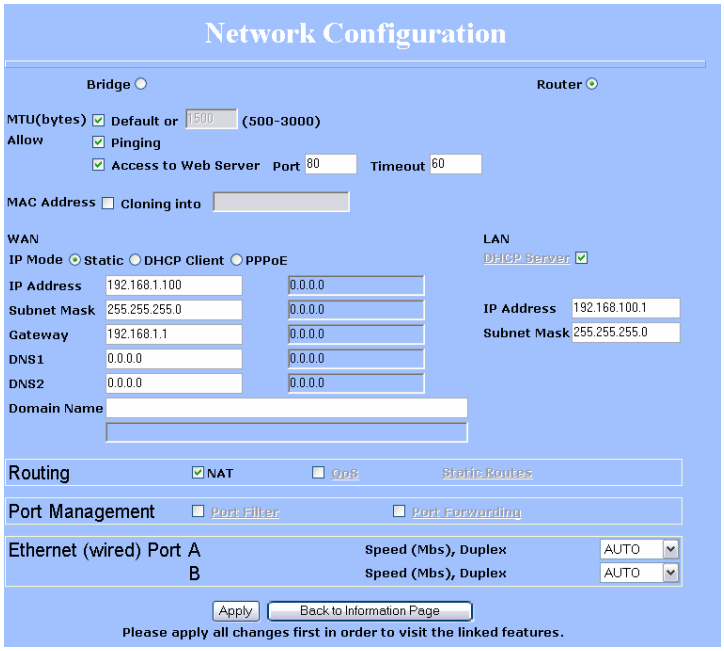
**IP Mode:** You can select to use **Static** IP or **DHCP Client** (dynamic). Note: If a DHCP server is not available, the device will try to get an IP. If has no success, it will use a fallback IP address.

**WAN:** Enter the information related to the WAN interface: IP Address, Subnet Mask, Gateway, DNS1, DNS2, and Domain Name.

**Ethernet Port Speed:** Set as **Auto** by default.

## Router Mode

From this window you can access specific windows to configure the DHCP Server, QoS, Static Routes, Port Filtering, and Port Forwarding. If the feature is available, it will appear like a link. To open an item, just click on it. These features are described in the next pages.




**MTU:** The Maximum Transmission Unit (MTU) refers to the size of the largest packet that the router can pass. The default value is 1500 bytes. If PPPoE is used, you should change the MTU to match the PPPoE server, typically 1492 bytes.

**Allow Pinging:** Enables ping responses on WAN interface.

**Allow Access to Web Server:** Allows access from WAN interface or change the port the WAN server responds to web server requests. Note: Access to web server from LAN interface is always enabled and set at port 80.

**Cloning MAC Address:** See description in Bridge Mode.

**IP Mode:** You can select to use **Static IP**, **DHCP Client** (dynamic), or **PPPoE**. Note: If a PPPoE server is not available, the device will try to get an IP. If has no success, it will use a fallback IP address.

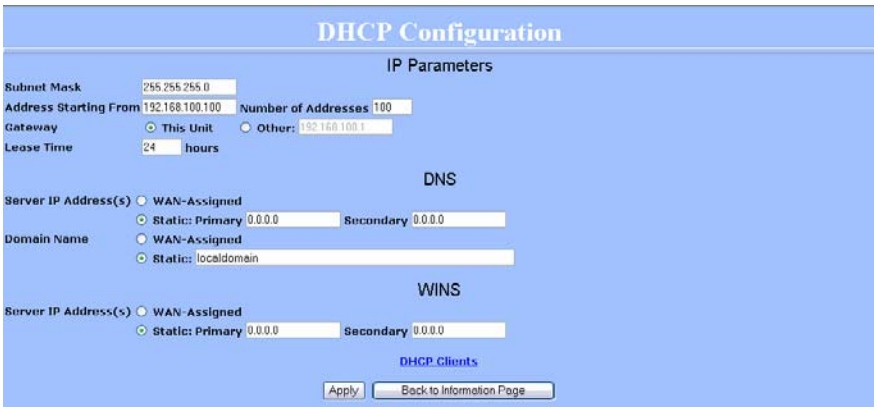
| | |
|---|---|
| **WAN:** | Enter the information related to the WAN interface: IP Address, Subnet Mask, Gateway, DNS1, DNS2, and Domain Name. |
| **LAN:** | Enter the information related to the LAN interface: IP address and subnet mask. |
| **DHCP Server:** | Check the box and click **Apply** to enable this feature. Click on the item (which now appears as a link) to open the DHCP Server configuration window. |
| **Routing:** | Enables NAT, QoS, and Static Routes. NAT should always be enabled when using private addressing. Click on **QoS** or **Static Routes** to configure. |
| **Port Management:** | Check the box and click **Apply** to enable port filtering and port forwarding. Click on any item to open the configuration window. |
| **Ethernet Port Speed:** | Set as **Auto** by default. |

Note:

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

## DHCP Configuration

This window shows the configuration of the DHCP server.




### *IP Parameters*

| | |
|---|---|
| **Subnet Mask:** | Enter your subnet mask in this field. |
| **Address Starting from:** | Indicates the first address in the DHCP pool. |
| **Number of Addresses:** | Indicates the number of addresses in the DHCP pool. |
| **Gateway:** | Select **This Unit** to use the gateway set on the WAN interface. Select **Other** to use a different gateway. |
| **Lease Time:** | Indicates the expiration time for the IP address assigned by the DHCP server. |

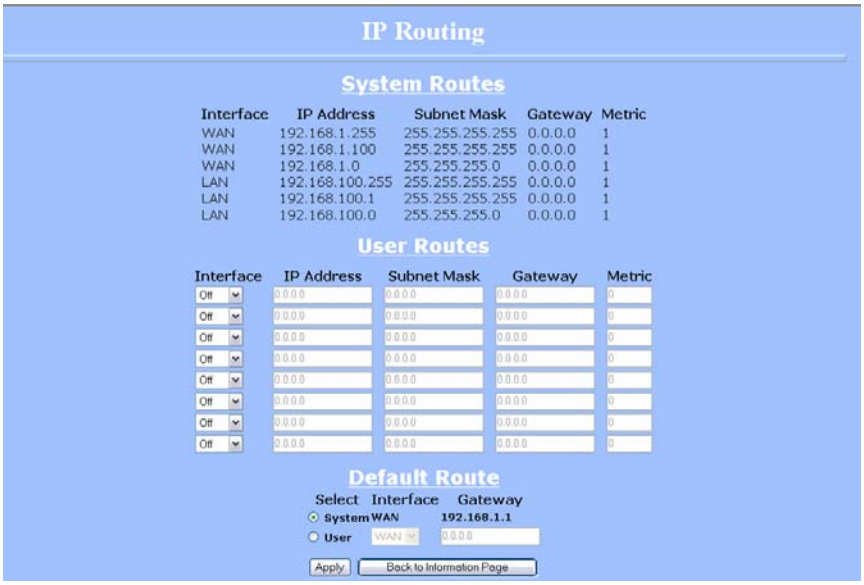
### *DNS*

| | |
|---|---|
| **Server IP Address:** | Select **WAN Assigned** to use the DNS server IP addresses assigned on the WAN side. To use different DNS servers, select **Static**, in which case you must enter the **Primary** and **Secondary** IP addresses. |
| **Domain Name:** | Apply the same configuration as for **Server IP Address**. |
| **WINS:** | Apply the same configuration as for **Server IP Address**. |

## IP Routing

This window is intended for those users who have a strong understanding of IP routing. Here you can see the System Routes, create your User Routes, and set the Default Route.

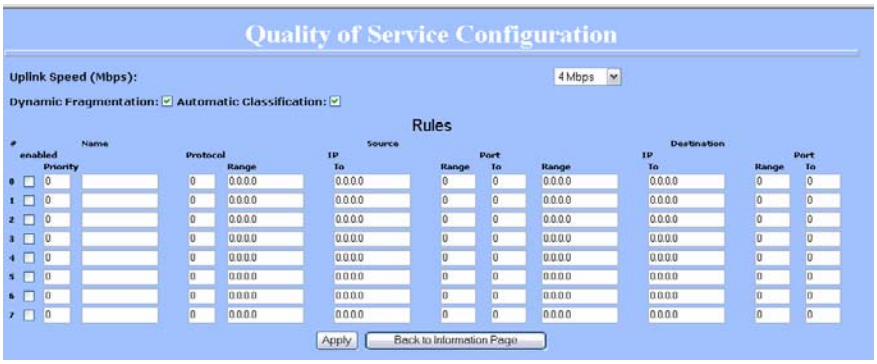
IMPORTANT! Be careful when making changes since misconfiguration could result in serious network problems and even the loss of functionality.




| | |
|---|---|
| **Interface:** | Specify if the interface is **WAN** or **LAN**. Select **Off** to disable the route. |
| **IP Address:** | This is the IP address or network that the packets will be attempting to access. |
| **Subnet Mask:** | Specifies the part of the destination IP that represents the network address and the part that represents the host address. Note: 255.255.255.255 represents only the host entered in the Destination IP field. |
| **Gateway:** | Indicates the next hop if this route is used. A gateway of 0.0.0.0 means there is no next hop and the IP address matched is directly connected to the router on the interface specified. |
| **Metric:** | This is the number of hops it will take to reach the destination. A hop occurs each time data passes 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:** | This option allows you to change the default route of the radio. Make changes with extreme caution. |

## Quality of Service Configuration (QoS)

In this window you can use the QoS features and set rules to prioritize the traffic.




| | |
|---|---|
| **Uplink Speed:** | This is the maximum speed of the uplink (from the source to the destination). The order and size of traffic is determined based on this value. |
| **Dynamic Fragmentation:** | Check to 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:** | This feature automatically classifies traffic and gives priority to certain applications. Applications such as VOIP and gaming are automatically given priority. |
| **Enabled:** | Check to activate a rule. |
| **Priority:** | Enter the priority of the rule between 0 and 255. |
| **Name:** | Enter the name of the rule here. |
| **Protocol:** | Enter the protocol number here. Common options are: 0 for ANY, 1 for ICMP, 6 for TCP, and 17 for UDP. See Appendix C for Protocol List. |
| **Source IP Range:** | Enter the range of IP addresses on the LAN side where the rule would apply. To cover all LAN IPs, enter 0.0.0.0. For a single IP, enter the IP in both boxes. |
| **Source Port Range:** | Enter the range of ports on the LAN side where the rule would apply. To cover all ports, enter 0. For a single port, enter this port in both boxes. |
| **Destination IP Range:** | Enter the range of IP addresses on the WAN side where the rule would apply. |
| **Destination Port Range:** | Enter the range of ports on the WAN side where the rule would apply. |

## Port Forwarding

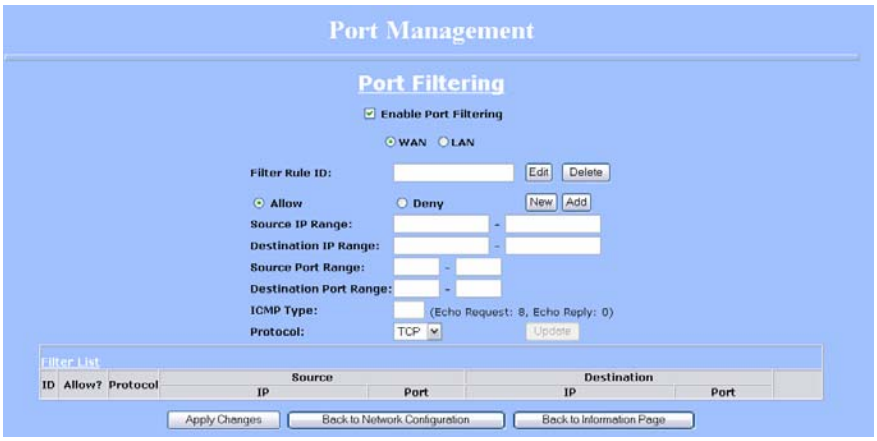
This feature allows the radio to forward requests for certain ports to devices behind a router. For example, you have a web server on a private IP that you want to be accessible to the world. You can forward all requests on port 80 to 192.168.1.2. For this to work, you have to change the management port of the radio from port 80 on the Network Configuration window.

In this window, you can create, edit, delete, and manage rules for port forwarding. A list of port forwarding rules appears at the bottom.


| | |
|---|---|
| **Enable Port Forwarding:** | Click to apply rules from the Rules list. |
| **Forward Rule ID:** | Enter the rule ID here to retrieve its information. |
| **Edit / Delete:** | Click to modify or remove the selected rule. |
| **Enabled / Disabled:** | Activate or deactivate the selected rule. |
| **External Port:** | Enter the port to which requests will be forwarded. |
| **Internal Port:** | Enter your port here. |
| **Internal Address:** | Enter your IP address. |
| **Protocol:** | Select the protocol used for this rule. |
| **New:** | Click to create a new rule. Fields will be cleared. |
| **Add:** | After creating a rule, click this button to include the new rule in the Port Forwarding Rules list. |
| **Update:** | Click to apply changes after editing or deleting a rule. |

## Port Filtering

This feature allows the radio to block requests to and from devices behind the router. A list of the devices filtered appears at the bottom of the window.




| | |
|---|---|
| **Enable Port Filtering:** | Click to apply the rules enabled from the Filter list. |
| **WAN / LAN:** | Select the network. |
| **Filter Rule ID:** | Enter the filter rule ID here to retrieve its information. |
| **Edit / Delete:** | Click to modify or eliminate the selected filter. |
| **Allow / Deny:** | The rule can either allow or deny ports. |
| **New:** | Click to create a new filter. Fields will be cleared and you may enter the information for the new filter. |
| **Add:** | After creating a filter, click this button to include the new filter in the Filter list. |
| **Source IP Range:** | Enter the range of IP addresses on the LAN side where the rule would apply. |
| **Destination IP Range:** | Enter the range of IP addresses on the WAN side where the rule would apply. |
| **Source Port Range:** | Enter the range of ports on the LAN side where the rule would apply. |
| **Destination Port Range:** | Enter the range of ports on the WAN side where the rule would apply. |
| **ICMP Type:** | This allows you to block certain types of ICMP as a prevention against port scanning and some viruses. |
| **Protocol:** | Select the protocol used for this rule. |
| **Update:** | Click to apply changes after editing or deleting a filter. |

# Appendix A: Grounding and Lightning Protection 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:

- The building or structure grounding electrode
- The grounded interior metal water piping system
- The power service accessible means external to enclosure
- The metallic power service raceway
- The service equipment enclosure
- The grounding electrode conductor

## Why is coiling the LMR or Cat 5 bad?

The myth is that lighting 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 (www.tranzeo.com).

## Is lightning damage covered by the warranty?

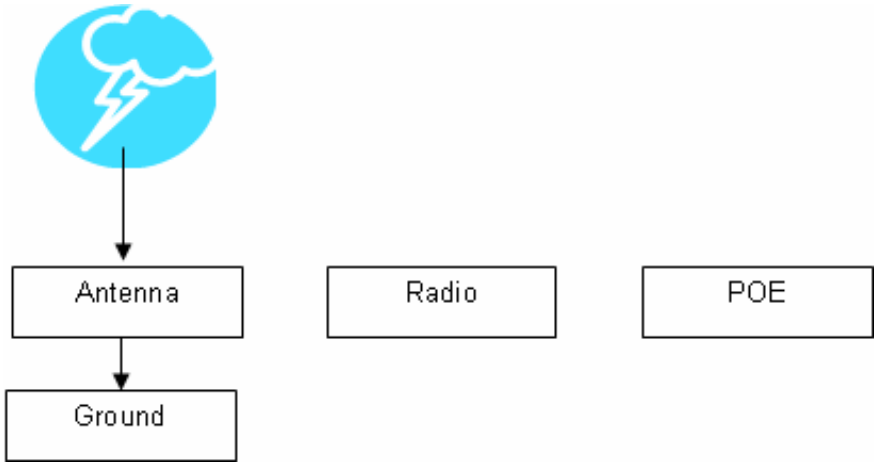
No. Lightning is not covered by the warranty. If you follow the instructions, your chances of lightning damage are greatly reduced, but nothing can protect a radio from a direct lightning strike.

## 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.

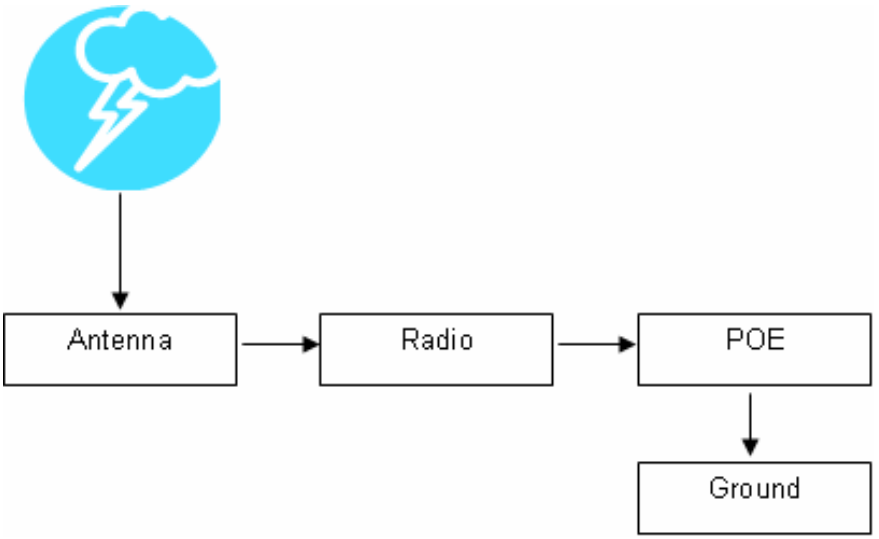
### Grounded Radio

A grounded radio causes the surge to pass directly to ground, bypassing the radio.



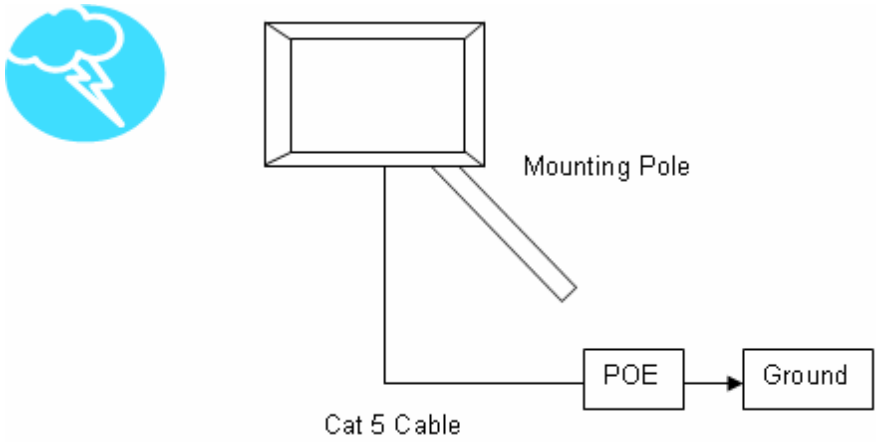

### Ungrounded Radio

An ungrounded radio causes the surge to pass through the radio. In this case, the radio most likely will be damaged.



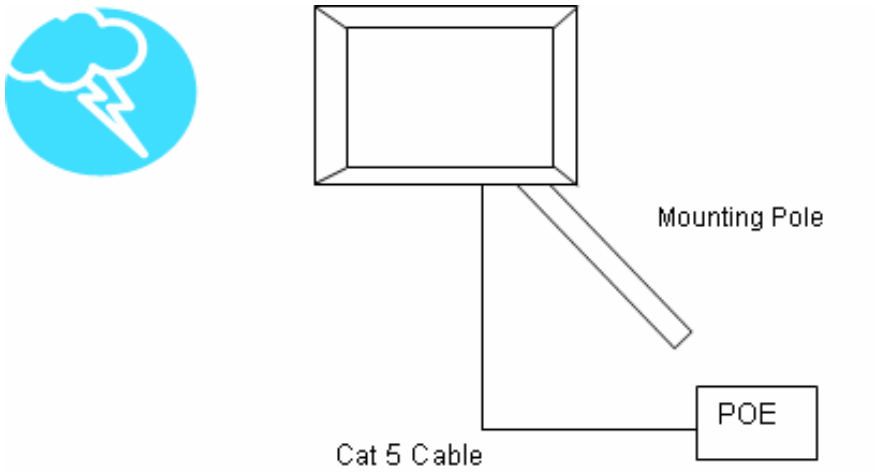
### Grounded POE

In this case, the surge will be picked up by the Cat 5 cable and since the POE is grounded, the route for the surge is through the POE to ground.




### Ungrounded POE

In this case, the surge will be picked up by the Cat 5 cable and since the POE is not grounded, the route for the surge is through the radio to the antenna, and out through the building.



# Appendix B: Quality of Service Configuration (QoS)

Tranzeo Wireless Technologies' software ensures a consistently high quality online 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 that 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—is 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 software effectively eliminates the lag and breakup problem in online gaming and other voice and 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's 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 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 use 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

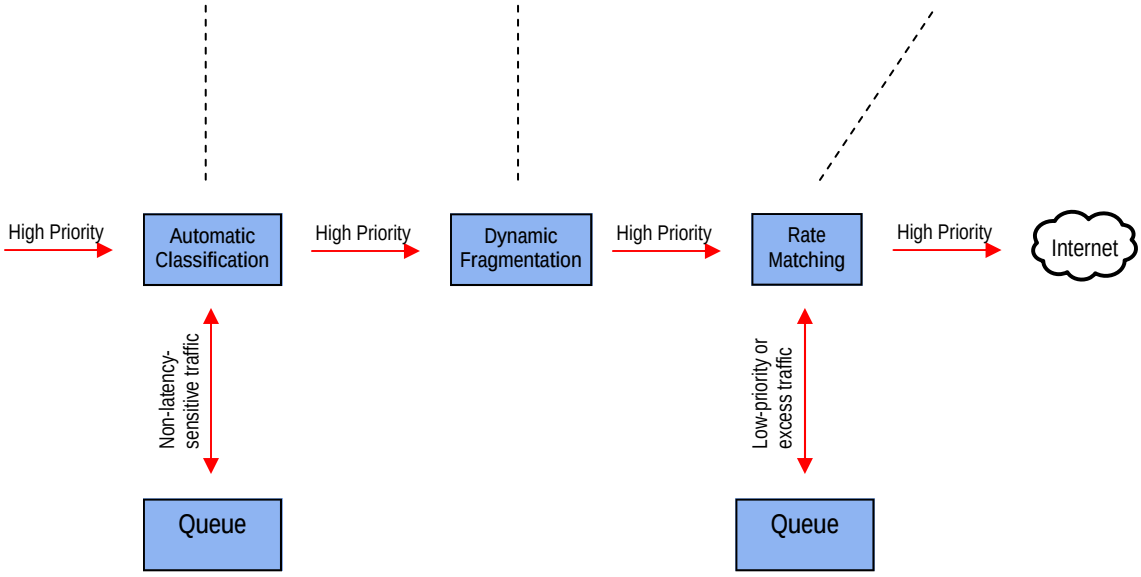
Low priority traffic is also fragmented to reduce the latency and jitter that can be introduced by long packets. Intelligent Stream Handling adjusts the fragment size based on the uplink speed and also stops fragmenting long packets when no latency-sensitive traffic is waiting to be sent, to improve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

# QoS Block Diagram

Tranzeo 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.

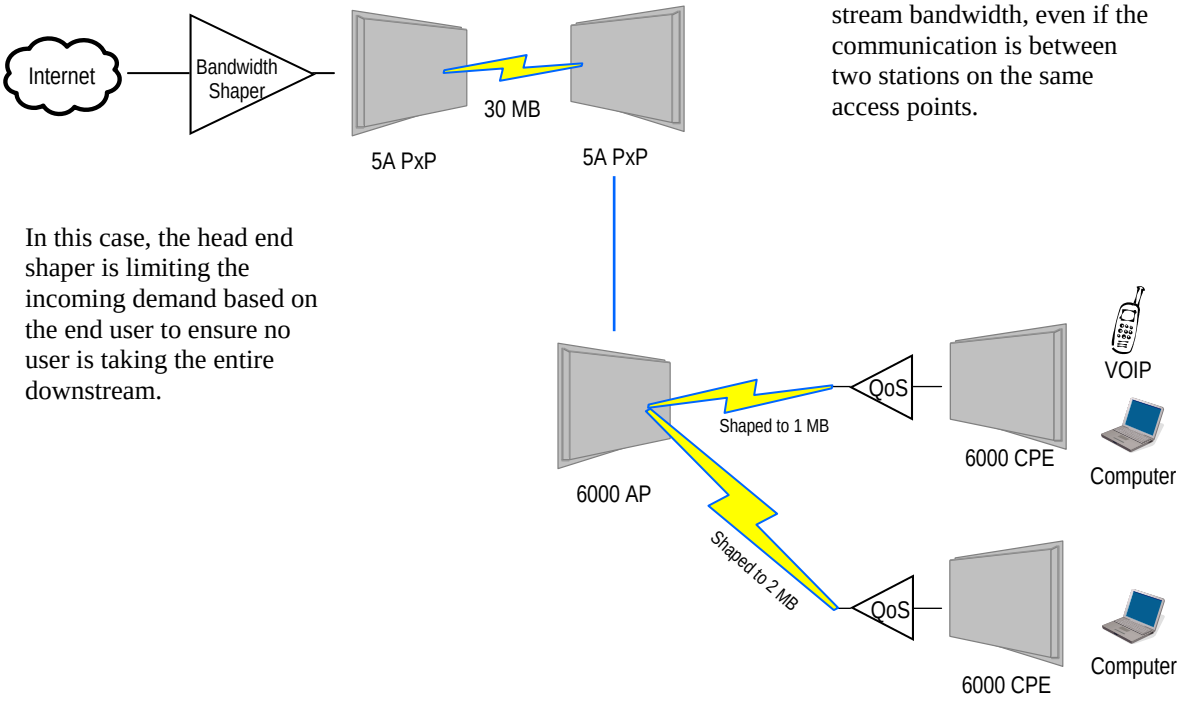
Intelligent Stream Handling adjusts the fragment size based on the uplink speed and also stops fragmenting long packets when no latency-sensitive traffic is waiting to be sent, to improve the overall efficiency of the broadband link and ensure voice can sustain a high MOS (Mean Opinion Score) rating.

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.



## Network QoS Example

In this case, no 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 access points.




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

# Appendix C: Protocol List

| Dec | 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 |
| 48 | 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 |
| 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 |

| Dec | Keyword | Protocol |
|---|---|---|
| 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 |
| 110 | Compaq-Peer | Compaq Peer Protocol |
| 111 | IPX-in-IP | IPX in IP |
| 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 |

| Dec | Keyword | Protocol |
|---|---|---|
| 121 | SMP | Simple Message Protocol |
| 122 | SM | SM |
| 123 | PTP | Performance Transparency |
| 124 | ISSIS | 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 | RSVP-E2E-IGNORE | |
| 135 | | Mobility header |
| 136 | UDPLite | |
| 137 | MPLS-in-IP | |
| 138-252 | | Unassigned |
| 253 | | Use for experimentation and testing |
| 254 | | Use for experimentation and testing |
| 255 | | Reserved |

# Appendix D: Common TCP Ports

Visit 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 |

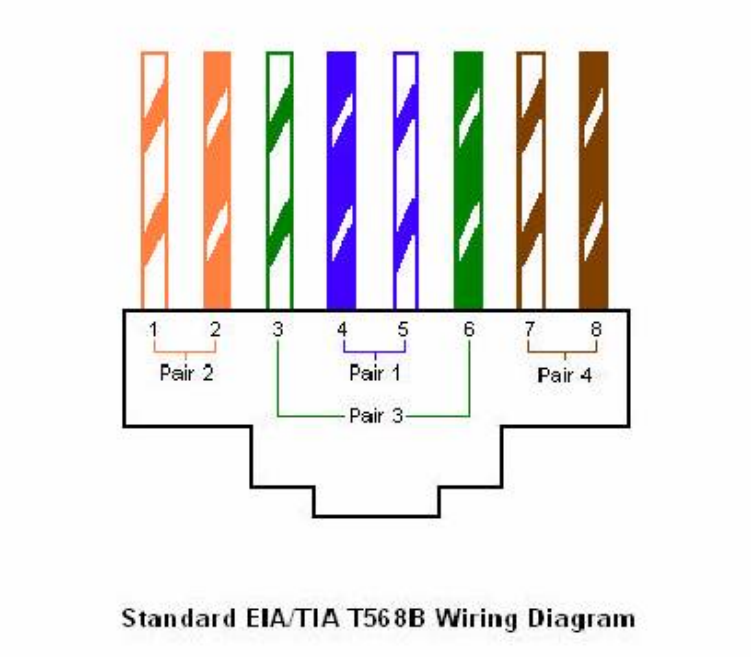
# Appendix E: Channel Allocations

This Table shows the channels available with the TR-900 series radios and the frequencies that they are on.

| Bandwidth | Channels | | | |
|---|---|---|---|---|
| 5 MHz | 903 to 908 | 909 to 914 | 915 to 919 | 920 to 925 |
| 10 MHz | 903 to 913 | | 915 to 925 | |
| 20 MHz | 903 to 923 | | | |

# Appendix F: Wiring Standard

TIA/EIA-568-B is a set of standards for cabling telecommunications products and services. Follow these standards, as described in the diagram below, to wire the Cat 5 cable during installation of the Tranzeo radio (see Step 3 in Chapter 2: Hardware Installation - Installing the Ethernet Cable).




Standard EIA/TIA T568B Wiring Diagram