WLAN OUTDOOR RADIO

FOR 5.8GHz Hotspot / PWLAN / PTP / PTMP

WR210 Series

User Manual

Includes install, configuration and trouble shooting information for the outdoor radio.

Azuretec™

go the extra mile

Ver 2.0 MAY 2005

Copyright

Copyright © 2004 Azuretec Co., LTD. 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

This manual includes install, configuration and trouble shooting for the WLAN outdoor radios. It can help you in avoiding the unforeseen problems and use the outdoor radio correctly.

Technical Support

If you have difficulty resolving the problem while installing or using the Wireless LAN ODU, please contact the supplier for support.

Copyright © 2004 Azuretec Co., LTD. all rights reserved.

Table of Contents

Chapter 1 Introduction.....1

1-1 Features and Benefits..... 1

1-2 Applications..... 2

1-3 System Configurations..... 3

Chapter 2 Hardware Installation 5

2-1 Product Kit..... 5

2-2 System Requirements..... 5

2-3 Mechanical Description..... 6

2-4 Hardware Installation..... 7

Chapter 3 Configuring the ODU 8

3-1 Configuration..... 8

3-2 Using the Web Management..... 23

3-3 Using the Telnet..... 29

Appendix A: Channels..... 36

Appendix B: Troubleshooting..... 37

Copyright © 2004 Azuretec Co., LTD. all rights reserved.

Chapter 1 Introduction

The Outdoor wireless LAN device – 11Mbps Wireless Outdoor Unit, are specially designed for Point-to-Point and Point-to-Multipoint applications, offering long distance connections between buildings at a speed of up to 11Mbps. Fully compliant with IEEE802.11b standard, the Outdoor Unit (ODU) provides powerful features such as the Windows-based configuration utility, MAC address filtering, WEP security and more.

1-1 Features and Benefits

- Creates a Point-to-Point connection linking two LANs, using 2 Indoor Units or Indoor and Outdoor total solutions.
- Creates a Point-to-Multipoint system using three or more Indoor Units or Indoor and Outdoor total solutions.
- Detachable antenna allows you for the use of external high gain antenna.
- With a data rate of 11Mbps and 5.5Mbps, the system is faster than an E1/T1 data link.
- 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 5.8GHz ISM band.
- Seamless roaming within the 802.11 & 802.11b wireless LAN infrastructure.
- Provides user authentication to enforce tight security.
- MAC address Access Control.
- Bandwidth control
- Advanced Security — 802.1x authentication (EAP)
- Provides Window-based configuration utility.
- Waterproof housing

Copyright © 2004 Azuretec Co., LTD. all rights reserved.

1-2 Applications

The 11Mbps Wireless LAN ODU offers 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. **High Security Connection**
   The secure wireless network can be installed quickly and provide flexibility. (Please refer to page 16 for more information on encryption configuration.)

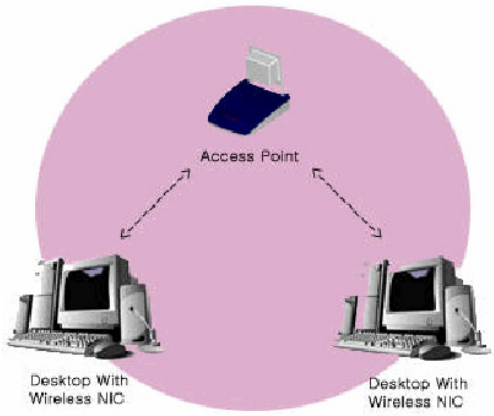
Copyright © 2004 Azuretec Co., LTD. all rights reserved.

1-3 System Configurations

The 11Mbps Wireless LAN ODU can be configured in a variety of network system configurations.

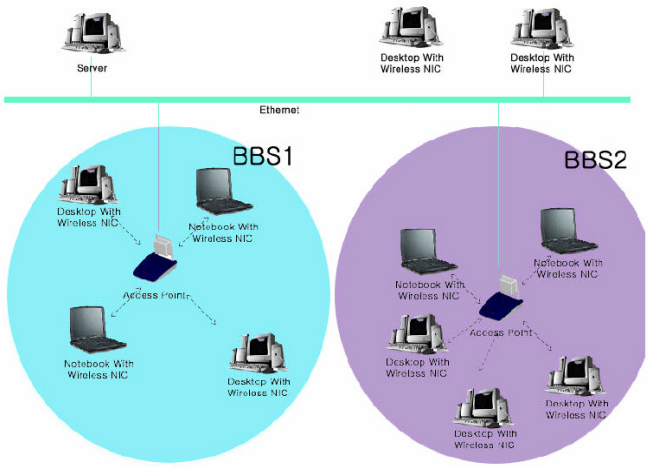
Wireless Infrastructure

In a wireless infrastructure, the ODU can act as a bridge. The ODU connects the wireless clients together. The ODU 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

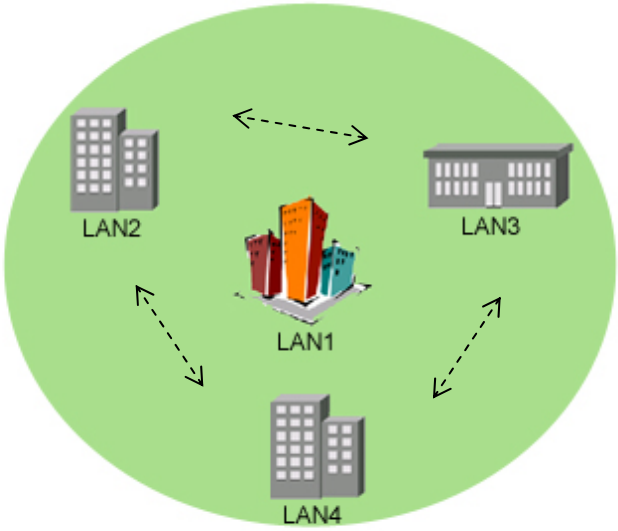
The 11Mbps Wireless LAN ODU will provide an access to the local LAN. An integration of wireless and wired LAN is called an Infrastructure configuration. A group of wireless LAN PC users and an ODU construct a Basic Service Set (BSS). Each wireless PC in this BSS can talk to each other on your network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



Copyright © 2004 Azuretec Co., LTD. all rights reserved.

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

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



Copyright © 2004 Azuretec Co., LTD. all rights reserved.

Chapter 2 Hardware Installation

This chapter describes initial setup of the Wireless LAN ODU subsystem.

2-1 Product Kit

Before installation, make sure that you the following items:

- **11Mbps Wireless LAN ODU Kit**……..……..……..x 1
- **Power over Ethernet**……..……x 1
- **Power Adapter**……..……..……x 1
- **Power Cord**……x 1
- **Mounting kit**..……..……...x 1
- **Product CD**……x 1
- **Quick Installation Guide**……..……x 1

NOTE: If any of the above items are missing or damaged, please contact your local dealer for support.

2-2 System Requirements

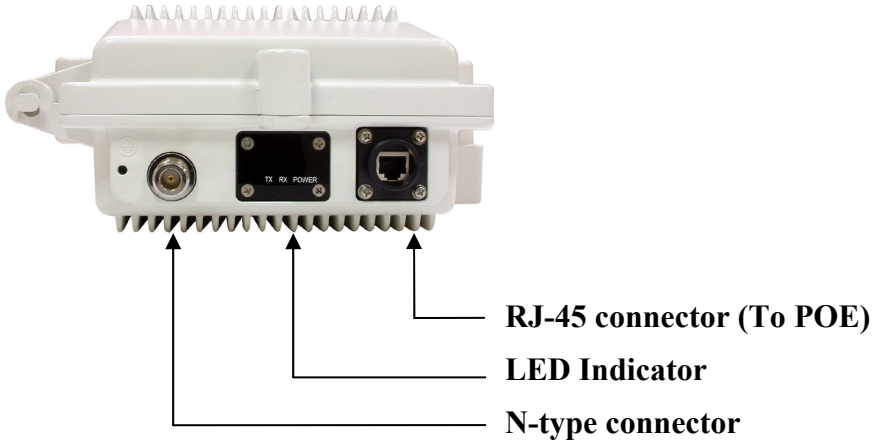
Installation of the 11Mbps Wireless LAN ODU requires:

1. A DC 15V adapter which supplies the power for the PoE (Power over Ethernet).
2. A 10/100 Base-T (UTP) Ethernet cable drop.
3. Operating system support: Windows 98/Me/NT4.0(SP4 or above)/2000/XP

Copyright © 2004 Azuretec Co., LTD. all rights reserved.

2-3 Mechanical Description

ODU:



LED Indicator

Power / Tx / Rx / Signal level

Waterproof RJ-45 connector

Connect to the POE with SFTP cable.

N-type connector

Connect to the antenna by the RF cable. The maximum RF cable length depend on the loss of the RF cable.

SFTP Cable

This cable is attached to the ODU. The default SFTP cable length is 25 meter.

Copyright © 2004 Azuretec Co., LTD. all rights reserved.

2-4 Hardware Installation

Take the following steps to set up your ODU.

- **Connect the Ethernet Cable**

  The 11Mbps Wireless LAN ODU supports 10/100M Ethernet connection. Connect the SFTP cable from the ODU to the RJ-45 connector of PoE (marked "To ODU") for ODU connection. Then connect the other end of the POE with straight RJ-45 cable to a hub or a switch. **Please note that, use the cross-over cable when you desire to connect the PoE of ODU to a PC.**

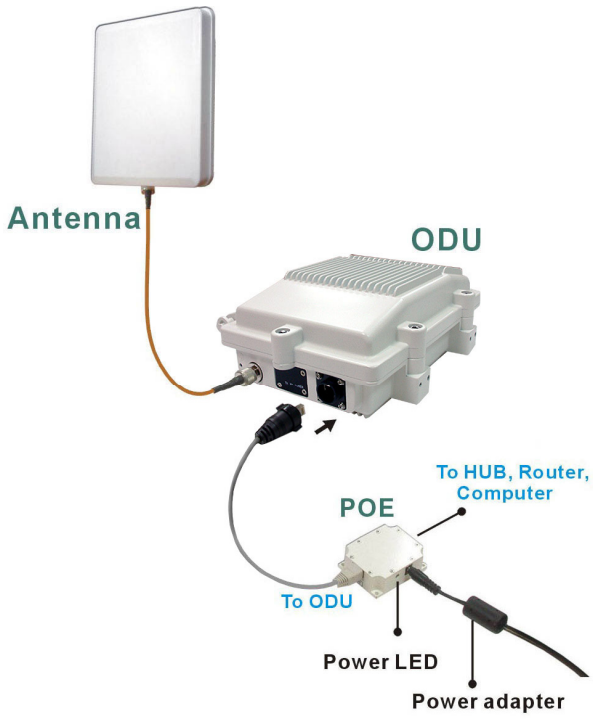
- **Connect the Antenna**

  In ODU connection, you can connect antenna to the N-type connector of ODU by RF cable.

- **Connect the Power Cable**

  Connect DC 15V adapter to the PoE, and plug the other end of the adapter into an electrical outlet.

NOTE: Only use the power adapter supplied with the PoE of ODU. Otherwise, the product may be damaged.



Copyright © 2004 Azuretec Co., LTD. all rights reserved.

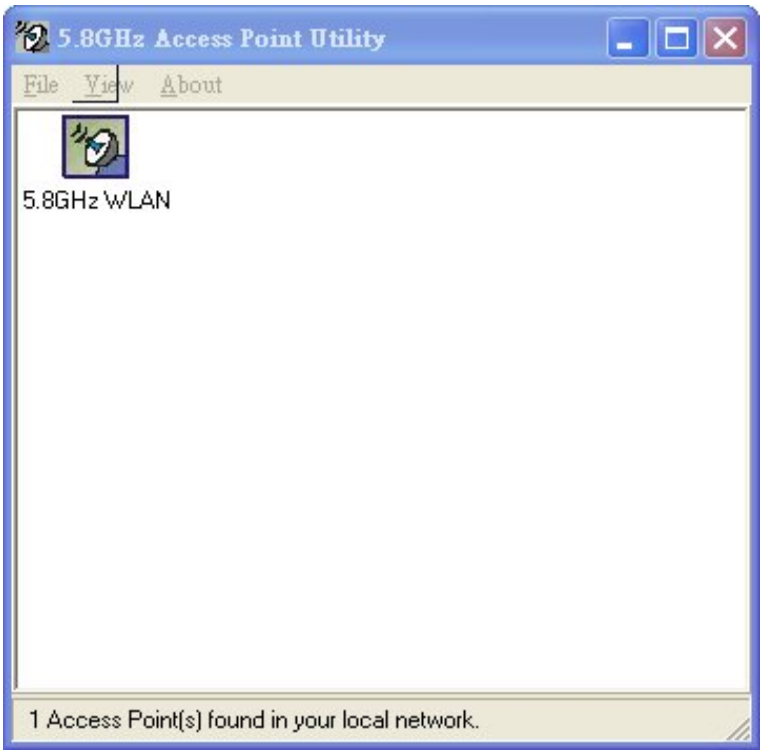
Chapter 3 Configuring the ODU

The 11Mbps Wireless LAN ODU is shipped with default parameters, which will be suitable for the typical **Point-to-Point and Point-to-Multipoint**. You can still adjust configuration settings depending on how you would like to manage your wireless network. The 11Mbps Wireless ODU allows for configuration either via the configuration utility, known as Access Point Manager, TCP/IP (Telnet) connection or Web Management.

3-1 Configuration

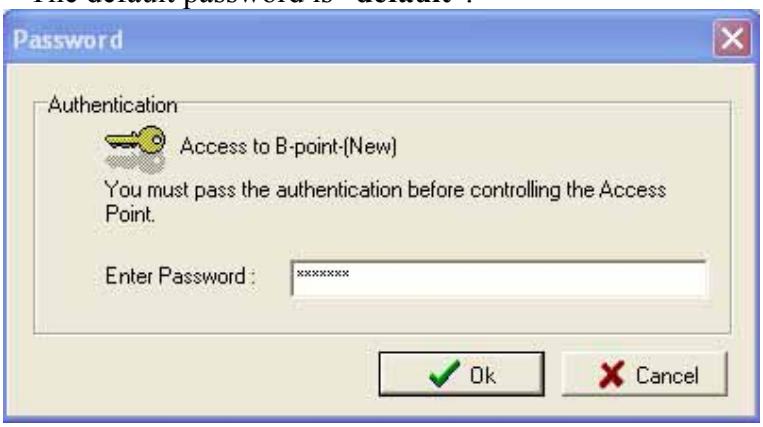
Installed on your Windows 95/98/NT/ME/2000/XP desktop computer, the Windows-based utility "***Access Point Utility***" provides a user-friendly interface. The ODU Utility enables you to configure all of your ODUs on the network more easily than ever before. The following gives instructions guiding you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

1. Insert the Product CD-ROM disk that came with your product kit into the corresponding 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, then click **OK**.
4. Follow the on-screen instructions to install the Access Point Utility.
5. Upon completion, go to **Program Files** and execute the Access Point Utility. It will begin to browse all the ODU available on the network.

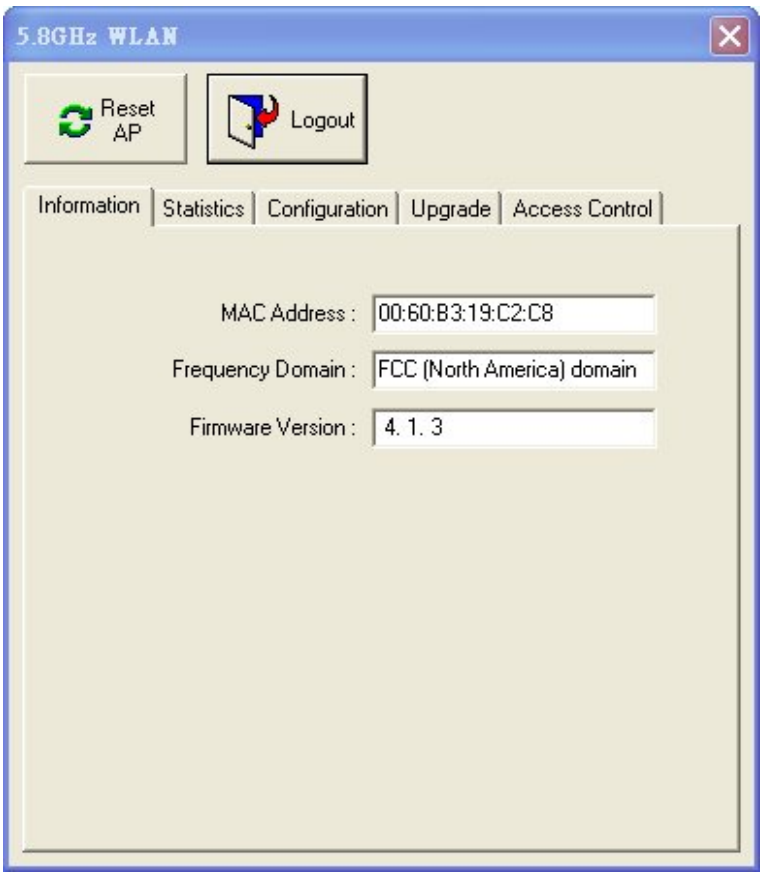


Copyright © 2004 Azuretec Co., LTD. all rights reserved.

6. Double click 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 ODU, such as MAC Address, Frequency Domain and Firmware Version.



MAC Address: It is a hardware identification number that distinguishes the unit from others.

Frequency Domain: The regulated operating frequency per country.

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

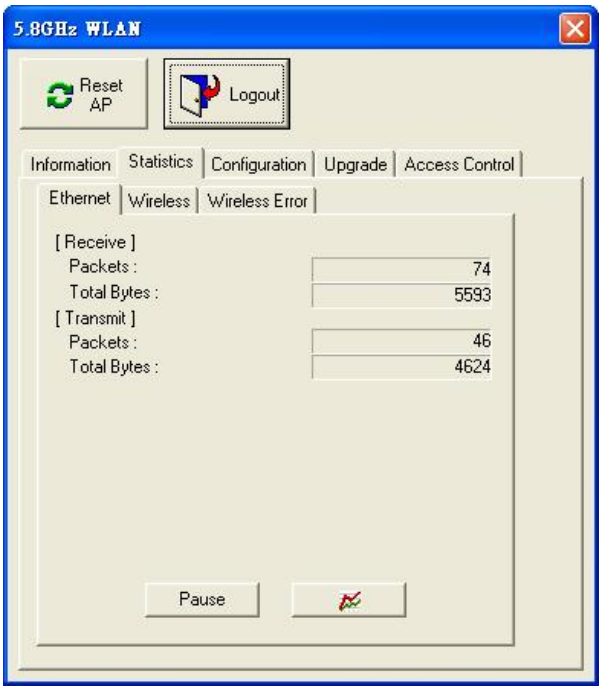
Copyright © 2004 Azuretec Co., LTD. all rights reserved.

Statistics

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

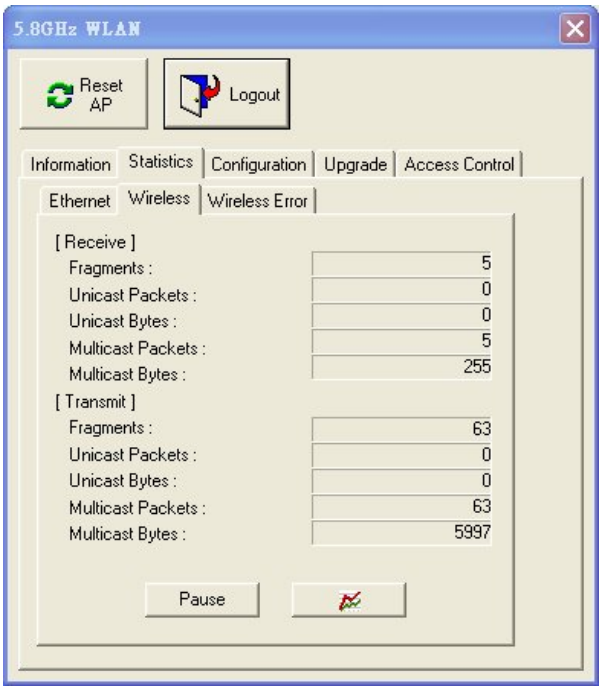
Ethernet:

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



Wireless:

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



Copyright © 2004 Azuretec Co., LTD. all rights reserved.

Wireless Error:

This item offers detailed information on error wireless packets that the ODU 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 ODU 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.

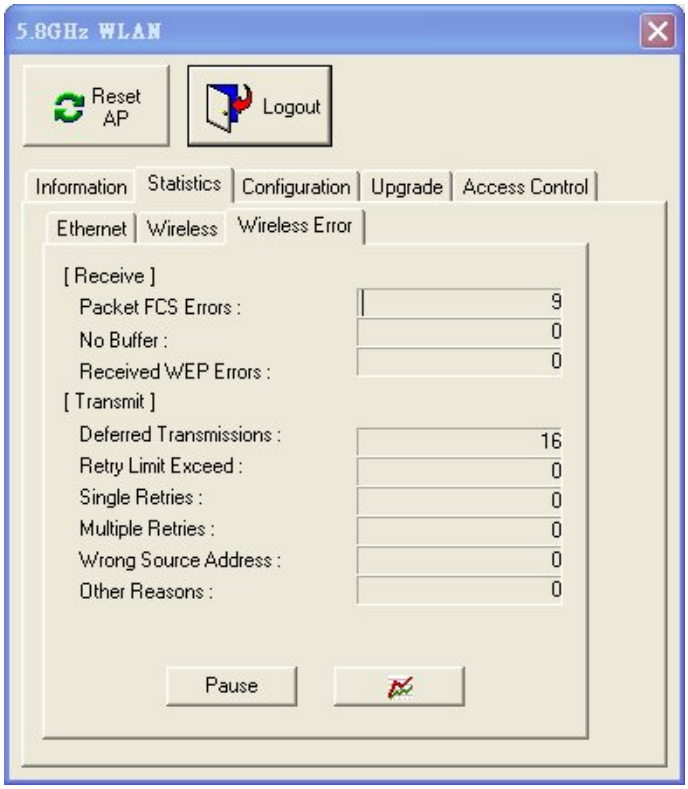
Retry Limit Exceed: The number of packets that are not sent due to the reason that the packets exceed the retry limits.

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 ODU because the source client is not in its BSS.

Other reasons: Other reasons that cause errors.



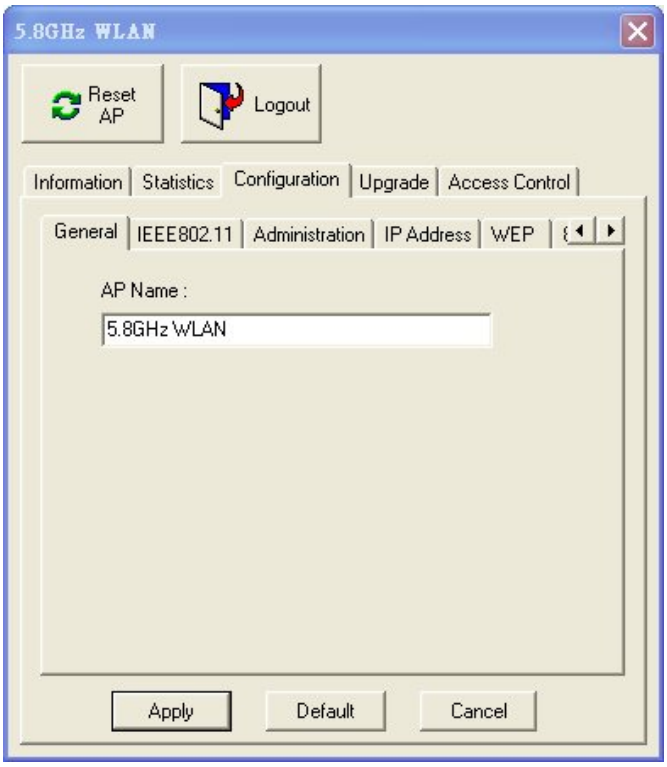
Copyright © 2004 Azuretec Co., LTD. all rights reserved.

Configuration

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

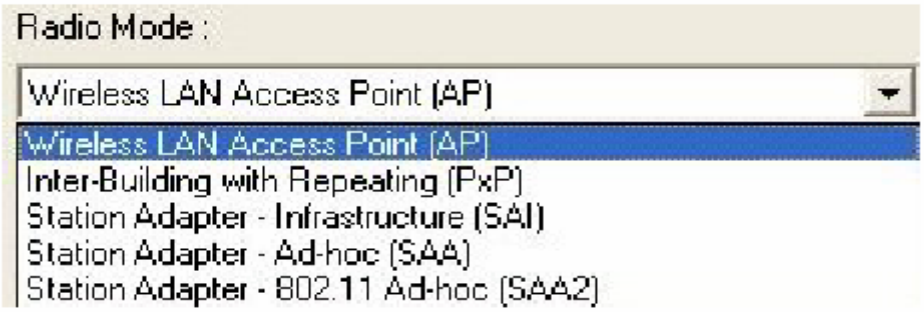
General:

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



IEEE802.11:

Radio Mode: The Wireless LAN ODU can operate total of 5 radio modes:

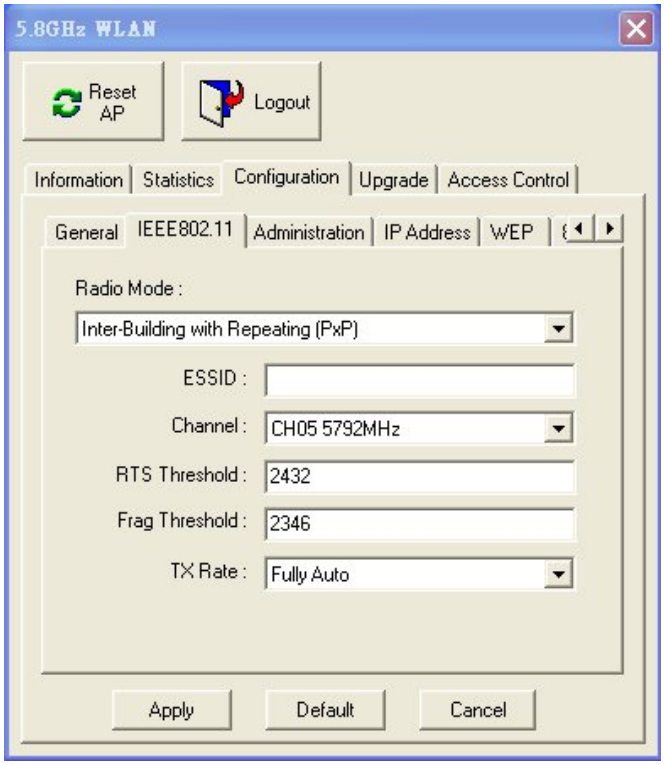


- ***Wireless LAN Access Point (AP)***: Enables the ODU to act as a wireless bridge connecting to your network backbone.
- ***Inter-building with Repeating (PxP)***: Allows for multi-point connection among LANs (default setting).

Copyright © 2004 Azuretec Co., LTD. all rights reserved.

- ***Station Adapter – Infrastructure (SAI)***: Served as a wireless station (infrastructure). Connect the ODU (SAI) to a PC with a cross over RJ-45 cable, and it is able to access the network via ODU.
- ***Station Adapter – Ad-Hoc (SAA)***: Served as a wireless station (Ad-hoc). Connecting to a PC with a cross-over RJ-45 cable, the station adapter along with other wireless stations can establish a small wireless network without ODUs.
- ***Station Adapter – 802.11 Ad-Hoc (SAA2)***: Similar to SAA, the ODU acts as a wireless stations (Ad-Hoc). The only difference is that 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 ODU with the ***same channel***. ESSID however can be ignored. When the **SAA2** is selected, you need to set the ODU the ***same ESSID and channel***.



ESSID: The ESSID is a unique ID given to the ODU. Wireless clients associating to the ODU 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 ODU. You may use the **Site Survey** tool came with the wireless PC Card utility to monitor each channel and choose a channel with good quality.

RTS Threshold: RTS Threshold is a mechanism implemented to prevent the "Hidden

Copyright © 2004 Azuretec Co., LTD. all rights reserved.

Node" problem. "Hidden Node" is a situation in which two stations are within range of the same ODU, but are not within range of each other. Therefore, they are hidden nodes for each other. When a hidden station starts data transmission with the ODU, it might not notice that another 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 ODU. 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 ODU will use a Request to Send/Clear to Send protocol (RTS/CTS). The station will send an RTS to the ODU, informing that it is going to transmit the data. Upon receipt, the ODU 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 ODU 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.

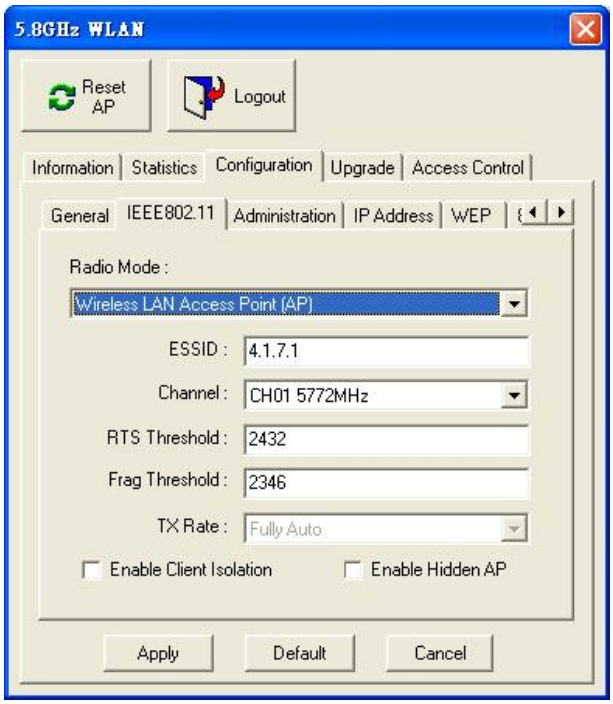
The mechanism will split the packet into the packet size you set.

TX Rate: When the ODU 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 ODU to operate at the maximum data rate as possible. When the communications quality drops below a certain level, the ODU 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 ODU will gradually increase the data rate again, until it has reached the highest available transmit rate**.**

Client Isolation and Hidden SSID:

only AP mode is available for the configuration of **"client isolation"** and **"Hidden AP"**.

Copyright © 2004 Azuretec Co., LTD. all rights reserved.



Enable Client Isolation

Enabling the parameter, the wireless clients will not be able to virtually "see" any others who associated with the same access point. **Remark**: supposedly there are two clients associated with the same access point, client A and B. In this case, the wireless client A will not be able to talk to the client B in any level of network protocol and vice versa. The function can prohibit users from accessing the unauthorized resources in your wireless network but can't prevent users from accessing your wired network though. To disable the function, the protection on the access point will be also disabled. When you have done your selection, please press the "Apply" button to have the function take effect. The default value is "disable".

> **IN DEPTH:** The function will only refine the efficient isolation on the area of a same BSS. It won't work out the same protection for those clients who associated with different access points (in different BSS). In this case, to adopt virtual LAN may be a wonderful solution.

Hidden AP Parameters

Enabling the function, the AP will stop processing the connecting request of the clients (in active scan mode) who aren't aware of the identity (SSID) of the wireless network (AP). In the case, the identity (SSID) must be given for a successful access to your network in advance. When you have done your selection, please press the "Apply" button to have the function take effect. The default value is "disable".

> **IN DEPTH:** The hidden function can bring up a natural protection that wireless standard naturally introduced, to implement it will be able to prohibit access point from responding the connecting request of the client who carries the known SSID. The protection is very preliminary and can setup a basic secured network in parallel with

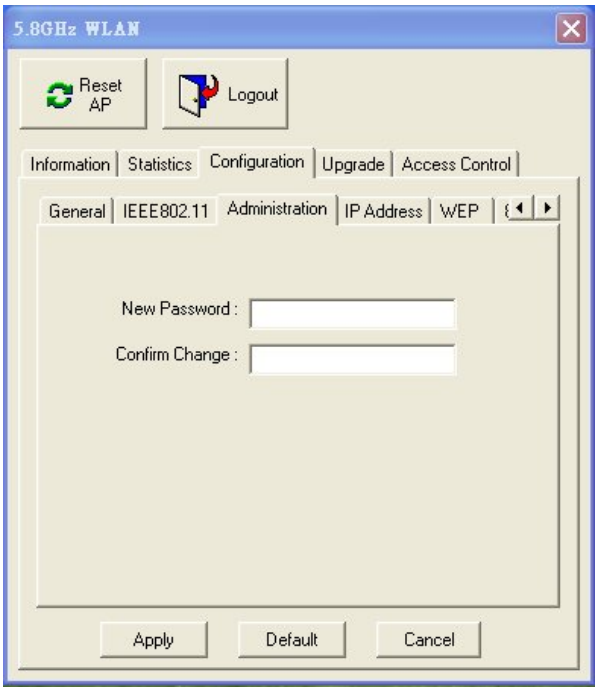
Copyright © 2004 Azuretec Co., LTD. all rights reserved.

access control and WEP security.

Copyright © 2004 Azuretec Co., LTD. all rights reserved.

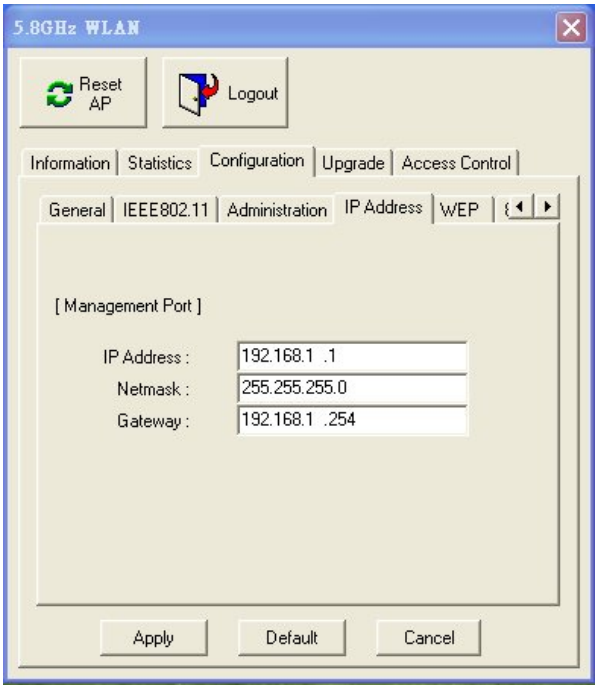
Administration:

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:

To enable remote access to the ODU using Telnet or Web Management, you must assign an IP address to the ODU. You may also assign other related Internet addressing options, such as subnet mask or gateway address. Consult your network administrator to obtain an available IP address. ***(Default setting is 192.168.1.1)***



Copyright © 2004 Azuretec Co., LTD. all rights reserved.

WEP:

If data transmission with high security is required on your network, it is recommended that the WEP encryption be used. To activate the WEP encryption, select Configuration, go to the WEP tab, and do the following:

Pull down the WEP Encryption menu and select WEP64 or WEP128.

You may identify up to 4 different encryption keys and select one of them to encrypt your transmission data. The key value of your choice may either be:
From the 4 Key entry field, enter the corresponding key value for each encryption method.

For WEP64 data encryption:

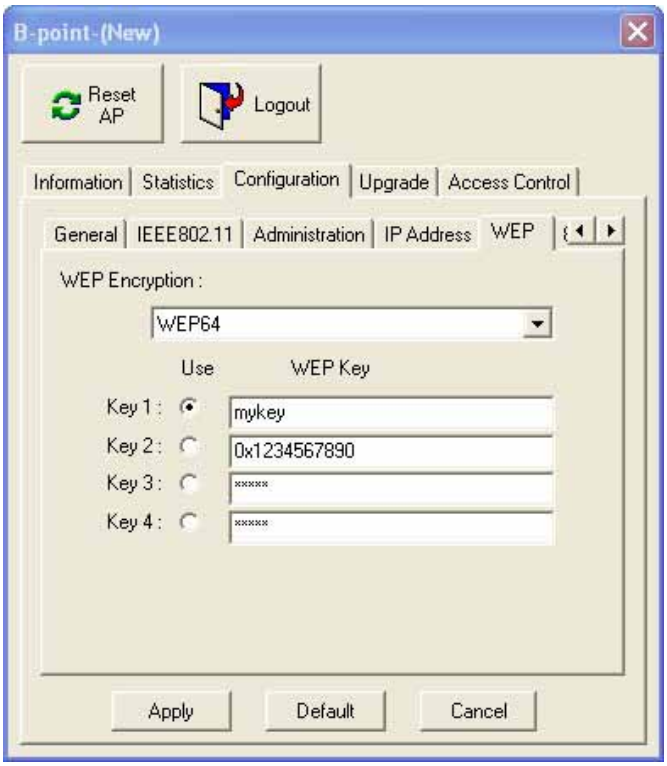
-- 5 alphanumeric characters in the range of "a-z", "A-Z" and "0-9" (e.g. MyKey).

-- 10 digit hexadecimal values in the range of "A-F" , "a-f" and "0-9", preceded by the characters "0x" values (e.g. 0x11AA22BB33).

For WEP128 data encryption:

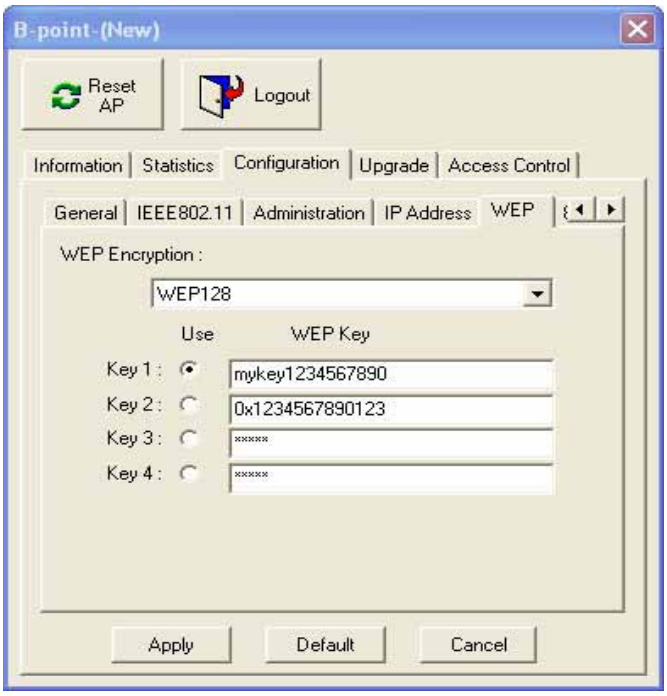
-- 13 alphanumeric characters in the range of "a-z", "A-Z" and "0-9" (e.g. MyKey12345678).

-- 26 digit hexadecimal values in the range of "A-F" , "a-f" and "0-9", preceded by the characters "0x" values (e.g. 0x00112233445566778899AABBCC).



WEP64 Key Setting

Copyright © 2004 Azuretec Co., LTD. all rights reserved.



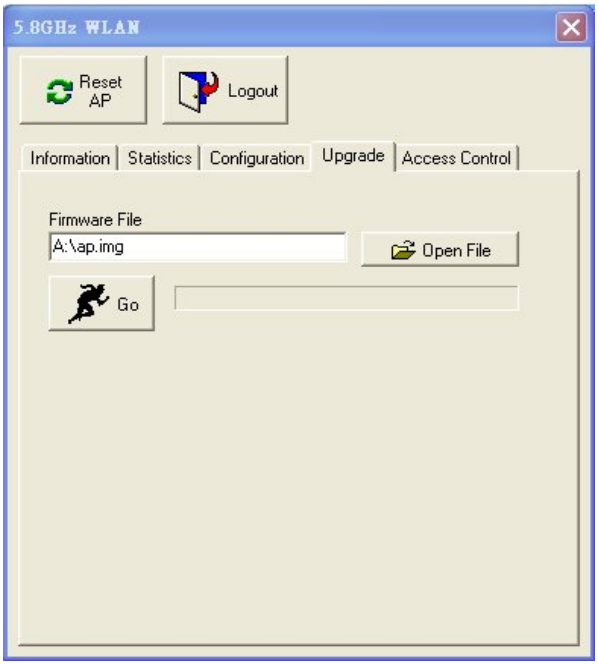
WEP128 Key Setting

NOTE: The WEP key must be set up exactly the same on the ODU as they are on other wireless client stations. For example, if you set "MyKey" for the ODU, the same WEP Key "MyKey" must be assigned to other client stations.

Upgrade

This item is used for uploading the newest firmware of the ODU. 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.

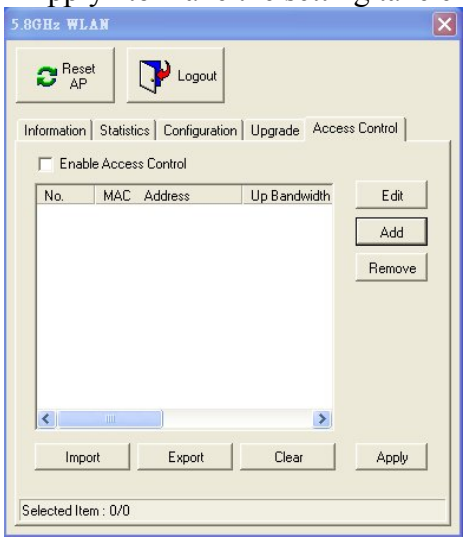
Copyright © 2004 Azuretec Co., LTD. all rights reserved.

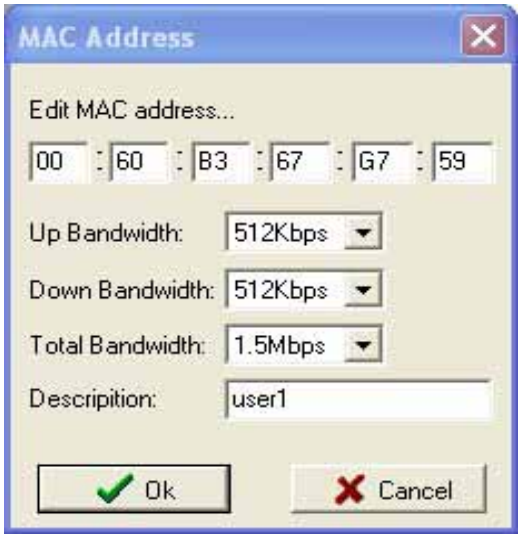


Access Control:

With the Access Control 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. Further more, the Bandwidth control function allows you to control the upstream/downstream bandwidth per client basis. Note that, only when the MAC addresses of the wireless stations are in the Access Control Table, they will be able to access network via Access Point. To create or edit the Access Control Table, do the following:

- Go to the Access Control tab and check "Enable Access Control".
- Click the "Add" button and enter the MAC addresses of the wireless stations you allow to access.
- Set "Up bandwidth", "Down bandwidth" and "Total bandwidth" if needed. Specify the desired bandwidth or unlimited if you do not need the bandwidth control.
- Click "Apply" to make the setting take effect.





Copyright © 2004 Azuretec Co., LTD. all rights reserved.

You can also configure the Access Control by using web-based management.

NOTE: Be aware 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. You may save the file as a text document.

Advanced Security

The 802.1x authentication (EAP) is designed to enhance the security of wireless networks. The 802.1x provides an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority. For wireless LANs, it also provides centralized, server-based authentication of end users. The standard is flexible enough to allow multiple authentication algorithms, and because it is an open standard, multiple vendors can innovate and offer enhancements.

For wireless LANs, the 802.1x authentication has three main components: The supplicant (usually the client software, such as zero configuration in window XP), the authenticator (usually the access point), and the authentication server (usually a Remote Authentication Dial-In User Service server, although RADIUS although 802.1X does not specify it).

The advanced security describes how to control authorized access to the Access Point with Authentication Dial-In User Service (RADIUS). There are many ways to enhance your wireless security: 802.1x Based Auth mode or MAC Address Based Auth mode. To enable 802.1x based authentication, please select 802.1x Based Auth mode. Moreover, you may enable the radius account function by check Enable Radius Account in the check box. To configure the Authentication and Account Server function, the parameter of Radius Authentication Server and Radius Account Server must set to the same with the Authentication Server and Account Server. Before you enable RADIUS account, you have select 802.1x Based Auth mode first.

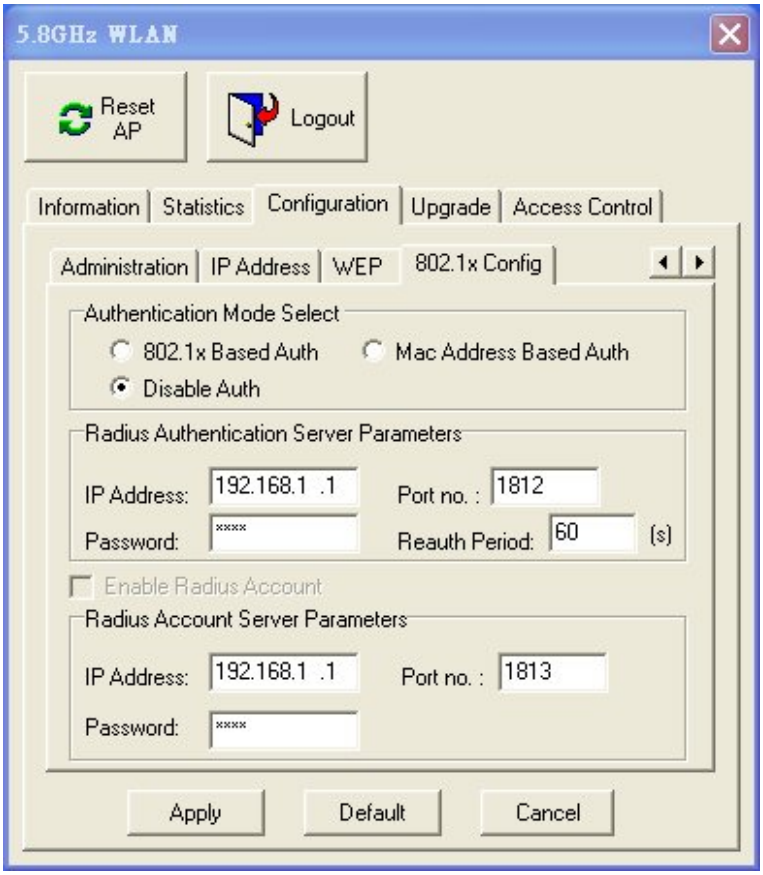
Copyright © 2004 Azuretec Co., LTD. all rights reserved.

Note: The Password is up to 16 bytes.

If you want to use MAC Address Based authentication, you should select MAC Address Based Auth mode. However, the RADIUS account server will not be supported here.

Most likely, the MAC Address Based authentication is less secure than 802.1x (EAP) authentication. MAC Address Based authentication provides an alternative for wireless 10 network security that does not support 802.1x capability.

Otherwise, you may select disable auth mode that adjusts to the 802.11 legacy network. For setting 802.1x Based Auth:

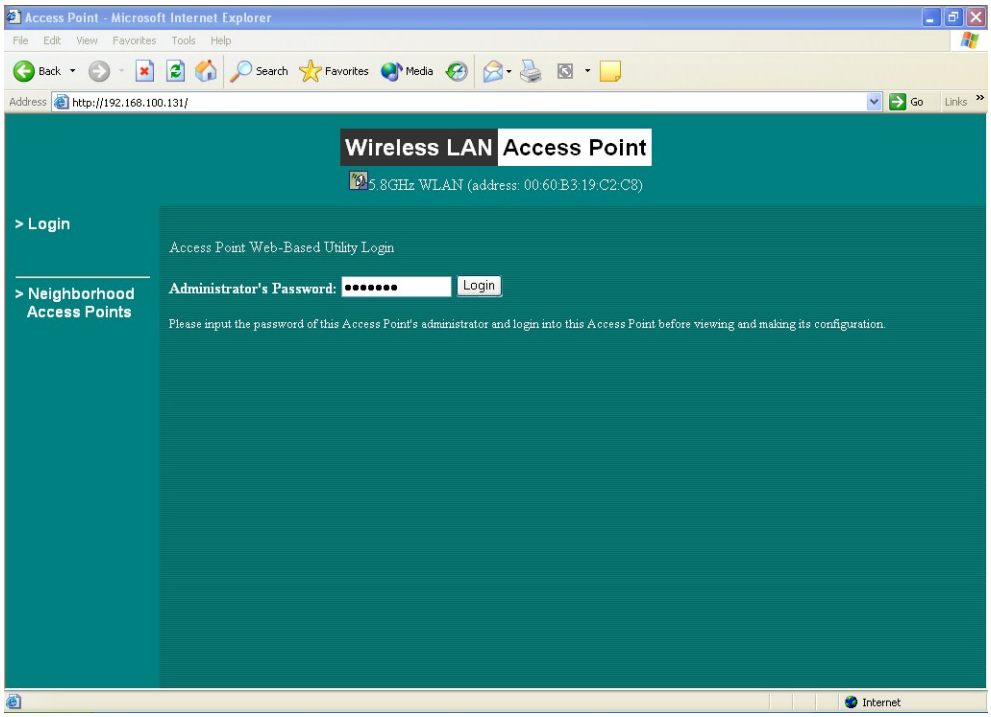


Copyright © 2004 Azuretec Co., LTD. all rights reserved.

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 ODU. An ODU with an assigned IP address (e.g. ***http://192.168.1.1***) will allow you to monitor and configure the ODU.

1. Open your web browser.
2. Enter the available IP address of your ODU in the Address field (e.g. http://192.168.1.1). You will have access to the **Wireless LAN Access Point Web Pages** of the ODU.



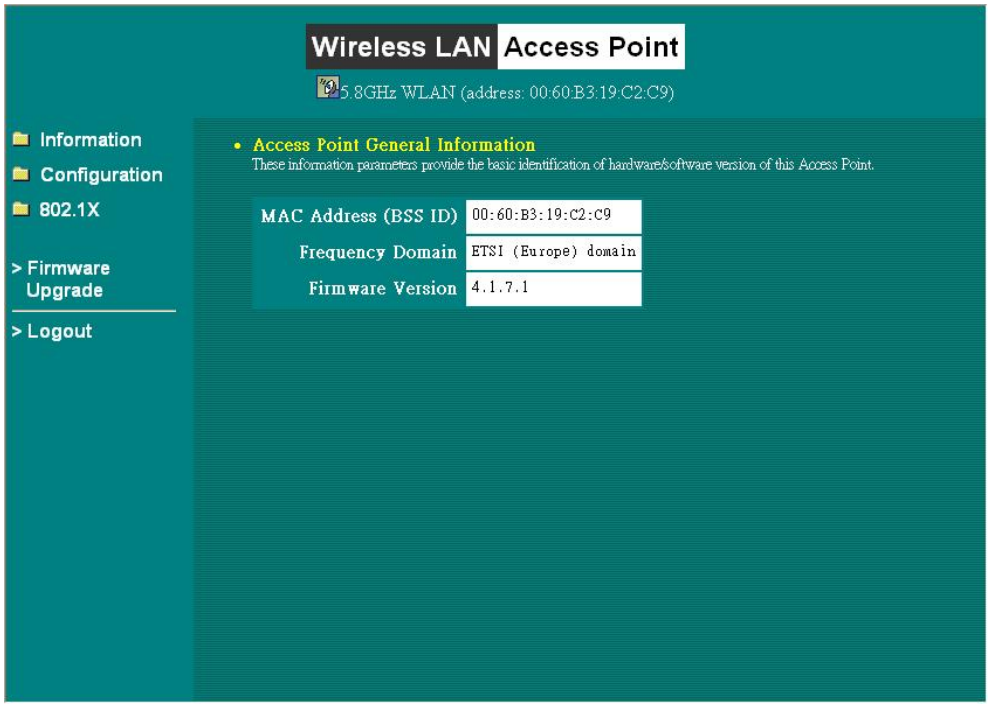
3. Enter the password to login to the ODU. The default password is **default**. The main page will show up. The ODU main page contains three items for you to manage your ODU.

Copyright © 2004 Azuretec Co., LTD. all rights reserved.

Information

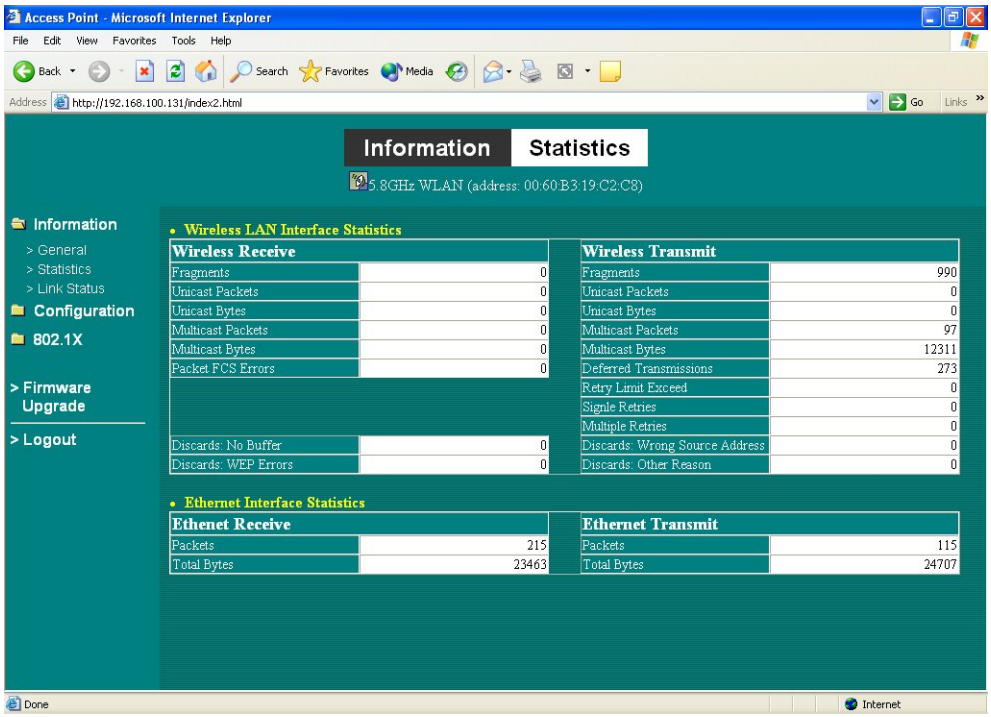
General

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



Statistics

This item displays the Ethernet and wireless network traffic.

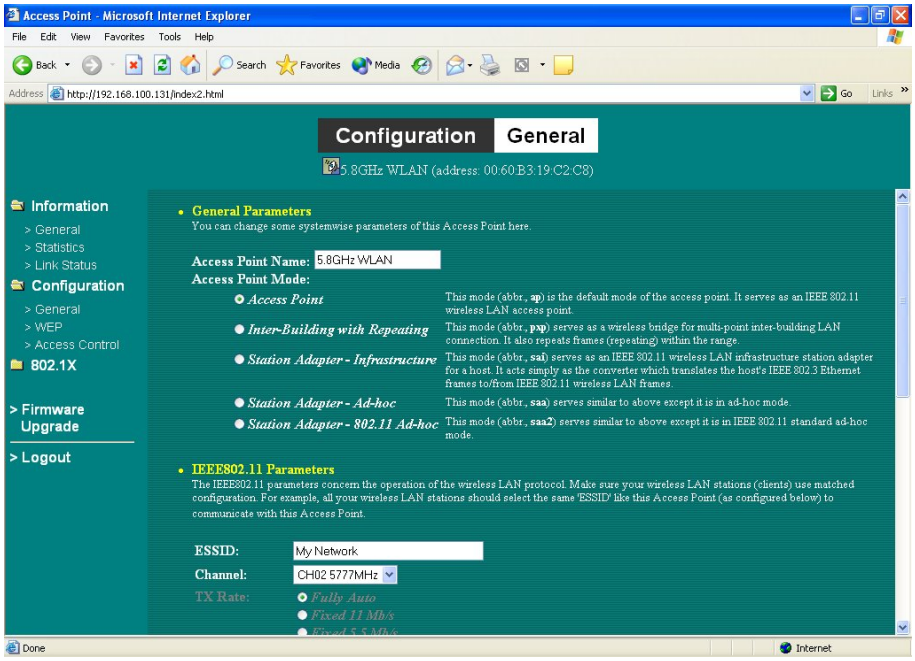


Copyright © 2004 Azuretec Co., LTD. all rights reserved.

Configuration

General

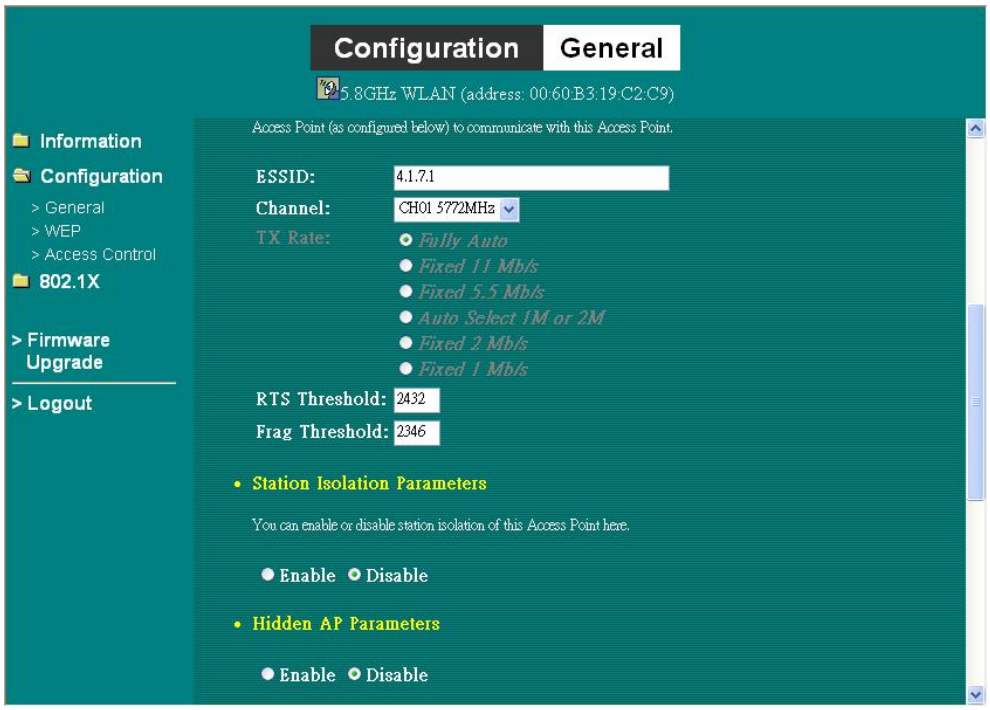
You may make the settings on the ODU such as AP Name, AP Mode, ESSID, Channel, RTS Threshold, Fragment Threshold, TX Rate and Password.



Station Isolation Parameters

By following the same steps of utility, it is easy to enable the parameter. Remember to apply the new configuration to have the function take effect. The default value is “disable”.

Copyright © 2004 Azuretec Co., LTD. all rights reserved.



IN DEPTH: The function will only refine the efficient isolation on the area of a same BSS. It won't work out the same protection for those clients who associated with different access points (in different BSS). In this case, to adopt virtual LAN may be a wonderful solution.

Hidden AP Parameters

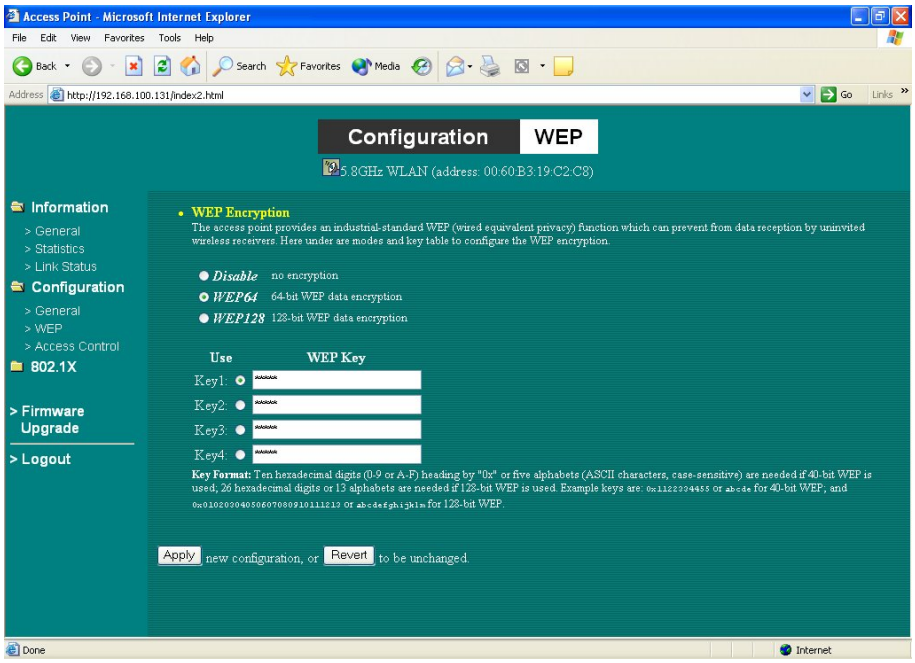
By following the same steps of utility, it is easy to enable the parameter. Remember to apply the new configuration to have the function take effect. The default value is "disable".

IN DEPTH: The hidden function can bring up a natural protection that wireless standard naturally introduced, to implement it will be able to prohibit access point from responding the connecting request of the client who carries the known SSID. The protection is very preliminary and can setup a basic secured network in parallel with access control and WEP security.

WEP

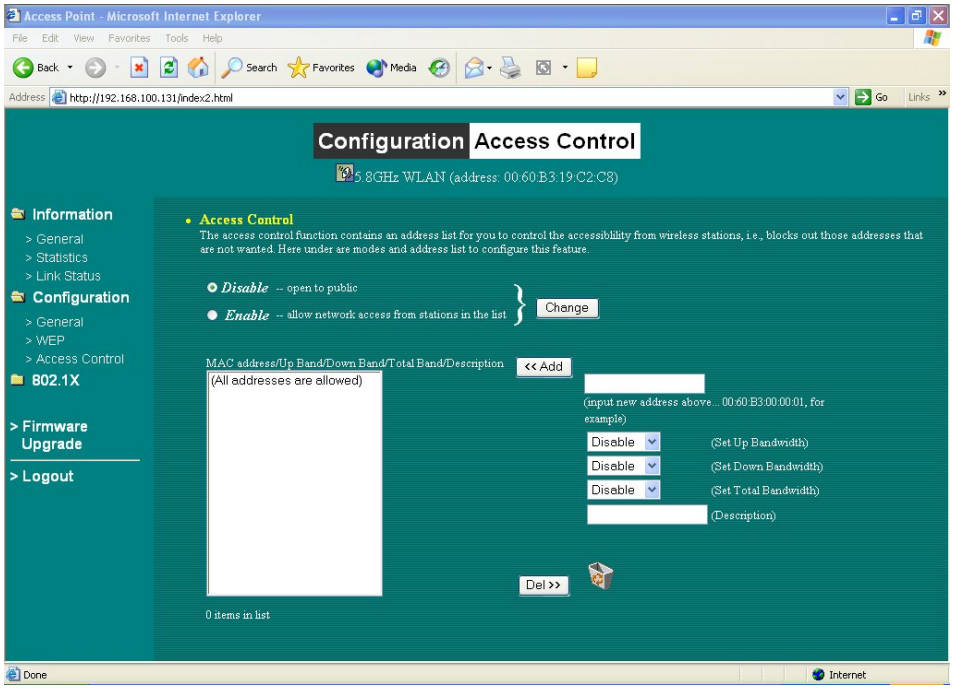
To prevent unauthorized wireless stations from accessing data transmitted over the network, the 11Mbps Wireless LAN ODU offers WEP (Wired Equivalency Privacy). You can set up 4 encryption keys but choose one key to encrypt your data.

Copyright © 2004 Azuretec Co., LTD. all rights reserved.



Access Control

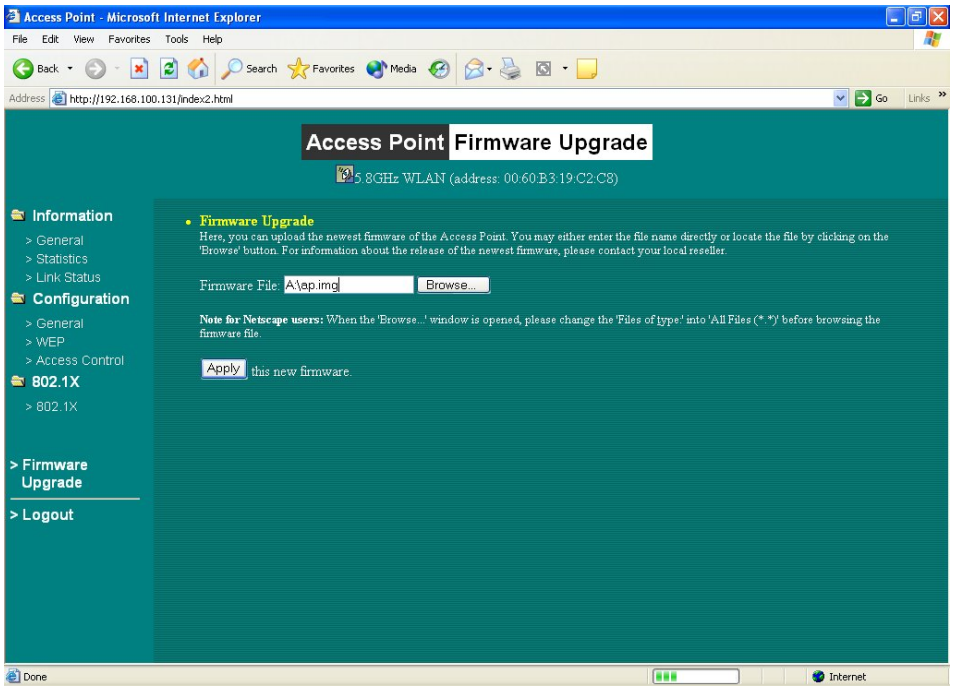
The Access Control Table enables you to restrict wireless stations accessing the ODUs by identifying the MAC address of the wireless devices.



Upgrade

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

Copyright © 2004 Azuretec Co., LTD. all rights reserved.



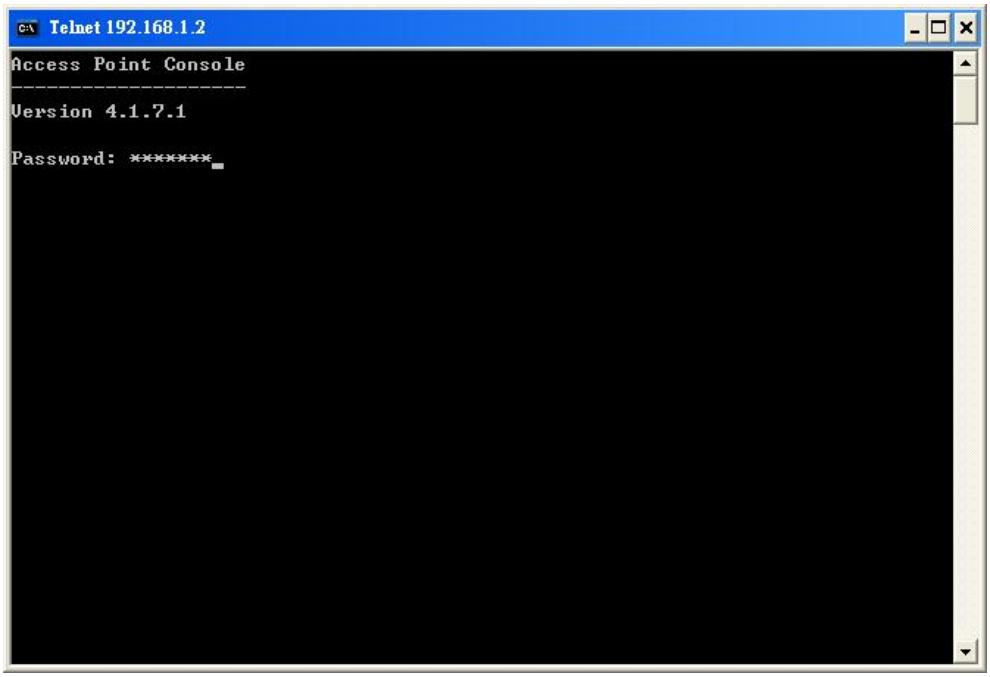
Copyright © 2004 Azuretec Co., LTD. all rights reserved.

3-3 Using the Telnet

The ODU can be configured via the command prompt console with TCP/IP:

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

1. Telnet to your ODU. A window will show up.
2. Enter the password. The default password is "**default**".



3-3-1 Basic Commands

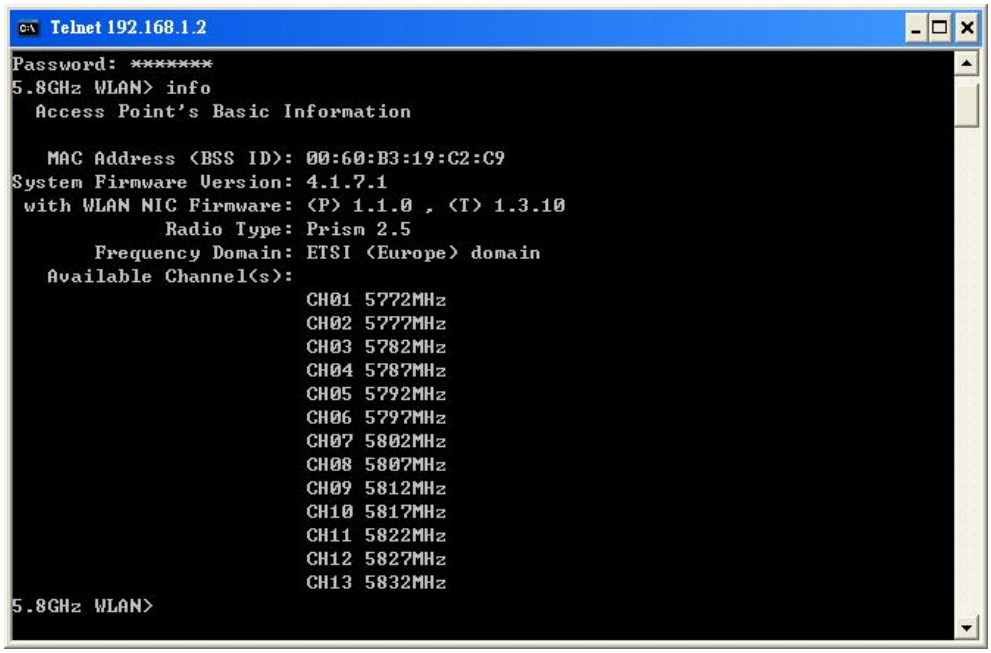
The following are the commands provided for configuring the ODU. In loader mode, i.e., no valid firmware in the ODU, only the commands with an asterisk (*) are provided.

NOTE: [xxx] stands for optional arguments.

Copyright © 2004 Azuretec Co., LTD. all rights reserved.

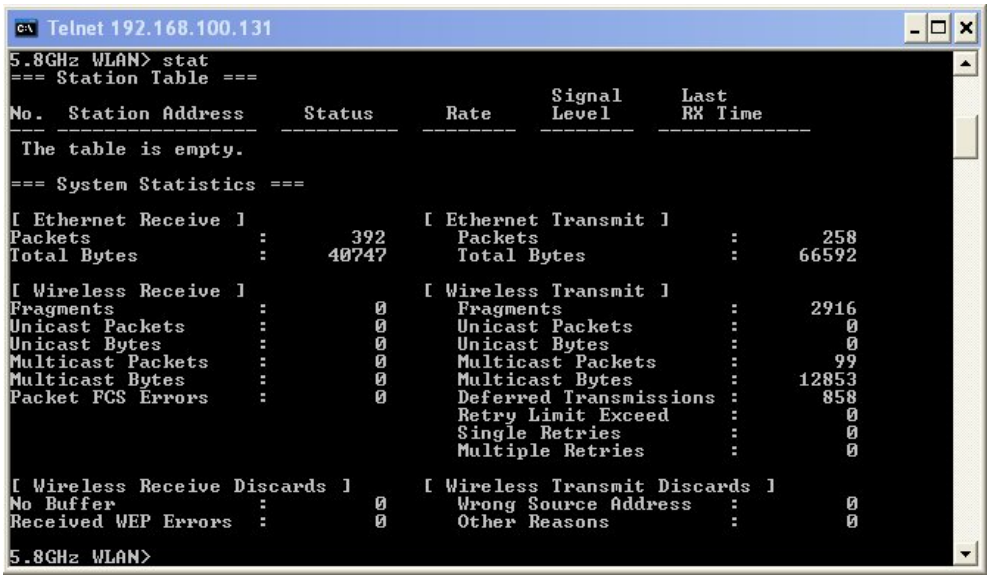
info[*]

Display some basic information of the ODU, for example, firmware version, frequency domain, etc.



stat

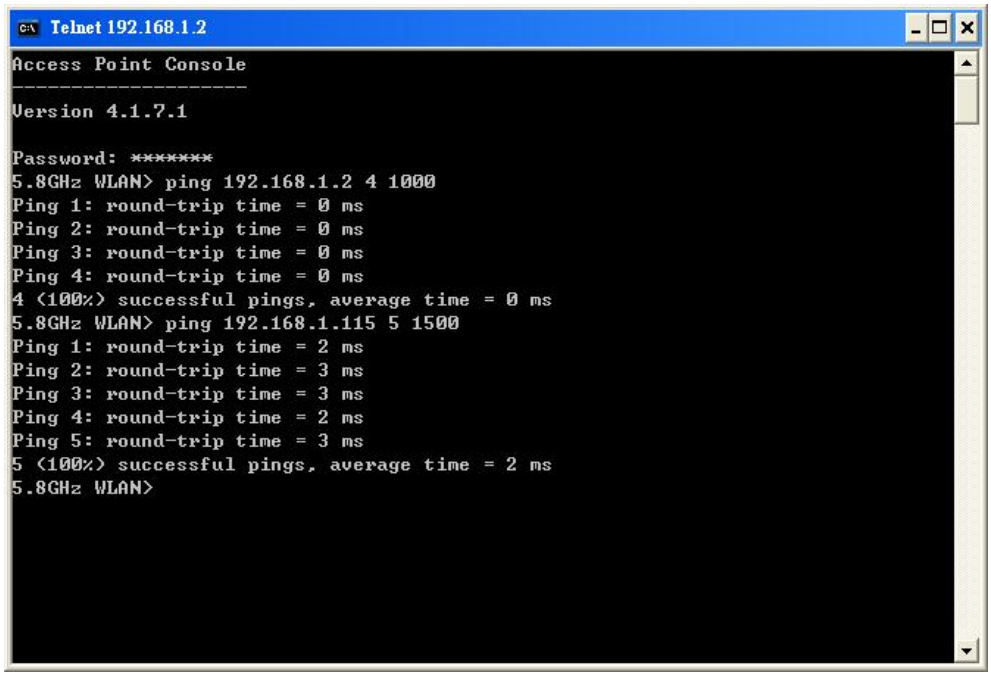
Display the statistical values of the operation of the ODU, for example, association status, LAN/WLAN interface load, etc.



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*.

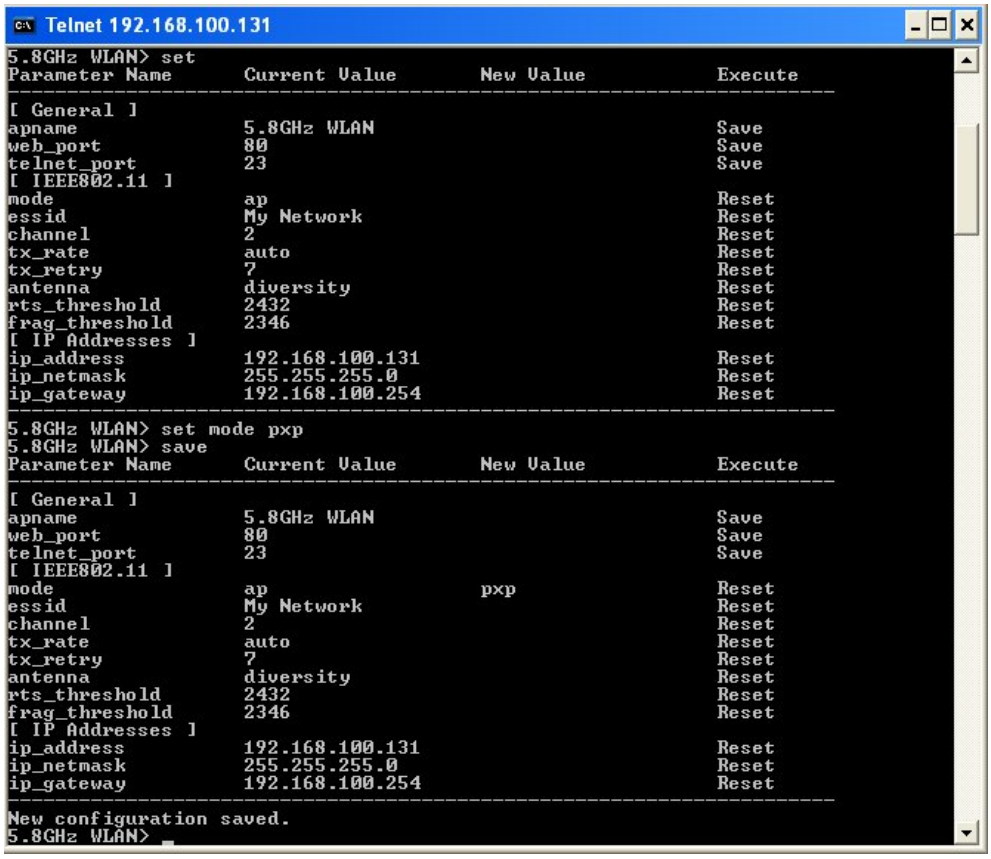
Copyright © 2004 Azuretec Co., LTD. all rights reserved.



set

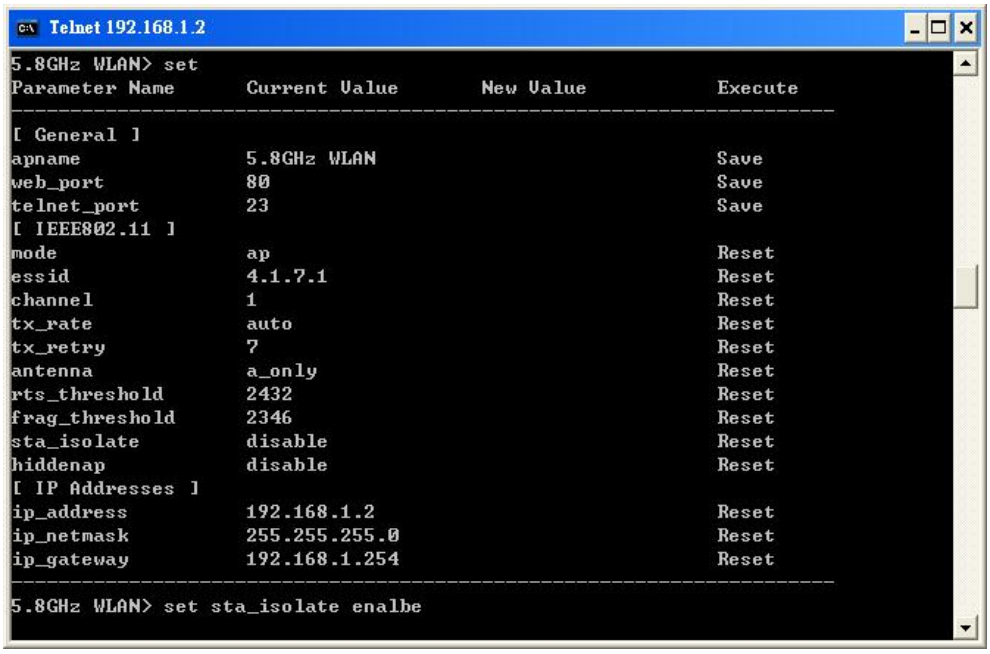
List the configuration information.

set apname | web_port | telnet_port | mode | channel | essid | tx_rate | tx_retry | antenna| rts_threshold | frag_threshold | ip_address | ip_netmask | ip_gateway



Copyright © 2004 Azuretec Co., LTD. all rights reserved.

To change factory default settings, type "set xxx (parameter) xxxx (value). For example, **"set sta_isolate enable"** command will enable the station isolation parameter. 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 ODU.

Parameter	Description	Default Value
apname	A textual name for the identification of the ODU.	apXXXXXX *(where XXXXXX is the last six octets of ODU's MAC address)*
web_port	Port number dedicated to WEB	80
telnet_port	Port number dedicated to Telnet	23
mode	Operation mode of the ODU	PxP
channel	The radio channel number.	1
essid	The ESS ID (a.k.a., SSID) of the ODU.	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 its frame size larger than this value will perform the RTS/CTS handshake. Range of value: 0~2432.	2432
frag_threshold	The threshold (number of bytes) for the fragmentation boundary. Data will be transmitted in fragments which its size does not exceed this value. Range of value: 256~2432.	2432
sta_isolate	Enable the function of Station isolation	Disable
hiddenap	Enabling the function of Hidden AP	Disable
ip_address	The IP address of the ODU.	192.168.1.1

Copyright © 2004 Azuretec Co., LTD. all rights reserved.

ip_netmask	The subnet mask address of the ODU.	255.255.255.0
ip_gateway	The default gateway address of the ODU.	192.168.1.254

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 ODU 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.

reset[*]

Issue a reset signal. The ODU will be reset if user confirms.

3-3-2 Advanced Settings for Security

This section describes the commands to control the security for ODU. To prevent unauthorized wireless stations from accessing data transmitted over the network, the 11Mbps Wireless LAN ODU offers the following levels of security options.

- Access Control Table restricts wireless stations to access the ODU.
- Data Encryption, known as WEP (Wired Equivalency Privacy), encrypts wireless data transmitted via wireless medium.

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 ODU. 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)

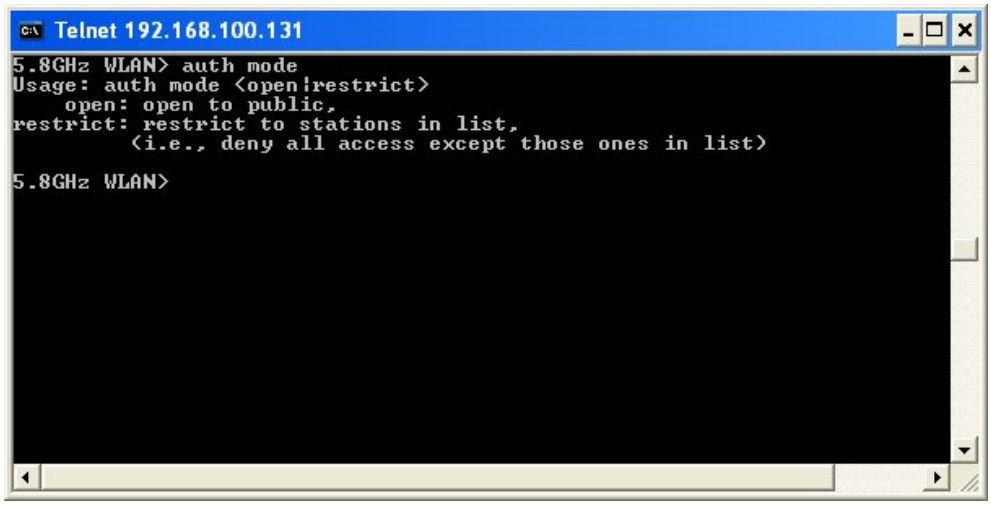
Copyright © 2004 Azuretec Co., LTD. all rights reserved.

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 ODU. The sub-commands are listed as follows:

mode disable | wep64: set the access control mode. The following are the definition of each data encryption mode.

- *none*: no encryption (default)
- *wep64*: use 64-bit WEP data encryption
- *wep128*: use 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 if 64-bit WEP is used.
Example: 0x1122334455, 0x0055AA55AA, abcde, or MyKey.

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.

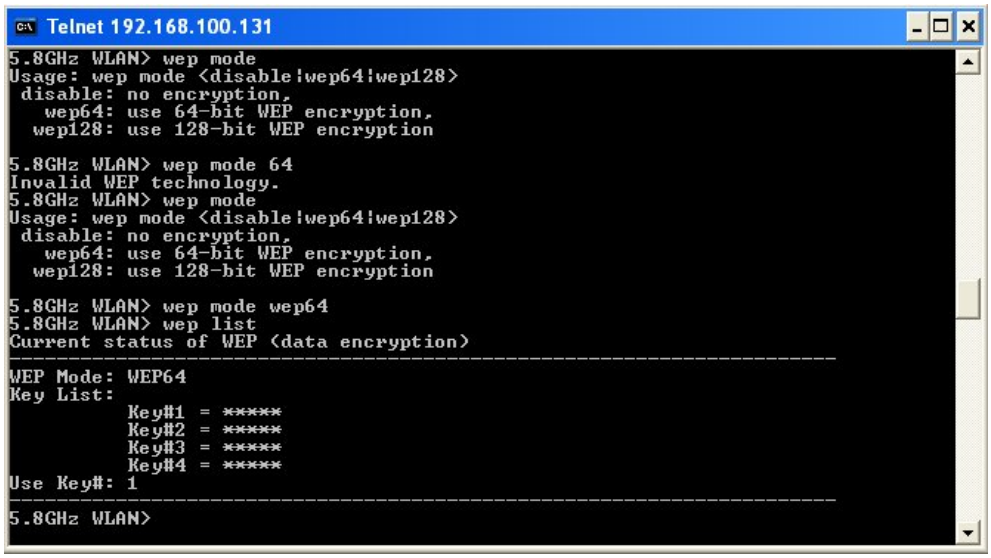
set key4 key_text: set WEP Key#2 as *key_text* with a same format as WEP Key#1.

set usekey 1|2|3|4: Select the WEP key to be used for encrypting data transmission. Only

Copyright © 2004 Azuretec Co., LTD. all rights reserved.

one key can be selected at a time.

list: Display current WEP settings.



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

Copyright © 2004 Azuretec Co., LTD. all rights reserved.

Appendix A: Channels

Conversion Table

802.11b Channel	Frequency(MHz)
1	5772
2	5777
3	5782
4	5787
5	5792
6	5797
7	5802
8	5807
9	5812
10	5817
11	5822

Copyright © 2004 Azuretec Co., LTD. all rights reserved.

Appendix B: Troubleshooting

If there is no signal output, please check the following item:

1. Check whether the LED indicator on the PoE and ODU is on. If not, it means there is problem with the power component.
   (1) Check if the power cord is correctly connected with the power adapter and the power outlet.
   (2) Check if there is electricity on power outlet.
2. Check if the connection between antenna and WLAN ODU is correct, or whether the connector is loose or not.
3. Check if the connection between WLAN ODU and PoE is correct, or whether the connector is loose or not.
4. Verify if the transmit power which calculated before is correct.
5. If none of the above measures could solve troubleshooting, please contact the supplier for further support.

Azuretec™
go the extra mile
Tel: +886-2-29101997
Fax:+886-2-29103996
Email:sales@azuretec.com
www.azuretec.com / www.azuretec.com.tw

Copyright © 2004 Azuretec Co., LTD. all rights reserved.