



TR-2000/TR-1000/TR-2015/TR-2018

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital devices pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communication.

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

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

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

1. Install the antenna in a location where a distance of 20 cm from the antenna may be maintained.
2. While installing the antenna in the location, please do not turn on the power of wireless card.
3. While the device is working, please do not contact the antenna.
4. RF exposure: The antenna used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter”

Copyright

Copyright © 2001 all rights reserved. No part of this publication may be reproduced, adapted, stored in a retrieval system, translated into any language, or transmitted in any form or by any means without the written permission of the supplier.

About This Manual

The purpose of this manual is for the setup of the 11Mbps Wireless LAN Access Point. This manual, revised as version 3.0.0 in 2001, includes procedures assisting you in avoiding unforeseen problems.

Table of Contents

Chapter 1 Introduction	4
1-1 Features and Benefits	4
1-2 Applications2	4
1-3 System Configurations	5
Chapter 2 Hardware Installation	6
2-1 Product Kit	6
2-2 System Requirements	6
2-3 Mechanical Description	6
2-4 Hardware Installation	6
Chapter 3 Configuring the Access Point	8
3-1 Using the Access Point Manager	8
3-2 Using the Web Management	12
3-3 Using the Console Mode	13
Chapter 4 Troubleshooting	19
Appendix A Network Configuration	19
A-1 Network Topology	20
Appendix B Specifications	20
Appendix C Glossary	21

Chapter 1 Introduction

The 11Mbps Wireless LAN Access Point is a high-speed wireless unit that performs as a transparent Media Access Control (MAC) bridge between wired Local Area Networks, and one or more wireless networks. It brings Ethernet-like performance to the wireless realm. Placed anywhere along an Ethernet LAN, the 11Mbps Wireless LAN Access Point allows wireless stations in their coverage area to transparently access the corporate network. Fully compliant with the IEEE 802.11(b) standard, the 11Mbps Wireless LAN Access Point also provides powerful features such as the Windows-based configuration utility, WEP security, SNMP and more. The 11Mbps Wireless LAN Access Point enables you to build a variety of network configurations.

1-1 Features and Benefits

- Features 11Mbps data rate by incorporating Direct Sequence Spread Spectrum technology
- Fully IEEE 802.11b compatible. Allow inter-operation among multiple vendors.
- Technique operating in the unlicensed 2.4Ghz ISM band
- Seamless roaming within the 802.11 & 802.11b wireless LAN infrastructure
- Provides user authentication to enforce tight security
- Highly secure system using data encryption levels of 64-bit and 128-bit WEP and MAC Access Control Table
- Dynamic Host Configuration Protocol client and server (DHCP) on both Wireless and Ethernet Side
- Creates a Point-to-Point and Point-to-Multipoint connection
- Highly efficient antenna provides a range of operation up to 800 feet in free space.
- Easy to install and friendly to user, just plug and play!
- Provides Window-based configuration utilities
- Provides Window-based Diagnostic, Statistics Tools and Traffic Monitor
- Tight design with light weight, compact size, and low power consumption

1-2 Applications

The 11Mbps Wireless LAN products offer a fast, reliable, cost-effective solution for wireless client access to the network in applications like these:

1. Remote access to corporate network information

E-mail, file transfer and terminal emulation.

2. Difficult-to-wire environments

Historical or old buildings, asbestos installations, and open area where wiring is difficult to deploy.

3. Frequently changing environments

Retailers, manufacturers and those who frequently rearrange the workplace and change location.

4. Temporary LANs for special projects or peak time

C1- Trade shows, exhibitions and construction sites where a temporary network will be practical. C2- Retailers, airline and shipping companies need additional workstations during peak period. C3- Auditors requiring workgroups at customer sites.

5. Access to database for mobile workers

Doctors, nurses, retailers, accessing their database while being mobile in the hospital, retail store or office campus.

6. SOHO (Small Office and Home Office) users

SOHO users need easy and quick installation of a small computer network.

7.High security connection

The secure wireless network can be installed quickly and provide flexibility. (Please refer to page 19 for more information on encryption configuration.)

1-3 System Configurations

The 11Mbps Wireless Access Point can be configured in a variety of network system configurations.

Wireless Infrastructure

In a wireless infrastructure, the 11Mbps Access Point acts as a bridge. The Access Point connects the wireless clients together. The Access Point acts as a center point for all wireless communications. This would increase efficiency of the communications since the wireless adapters do not need to be within direct range of each other.

Wireless Infrastructure with Stations Attaching to a Wired LAN

The 11Mbps Wireless LAN Access Point will provide access to your local LAN. An integrated wireless and wired LAN is called an Infrastructure configuration. A group of wireless LAN PC users and an Access Point construct a Basic Service Set (BSS). Each wireless PC in this BSS can talk to any computer on your network via the Access Point.

Connecting the Wireless LAN Micro Access Point to your network

Connecting with Cable/DSL mode, the 11Mbps Wireless LAN Access Point provides you high-speed broadband-sharing gateway.

Point-to-Point/Point-to-Multipoint Connection

The 11Mbps Wireless Access Point provides ideal bridging solution for inter-building LANs connection. In an inter-building application, the 11Mbps Access Point acts as a repeater, thus expanding and connecting corporate LANs with reliable and high-speed connection.

Chapter 2 Hardware Installation

This chapter describes initial setup of the Access Point.

2-1 Product Kit

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

The 11Mbps Wireless LAN Access Point.....x 1
Quick Start Guidex 1
Power Adapter.....x 1
Product CDx 1

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

2-2 System Requirements

Installation of the 11Mbps Wireless LAN Access Point requires:

1. An AC power outlet (100~240V, 50~60Hz), which supplies the power for the Access Point.
2. A 10/100 Base-T (UTP) Ethernet cable drop.

2-3 Mechanical Description

The following table provides an overview of each LED activity:

LED Definition	Activity	Description
PWR	Continuous Green (TR-1000); Continuous Red (Tr-20XX Series)	Power Enabled
Link	Continuous Green	When on, link to at least one unit.
AP *	Continuous Green	Ready. On when in AP mode.
WLAN *	Flashing Green	Flashes when there is RX/TX activity
LAN *	Flashing Green	Flashes when there is wired LAN Activity

* Only apply to the TR-1000

2-4 Hardware Installations

Take the following steps to set up your Access Point.

Site Selection: Before installation, determine the Access Point location. Proper placement of the Access Point is critical to ensure optimum radio range and performance. You may use the Site Survey and Access Points Browser utility (The utilities included with the wireless PC Card) to choose a proper placement for your Access Point. Typically, the best location to place your Access Point at your site is the center of your wireless coverage area. Try to place your mobile stations within the line of sight. Obstructions may impede performance of the Access Point.

Access Point Placement You can place the Access Point on a flat surface such as a table or cabinet, or mount the unit on a vertical surface like a wall. The integrated antenna of your Access Point performs best in an open environment with as few obstructions as possible. In most situations placing the Access Point as pictured below will provide satisfactory performance results.

Connect the Ethernet Cable The 11Mbps Wireless LAN Access Point supports 10/100M Ethernet connection. Attach your UTP Ethernet cable to the RJ-45 connector on

the Access Point. Then connect the other end of the RJ-45 cable to a hub or a station. Please be aware that, use the MDI port to connect the Access Point to a hub. Otherwise, please use the MDI-X port to connect the Access Point to a computer/station.

Connect the Power Cable Connect the power adapter to the power socket on the Access Point, and plug the other end of the power into an electrical outlet. The Access Point will be powered on and all five indicators on the top panel will flash in sequence to test the functionality of the indicators.

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

Chapter 3 Configuring the Access Point

The 11Mbps Wireless LAN Access Point is shipped with default parameters, which will be suitable for the typical **infrastructure wireless LAN**. Just simply install the Access Point, power it on, and it is now ready to work. Nevertheless, you can still adjust configuration settings depending on how you would like to manage your wireless network. The 11Mbps Wireless Access Point allows for configuration either via the configuration utility, known as Access Point Manager, console port connection, or anywhere through a TCP/IP (Telnet) connection.

3-1 Using the Access Point Manager

Installed on your Windows 95/98/NT/2000 desktop computer, the Windows-based utility “**Access Point Manager**” provides a user-friendly interface. The Access Point Manager enables you to configure all of your Access Points on the network more easily than ever before. The following gives instructions guiding you through the installations of the Access Point Manager utility.

1. Insert the Software and Documentation CD into the CD-ROM drive, or the floppy disk that came with your product kit into the floppy drive on your computer.
2. From the Start menu on the Windows desktop, choose **Run**.
3. In the Run dialog box, type the path where the utility is located, and click **OK**. For floppy installation: **A:\setup**.
4. Follow the on-screen instructions to install the Access Point Manager.
5. Upon completion, go to **Program Files** and execute the Access Point Manager utility. It will begin to browse all the Access Points available on the network.
6. Double click an Access Point icon to access its property dialog box. Enter the password in the entry field. The default password is “**default**”.
7. After entering the correct password, a configuration window appears. You will see the basic information of the Access Point, such as MAC Address, Frequency Domain and Firmware Version.

MAC Address: It is a hardware identification number that distinguishes the unit from others. You will see the number on the label located on the bottom of the access point.

Frequency Domain: The regulated operating frequency per country.

Firmware Version: Displays the firmware version that is equipped with your hardware.

Statistics

The statistics tab contains three of the following items for you to monitor the Ethernet and Wireless network traffic.

Ethernet:

You may monitor the TX/RX on the wired network.

Wireless:

You may monitor the TX/RX of the wireless network.

Wireless Error:

This item offers detailed information on error wireless packets that the AP receives and transmits.

Receive:

Packet FCS Errors: The number of wireless packets that fail during FCS transmission (Frame Check Status when accessing the wired network).

No Buffer: The number of wireless packets that the AP ignores due to insufficient memory.

Received WEP Errors: The number of wireless packets that have WEP encryption errors.

Transmit:

Deferred Transmission: The number of packets that have deferred transmission due to the fact that the medium is busy.

Retry Limit Exceed: The number of packets that are not sent due to the reason that the packets exceed the retry limits.

Single Tries: The number of packets that are successfully sent on the first retry.

Multiple Retries: The number of packets that are successfully sent after several retries.

Wrong Source Address: The number of packets that are ignored by the Access Point because the source client is not in its BSS.

Other reasons: Other reasons that cause errors.

Configuration

The configuration tab contains 5 following items for you to make changes for the Access Point.

General:

AP name: In this entry field, you may enter any name. This will enable you to manage your Access Points with more ease if you have multiple Access Point on the network.

IEEE802.11:

Radio mode: You may select the operation mode for your Access Point.

Wireless LAN Access Point (AP): Served as a transparent Media Access Control (MAC) bridge between wired and wireless network.

Inter-Building with Repeating (PxP): Connect several separated networks with Access Points. (To be available soon)

Station Adapter – Infrastructure (SAI): Served as a wireless station (infrastructure). Connected to a PC, it is able to access the network via Access Point.

Station Adapter – Ad-hoc (SAA): Served as a wireless station (Ad-hoc). Connected to a PC, this station adapter along with other wireless stations can establish a small wireless network without Access Points.

Station Adapter – 802.11 Ad-Hoc (SAA2): Same to SAA. This Ad-Hoc mode complies with 802.11 standard.

NOTE: When setting the operation mode to either PxP or SAA, you need to set the Access Points with the same channel. ESSID however can be ignored. When the SAA2 is selected, you need to set both the ESSID and channel for the Access Point.

ESSID: The ESSID is a unique ID given to the Access Point. Wireless clients associating to the Access Point must have the same ESSID. The ESSID can have up to 32 characters.

Channel: You may select any of the available channels as an operational channel for your Access Point.

RTS Threshold: RTS Threshold is a mechanism implemented to prevent the “Hidden Node” problem. “Hidden Node” is a situation in which two stations are within range of the same Access Point, but are not within range of each other. Therefore, they are hidden nodes to each other. When a hidden station starts data transmission with the Access Point, it might not notice that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the Access Point. The collision will most certainly result in a loss of messages for both stations. Thus, the RTS Threshold mechanism will provide the solution to prevent data collisions. When the RTS is activated, the station and its Access Point will use a Request to Send/Clear to Send protocol (RTS/CTS). The station will send an RTS to the Access Point, informing that it is going to transmit the data. Upon receipt, the Access Point will respond with a CTS message to all station within its range to notify all other stations to defer transmission. It will also confirm to the requesting station that the Access Point has reserved the channel for transmission.

Fragmentation Threshold: Fragmentation mechanism is used for improving the efficiency when there is high traffic within the wireless network. If you transmit large files in a wireless network, you can enable the Fragmentation Threshold and specify the packet size.

The mechanism will split the packet into the packet size you set.

TX Rate: When the Access Point is under PXP, SAI, SAA, and SAA2, it provides various data rate options for you to select. Data rates options include Fully Auto, Fixed 1Mb/s, Fixed 2Mb/s, Auto Select 1M or 2M, Fixed 5.5Mb/s, and Fixed 11Mb/s. In most networking scenarios, you will see that the factory-set default “Fully Auto” will prove the most efficient. This setting will allow your 11Mbps Wireless LAN Access Point to operate at the maximum data rate as possible. When the communications quality drops below a certain level, the Access Point will automatically switch to a lower data rate. Transmission at lower data speeds is usually more reliable. However, when the communications quality improves again, the 11Mbps Wireless LAN Access Point will gradually increase the data rate again, until it has reached the highest available transmit rate.

Administration:

You may change the default password by entering the new password. Enter the new password in the **Confirm Change** field to make the new setting take affect.

IP Address:

In the IP Address tab, there are two TCP/IP modes for the Wireless Access Point: **Bridge-Only** and **IP Router**.

Bridge-Only To enable remote access to the Wireless Access Point using Telnet or Web Management, you need to select the **Bridge-Only** mode and assign an IP address to the wireless Router. You may either give a fixed IP address to your Wireless Access Point by choosing the **Manual** item, or set your wireless Access Point to function as DHCP client with the DHCP item selected. It will obtain the IP address automatically from your DHCP server.

IP Router

In the **IP Router** mode, the Wireless Micro Access Point not only acts the bridge but also manages the IP routing with Ethernet port and Wireless LAN port. For example, the Ethernet port of the Wireless Router is connected to your enterprise TCP/IP network (or WAN with Cable/DSL modem) while all the wireless clients being connected with its own IP sub-network. The wireless clients can have private IP addresses and access the Internet by sharing the IP address of Ethernet port with **NAT**.

For further configuration on the **IP Router** mode, you need to configure the Ethernet Port (WAN) and Wireless LAN Port by entering the **Setup** item.

Ethernet Port (WAN): The values refer to the outside network you connect to whenever you access the Internet connection. When the **IP Router** mode is enabled, the Wireless Access Point will act as a DHCP client and automatically obtain the IP address. You may also assign a fixed IP address to your Wireless Access Point by choosing the **Manual** item. If you wish to activate the IP sharing, check the **NAT (IP Sharing) through this port** check box. Moreover, you may have the Wireless Access Point to bridge the non-TCP/IP traffic by checking the “**Enable Bridge**” check box.

PPPoE Setup

If you wish to have the Wireless Access Point connected to a Cable/DSL modem, you will need to manage the PPPoE settings. Once the PPPoE is enabled, the Access Point will get IP configuration through PPPoE regardless of the settings of **Manual** or **DHCP** IP Address. When the **IP Router** mode is selected, the PPPoE will be enabled at the same time (default value). Click the **Setup** button and set the **User Name** and **Password** provided by your ISP. Click **Apply** to make the changes take effect. The Wireless Access Point will then automatically obtain an IP address from the PPPoE server and establish a connection. The wireless clients will be able to access Internet via the Wireless Access Point. To disconnect the link, click on the **Disconnect** button. If you want to re-start a connection, click on the **Connect** button. With **Connect on Demand** checked, together with defined **Max. Idle Time**, the PPPoE connection will be automatically disconnected when the Wireless Access Point does not transmit or receive data within the specified idle time.

Wireless LAN port: These values refer to your internal network settings. Unless you have specific internal needs, there should be no reason to change these values. The default IP Address is 192.168.1.1. If you wish to have the Wireless Access Point to act as a DHCP server of the wireless clients, please enable the **Enable DHCP server (wireless LAN)** check box and configure some network parameters such as IP Address Start, IP Address End, DNS server, etc. For other network parameters such as Netmask, Gateway, DNS

server, WINS server, you may either choose to set manually or obtain these parameter via your DHCP server.

WEP:

The 11Mbps Wireless Access Point allows you to create 4 data encryption keys to secure your data from being eavesdropped by unauthorized wireless user. To activate and set the WEP keys, do the following:

From the WEP encryption item, pull down the menu and it will list three options:

Disable – Allows wireless adapters to communicate with Wireless Access Points without any data encryption.

WEP40 – Requires wireless stations to use data encryption with 64-bit algorithm when communicating with the Wireless Access Point.

WEP128 - Allows wireless clients to communicate with the Wireless Access Point with data 128 Bit encryption algorithm.

When WEP40 is selected, type five alphanumeric characters in the range of “a-z”, “A-Z” and “0-9” (e.g. MyKey) in the WEP Key 1 entry field. Alternatively, you may enter 10 digit hexadecimal values in the range of “A-F” , “a-f” and “0-9”, preceded by the characters “0x” values (e.g. 0x11AA22BB33).

When WEP128 is selected, enter 13 alphanumeric characters in the range of “a-z”, “A-Z” and “0-9” in the WEP Key fields. Alternatively, you may enter 26 digit hexadecimal values in the range of “A-F”, “a-f” and “0-9”, preceded by the characters “0x” values (e.g. 0x00112233445566778899AABBCC).

Enter the 4 WEP keys in the Key 1, Key 2, Key 3 and Key 4 entry filed. Select one WEP key as an active key before enabling use of encryption.

NOTE: The WEP key must be set up exactly the same on the Wireless Access Points as they are on the wireless client stations. If you use Key 1 on the Wireless Access Point and the value is (e.g. MyCar), the same must be assigned to Key 1 for all client stations.

Upgrade

This item is used for uploading the newest firmware of the Access Point. You may either enter the file name in the entry field or browse the file by clicking the **Open File** button. For information about the release of the newest firmware, contact your local reseller.

Access Control:

With the Access Control Table enabled, you can authorize wireless units to access the Access Point by identifying the MAC address of the wireless devices that are allowed access to transmit data. To create or edit the Access Control Table, do the following:

Go to the Access Control tab and select “**Enable Access Control**”. Note that when you enable the Access Control Table without any MAC address in the table, no access is allowed to communicate with the Access Point.

Use the following buttons to manage the Access Control Table:

Add – to enter MAC addresses of authorized wireless devices one at a time

Edit – to change the entries in the table if you enter the incorrect MAC address

Remove – to remove MAC addresses one at a time

Clear – to remove all MAC addresses in the table

Import – to import an existing Access Control Table

Export – to save the current Access Control Table to a location on your computer

- The import/export file is in a plain text format.

3-2 Using the Web Management

The built-in Web Management provides you with a user-friendly graphical user interface (web pages) to manage your Wireless Access Points. An AP with an assigned IP address (e.g. ***http://192.168.1.1***) will allow you via web browser (e.g., Netscape Navigator 3.0 ~ 4.5 or MS Internet Explorer 4.0 or later) to monitor and configure the Wireless Access Point.

1. Open your web browser.
2. Enter the IP address of your Wireless Access Point in the Address field (e.g. <http://192.168.1.1>). You will have access to the **Wireless Access Point Web Pages** of the Wireless Access Point.
3. Click on the **Neighborhood Access Point** item and you will see all the other Access Points available on the network.
4. Enter the password to login to the Wireless Access Point. The default password is **default**. The main page will show up.

The Wireless Access Point main page contains three items for you to manage your Wireless Access Point.

Information

General

This item displays the general information of the Wireless Access Point such as the MAC address, Frequency Domain, and Firmware Version.

Statistics

This item displays the Ethernet and wireless network traffic.

Configuration

General

You may make the settings on the Wireless Access Point such as ESSID, Radio mode, channel, RTS threshold, fragment threshold and password.

WEP

To prevent unauthorized wireless stations from accessing data transmitted over the network, the 11Mbps Wireless LAN Access Point offers WEP (Wired Equivalency Privacy). You can set up 4 encryption keys but choose one key to encrypt your data. For detailed configuration please refer to page 19.

Access Control

The Access Control Table enables you to restrict wireless stations accessing the Wireless Access Points by identifying the MAC address of the wireless devices.

TCP/IP

The Access Control Table enables you to set the Wireless Access Point act as either a bridge with DHCP client enabled, or a wireless Router with DHCP server and PPPoE enabled.

Upgrade

Here, you can upload the newest firmware of the Wireless Access Point. You may either enter the file name in the entry field or browse the file by clicking the **Browse** button.

3-3 Using the Console Mode

The Access Point can be configured via the command prompt console with either:

RS232 (serial) Connection: The RS232 port configuration is provided for advanced users to manage the Access Point. You may use any terminal emulation program with a RS232 (serial) connection (e.g., Telix, ProCOMM, Windows 95/98/NT/ME/2000's HyperTerminal) to configure the Access Point.

Telnet (TCP/IP) Connection: Assign an IP address to your Access Point through the RS232 connection or Access Point Manager and then telnet to the Access Point anywhere to get access to the Access Point console. Thus, you will be able to make the configuration via the TCP/IP connection.

The following are the instructions to configure the Access Point through RS232 connection under Windows. Configuration through **Telnet** is the same as the RS232 configuration.

1. Attach the 9-pin or 25-pin connector of the RS232 cable to the COM port on your computer.
2. Connect the other end of the RS232 cable to the RS-232 port on your Access Point.
3. From the **Start** menu, select **Program Files** and open the Terminal program.
4. Assign a name for the connection.
5. Select the Com port and click **OK**.
6. Set the port settings to **57600 bps, 8 data bits, no parity, no flow control**. Click **OK**.
7. The Access Point console screen appears when the connection has been established.

3-3-1 Basic Commands

The following are the commands provided for configuring the Access Point. In loader mode, i.e., no valid firmware in the Access Point, only the commands with an asterisk (*) are provided.

NOTE: [xxx] stands for optional arguments.

*Info**

Display some basic information of the Access Point such as firmware version, frequency domain, etc.

stat

Display the statistical values of the operation of the Access Point such as association status, LAN/WLAN interface load, etc.

passwd [clear]

Change the password of the Access Point. The *clear* option is used to delete the existing password if you miss it (This option is only available in RS232 console). ping ip_addr [num_pings] [data_size]

Ping (ICMP echo) to an *ip_addr* host with optional *num_pings* times with optional data size in a length of *data_size*.

set

List the configuration information.

Set apname | channel | essid | rts_threshold | frag_threshold | ip_address | ip_netmask | ip_gateway

To change factory default settings, type “set xxx (parameter) xxxx (value) based on the chart below. For example, set channel 7 command will set the channel to number 7; set essid “Your Network” command will set the ESSID as *Your Network*. Remember that, a ‘save’ command is required for changes to take effect. Always reset your AP with the “Reset” command.

The following is a list of parameters you can make changes on the Access Point.

Parameter	Description	Default Value
apname	name of the unit	ApXXXXXX (X's are the units MAC Address)
mode	The operation mode of the unit: AP- Wireless Access Point SAI- Station Adapter Infrastructure PxP - Inter-Building with Repeating SAA - Station Adapter - Ad-hoc SAA2 - Station Adapter - 802.11 Ad-hoc	AP
channel	The Radio Channel Number	1
essid	The ESSID of the unit.	My Network
tx_rate	Transmission Rate	Auto
TX_retry	Number of retries for data transmission	7
rts_threshold	The threshold (number of bytes) for enabling RTS/CTS handshake. Data with frame size larger than this value will perform the RTS/CTS handshake. Range 0 - 2432	2432
frag_threshold	The threshold (number of bytes) for the fragmentation boundary. Data will be received in fragments which its size does not exceed this value. Range 256 - 2432	2432
lan_speed	transmission speed of the LAN port: 10/100 Mbps	Auto

save

Save your new configuration. Remember that the “save command” is required every time you make the new configuration.

set default

Return the factory default settings of the Access Point except for the IP addresses. A 'save' command is required for changes to take effect.

*cls**

Clear the console screen.

*exit**

Exit the console.

*? * or help**

Print a help screen.

*rz**

Receive a firmware file by the Zmodem protocol. The console will enter Zmodem receiving mode and then use the "file upload" function of your terminal emulation program to upload a new firmware file (ap.img) to the Access Point. Upon completion, always remember to type the 'reset' command for running the Access Point with the new firmware.

*reset**

Issue a reset signal. The Access Point will be reset if the user confirms.

3-3-2 Advanced Setup

This section describes the advanced commands to configure the 11Mbps Wireless Access Point. The advanced parameters include **Access Control Table**, **WEP**, **DHCP/IP Router Mode**, **PPPOE**, **Wireless DHCP Server** and **NAT**. Please follow the instructions of each command to set your Access Point.

Access Control

auth mode | add | del | list | clear

The 'auth' command contains sub-commands that allow you to manage the access control (MAC address filter) of the Access Point. The access control table consists of a list for you to control the accessibility of any wireless stations or repeaters. The sub-commands are listed below:

mode open | allow: set the access control mode. The definition of each mode is specified as follows:

- *open*: open to public (default)
- *restrict*: only allow access of the authorized stations/repeaters in the table (no access is allowed if the list stays empty)

add mac_addr: add an address into the access control table

del mac_addr | index: delete a MAC address, or index an address from the access control table

list [start/end]: display the content of the access control mode and the address list. The optional arguments, start and end, can be affixed to select the range of items to be listed.

clear: clear all the addresses in the access control table.

WEP Keys

wep mode | set | list

The 'wep' command contains sub-commands that allow you to manage the data encryption (WEP, wired equivalent privacy) function provided with the Wireless Micro Access Point. The sub-commands are listed as follows:

mode disable | wep40: set the access control mode. The following are the definition of each data encryption mode.

- *none*: no encryption (default)
- *wep40*: use 40-bit WEP data encryption
- *wep128*: user 128-bit WEP data encryption

set key1 key_text: set WEP Key#1 as *key_text*. 10 hexadecimal digits (0-9 or A-F) heading by "0x" or five alphanumeric values (ASCII characters, case-sensitive) are required (e.g. 0x1122334455, 0x0055AA55AA, abcde, or MyKey.) if 40-bit WEP is used. Type 26 hexadecimal digits (0-9, a-f, or A-F) heading by "0x" or 13 alphanumeric characters ranging from "a-z", "A-Z" and "0-9" if 128-bit WEP is used (e.g. 0x12345678901234567890123456, or MyKey12345000).

set key2 key_text: set WEP Key#2 as *key_text* with a same format as WEP Key#1.

set key3 key_text: set WEP Key#3 as *key_text* with a same format as WEP Key#1.

set key4 key_text: set WEP Key#2 as *key_text* with a same format as WEP Key#1.
set usekey 1|2|3|4: Select the WEP key to be used for encrypting data transmission.
Only one key can be selected at a time.

list: Display current WEP settings.

Note: Your new WEP settings will take effect after resetting the Access Point.

DHCP/IP Router Mode

ipcfg set | renew | release

The 'ipcfg' command contains sub-commands that allow you to manage Ethernet port of the Wireless Micro Access Point. You may set the Wireless Access Point act as either a bridge with DHCP client enabled, or a wireless Router with DHCP server and PPPoE enabled. The sub-commands are described as follows:

set mode | obtain | ip_address | ip_netmask: set TCP/IP mode and other related parameters for the Wireless Access Point. The definition of each mode is specified as follows:

- *mode [bridge/router/brouer]*: Set the TCP/IP mode.
- *obtain [manual/dhcp]*: manually assign an IP address to your Wireless Access Point or obtain an IP address from your DHCP server.
- *ip_address [1/2] xxx.xxx.xxx.xxx*: enter a fixed IP address for the Wireless Access Point.
- *ip_netmask [1/2] xxx.xxx.xxx.xxx*: enter the address of the netmask
- *ip_gateway [1/2] xxx.xxx.xxx.xxx*: enter the address of the default gateway

renew: re-assign an IP address to the Wireless Access Point via your DHCP server.

release: release the current IP address of the Wireless Access Point.

PPPoE Setup

The 'pppoe' command contains sub-commands that allow you to configure the pppoe setup for the Wireless Access Point. When you enter the "pppoe" command, you will see some information such as pppoe mode, username, password and IP address, etc. The sub-commands are described as follows:

set mode | username | passwd | cm | idle_time: set the pppoe mode and other parameters for the Wireless Access Point. The definition of each command is listed as follows:

- *mode [disable/enable]*: disable or enable the pppoe function
- *username*: authentication for the connection to your ISP.
- *passwd*: authentication for the connection to your ISP.
- *cm [disable/enable]*: you may choose to always connect to PPPoE or connect the PPPoE on demands.
- *idle_time*: set the time limit for the PPPoE to be closed when there is no data being transmitted or received within this specified time.

connect: establish a PPPoE connection.

Disconnect: terminate the PPPoE connection

Wireless DHCP Server

The 'dhcps' command contains sub-commands that allow you to manage Wireless LAN port of the Wireless Access Point. You may set the Wireless Access Point act as wireless DHCP server. All the wireless clients can automatically obtain an IP address from the Wireless Access Point. The sub-commands are described as follows:

set mode | ip_start | ip_end | ip_netmask | ip_gateway | ip_dns1 | ip_dns2 | ip_wins1 | ip_wins2 |wizard: set the DHCP server mode and other related network parameters for the Wireless Access Point. The definition of “dhcp set mode” command is listed as follows:

- mode [*disable/enable*]: disable or enable the DHCP server function

stat: display IP addresses and MAC addresses of wireless clients.

NAT Setup

The 'nat' command contains sub-commands that allow you to manage NAT configuration for the Wireless Access Point. All the wireless clients can access Internet with a single IP address. Note that NAT will function only when the Wireless Access Point is set to IP Router mode. The sub-commands are described as follows:

mode[disable/enable]: enable or disable the NAT function

stat: display status of the wireless clients

Chapter 4 Troubleshooting

If you have trouble using the 11Mbps Wireless LAN Access Point, the starting point to troubleshoot the problem with your Access Point is looking at the LED activity of the Access Point. The following is “LED Error Table” provided to assist you in diagnosing and solving operational problems.

TR- 1000 LED Activity Table

PWR	AP	WLAN	LAN	LINK	DESCRIPTION/ACTION
Continuous Green	Continuous Green	Flash Green	Flash Green	Steady Green	Normal Activity ? No Action Required
	On	Off	Off	—	No LAN Activity ? No Action Required
Off	Off	Off	Off	Off	Power failure ? Check power chord/supply
Continuous Green	Off	Off	Off	Off	Invalid loader Firmware or micro-controller dead ? Return to Dealer for support
	Blink Green	—	—	—	Invalid Access Point Firmware ? Upgrade firmware
	Blink Green	Blink Green	—	—	Wireless LAN initialization failure ? check whether the wireless module has been properly installed
	Blink Green	—	Blink Green	—	Ethernet initialization failure ? Return device to the vendor for support

TR-2000 LED Activity Table

PWR	LINK	DESCRIPTION/ACTION
Continuous Red	Steady Green	Normal Activity ? No Action Required
	—	No LAN Activity ? No Action Required
Off	Off	Power failure ? Check power chord/supply
Continuous Red	Off	Invalid loader Firmware or micro-controller dead ? Return to Dealer for support
	—	Invalid Access Point Firmware ? Upgrade firmware
	—	Wireless LAN initialization failure ? check whether the wireless module has been properly installed
	—	Ethernet initialization failure ? Return device to the vendor for support

If you are still unable to solve the problem by checking the LED activity, the error may be caused from configuration mismatch, which prevents the Access Point from establishing a wireless connection with the network. You may check the following to ensure normal operation of the Access Point.

WEP keys: If data encryption is activated, always remember to set WEP keys exactly the same on the Access Point as are on the wireless stations.

Access Control: Make sure that the MAC address of your Access Point is not included in the Access Control table of other wireless devices.

Appendix A Tutorial on Network Configuration

The 11Mbps Wireless LAN products support the same network configuration options of the legacy Ethernet LANs as defined by IEEE 802 standard committee.

The 11Mbps Wireless LAN products can be configured as:

Ad-Hoc for departmental or SOHO LANs

Infrastructure for enterprise LANs

LAN-Interconnection for point-to-point link as a campus backbone.

A-1 Network Topology

Ad-Hoc

An Ad-Hoc wireless LAN is a group of computers, each equipped with one wireless adapter, connected as an independent wireless LAN. Computers in a specific Ad-Hoc wireless LAN must be configured at the same radio channel.

Ad-Hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

Infrastructure

The 11Mbps Wireless LAN devices provide access to a wired LAN for wireless workstations. An integrated wireless and wired LAN is called an Infrastructure configuration. A group of wireless LAN PC users and an Access Point construct a Basic Service Set (BSS). Each wireless-equipped PC in this BSS can talk to any computer in the wired LAN infrastructure via the Access Point.

Infrastructure configuration will extend the accessibility of a wireless station to the wired LAN. Multiple Access Points will allow roaming and it will increase the transmission range. The Access Point is also able to forward data within its BSS. The effective transmission range in an infrastructure LAN is **doubled**.

Appendix B Specifications

Product	11Mbps Wireless LAN Access Point
Wired Interface	10/100 base T (RJ-45)
Serial Port (TR-1000 only)	DB9 RS-232 (configuration port)
Wireless Interface	11Mbps Wireless LAN
Modulation	DSSS (CCK, DQPSK, DBPSK)
Operation Frequency	N. America/FCC: 2412~2.462 GHz (11 channels) Europe CE/ETSI: 2.412~2.472 GHz (13 channels) Japan: 2.412~2.484 GHz (14 channels) France: 2.457~2.472 GHz (4 channels) Spain: 2.457~2.462 GHz (2 channels)
Speed Options	11M/5.5M/2M/1M, also support Auto Rate Selections
RF Technology	Direct Sequence Spread Spectrum
Power Supply	DC 12V (External power supply included)
RF Output Power	13 dBm
Sensitivity	-84dBm @ 11Mbps, PER < 8* 10 ⁻²
Antenna	TR-1000 and TR-2000 N-female connector
	TR-2015 15 dBi integrated panel
	TR-2018 18 dBi integrated panel

Appendix C Glossary

Access Point - An internetworking device that seamlessly connects wired and wireless networks.

Ad-Hoc - An Ad-Hoc wireless LAN is a group of computers each with wireless adapters, connected as an independent wireless LAN.

Backbone - The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is off-loaded onto a local system.

Base Station - In mobile telecommunications, a base station is the central radio transmitter/receiver that maintains communications with the mobile radio telephone sets

within range. In cellular and personal communications applications, each cell or microcell has its own base station; each base station in turn is interconnected with other cells' base.

Bridge - An internetworking function that incorporates the lowest 2 layers of the OSI network protocol model.

BSS - Stands for "Basic Service Set," an Access Point and all the wireless clients that associated with it.

ESS - Stands for "Extended Service Set." More than one BSS can be configured as an Extended Service Set. Mobile users can roam between BSS in an ESS.

Ethernet - A popular local area data communications network, originally developed by Xerox Corp., which accepts transmission from computers and terminals. Ethernet operates on 10 Mbps baseband transmission over shielded coaxial cable or over shielded twisted pair telephone wire.

Infrastructure - An integrated wireless and wired LAN is called an Infrastructure configuration.

PCMCIA - Personal Computer Memory Card International Association, which develops standards for PC cards, formerly known as PCMCIA cards, are available in three "types" which are about the same length and width as credit cards, but range in thickness from 3.3 mm (Type I) to 5.0 mm (Type II) to 10.5 mm (Type III). These cards can be used for many functions, including memory storage, landline modems and wireless modems.

Roaming - A wireless clients around an ESS and get the continuous connection to the Infrastructure network.

RTS Threshold – Transmitters contending for the medium may not hear each other. RTS/CTS mechanism can solve this " Hidden Node Problem". If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

Web Management - Network management by using web browser connecting to the target devices.