

TRANZEO TR-6600



Tranzeo TR-6600 Series **User Guide**

Revision: 1.0
Firmware: 2.0.11
Date: 20/05/06

Document Revisions:

Version 1.0

June 9, 2006

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 could void 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 67 cm 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: TR-OD24-12, TR-24H-90-17, TR-GD24-24.
- In order to ensure compliance with local regulations, the installer **MUST** enter the gain of the antenna at the time of installation. See section 3 for details.

Professional Installation Required

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

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 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 a 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.

Table of Contents

Chapter 1: Overview	1-1
Product Description	1-1
Product Kit.....	1-1
LED Panel Indicators	1-1
Chapter 2: Hardware Installation.....	2-1
Getting Ready.....	2-1
Tools Required.....	2-1
Site Selection	2-1
Orientation of the Device.....	2-1
Power Supply.....	2-1
Installing the Ethernet Boot.....	2-2
Mounting the Radio.....	2-4
Grounding the Antenna	2-4
Connecting the Radio	2-5
Best Practices.....	2-6
Chapter 3: Configuration.....	3-1
Setting the Network Connection	3-1
Login to the Configuration Interface.....	3-2
Information Page	3-3
Setup Menu.....	3-4
Wireless Settings	3-4
Administrative Settings	3-6
WDS	3-7
Security.....	3-8
Basic Security Settings	3-8
Advanced Security Settings	3-8
Access Control	3-9
Status	3-10
Stations List	3-10
ARP Table	3-11
Statistics	3-12
Performance	3-14

Network Configuration	3-15
Common Features	3-15
Router Mode	3-16
DHCP Configuration	3-17
IP Routing	3-18
Quality of Service Configuration	3-19
Port Forwarding	3-20
Port Filtering	3-21

Appendix A: Grounding and Lightning Protection Information A-1

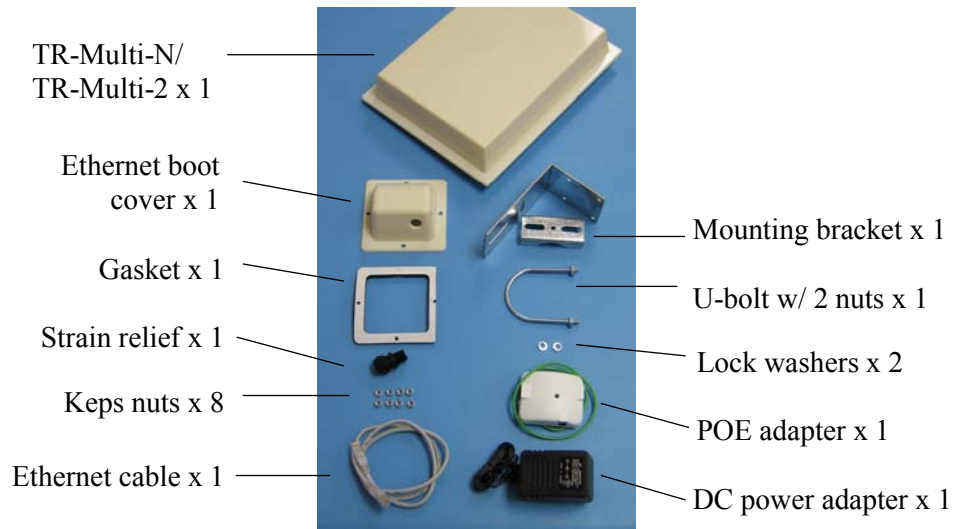
Chapter 1: Overview

Product Description

This next-generation wireless LAN device—the Tranzeo TR-6600 series—brings Ethernet-like performance to the wireless realm. Fully compliant with the IEEE802.11a standard, the TR-6600 series also provides powerful features such as the Internet-based configuration utility as well as WEP and WPA security.

Product Kit

The TR-6600 product kit contains the items shown below. If any item is missing or damaged, contact your local dealer for support.



LED Panel Indicators

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 (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 Flashing: WEP/64 enabled Off: WEP off
	Amber	On: WPA/AES enabled Flashing: WPA/TKIP enabled Off: WPA off
	Amber	On: 5.8 operation Off: 5.3 operation
	Green	On: ACL enabled Off: ACL off
	Green	On: WDS enabled Off: WDS off

Chapter 2: Hardware Installation

The TR-6600 series devices 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 connect the Ethernet cable, mount the device, and ground the antenna in order to get a proper installation of the device.

Getting Ready

Tools Required

To install the TR-6600 you will need the following tools:

- 3/8" wrench x 1
- 3/4" wrench x 1
- RJ-45 crimper x 1
- Cat 5 cable, enough to bring the signal from the radio to the Power over Ethernet (POE) adapter
- RJ-45 connectors x 2
- #6 green grounding wire

Site Selection

Determine the location of the device 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 (AP). Obstructions may impede performance of this device.

Orientation of the device

Determine if the orientation of the device will be horizontal or vertical before installation. The TR-6600 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.

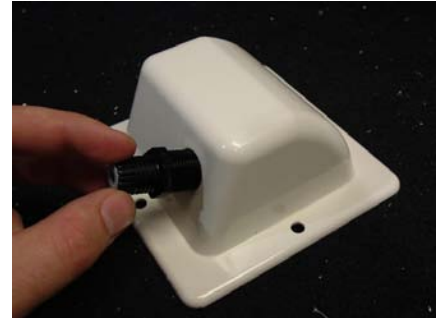
Power Supply

Only use the power adapter supplied with the TR-6600. Otherwise, the product may be damaged.

Installing the Ethernet Cable

Step 1:

Insert the strain relief, without the cap nut, into 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. Attach the RJ-45 connectors to both ends of the Cat 5 cable.



Step 4:

If you bought the device with dual port, 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.



Step 5:

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

**Step 6:**

Pull the Cat 5 cable inserted in the boot cover and plug it into the port of the radio.

**Step 7:**

Fit the boot cover over the 4 mounting studs and the gasket. Secure with 4 keps nuts, and 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. Tighten the nuts enough to prevent any movement after alignment.



Step 10:

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

IMPORTANT! The strain relief must be always facing down.



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.

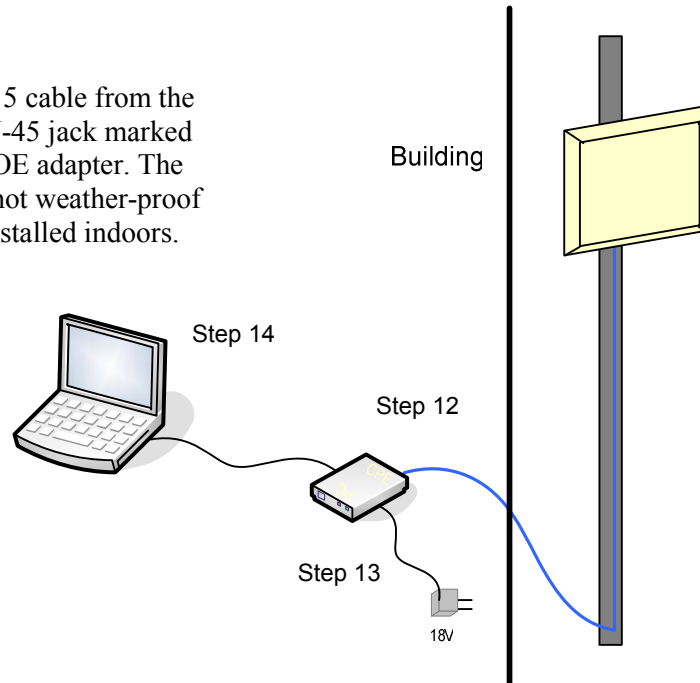


IMPORTANT: This device must be grounded. Connect the green grounding wire to a known good earth ground, as outlined in the National Electrical Code.

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.

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

Step 14:

To configure the TR-Multi 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 328 feet.

Best Practices

Follow these practices to ensure a correct installation and grounding.

- Always try to run the 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-6600 series devices 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:

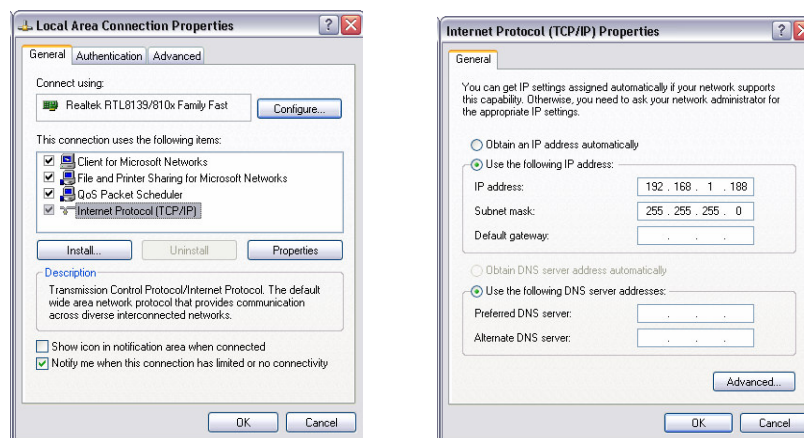
- Access the configuration interface from your computer
- Configure the TR-6600 series radio
- Interpret the information displayed in the interface

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.

Setting the Network Connection

Before accessing the configuration interface, you have to change the network connection settings in your computer.

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**.
6. Click **OK** and **Close**.



Login to the Configuration Interface

After setting the network connection, follow these steps to login into the Tranzeo Configuration Interface.

1. Open your Internet browser (Explorer, Netscape, or Firefox).
2. In the address bar, type **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 username **admin** and 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. You will access the configuration interface.

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:

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

Recovery Password

Username:

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

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

Information Page

This is the first window of the interface. It shows the main menu and general information about the configuration of the device.

The content of the menu varies depending on whether your device is configured as an AP or CPE.

Information Page - AP

Information Page	
802.11b (2.4GHz) Tr6 Router with External 0 dBi Antenna	
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: 192.168.1.188	
Security Encryption: Off Authentication: None	
Radio Country / Regulatory: US: United States (FCC1_FCCA) MAC Address: 0060B3DD29AF Channel: 1	
Board OS: 6.3.34P (1019) Software: 2.10 (TR6-2.0.9RT)	
Event Log Hardware Events: (none)	

Information Page - CPE

Information Page	
802.11b (2.4GHz) Tr-Rt Router with External 0 dBi Antenna	
Wireless Settings DFS/TPC Enabled: No Link Status: No Link Primary SSID: TR6Rt Secondary 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: 192.168.1.188	
Security Encryption: Off Authentication: None	
Radio Country / Regulatory: US: United States (FCC1_FCCA) MAC Address: 0060B3DD29AF Channel: 9	
Board OS: 6.3.34P (1019) Software: 2.10 (TR6-2.0.9RT)	
Event Log Hardware Events: (none)	

Setup Menu

In this section you would be able to configure wireless and administrative settings for the TR-6600.

Wireless Settings

This window displays the general 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:

This is a unique ID given to an access point. Clients associating to the access point must have the same SSID. In Infrastructure Station mode (CPE), you can enter Primary and Secondary SSIDs.

Visibility Status*:

You can set your access point to be **Visible** or **Invisible** to clients.

Channel*:

Select the channel that the access point and clients use.

TX Rate:

The rate at which the access point communicates with its clients. 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:

Enter the RTS that works best in your location. Usually, the more clients you have, the lower the threshold value.

Fragmentation Threshold:

Enter the fragmentation that works best in your location. The lower the fragmentation, the smaller the packets.

* Feature available only in access point wireless mode.

Link Distance:	Enter the distance of the link for correct ACK timing.
ACK Timeout Tuning:	Use if the ACK timing requires fine tuning.
Beacon Interval*:	This is the rate at which the access point will broadcast its beacons.
DTIM Interval*:	Enter the (Delivery Traffic Indication Message). This 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 that 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:	To operate in this mode, follow the instructions below.
PxP Mac Address:	Fill this field as indicated in the instructions below.
Block Inter-Client Traffic*:	Check to block wireless communications between clients on the access point.
Power Cap:	Select the output power of the radio.
Country:	Select the country from where the device is operating. Setting an incorrect country may be considered a violation of the applicable law.
Antenna Gain:	Select the gain of the antenna used. This information MUST be entered by the installer at the time of installation.
Preamble:	Select type: Long uses long preamble only, Auto tries short preamble first, then long preamble.

* 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 read community string, contact and location data.

Upgrade Software:	Enter the location of the software update file or Browse to locate the file in your computer. Click Upgrade Software . You may be prompted to reboot your computer.
Defaults:	Returns all settings to factory defaults.
Reboot:	Restarts the system without changing settings.
Rollback:	To undo the most recent change.
Device Name:	This is the network name of the device.
User Name:	This is the access user name.
Password:	Enter a new password if you want to change it.
Confirm Password:	Re-type the new password.
Extended Wireless Information:	Enables extended information, 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.

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

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 P×P 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.
2. Click **Apply**.
3. Go to the Administrative Settings window and change the settings to **Defaults**.
4. Go to the Wireless Settings window and set the same **Channels** for both access points.
5. In the WDS settings window, enter the **Mac address** of the peer. Do not insert colons or commas.
6. Click **Apply**.
7. Ping a station connected to the opposite end. It should reply.

Note:

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

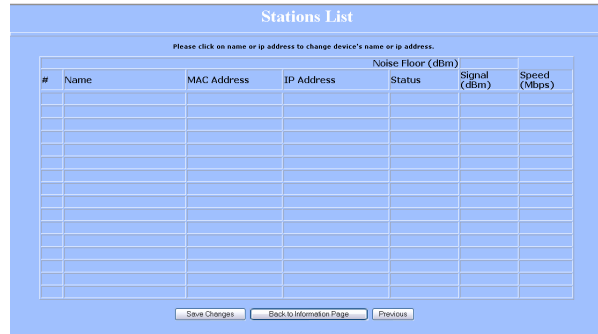
Enable Access Control:	Enable to control accessibility from wireless devices.
Edit Mode:	Check to make changes in access control settings.
Authorized Station Devices:	This is the list of the authorized devices. To change current settings, check the devices and click Copy All or Copy Selected . The devices will appear in the Mac Address box on the right. Note: If you are working via a radio link, add first the address of the station you are connecting from. Otherwise, you will lock yourself 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 device. Most options and information cannot be modified here.

Stations List (AP only)

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



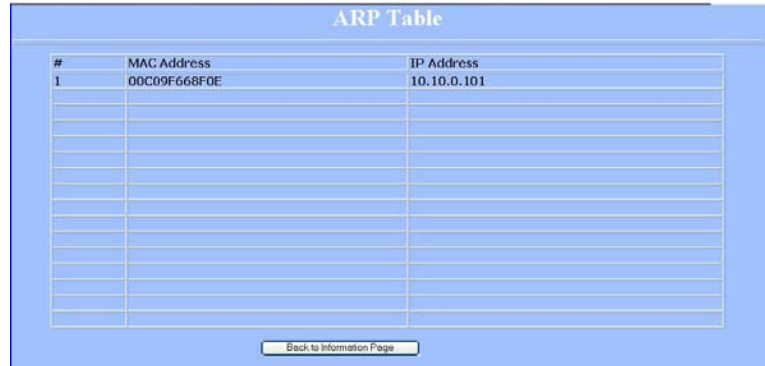
#	Name	MAC Address	IP Address	Status	Signal (dBm)	Noise Floor (dBm)	Speed (Mbps)

Save Changes Back to Information Page Previous

Name:	This information appears here when the device is a Tranzeo 6600 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.

ARP Table

This table lists the devices that have either sent a broadcast or directly tried to communicate with your device. There should be a limited number of entries in this table, especially if you have interstation blocking turned on at the access point.

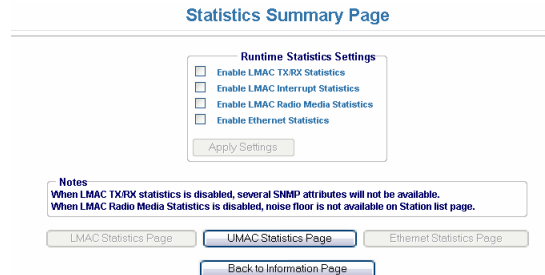
The screenshot displays a web-based interface titled "ARP Table". It contains a table with three columns: "#", "MAC Address", and "IP Address". The first row is populated with the values "1", "00C09F668F0E", and "10.10.0.101". Below the table, there is a button labeled "Back to Information Page".

#	MAC Address	IP Address
1	00C09F668F0E	10.10.0.101

[Back to Information Page](#)

Statistics

The Statistics section is divided in 3 windows: LMAC (Lower Mac), UMAC (Upper Mac), and Ethernet.



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.

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
16 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

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 stations always occurs at the lowest rate. Therefore, 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 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.

UMAC Statistics

Select Refresh Rate (s) 10 15 20

	Previous Statistics	Life Statistics
RX		
Sample Period (in sec)	10.000	688.101
Bytes	88	43.233 KB
Packets	2	1188
Clean Packets	2 (100.0%)	1035 (93.4%)
Failed Packets	0 (0.0%)	73 (6.0%)
TX		
Bytes	1054	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](#)

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 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 be the result of a bad radio link, or a bad Ethernet cable.

Ethernet Statistics

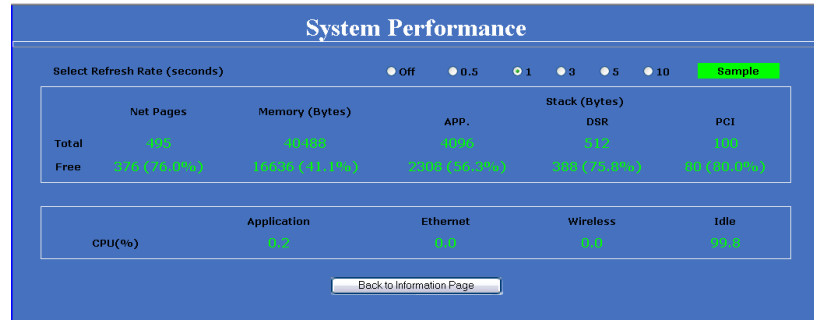
Select Refresh Rate (s) 30 45 60

	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](#)

System Performance (CPE and PxP only)

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.



Network Configuration

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

Router

Bridge

Common Features

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 original Mac address in the field **Cloning into**.

IP Mode:

You can select to use a **Static IP**, **DHCP Client** (dynamic), or **PPPoE** (available only for router). Note: If a DHCP server is not available, the device will try to get an IP for up to 5 minutes. After that, it will fall back to a static IP.

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

The following features are available if you select Router mode in the Network Configuration window.

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 in blue and underlined. To open these windows, just click on the item. 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.
PPPoE:	If no PPPoE server is found, you may not be able to access the device from the WAN side, but you will still be able to access it from the non-PPPoE interface.
Allow Pinging:	Enables ping responses on WAN interface to determine whether a specific IP address is accessible. Used mainly for troubleshooting.
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.
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 in blue) to open the DHCP Server configuration window.
Routing:	Enable NAT, QoS, and Static Routes. NAT should be enabled when using private addressing. Click on QoS or Static Routes to configure these features.
Port Management:	Check the box and click Apply to enable port filtering and port forwarding. Click on an item (which now appears in blue) to open the configuration window.

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 cannot support 100 / Half, you should replace the device or place a switch in line.

DHCP Configuration

This window shows the configuration of the DHCP server.

IP Parameters

Address Range:	Indicates the Starting Address and 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. The client must renew the lease within 24 hours.

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. Note: If you 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:	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. Be careful when making changes since misconfiguration could result in serious network problems and even the loss of functionality.

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
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

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.

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 this 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:

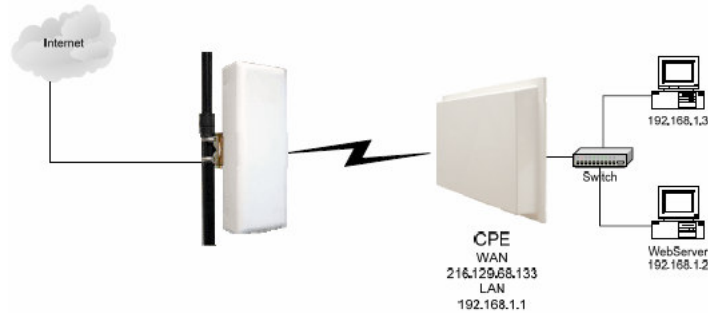
Enter the range of IP addresses on the WAN side where the rule would apply.

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 of the window.

Enable Port Forwarding:	Click to apply rules from the Port Forwarding 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 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 (www.tranzeo.com).

Is lightning damage covered by the warranty?

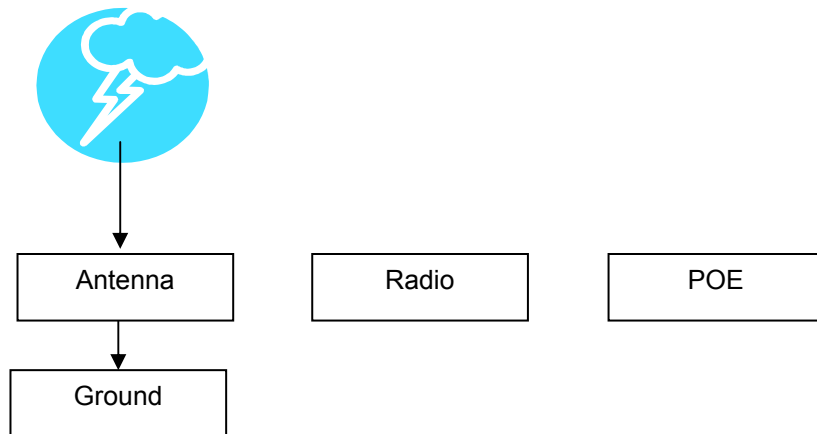
No. Lightning is not covered by the warranty. If you follow the instructions, your chances of lightning damage are greatly reduced, but nothing can protect a radio from a direct lightning strike.

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.

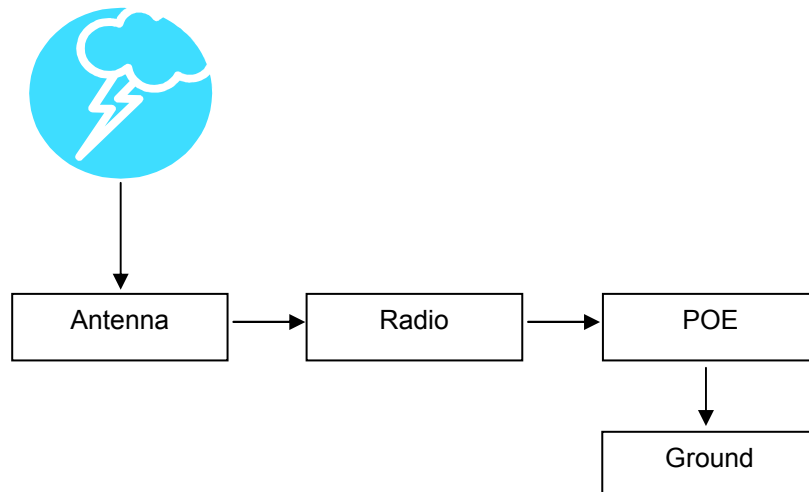
Grounded Radio

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



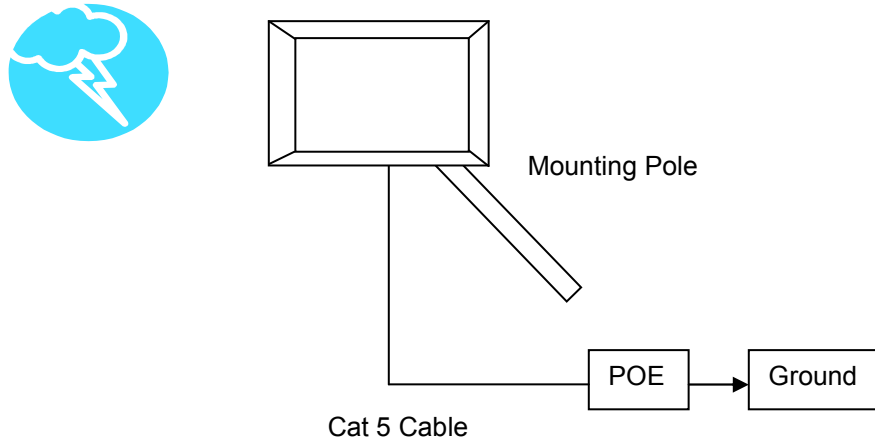
Ungrounded Radio

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.

