

# AIRNET Outdoor Bridge Point to Point kit Series



## User's Manual

July, 2008

# Table of Contents

---

<b>CHAPTER 1: PRODUCT OVERVIEW .....</b>	<b>1</b>
<b>Introduction .....</b>	<b>1</b>
<b>Features and Benefits .....</b>	<b>1</b>
<b>When to use which mode .....</b>	<b>2</b>
Access Point Mode .....	2
Access Point Client Mode .....	3
Wireless Routing Client Mode .....	4
Gateway Mode.....	5
Wireless Adapter Mode .....	6
Transparent Client Mode.....	7
Repeater Mode.....	8
<b>CHAPTER 2: HARDWARE INSTALLATION.....</b>	<b>9</b>
<b>Warnings .....</b>	<b>9</b>
<b>Package contents .....</b>	<b>10</b>
<b>Setup Requirements.....</b>	<b>11</b>
<b>AIRNET Outdoor Bridge Point to Point installations.....</b>	<b>12</b>
Mounting AIRNET Outdoor Bridge in the pole or tower.....	16
<b>CHAPTER 3: ACCESS TO WEB-BASED INTERFACE.....</b>	<b>17</b>
<b>Access to the Web interface with uConfig.....</b>	<b>17</b>
<b>Verify the IP address of the AIRNET Outdoor Bridge with NpFind .....</b>	<b>21</b>
<b>Manual access to web-based interface via Internet Explorer .....</b>	<b>22</b>
<b>CHAPTER 4: COMMON CONFIGURATION .....</b>	<b>27</b>
<b>Management Port Setup .....</b>	<b>27</b>
To Setup DHCP Server .....	32
View Active DHCP Leases .....	36
Reserve IP addresses for predetermined DHCP clients.....	37
<b>WLAN Setup .....</b>	<b>40</b>
Antenna Alignment .....	51
Configure the Advanced setup of the Wireless Mode .....	53
View the Statistics.....	55
<b>WAN Setup (Available in Wireless Routing Client and Gateway modes) ...</b>	<b>56</b>
<b>Setup Telnet / SSH .....</b>	<b>63</b>
Access the TELNET Command Line Interface .....	65

# Table of Contents

---

Access the Secure Shell Host Command Line Interface .....	66
Set the WEB Mode.....	67
SNMP Setup .....	68
Setup SNMP Trap .....	69
STP Setup (Only available in Access Point, Transparent Client and Repeater modes).....	70
Use MAC Filtering.....	74

## **CHAPTER 5: ADVANCED CONFIGURATION .....84**

<b>Setup Routing (only supported by Wireless Routing Client and Gateway) ..</b>	<b>84</b>
Configure Static Routing.....	85
Using Routing Information Protocol-RIP.....	86
NAT – Network Address Translation (only supported by Wireless Routing Client and Gateway) .....	87
Configure Virtual Servers based on De-Militarized Zone (DMZ) Host .....	88
Configure Virtual Servers based on Port Forwarding.....	90
Configure Virtual Servers based on IP Forwarding .....	93
<b>Bandwidth Control (only supported by Wireless Routing Client and Gateway) .....</b>	<b>94</b>
To enable or disable Bandwidth Control.....	94
To configure WAN Bandwidth Control Setting .....	95
To configure LAN Bandwidth Control Setting .....	96
<b>Remote Management (only supported by Wireless Routing Client and Gateway) .....</b>	<b>98</b>
To set up Remote Management.....	98
<b>Parallel Broadband (only supported by Gateway Mode) .....</b>	<b>99</b>
Enable Parallel Broadband on the Access Point .....	99
Enable Parallel Broadband on the Access Point .....	100
<b>Email Notification.....</b>	<b>101</b>
<b>Static Address Translation (only supported by Wireless Routing Client and Gateway) .....</b>	<b>103</b>
<b>DNS Redirection (only supported by Wireless Routing Client and Gateway) .....</b>	<b>104</b>
To enable/disable DNS Redirection.....	105
<b>Dynamic DNS Setup.....</b>	<b>106</b>
To enable/disable Dynamic DNS Setup.....	106
To manage Dynamic DNS List (DDNS).....	107

## **CHAPTER 6: WIRELESS EXTENDED FEATURES .....113**

Setup WDS2.....	113
-----------------	-----

# Table of Contents

---

Set Virtual AP (Multiple SSID) .....	117
Set Preferred APs (Available in Client Mode) .....	119
Long Distance Parameters.....	120
Set Wireless Multimedia .....	122
Setup Point-to-Point & Point-to-MultiPoint Connection .....	126
Setup Repeater .....	129

## **CHAPTER 7: WLAN SECURITY ..... 134**

How to set up WEP .....	135
How to set up WPA-Personal (Only available in Access Point mode) .....	136
How to set up 802.1x/RADIUS (Only available in Access Point mode) .....	138
How to set up WPA Enterprise (Only Access Point mode supports WPA2-EAP and WPA-EAP-AUTO).....	140

## **CHAPTER 8: SECURITY CONFIGURATION..... 142**

<b>Packet Filtering</b> .....	<b>142</b>
Configure Packet Filtering .....	142
<b>URL Filtering</b> .....	<b>146</b>
To configure URL Filtering.....	146
<b>Firewall Configuration</b> .....	<b>147</b>
To configure SPI Firewall.....	147
<b>Firewall Logs</b> .....	<b>151</b>
To view Firewall Logs.....	151

## **CHAPTER 9: SYSTEM UTILITIES ..... 152**

<b>Using the SYSTEM TOOLS Menu</b> .....	<b>152</b>
Ping Utility.....	152
Use Syslog .....	153
System Identity.....	156
Set System's Clock .....	157
Firmware Upgrade .....	158
Backup or Reset Settings .....	160
Reboot System.....	163
Change Password.....	164
Logout .....	165
<b>Using the HELP menu</b> .....	<b>166</b>
About System.....	166

## Table of Contents

---

<b>APPENDIX I: FIRMWARE RECOVERY.....</b>	<b>167</b>
<b>APPENDIX II: TCP/IP CONFIGURATION.....</b>	<b>169</b>
For Windows 95/98/98SE/ME/NT .....	169
For Windows XP/2000.....	172
<b>APPENDIX III: PANEL VIEWS &amp; DESCRIPTIONS .....</b>	<b>174</b>
<b>APPENDIX IV: VIRTUAL AP (MULTI-SSID) FAQ.....</b>	<b>176</b>

# Chapter 1: Product Overview

## INTRODUCTION

AIRNET Outdoor Bridge Point to Point kit series are used to provide internet access to end-users using point-to-point architecture at 54Mbps in 900MHz, 2.4GHz, 3.5GHz and 5GHz frequency bands. Wireless data links take place where there is no infrastructure for internet access or in places where bandwidth offered by current channels is too low. With our wireless equipment you can get high bandwidth on very long distances at very reasonable price. Our equipment provides various features including Routing, Firewall NAT, DHCP, bandwidth control and many more.

The AIRNET Outdoor Bridge Point to Point kit series with Integrated Antenna is the most comprehensive wireless solution, which includes powerful wireless router with Power over Ethernet (PoE) feature, all embedded in high-gain directional antenna. Flat Panel Antenna offers wide territorial coverage with no signal waste and the Power over Ethernet injector provides the possibility to deliver both necessary power and data to your router (which is attached to the antennas) over a single Ethernet cable.

## FEATURES AND BENEFITS

- Cost effective solution
- Complete Outdoor Weatherproof Solution
- All-in-One Wireless device (radio and antenna in only one package)
- Integrated Power over Ethernet
- Web Management and SNMP support
- High-speed wireless data links (Up to 54Mbps)
- Connection distance up to 15 miles (24km)
- Virtual AP (Multiple SSID)
- WDS2
- Firewall, NAT, IP Routing, DHCP
- Bandwidth control
- High level security with full 64/128Bit WEP Encryption
- Atheros XR Chipset - Advanced long-range features
- WDS - Wireless Distribution System
- Antenna Alignment and Wireless Site Survey
- Fast and simple installation for base station and Clients

## Product Overview

---

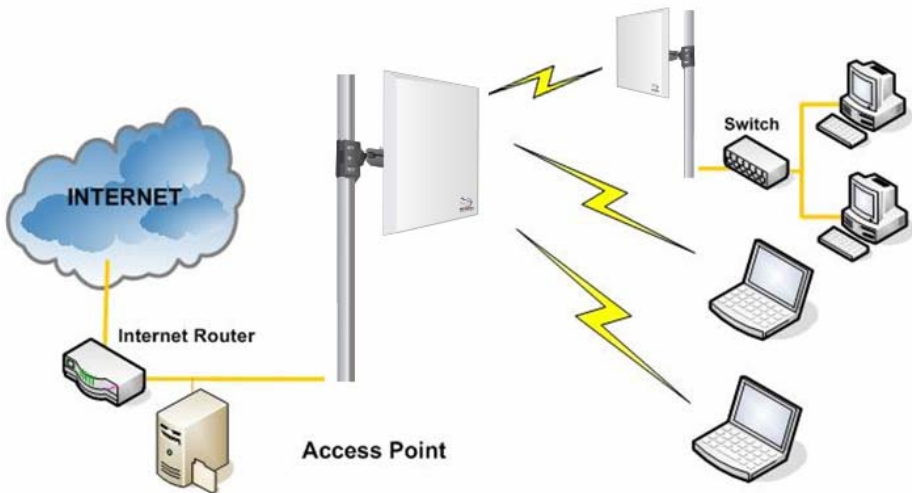
### WHEN TO USE WHICH MODE

The AIRNET Outdoor Bridge Point to Point kit series is versatile in the sense that it may operate in seven different types of modes: **Access Point Mode**, **Client Mode**, **Point to Point**, **Point to Multiple Point**, **Wireless Routing Client**, **Gateway** and **Wireless Adapter**.

This section presents a brief outline of the different network applications that can be accommodated through the different modes of the AIRNET Outdoor Bridge Point to Point kit.

### ACCESS POINT MODE

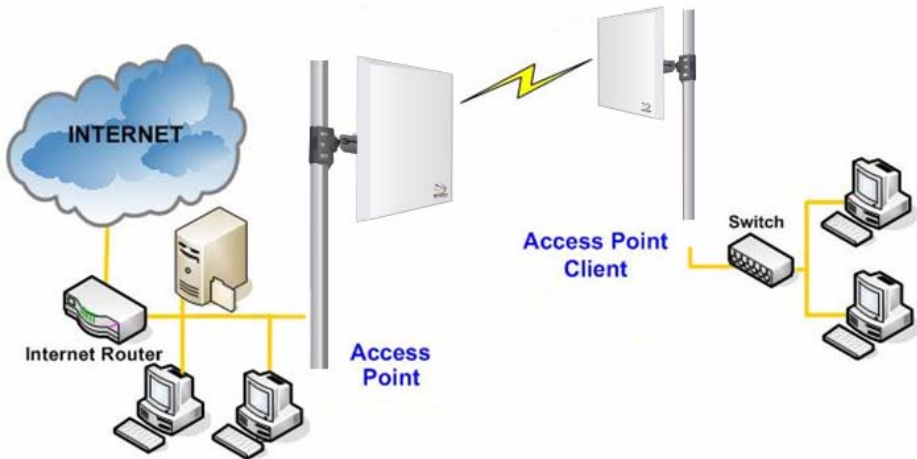
This is the default mode of your AIRNET Outdoor Bridge. The **Access Point** mode enables you to bridge wireless clients to access the wired network infrastructure and to communicate with each other.



In the example above, the wireless users will be able to access the file server connected to the switch through the AIRNET Outdoor Bridge in **Access Point** mode.

## ACCESS POINT CLIENT MODE

In **Access Point Client** mode, the AIRNET Outdoor Bridge acts as a wireless client that can operate wirelessly with another access point to perform bridging between two Fast Ethernet networks. The Access Point client cannot communicate directly with any other wireless device.

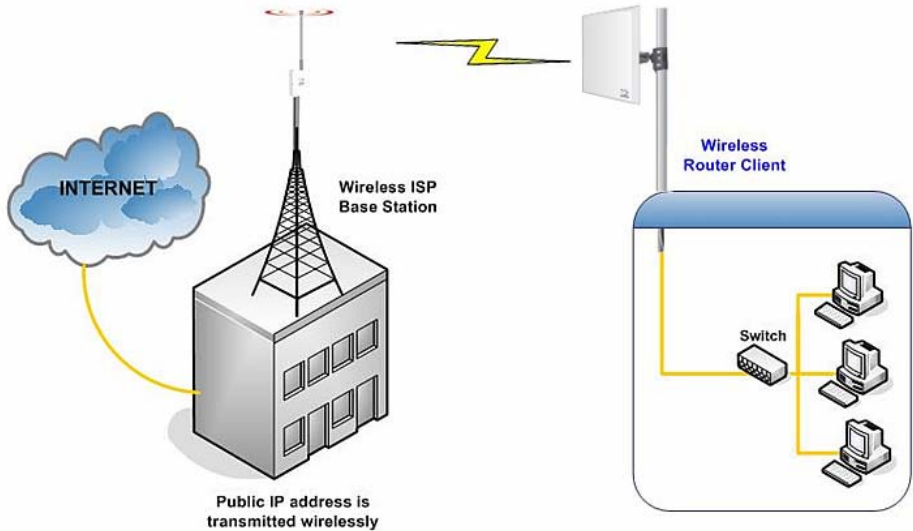


In the example above, the workgroup PCs will be able to access the PCs connected to the AIRNET Outdoor Bridge in **Access Point Client** mode.



## WIRELESS ROUTING CLIENT MODE

An application of this mode would be for the Ethernet port of the **Wireless Routing Client** to be used for connection with other devices on the network while access to the Internet would be achieved through wireless communication with wireless ISP.



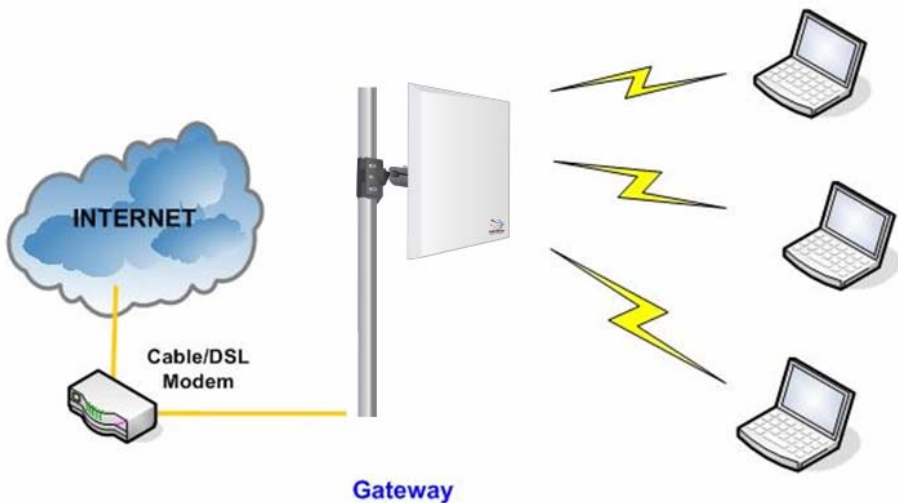
The above illustration describes how this mode operates.

## Product Overview

### GATEWAY MODE

Or put it more simply, Broadband Internet sharing in a wireless network!

Since the AIRNET Outdoor Bridge supports several types of broadband connections, the first step in setting up the AIRNET Outdoor Bridge as a *Broadband Internet Gateway* is to identify the type of broadband Internet access you are subscribed to.



#### Static IP address

Use this type of connection if you have subscribed to a fixed IP address or to a range of fixed IP addresses from your Internet Service Provider.

#### Dynamic IP address

When powered using this type of connection, the access point requests for an IP address which will be automatically assigned to it by your Internet Service Provider.

This type of connection applies for instance, to:

- Singapore Cable Vision subscribers
- @HOME Cable Service users

## Product Overview

---

### PPP over Ethernet (PPPoE)

Select this type of connection if you are using ADSL services in a country utilising standard PPP over Ethernet for authentication.

For instance:

If you are in Germany which uses T-1 connection or

If you are using SingNet Broadband or Pacific Internet Broadband in Singapore.

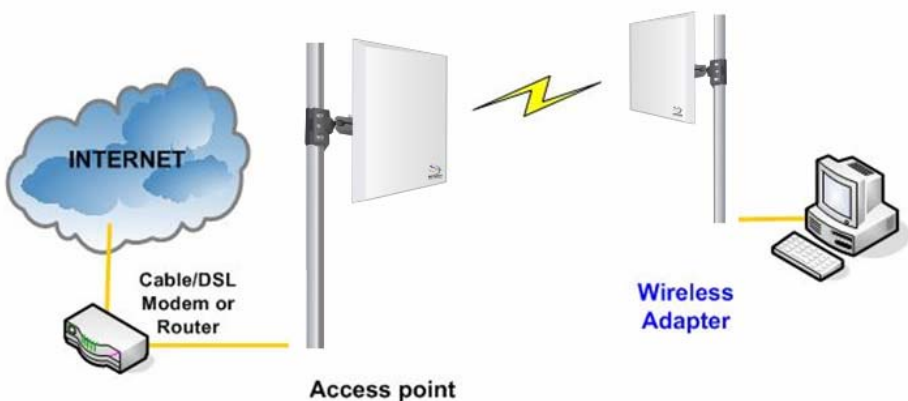
### PPTP

Select this type of connection if you are using ADSL services in a country utilising PPTP connection and authentication.

## WIRELESS ADAPTER MODE

Similarly to the Access Point Client mode, the AIRNET Outdoor Bridge used in this mode, is able to communicate wirelessly with another access point to perform transparent bridging between two networks.

However here, the **Wireless Adapter** connects a single wired workstation only. No client software or drivers are required while using this mode.

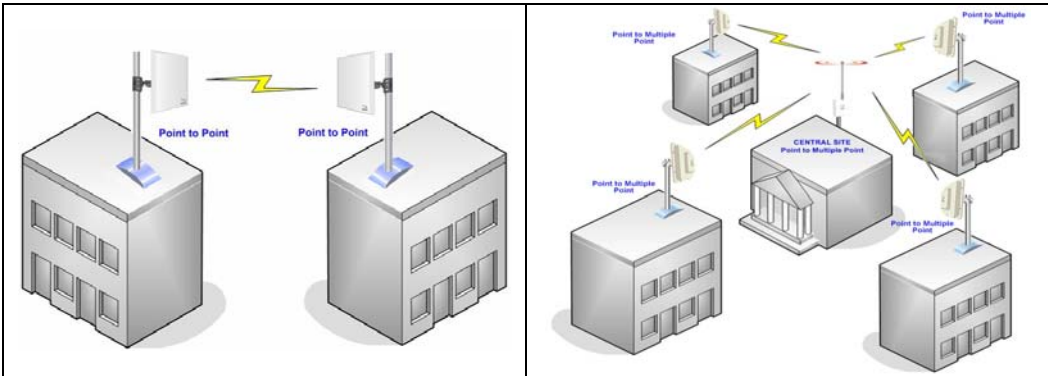


# Product Overview

## TRANSPARENT CLIENT MODE

In **Transparent Client Mode**, the access point provides connection with an access point acting as the RootAP. This operation is designed for the implementation of Point-to-Point and Point-to-Multipoint connections

Point-to-Point	Point-to-MultiPoint
An access point acts as Root AP and 1 other access point acts as Transparent Client.	An access point acts as Root AP and several other access point acts as Transparent Clients.



Difference Between other client modes and Transparent Client Mode	
Other client modes	Transparent Client Mode
Connectivity with any standard APs.	Connectivity with RootAP-supported APs.
All devices connected to the Ethernet ports use a common MAC address for communications with the AP.	Devices connected to the Ethernet ports flow through freely and transparently without the MAC address restriction.

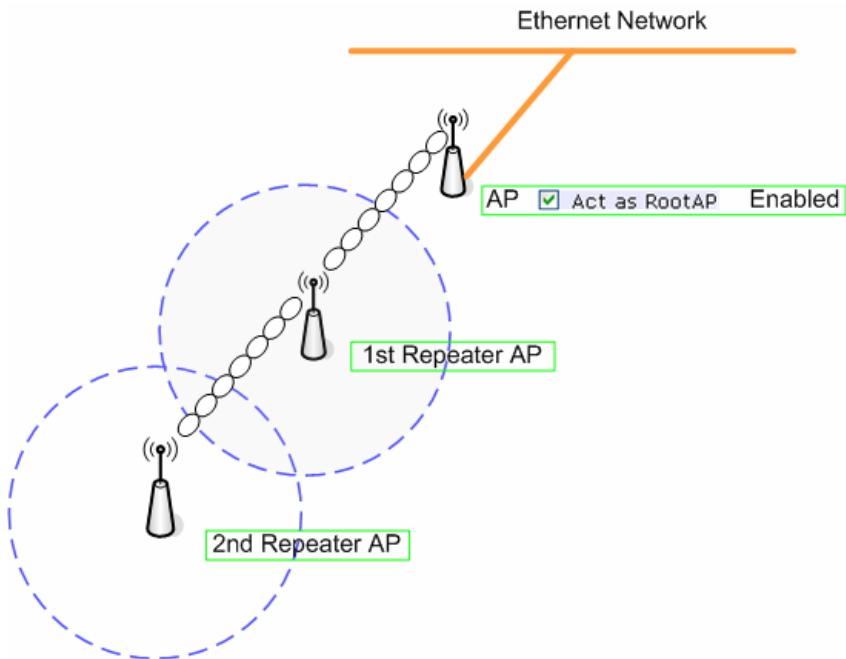
## Product Overview

### REPEATER MODE

The access point comes with a built-in Repeater Mode to extend the range, and substantially enhance the performance of the wireless network by allowing communications over much greater distances.

In Repeater Mode, the access point acts as a relay for network signals on the network by regenerating the signals it receives, and retransmitting them to extend the range of the existing network infrastructure.

Detailed information on the Repeater Mode is available in the Repeater Setup section.



---

## Chapter 2: Hardware Installation

### WARNINGS

- Do not work on the system or connect or disconnect cables during periods of lightning activity.
- Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death.
- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
- To meet regulatory restrictions, the radio and the external antenna must be professionally installed. The network administrator or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password protected by the network administrator to maintain regulatory compliance.
- The AIRNET Outdoor Bridge Point to Point kit and PoE injector can be damaged by incorrect power application. Read and carefully follow the installation instructions before connecting the system to its power source.

# Hardware Installation

## PACKAGE CONTENTS

Take a moment to ensure you have all of the following parts in your Outdoor Waterproof Unit installation kit before you begin installing the product. If any parts are missing, please contact your local vendor or contact us at 305-4182232.

### AIRNET Outdoor Bridge Point to Point kit - Package Content



#### KIT CONTAINS:

1. Two Netkrom AIRNET Outdoor Bridge Units
2. Two Mounting brackets (include: 2 Wall/ Pole mounting system and 4 screw nuts)
3. Two PoE Injector
4. Two Power Cables
5. Two RJ45 Waterproof Connector System
6. CD ROM
7. Two 75' Outdoor Rated CAT5e shielded cables

# Hardware Installation

---

## SETUP REQUIREMENTS

Before starting, please verify that the following is available:

- CAT5/5e or FTP Outdoor Ethernet cable (from the AIRNET Outdoor Bridge to PoE Injector)
- At least one computer is installed with a Web browser and a wired or wireless network interface adapter
- TCP/IP protocol is installed and IP address parameters are properly configured on all your network's nodes

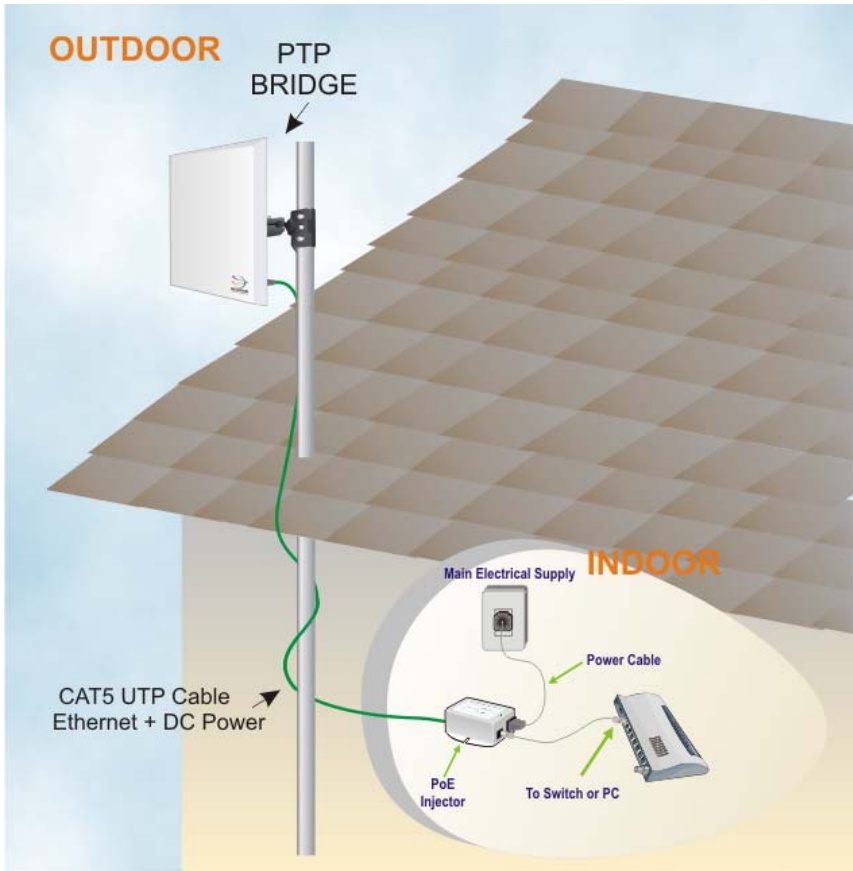
### Important!

- Configure and verify the AIRNET Outdoor Bridge kit operations first before you mount the unit in a remote location.
- You may need to install a lightning arrestor to protect your AIRNET Outdoor Bridge kit from the lightning.
- For choosing the best location for your AIRNET Outdoor Bridge choose an elevated location where trees, buildings and large steel structures will not obstruct the antenna signals and which offers maximum line-of-sight propagation with the users.



## AIRNET OUTDOOR BRIDGE POINT TO POINT INSTALLATIONS

The diagram below shows the overall setup of AIRNET Outdoor Bridge unit.



# Hardware Installation

## Step 1:

Connect your UTP or FTP Outdoor cat.5 Ethernet cable with waterproof connector to the RJ-45 connector on the AIRNET Outdoor Bridge unit. Then connect the other end of the cable to the PoE injector.

For the Netkrom PoE, the recommended length of the RJ45 Category 5 cable is up to 150 feet or 50 meters.

1.- Remove the thin enclosure nut from the feedthru assembly. This can be discarded. Loosen the compression nut completely



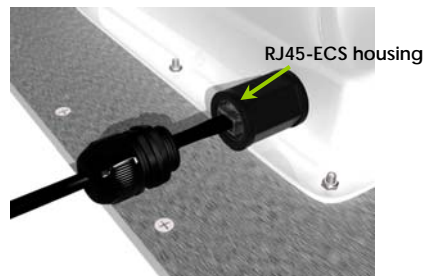
2.- Insert the RJ45 connector thru the feedthru assembly



3.- Tighten the compression nut loosely to the feedthru assembly

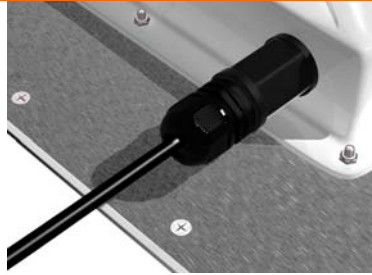


4.- Screw the entire feedthru assembly into the RJ45-ECS housing which is already mounted in the AIRNET Outdoor Bridge unit. There should be a rubber gasket between the two assemblies. Tighten the feedthru assembly to create a seal.



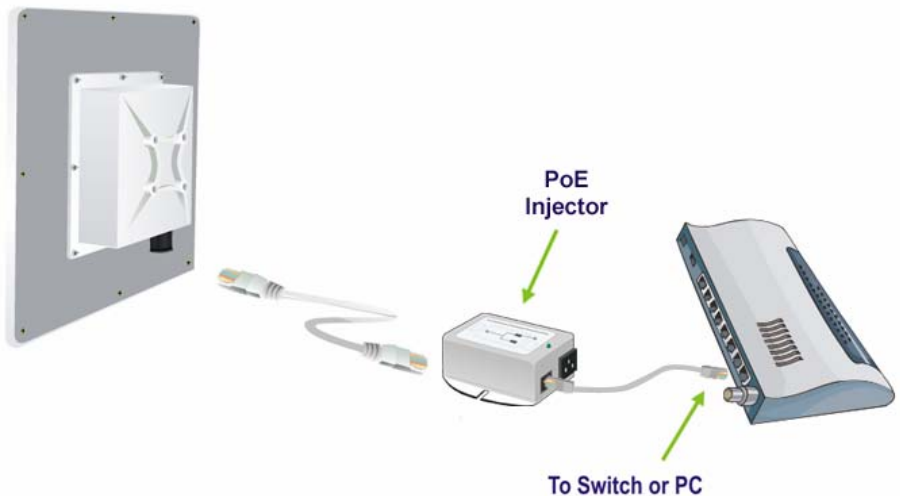
## Hardware Installation

5.- The final step is to tighten the compression nut until the gaskets are tight around the Cat5 cable. Always push the cable toward the connector while tightening to ensure good strain relief of cable to connector.



### Step 2:

From the PoE injector connect one cat.5 Ethernet cable to the AIRNET Outdoor Bridge unit and another cat.5 cable to a switch or PC.



## Hardware Installation

### Step 3:

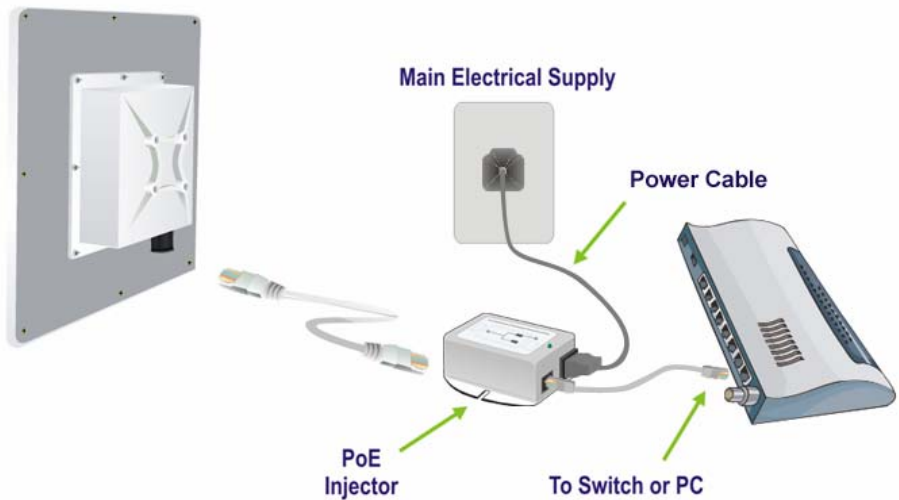
Connect the power cable supplied in the Netkrom PoE kit to the main electrical supply and the power plug into the socket of the injector.

Now, turn on your power supply. Notice that the POWER LED has lighted up.

This indicates that the AIRNET Outdoor Bridge is receiving power through the Netkrom PoE Injector and that connection between your AIRNET Outdoor Bridge unit and your network has been established.

#### Note:

Please use the PoE injector provided in the package. Using a PoE with a different voltage rating will damage this product.



## Hardware Installation

### MOUNTING AIRNET OUTDOOR BRIDGE IN THE POLE OR TOWER

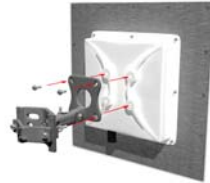
Netkrom AIRNET Outdoor Bridge device can be mounted on the pole or tower as shown in following:

1.- Attach the mounting bracket to the back of the radio using the four hex screws provided. (Do not over tighten the screws.)

**Note:** The bracket in the illustration side shows the normal orientation which allows the wireless unit to be pointed up towards the base station antenna. However, if you live somewhere that would require you pointing the device down towards the base station antenna (for example, you are on the side of a mountain in view of the base station antenna below), reverse the bracket so the Netkrom wireless radio Unit can be “tilted” downward when you aim the AIRNET Outdoor Bridge in a later step.

2.- You can use the pipe bracket assembly for either thin or thick poles by just inverting the position of one of the elements as it shown on the right.

3.- Mount the AIRNET Outdoor Bridge to the top of the pipe or other support and point the AIRNET Outdoor Bridge in the approximate direction of the base station antenna, then hand-tighten the nuts on the mounting system.



## Chapter 3: Access to Web-based Interface

There are two methods to access to the web-based Interface of your access point:

- **Through our Utility – uConfig**  
You can access to the web-based interface directly without the need to assign a different IP address to your PC.
- **By entering the IP address of the wireless device in the address bar of Internet Explorer**  
You need to assign an IP address to your PC, such as 192.168.168.x, where **x** can take any value from 2 to 254, so that it is in the same subnet as AIRNET Outdoor Bridge is.

### ACCESS TO THE WEB INTERFACE WITH UCONFIG

The powerful uConfig utility has been designed to give you direct access to the Web interface.

#### Step 1:

Insert the Product CD into your CD-ROM drive. The CD will run automatically.

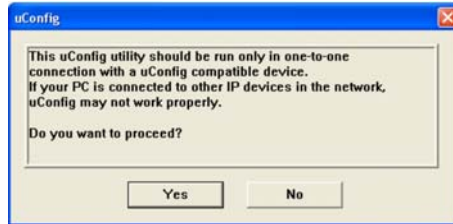
#### Step 2:

From the **Utilities** section, select to install the **uConfig** utility to your hard disk.

## Access to Web-based Interface

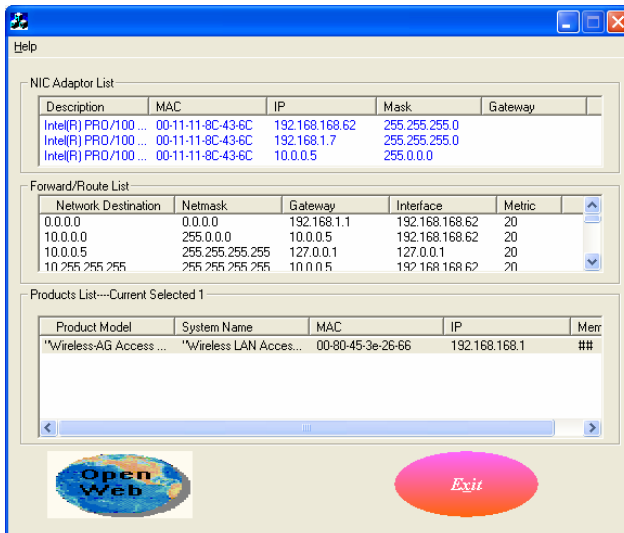
### Step 3:

When the utility has been installed, double-click on the **uConfig** icon. The following screen will appear, click on the **Yes** button to proceed.



### Step 4:

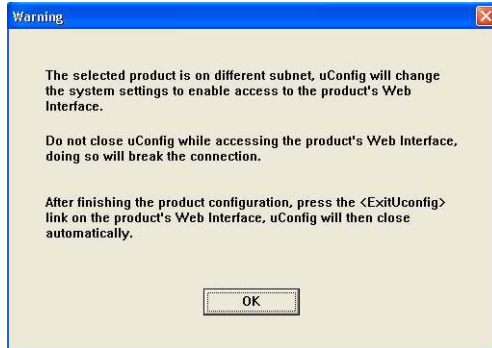
Select **Wireless-AG Access Point** in the **Products List** section and click on the **Open Web** button. To retrieve and display the latest device(s) in the list, click on the **Refresh** button.



## Access to Web-based Interface

### Step 5:

Do not exit the uConfig program while accessing to the web-based interface. This will disconnect you from the device. Click on the **OK** button to proceed.



### Step 6:

At the login page, press the **LOGIN!** button to enter the configuration page. The default password is "password".

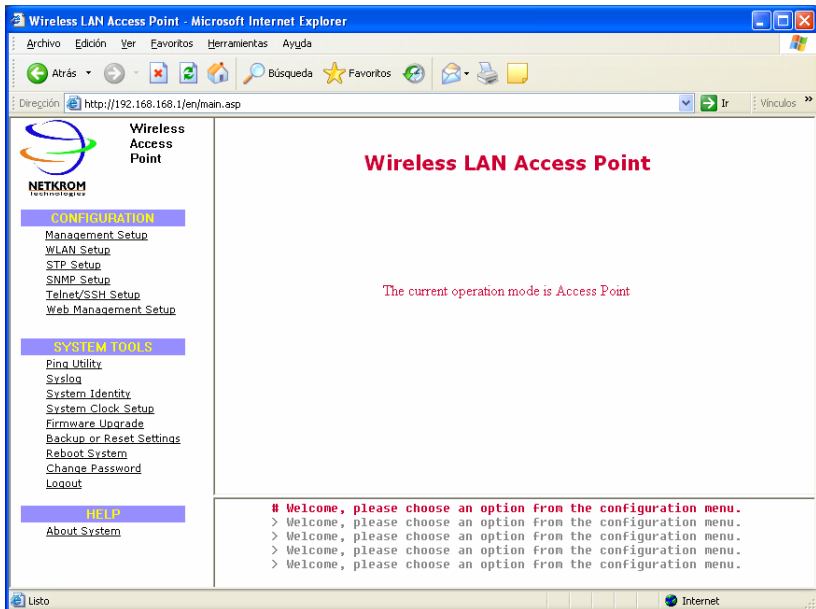




## Access to Web-based Interface

### Step 7:

You will then reach the home page of your AIRNET Outdoor Bridge's web-based interface.



### VERIFY THE IP ADDRESS OF THE AIRNET OUTDOOR BRIDGE WITH NPFind

Another utility program **NpFind**, intended to help you verify the IP address of your product.

Follow the next steps to check the IP address of your AIRNET Outdoor Bridge.

#### Step 1:

Insert the Product CD into the CD-ROM drive. It will automatically run.

#### Step 2:

Click on **Utilities** and select **NpFind** program to run it.

The screen will then display the IP address of the device detected.



### MANUAL ACCESS TO WEB-BASED INTERFACE VIA INTERNET EXPLORER

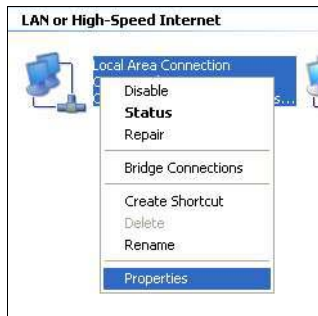
For this method, you need to assign an IP address to your PC so that it belongs to the same subnet as your AIRNET Outdoor Bridge. In this example, we are using Windows XP for illustration. For Windows 98/98SE/2000/NT/ME, kindly refer to **Appendix II "TCP/IP Configuration"**.

#### Step 1:

Go to your desktop, right-click on **My Network Places** icon and select **Properties**.

#### Step 2:

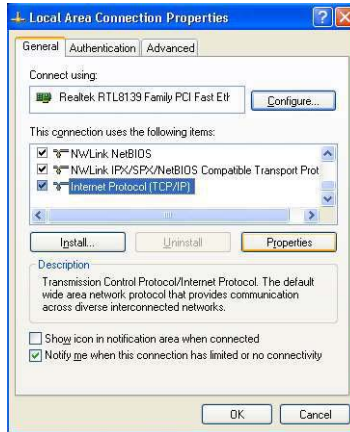
Go to your network adapter icon, right click and select **Properties**.



## Access to Web-based Interface

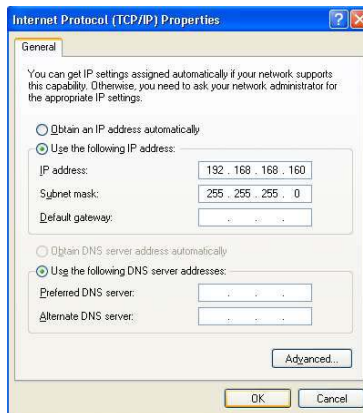
### Step 3:

Highlight **Internet Protocol (TCP/IP)** and click on the **Properties** button.



### Step 4:

Select the radio button for **Use the following IP address**. Enter the IP Address and Subnet Mask as 192.168.168.x and 255.255.255.0, where **x** can be any number from 2 to 254, except 1. In this example, we are using 192.168.168.160 as the static IP Address.



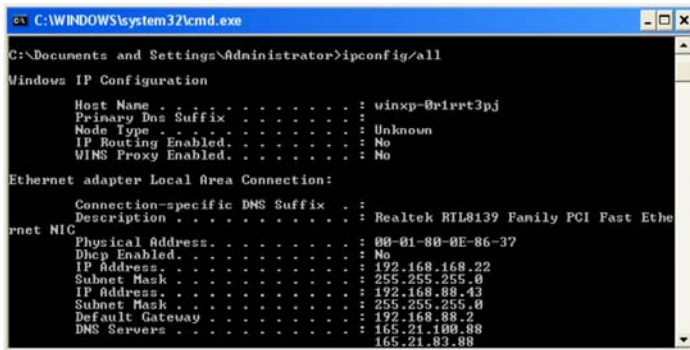
## Access to Web-based Interface

### Step 5:

Click on the **OK** button to close all windows.

### Step 6:

Next, in order to check if the IP address has been correctly assigned to your PC, go to **Start** menu, **Accessories**, select **Command Prompt** and type the command *ipconfig/all*.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig/all

Windows IP Configuration

Host Name . . . . . : winxp-0r1ert3pj
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  :
   Description . . . . . : Realtek RTL8139 Family PCI Fast Eth
   Physical Address. . . . . : 00-01-80-0E-86-37
   DHCP Enabled. . . . . : No
   IP Address. . . . . : 192.168.168.22
   Subnet Mask . . . . . : 255.255.255.0
   IP Address. . . . . : 192.168.88.43
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 192.168.88.2
   DNS Servers . . . . . : 165.21.100.88
                           165.21.83.88
```

Your PC is now ready to configure your AIRNET Outdoor Bridge.

### Step 7:

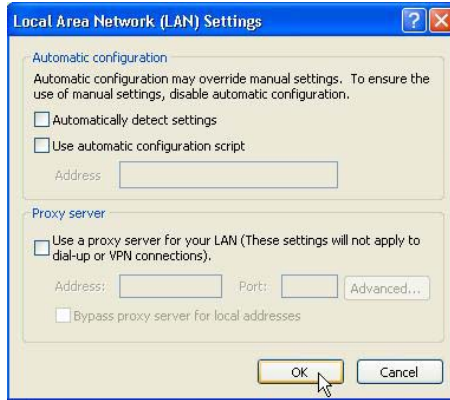
Launch your Web browser. Under the **Tools** tab, select **Internet Options**.



## Access to Web-based Interface

### Step 8:

Open the **Connections** tab and in the **LAN Settings** section, disable all the option boxes. Click on the **OK** button to update the changes.



### Step 9:

At the **Address** bar, enter `http://192.168.168.1` and press **Enter** on your keyboard.

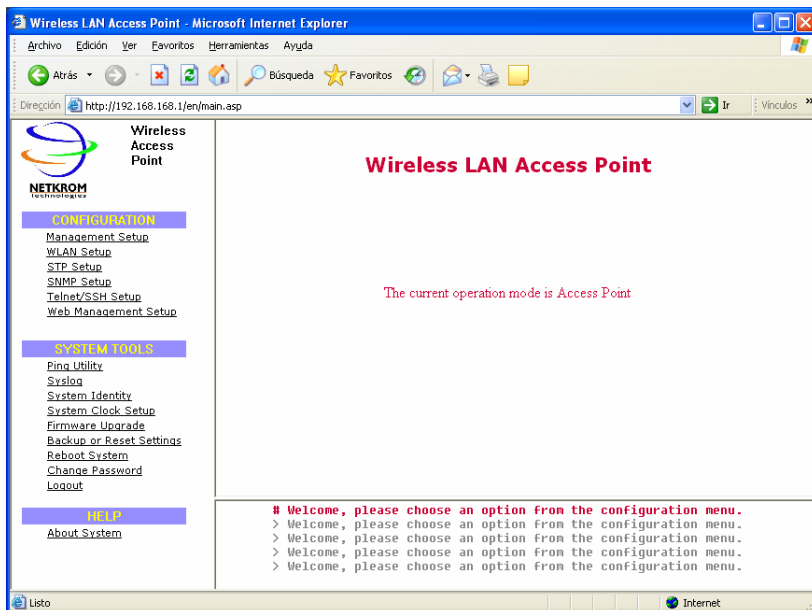
### Step 10:

At the login page, click on the **LOGIN!** button to enter the configuration pages.



## Access to Web-based Interface

You will then reach the home page of your AIRNET Outdoor Bridge's Web interface.



# Chapter 4: Common Configuration

## MANAGEMENT PORT SETUP

At the Management Port Setup page, you may:

Automatically obtain IP address from DHCP server. The default IP 192.168.168.1 is used until a new IP is obtained. Access Point Clients also allows PCs connected to the Ethernet port to obtain IP from the DHCP server at the access point end network.

Manually define IP address

Follow these steps to automatically obtain the IP address from DHCP server.

### Step 1:

Click on **TCP/IP Settings** from **Management Setup** from the **CONFIGURATION** menu.

### Step 2:

Select to **Automatically obtain IP address**.



## Common Configuration

### Step 3:

Select to either **Automatically obtain DNS server** address or **Use the following DNS server** addresses and enter the parameters, if any.

In the **Management Port Setup** page, refer to the table below to replace the default settings of Access point with appropriate values to suit the needs of your network.

### Management Port Setup

Ethernet Link Speed	Auto
<input checked="" type="radio"/> Automatically obtain IP address	
<input type="radio"/> Use the following IP address:	
IP Address:	192.168.168.1
Network Mask:	255.255.255.0
Default Gateway IP:	192.168.88.2
<input checked="" type="radio"/> Automatically obtain DNS server address	
<input type="radio"/> Use the following DNS server addresses:	
Primary DNS IP Address:	210.23.1.4
Secondary DNS IP Address:	210.23.4.6
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

If you choose to **Automatically obtain DNS server address**.

## Common Configuration

### Management Port Setup

Ethernet Link Speed

Automatically obtain IP address

Use the following IP address:

IP Address:

Network Mask:

Default Gateway IP:

Automatically obtain DNS server address

Use the following DNS server addresses:

Primary DNS IP Address:

Secondary DNS IP Address:

If you choose to **Use the following DNS server addresses**.

#### Step 4:

Click on the **Apply** button to save your new parameters.

This table describes the parameters that can be modified in the **Management Port Setup** page if you select to **Use the following DNS server addresses**.

Parameters	Description
<b>Primary DNS IP Address</b>	Your ISP usually provides the IP address of the DNS server.
<b>Secondary DNS IP Address</b>	This optional field is reserved for the IP address of a secondary DNS server.

# Common Configuration

Follow these steps to manually define the IP address.

## Step 1:

Click on **TCP/IP Settings** from **Management Setup** from the **CONFIGURATION** menu.

## Step 2:

Select to **Use the following IP address**.

In the **Management Port Setup** page, refer to the table below to replace the default settings of Access point with appropriate values to suit the needs of your network.

### Management Port Setup

Ethernet Link Speed: Auto

Automatically obtain IP address

Use the following IP address:

IP Address: 192.168.168.1

Network Mask: 255.255.255.0

Default Gateway IP: 192.168.88.2

Automatically obtain DNS server address

Use the following DNS server addresses:

Primary DNS IP Address: 210.23.1.4

Secondary DNS IP Address: 210.23.4.6

Apply Help

## Common Configuration

### Management Port Setup

Ethernet Link Speed	Auto
IP Address:	192.168.168.1
Network Mask:	255.255.255.0
Default Gateway IP:	192.168.168.2
Primary DNS IP Address:	210.23.1.4
Secondary DNS IP Address:	210.23.4.6
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

The parameters are the same in routing mode.

#### Step 3:

Click on the **Apply** button to save your new parameters.

Parameters	Description
<b>IP Address</b>	<p>When the DHCP server of the access point is enabled (unless you set a different <b>DHCP Gateway IP Address</b>), this LAN <b>IP Address</b> would be allocated as the Default Gateway of the DHCP client.</p> <p>The IP address of your Access point is set by default to <b>192.168.168.1</b>.</p>
<b>Network Mask</b>	<p>The Network Mask serves to identify the subnet in which your Access point resides. The default network mask is <b>255.255.255.0</b>.</p>
<b>Default Gateway IP</b>	<p>(Optional) As a bridge Access Point, the access point does not usually communicate with devices on other IP subnets. However, the Default Gateway here acts as the equivalent of the Default Gateway of a PC, to allow the access point to communicate with devices on different subnets. For instance, if you want to access the access point from the Internet or from a router on the LAN, enter the router IP address in the Default Gateway IP field.</p> <p>The Default Gateway IP address of your access point is set to nil by default.</p>

## Common Configuration

### To SETUP DHCP SERVER

There are 3 DHCP modes:

- NONE  
By default, DHCP Mode is set to NONE. Leave the selection at this mode if you do not wish to use DHCP.
- DHCP Server  
Select this mode to setup a DHCP server.
- DHCP Relay  
Select this mode to setup a DHCP relay.  
By default, DHCP broadcast messages do not cross router interfaces. DHCP Relay supports DHCP Clients and DHCP Servers on different networks by configuring the router to pass selective DHCP messages.

Follow these steps if you do not wish to use DHCP.

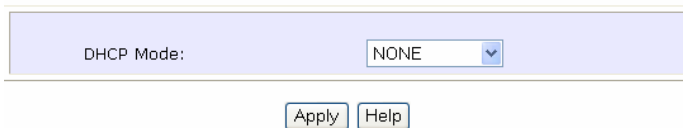
#### Step 1:

Click on **Advanced Settings** from **Management Setup** from the **CONFIGURATION** menu.

#### Step 2:

Set **DHCP Mode** to **NONE**.

#### DHCP Server Setup



The screenshot shows a configuration interface for DHCP Server Setup. It features a light blue header with the title "DHCP Server Setup". Below the header is a form with a label "DHCP Mode:" and a dropdown menu currently set to "NONE". At the bottom of the form are two buttons: "Apply" and "Help".

#### Step 3:

Click on the **Apply** button.

## Common Configuration

The following will guide you to setup the DHCP Server.

### Step 1:

Click on **Advanced Settings** from **Management Setup** from the **CONFIGURATION** menu.

### Step 2:

Set **DHCP Mode** to **DHCP Server**.

In **DHCP Server Setup**, refer to the table below to set the appropriate values to suit the needs of your network.

### DHCP Server Setup

DHCP Mode:	<input type="text" value="DHCP Server"/>
DHCP Start IP Address:	<input type="text" value="192.168.168.100"/>
DHCP End IP Address:	<input type="text" value="192.168.168.254"/>
DHCP Gateway IP Address:	<input type="text" value="192.168.88.2"/>
DHCP Lease Time:	<input type="text" value="3600"/> (seconds)
<input checked="" type="checkbox"/> Always use these DNS servers	
Primary DNS IP Address:	<input type="text" value="210.23.1.4"/>
Secondary DNS IP Address:	<input type="text" value="210.23.4.6"/>

### Step 3:

Click on the **Apply** button.

## Common Configuration

This table describes the parameters that can be modified in **DHCP Server Setup**

Parameters	Description
	The fields DHCP Start IP Address and DHCP End IP Address fields allow you to define the range of IP addresses from which the DHCP Server can assign an IP address to the LAN.
<b>DHCP Start IP Address</b>	This is the first IP address that the DHCP server will assign. The value that you input here should belong to the same subnet as your access point. For example, if the IP address and network mask of your access point are 192.168.168.1 and 255.255.255.0 respectively, the DHCP Start IP Address should be 192.168.168.X, where X can take any value from 2 to 254. It is pre-set to <b>192.168.168.100</b> .
<b>DHCP End IP Address</b>	This is the last IP address that the DHCP server can assign. It should also belong to the same subnet as your access point. For instance, if the IP address and network mask of your access point are 192.168.168.1 and 255.255.255.0 respectively, the DHCP End IP Address should be 192.168.168.X, where X can take any value from 2 to 254. It is pre-set as <b>192.168.168.254</b> .
<b>DHCP Gateway IP Address</b>	<p>Though the DHCP server usually also acts as the Default Gateway of the DHCP client, the access point allows you to define a different <b>DHCP Gateway IP Address</b>, which will be allocated as the Default Gateway IP of the DHCP client. The DHCP client will thus receive its dynamic IP address from the access point but will access to the Internet or to the other LAN through the Default Gateway defined by the <b>DHCP Gateway IP Address</b>.</p> <p>For instance, if the access point is used in Access Point Client mode connects to an Internet gateway <b>X</b>, a PC wired to the access point will be unable to obtain a dynamic IP address directly from <b>X</b>. But if you enable the DHCP server of the access point and set the IP address of <b>X</b> as the <b>DHCP Gateway IP Address</b>, the PC will then obtain its IP address from the access point and access the Internet through <b>X</b>.</p>
<b>DHCP Lease Time</b>	This is the length of time that the client may use the assigned address before having to check with the DHCP Server to see if the Address is still valid.
<b>Primary DNS Address</b>	Your ISP usually provides the IP address of the DNS Server
<b>Secondary DNS Address</b>	This optional setting is the IP address of a secondary DNS server.

## Common Configuration

The following will guide you to setup the DHCP Relay.

### Step 1:

Click on **Advanced Settings** from **Management Setup** from the **CONFIGURATION** menu.

### Step 2:

Set **DHCP Mode** to **DHCP Relay**.

In **DHCP Server Setup**, refer to the table below to set the appropriate values to suit the needs of your network.

### DHCP Server Setup

DHCP Mode:	<input type="text" value="DHCP Relay"/>
DHCP server IP:	<input type="text" value="192.168.168.254"/>
DHCP Gateway IP:	<input type="text" value="192.168.1.1"/>

### Step 3:

Click on the **Apply** button.

This table describes the parameters that can be modified in **DHCP Server Setup**.

Parameters	Description
<b>DHCP Server IP</b>	This is the IP address of the DHCP Server
<b>DHCP Gateway IP Address</b>	<p>Though the DHCP server usually also acts as the Default Gateway of the DHCP client, the access point allows you to define a different <b>DHCP Gateway IP Address</b>, which will be allocated as the Default Gateway IP of the DHCP client. The DHCP client will thus receive its dynamic IP address from the access point but will access to the Internet or to the other LAN through the Default Gateway defined by the <b>DHCP Gateway IP Address</b>.</p> <p>For instance, if the access point is used in Access Point Client mode connects to an Internet gateway <b>X</b>, a PC wired to the access point will be unable to obtain a dynamic IP address directly from <b>X</b>. But if you enable the DHCP server of the access point and set the IP address of <b>X</b> as the <b>DHCP Gateway IP Address</b>, the PC will then obtain its IP address from the access point and access the Internet through <b>X</b>.</p>



## Common Configuration

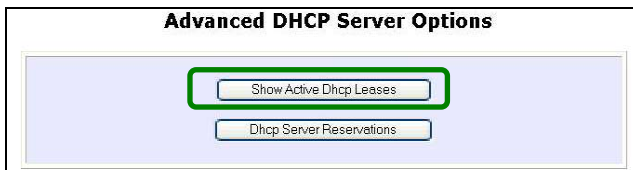
### VIEW ACTIVE DHCP LEASES

#### Step 1:

Select **Management Setup** from the **CONFIGURATION** menu.

#### Step 2:

Go to the **Advanced DHCP Server Options** section and click on the **Show Active DHCP leases** button.



The **DHCP Active Leases** table displays:

- The **Host Name** of the DHCP client
- The **IP Address** allocated to the DHCP client
- The **Hardware (MAC) Address** of the DHCP Client
- The **Lease Expired Time**



#### NOTE

Invalid date and time displayed in the **Lease Expired Time** column indicates that the clock of your access point has not been set properly.

## Common Configuration

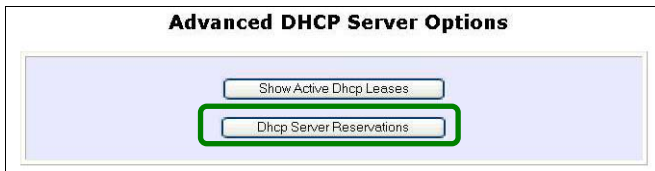
### RESERVE IP ADDRESSES FOR PREDETERMINED DHCP CLIENTS

A reserved IP address is excluded from the pool of free IP addresses the DHCP server draws on for dynamic IP address allocation.

For instance, if you set up a publicly accessible FTP/HTTP server within your private LAN, while that server requires a fixed IP address you would still want the DHCP server to dynamically allocate IP addresses to the rest of the PCs on the LAN.

#### Step 1:

From the **Advanced DHCP Server** Options section, click on the **DHCP Server Reservations** button.



#### Step 2:

Click on **Add** button.



## Common Configuration

### Step 3:

Fill in:

The host portion of the **IP Address** to be reserved.

The **Hardware Address**, in pairs of two hexadecimal values

Press the **Apply** button to effect your new entry.

**DHCP Server Reservations**

IP Address:	192.168.168.	<input type="text" value="20"/>
Hardware Address:	<input type="text" value="00-80-45-e5-0d-05"/>	(XX-XX-XX-XX-XX-XX)

The **DHCP Server Reservations** page will then be refreshed to illustrate the currently reserved IP addresses.

**DHCP Server Reservations**

IP Address	Hardware Address
<a href="#">192.168.168.20</a>	00-80-45-e5-0d-05

# Common Configuration

## DELETE DHCP SERVER RESERVATION

If you do not need the DHCP server to reserve an IP address anymore, you can delete the DHCP Server Reservation.

### Step 1:

Click on the reserved IP address that you wish to delete, e.g. *192.168.168.20*.

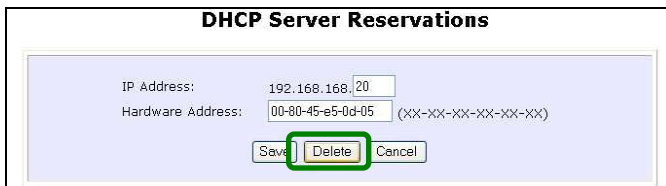


**DHCP Server Reservations**

IP Address	Hardware Address
192.168.168.20	00-80-45-e5-0d-05

### Step 2:

Click on the **Delete** button.



**DHCP Server Reservations**

IP Address: 192.168.168.20  
Hardware Address: 00-80-45-e5-0d-05 (XX-XX-XX-XX-XX-XX)

The **DHCP Server Reservations** table will then be refreshed to reflect your changes.

# Common Configuration

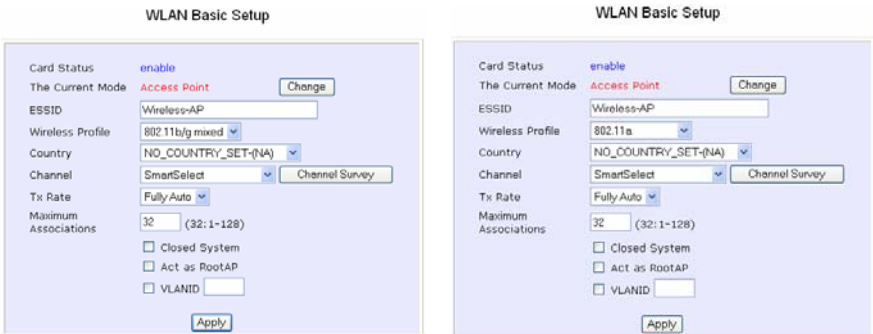
## WLAN SETUP

### TO CONFIGURE THE BASIC SETUP OF THE WIRELESS MODE

#### Step 1:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Basic**.

The default operating mode of the access point is the **Access Point** mode.



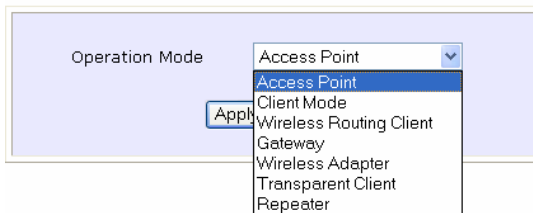
ISP-CPE500GX

ISP-CPE500AX

#### Step 2: (Optional: Change Current mode)

If you wish to change the current mode of your access point, click on **Change**, select your **Operation Mode** and click on the **Apply** button to access the setup page of your selected mode. Then you are prompted to reboot the access point so as to effect the mode setting.

#### WLAN Operation Mode



## Common Configuration

### Step 3:

Enter the parameters in their respective fields, click on the **Apply** button and reboot your device to let your changes take effect.

Note that the **WLAN Basic Setup** pages for the modes are different.

Example: **WLAN Basic Setup** page for **Client Mode**

#### WLAN Basic Setup

Card Status	enable
The Current Mode	Client <input type="button" value="Change"/>
ESSID	Wireless-AP <input type="button" value="Site Survey"/>
Remote AP MAC	00:00:00:00:00:00 <input type="checkbox"/>
Wireless Profile	802.11b/g mixed ▼
Country	NO_COUNTRY_SET-(NA) ▼
Tx Rate	Fully Auto ▼
<input type="button" value="Apply"/>	

Example: **WLAN Basic Setup** page for **Access Point**

#### WLAN Basic Setup

Card Status	enable
The Current Mode	Access Point <input type="button" value="Change"/>
ESSID	Wireless-AP
Wireless Profile	802.11b/g mixed ▼
Country	NO_COUNTRY_SET-(NA) ▼
Channel	SmartSelect ▼ <input type="button" value="Channel Survey"/>
Tx Rate	Fully Auto ▼
Maximum Associations	32 (32: 1-128)
	<input type="checkbox"/> Closed System
	<input type="checkbox"/> Act as RootAP
	<input type="checkbox"/> VLANID <input type="text"/>
<input type="button" value="Apply"/>	

# Common Configuration

This table describes the parameters that can be modified in the [WLAN Basic Setup](#) page.

Parameters	Description
<b>The Current Mode</b>	<p>The default operating mode is the <b>Access Point</b> mode.</p> <p>Operating modes:</p> <ul style="list-style-type: none"><li>• Access Point Mode</li><li>• Client Mode</li><li>• Wireless Routing Client</li><li>• Gateway Mode</li><li>• Wireless Adapter Mode</li><li>• Transparent Client Mode</li><li>• Repeater mode</li></ul> <p>You can toggle the modes by clicking on the <b>Change</b> button.</p>
<b>ESSID</b>	<p>Enter a preferred name for the wireless network. Your wireless clients must be configured with the same ESSID. This case-sensitive entry can consist of a maximum of 32 characters.</p>
<b>Site Survey</b>	<p>A list of wireless devices in the WLAN that are detected by your access point. Information such as MAC address, channel, SSID, algorithm and signal strength can be found in the listing.</p> <p>This feature is supported by the Access Point Client and Wireless Routing Client modes.</p>
<b>Wireless Profile</b>	<p>A selection of network environment types in which to operate the access point:</p> <ul style="list-style-type: none"><li>• <b>802.11a only (only for ISP-CPE500AX)</b> Supports wireless A clients with data rates of up to 54 Mbps in the frequency range of 5.8 Ghz.</li><li>• <b>802.11b only (only for ISP-CPE500GX)</b> Supports wireless B clients with data rates of up to 11Mbps in the frequency range of 2.4GHz.</li></ul>

## Common Configuration

	<ul style="list-style-type: none"> <li>• <b>802.11b/g mixed (only for ISP-CPE500GX)</b> Supports both wireless B and G clients.</li> <li>• <b>802.11g only (only for ISP-CPE500GX)</b> Supports wireless-G clients that offer transmission rates of up to 54Mbps in the 2.4GHz frequency band.</li> </ul>
<b>Country</b>	Choose the <b>Country</b> where you are located.
<b>Channel</b>	This option allows you to select a frequency channel for the wireless communication. Select SmartSelect to automatically scan and recommend the best channel that the access point can utilize.
<b>Tx Rate</b>	Allow you to choose the rate of data transmission from <b>1Mbps to Fully Auto</b> and from <b>6Mbps to Fully Auto</b> .
<b>Closed System</b>	The access point will not broadcast its <b>WLAN name (ESSID)</b> when <b>Closed system</b> is enabled. By default <b>Closed system</b> is disabled.
<b>Act as RootAP</b>	The access point will connect with 1, or multiple clients to create a point-to-point and point-to-multi-point connection network with 2 or more access points. This connection mode is fully compliant with 802.1h standards.
<b>VLAN ID</b>	This is the number that identifies the different virtual network segments to which the network devices are grouped. This can be any number from 1 to 4094.
<b>Channel Survey</b>	A list of channels that are detected by your access point in the WLAN. Information such as frequency, channel, MyQuality, NeighQuality, APCount and Recommendation can be found in the listing. The Access Point and Gateway modes support this feature.

**SCAN FOR SITE SURVEY**

**(ONLY FOR CLIENT MODE AND WIRELESS ROUTING CLIENT MODE )**



## Common Configuration

### Step 1:

In the **Mode Setup** page, click on the **Site Survey** button.

**WLAN Basic Setup**

Card Status	enable	
The Current Mode	Client	<input type="button" value="Change"/>
ESSID	<input type="text" value="Wireless-AP"/>	<input type="button" value="Site Survey"/>
Remote AP MAC	<input type="text" value="00:00:00:00:00:00"/>	<input type="checkbox"/>
Wireless Profile	802.11b/g mixed	
Country	NO_COUNTRY_SET-(NA)	
Tx Rate	Fully Auto	

The **Site Survey** provides a list of the **MAC addresses (BSSID)** and **SSID** of neighboring access points detected, the **Chan** (channels), **Auth** (Authentication), **Alg** (Algorithm) used, and the strength of the **Signal** received.

**Site Survey**

Bssid	SSID	Chan	Auth	Alg	Signal
<input type="radio"/> 008045003472	PMD-28G-Online	6	WPA-PSK	TKIP	8
<input type="radio"/> 008045015403	wp54-1C	1	RSN-PSK	AES	3
<input type="radio"/> 00804530b5bd	wpe-A	6	WPA-PSK	TKIP	3
<input type="radio"/> 00804521f877	np18a-tang	10	WPA-EAP	TKIP	2
<input type="radio"/> 00804535891e		10	OPEN	NONE	22
<input type="radio"/> 00804500348d	OMEGA1	8	OPEN	NONE	9
<input type="radio"/> 00804500345d	Any1	7	OPEN	NONE	5
<input type="radio"/> 00804524c675	Any	3	OPEN	NONE	3
<input type="radio"/> 008045358861	np28g	6	OPEN	NONE	7

**Site Survey on the 2.4 Ghz frequency band**

## Common Configuration

---

### Step 2:

To connect the client to one of the access points detected, select the radio button corresponding to the access point you want to connect to.

### Step 3:

Click on the **Apply** button to effect the change and return to the setup page.

### Step 4:

Click on the **Refresh** button to update the screen.

## Common Configuration

---

This table describes the read-only parameters of neighboring access points that can be viewed from the **Site Survey** page.

Parameters	Description
<b>Bssid</b>	In an infrastructure wireless network, the BSSID refers to the wireless MAC address of the access point.
<b>SSID</b>	Refers to the network name that uniquely identifies the network to which the access point is connected.
<b>Chan</b>	Refers to the channel being used for transmission.
<b>Auth</b>	Refers to the types of authentication, such as WPA, WPA-Personal, etc being used by the access point.
<b>Alg</b>	Refers to the types of algorithm, such as WEP, TKIP, etc being used by the access point.
<b>Signal</b>	Describes the strength of the signal received in percentage.



### NOTE

The purpose of using **Site Survey** is to scan and display all access points based on the current security setting of your access point. Explanation of the following information supplied by the Site Survey according to the security setting:

- If the security mode is set to **None** or **WEP**, the scan will show all available access points that have no security or WEP security
  - If the security mode is set to **WPA-Personal**, the scan will show all available access points with all types of security from **no** security, **WEP** security to **WPA-Personal** security.
-

# Common Configuration

## VIEW LINK INFORMATION

(ONLY FOR CLIENT MODE AND WIRELESS ROUTING CLIENT MODE)

### Step 1:

To view the connection status when the client is linked to another access point, click on the **Show Link Information** button.

WLAN Basic Setup

Card Status: enable  
The Current Mode: Client [Change]  
ESSID: Wireless-AP [Site Survey]  
Remote AP MAC: 00:00:00:00:00:00 [ ]  
Wireless Profile: 802.11b/g mixed [v]  
Country: NO\_COUNTRY\_SET-(NA) [v]  
Tx Rate: Fully Auto [v]  
[Apply]

### Link Information

Show Link Information

The **Link Information** table displays the following data:

Link Information	
State	Scanning: ff:ff:ff:ff:ff:ff
Current Channel	11
TxRate	1Mbps
Signal Strength	6

This table describes the parameters that can be viewed from the **Link Information** page.

Parameters	Description
<b>State</b>	Displays whether the <b>State</b> is <b>Scanning</b> or <b>Associated</b> , and MAC address of the access point to which the client is connected.
<b>Current Channel</b>	Channel presently being used for transmission.
<b>Tx Rate</b>	Rate of data transmission in Mbps.
<b>Signal Strength</b>	Intensity of the signal received, in percentage

# Common Configuration

## SCAN FOR CHANNEL SURVEY (AVAILABLE FOR ACCESS POINT MODE AND GATEWAY MODE)

Channel Survey provides a list of all channels that are supported by the access point. This feature will show relative interference of all channels and recommend the least congested channel.

### Step 1:

In the **Mode Setup** page, click on the **Channel Survey** button.

**WLAN Basic Setup**

Card Status	enable
The Current Mode	Access Point <input type="button" value="Change"/>
ESSID	<input type="text" value="Wireless-AP"/>
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA) <input type="button" value="Change"/>
Channel	SmartSelect <input type="button" value="Channel Survey"/>
Tx Rate	Fully Auto
Maximum Associations	<input type="text" value="32"/> (32: 1-128)
	<input type="checkbox"/> Closed System
	<input type="checkbox"/> Act as RootAP
	<input type="checkbox"/> VLANID <input type="text"/>
	<input type="button" value="Apply"/>

The **Channel Survey** provides a list of the **Freq** (frequency) and **Channel** of the access point detected, the **APCount**, **MyQuality** (your access point's interference from your access point's channel signal) received and **NeighQuality** (interference from the neighboring access points' channel signals) received.

## Common Configuration

**Channel Survey Status**

	Freq	Channel	MyQuality	APCount	NeighQuality	Recommendation
<input type="radio"/>	2437	6	0	0	28	
<input type="radio"/>	2447	8	0	0	23	
<input type="radio"/>	2452	9	0	0	9	
<input type="radio"/>	2462	11	0	0	9	Recommended
<input type="radio"/>	2417	2	4	2	130	
<input type="radio"/>	2432	5	5	1	194	
<input checked="" type="radio"/>	2457	10	9	1	0	
<input type="radio"/>	2412	1	23	2	4	
<input type="radio"/>	2442	7	23	1	0	
<input type="radio"/>	2422	3	107	3	198	
<input type="radio"/>	2427	4	194	5	112	

### Channel Survey on the 2.4 Ghz frequency band

Please take note that the MYQuality and NeighQuality are RSSI values.

If the value is higher which means that you receive the stronger signal strength from several APs, it indicates that the higher interference from these APS will occur as well. The value of zero indicates no interference.

#### Step 2:

To connect the client to one of the channels detected, select the radio button corresponding to the channel you want to connect to.

#### Step 1:

Click on the **Apply** button to effect the change and return to the setup page.

#### Step 2:

Click on the **Refresh** button to update this screen.

## Common Configuration

This table describes the read-only parameters of all channels that can be viewed from the **Channel Survey** page.

Parameters	Description
<b>Freq</b>	Frequency of the channel at which your access point is operating.
<b>Channel</b>	Channel of the access point being used for transmission depending on its origin of country.
<b>MyQuality</b>	Interference level of the respective channel with this AP. The lower the value, the less interference. If the value is zero, there is no interference.
<b>APCount</b>	Total number of access points operating at the current channel.
<b>NeighQuality</b>	Interference level with those discovered APs at those respective channels. The lower the value, the less interference. If the value is zero, there is no interference.
<b>Recommendation</b>	Best channel for the device to use in its current environment.

# Common Configuration

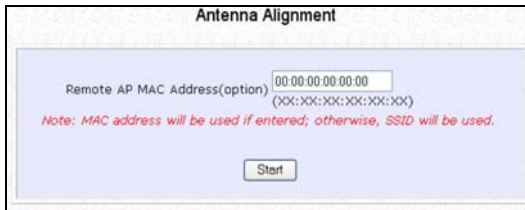
## ANTENNA ALIGNMENT

### (AVAILABLE FOR ALL MODES)

The **Antenna Alignment** feature in the access point is designed to precisely align the antenna over such a long distance so that the connectivity communication between your access point and another remote or neighboring access point could be improved as indicated by higher signal strength.

#### Step 1:

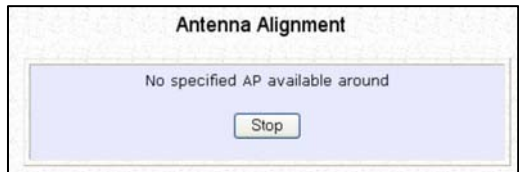
Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Antenna Alignment**. The **Antenna Alignment** page can act as a diagnostic tool to check the communication with a remote device. The remote AP MAC Address is preset to all zeros by default.



#### Step 2:

If you wish to specify the MAC address of the remote AP, key in the field next to **Remote AP Address (option)**, followed by clicking on the **Start** button. A pop-up status screen will display, allowing you to monitor the signal strength received from the remote access points.

If there is no specified AP with its MAC address you have keyed in, the screen on the right will be displayed. To abort or to key in the MAC address of another available remote AP, click on the **Stop** button.





## Common Configuration

---



### NOTE

If no MAC address is entered, the **Antenna Alignment** tool will make use of the SSID to align the antenna. Please make sure that the correct SSID is entered. If more than one access point (AP) shares the same SSID, the **Antenna Alignment** tool will show the strongest signal AP.

---

Signal Strength (RSSI value)	Status of DIAG LED
Above 20	Stays turned on
Between 19 and 17	Flashes 6 times
Between 17 and 14	Flashes 3 times
Between 13 and 10	Flashes once
Below 10	Turns OFF



### NOTE

Outdoor long distance connection should preferably have signal strength of a RSSI of 10 and above.

### NOTE

To ensure proper functionality of the device, select to Stop antenna alignment. Alternatively, you may also reboot the device.

---

## Common Configuration

### CONFIGURE THE ADVANCED SETUP OF THE WIRELESS MODE

#### Step 1:

Select **WLAN Setup** from the **CONFIGURATION** menu to expand four sub-menus. From here, click on **Advanced**.

#### Step 2:

Enter the parameters in the **WLAN Advanced Setup** page.

#### Step 3:

Click on the **Apply** button to update the changes.

#### WLAN Advanced Setup

Beacon Interval	<input type="text" value="100"/>	(100:20-1000)
Data Beacon Rate (DTIM)	<input type="text" value="1"/>	(1:1-16384)
RTS/CTS Threshold	<input type="text" value="2312"/>	(2312:1-2312)
Frag Threshold	<input type="text" value="2346"/>	(2346:256-2346)
Transmit Power	<input type="text" value="Maximum"/>	
Antenna Control	<input type="text" value="Auto"/>	
DFS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Station Isolation	<input type="checkbox"/>	
Radio Off When Ethernet Link Down	<input type="checkbox"/>	
<input type="button" value="Apply"/>		

## Common Configuration

This table describes the parameters that can be modified in the [WLAN Advanced Setup](#) page.

Parameters	Description
<b>Beacon Interval</b> (Only in Access Point mode)	<p>The <b>Beacon Interval</b> is the amount of time between beacon transmissions. This tells the client when to receive the beacon. A beacon is a guidance signal sent by the access point to announce its presence to other devices in the network.</p> <p>Before a client enters the power-save mode, it needs the <i>beacon interval</i> to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).</p>
<b>Data Beacon Rate (DTIM)</b> (Only in Access Point mode)	<p>The <b>Data Beacon Rate (DTIM)</b> determines how often the beacon contains a delivery traffic indication message (DTIM). The DTIM identifies which clients (in power-save mode) have data frames waiting for them in the access point's buffer.</p> <p>If the beacon period is set at 100 (default value), and the data beacon rate is set at 1 (default value), then the access point sends a beacon containing a DTIM every 100 Kμsecs (1 Kμsec equals 1,024 μsec).</p>
<b>RTS/CTS Threshold</b>	<p>The <b>RTS/CTS Threshold</b> value determines the minimum size of a packet in bytes that would trigger the RTS/CTS mechanism.</p> <p>This value extends from 1 to 2312 bytes.</p>
<b>Frag Threshold</b>	<p>The <b>Frag Threshold</b> value indicates the maximum size that a packet can reach without being fragmented.</p> <p>This value extends from 256 to 2346 bytes, where a value of 0 indicates that all the packets should be transmitted using RTS.</p>
<b>Transmit Power</b>	<p>The <b>Transmit Power</b> drop-down list lets you pick from a range of transmission power.</p>
<b>Radio Off When Ethernet Link Down</b>	<p>Disables the radio card automatically when the Ethernet link is down.</p>



### NOTE

The values illustrated in the examples are suggested values for their respective parameters.

# Common Configuration

## VIEW THE STATISTICS

The Statistics feature reveals information on the wireless device connected to the WLAN.

### Step 1:

Select **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus under **WLAN Setup**. Click on **Statistics**.

Wireless clients that are connected to the WLAN are shown in the WLAN Station List.

### Step 2:

Click on the **Refresh** button to get the latest information on the availability of wireless clients in the wireless network.

WLAN Station List			
ID	MAC Address	RSSI	TxRate
AP	<a href="#">00:80:45:37:86:dd</a>	1	36Mbps

### Step 3:

To check the details on an individual wireless client, click on the corresponding MAC Address in the WLAN Station List.

The following screen will show the statistics of the selected wireless client.

00:80:45:37:86:dd Statistics						
Authentication Type			Encryption			
Open-System			No			
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	2122	0	0
Transmit	0	0	0	11	0	0

In **Client** mode you are not allowed to view the information of other wireless clients, to do that you need to change to Access Point mode.

# WAN SETUP (AVAILABLE IN WIRELESS ROUTING CLIENT AND GATEWAY MODES)



### NOTE

Any changes to the WAN Setup will only take effect after rebooting.

Setup your WAN to share Internet connection among the clients of the access point.

Setup your WAN for Cable Internet whereby WAN IP address is dynamically assigned by ISP

The access point is pre-configured to support this WAN type. However, you may verify the WAN settings with the following steps:

Step 1: Under **CONFIGURATION** on the command menu, click on **WAN Setup**.

Step 2:

On the **WAN Dynamic Setup** screen, verify that the **WAN Type** is **Dynamic (DHCP)**. Otherwise, click on the **Change** button.

**WAN Dynamic Setup**

WAN Type	Dynamic (DHCP)	<input type="button" value="Change"/>
IP Address		<input type="button" value="Refresh"/>
Network Mask		
Gateway IP Address		
Primary DNS		
Secondary DNS		

Step 3:

Simply select **Dynamic IP Address** and hit the **Apply** button.

Please remember to click **Reboot System** under **SYSTEM TOOLS** and hit the **Reboot** button to let the settings take effect.

**Select WAN Type**

- Static IP Address
- Dynamic IP Address
- PPP over Ethernet
- PPTP

## Common Configuration

**Note:** There are exceptional cases where additional configuration is required before an IP address will be allocated by your ISP to the access point.

- a. Certain ISPs log the MAC address of the first device used to connect to the broadband channel and will not release a WAN IP address unless the MAC address matches the one in their log. Therefore, if yours is not a new Cable Internet subscription (i.e. your PC was formerly connected directly to your cable modem), refer to **steps 4 - 5** to clone the “approved” MAC address onto the access point.
- b. Certain ISPs require authentication through a DHCP Client ID before releasing a public IP address to you. The access point uses the System Name in the System Identity as the DHCP Client ID.

Therefore, if this is the case, refer to your ISP for the correct DHCP Client ID to be set and follow **steps 6 - 7** to accomplish the setup.

### Step 4:

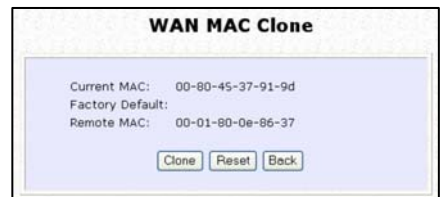
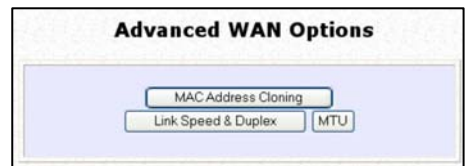
Steps 4 - 5 are for those who need to clone their Ethernet adapter’s MAC address.

In the **WAN Setup** found under the **CONFIGURATION** command menu, you will see the **Advanced WAN Options**. Click **MAC Clone** to continue.

### Step 5:

Simply click on the **Clone** button so that your access point clones the ISP-recognized MAC address of your Ethernet adapter.

Please remember to click **Reboot System** under **SYSTEM TOOLS** and hit the **Reboot** button to let the settings take effect.



Take note: (If required, you may reset the access point’s MAC address to its factory default by clicking **Reset** on that same page)

## Common Configuration

### Step 6:

Steps 6 - 7 are for those who need to set up the **System Name** in **System Identity** so that your ISP can authenticate it as a valid DHCP Client ID.

Click on **System Identity** under the **SYSTEM TOOLS** command menu.



The screenshot shows a web interface titled "System Identity". It contains three input fields: "System Name" with the value "Wireless LAN Access Point", "System Contact" with the value "unknown", and "System Location" with the value "unknown". Below the fields is an "Apply" button.



### Step 7:

On the following screen, key in the ISP assigned DHCP Client ID as the **System Name** (You may also like to key in a preferred **Systems Contact** person and the **System Location** of the access point). Click the **Apply** button to complete.

Please remember to click **Reboot System** under **SYSTEM TOOLS** and hit the **Reboot** button to let the settings take effect.

# Common Configuration

## WAN Setup - Cable Internet with Static IP Assignment

If you have an ISP that leases a static WAN IP for your subscription, you will need to configure your access point's WAN type accordingly. For example, if the ISP provided you with the following setup information, you can set up your WAN as described below:

IP Address : 203.120.12.240  
Network Mask : 255.255.255.0  
Gateway IP Address : 203.120.12.2

### Step 1:

Under **CONFIGURATION** on the command menu, click on **WAN Setup**.



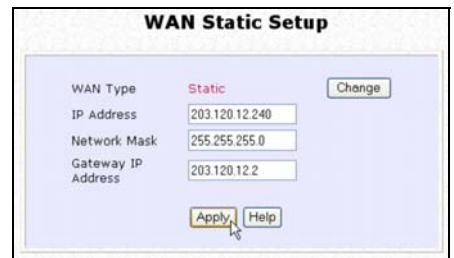
### Step 2:

Access the **Select WAN Type** page and choose **Static IP Address** before clicking the **Apply** button. You will then be brought to the following page requiring your inputs.

### Step 3:

Fill in the information provided by your ISP in the **IP Address**, **Network Mask** and **Gateway IP Address** fields, before clicking the **Apply** button.

Please remember to click **Reboot System** under **SYSTEM TOOLS** and hit the **Reboot** button to let the settings take effect.






## Common Configuration

### WAN Setup - ADSL Internet using PPP over Ethernet (PPPoE)

If you subscribe to an ADSL service using PPP over Ethernet (PPPoE) authentication, you can set up your access point's WAN type as follows. For example, you may configure an account whose username is 'guest' as described below:



**Select WAN Type**

Static IP Address

Dynamic IP Address

PPP over Ethernet

PPPoE

#### Step 1:

Under **CONFIGURATION** on the command menu, click on **WAN Setup**.

#### Step 2:

Access the **Select WAN Type** page and choose **PPP over Ethernet** before clicking the **Apply** button. You will then be brought to the following page requiring your inputs.

#### Step 3:

For **Username**, key in your ISP assigned account name (e.g. guest for this example), followed by your account **Password**.

#### Step 4:

Select **Always-On** if you want your access point to always maintain a connection with the ISP. Otherwise, you may select **On-Demand**. The access point will then connect to the ISP automatically when it receives Internet requests from the PCs in your network.



**WAN PPPoE Setup**

WAN Type : **PPPoE**

Username

Password

On-Demand Idle Timeout (0: disabled)  seconds

Always-On Reconnect Time Factor  seconds

Status : **Connecting**

IP Address  
Network Mask  
Default Gateway  
Primary DNS  
Secondary DNS

## Common Configuration

The **Idle Timeout** setting is associated with the **On-Demand** option, allowing you to specify the value (in seconds) after which the access point will disconnect from the ISP after the last Internet activity. A value of "0" will disable idle timeout. **Reconnect Time Factor** is associated with the **Always-on** option and specifies the maximum time the access point will wait before re-attempting to connect with your ISP. Hit the **Apply** button and **Reboot** the access point.

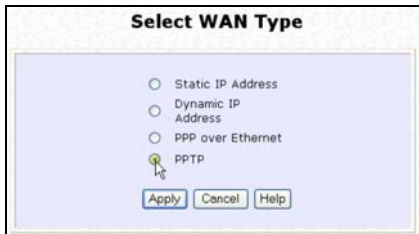
### WAN Setup – ADSL Internet using PPTP

If you subscribe to an ADSL service using Point to Point Tunneling Protocol (PPTP) authentication, you can set up your access point's WAN type from the steps that follow. For example, if the ISP provided you with the following set up information, you can set up your WAN as described below:

IP Address : 203.120.12.47  
Network Mask : 255.255.255.0  
VPN Server : 203.120.12.15

#### Step 1:

Under **CONFIGURATION** on the command menu, click on **WAN Setup**.



#### Step 2:

Access the **Select WAN Type** page and choose **PPTP** before clicking the **Apply** button. You will then be brought to the following page requiring your inputs.

#### Step 3:

Fill in the information provided by your ISP in the **IP Address**, **Network Mask** and **VPN Server** fields, followed by clicking the **Apply** button.

Please remember to click **Reboot System** under **SYSTEM TOOLS** and hit the **Reboot** button to let the settings

## Common Configuration

take effect.

The **Idle Timeout** setting allows you to specify the value (in seconds) after which the access point will disconnect from the ISP after the last Internet activity. A value of "0" will disable idle timeout.

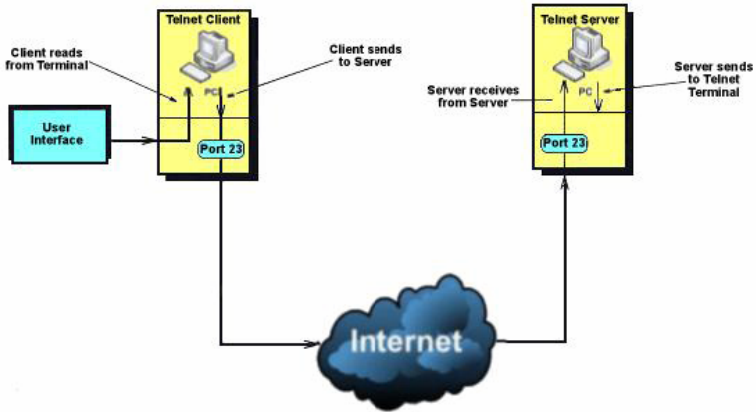


The image shows a web-based configuration page titled "WAN PPTP Setup". The page has a light blue background and contains the following fields and controls:

- WAN Type:** Set to "PPTP" with a "Change" button next to it.
- IP Address:** An empty text input field.
- Network Mask:** An empty text input field.
- Username:** An empty text input field.
- Password:** An empty text input field.
- VPN Server:** An empty text input field.
- Idle Timeout:** A text input field containing "0" with a note "(30-3600, 0: disabled)" to its right.
- Status:** Displayed as "Disconnected" in red text, with a "Refresh Status" button to its right.
- IP Address:** A label for the current IP address.
- Network Mask:** A label for the current network mask.
- Gateway IP Address:** A label for the current gateway IP address.
- Buttons:** "Apply" and "Email Notification" buttons are located at the bottom of the form.

# Common Configuration

## SETUP TELNET / SSH



Telnet allows a computer to remotely connect to the access point CLI (Command Line Interface) for control and monitoring  
SSH (Secure Shell Host) establishes a secure host connection to the access point CLI for control and monitoring

### Step 1:

Select **Telnet/SSH Setup** from the **CONFIGURATION** menu.

### Step 2:

1. Select Telnet Server Enable and enter the Port Number to enable
2. Select SSH Server Enable and enter the Port Number to enable

Click the **Apply** button

### Telnet/SSH Setup

<input type="checkbox"/> Telnet Enable	Port Number 23	Time out(seconds) 600
<input type="checkbox"/> SSH Enable	Port Number 22	

**Apply**

# Common Configuration

## Step 3:

To add user:

1. Click the **Add** button.

### User Management

Select	User Name	Permission
--------	-----------	------------

2. In Add User Entry Page, enter the User Name, Password and specify whether the user is granted permission to Read Only or Read/Write.
3. Click the **Apply** button.

### Add User Entry

User Name

Password

Permission:

To delete user:

1. Select which user to delete.
2. Click the **Delete** button.

### User Management

Select	User Name	Permission
<input checked="" type="checkbox"/>	<a href="#">username</a>	RO
<input type="checkbox"/>	<a href="#">username2</a>	RW

To Refresh User Management list click the **Refresh** button.

### User Management

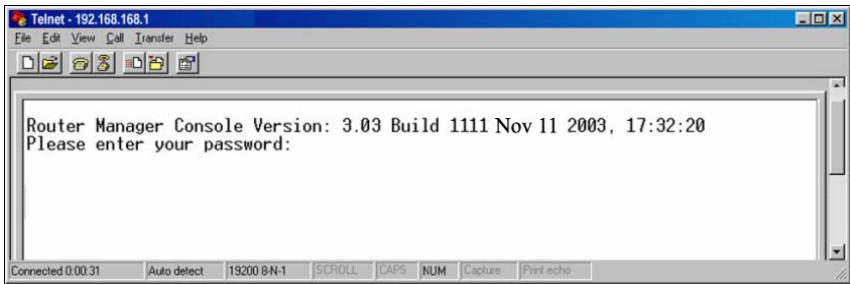
Select	User Name	Permission
<input type="checkbox"/>	<a href="#">username2</a>	RW

## Common Configuration

### ACCESS THE TELNET COMMAND LINE INTERFACE

You may connect to the CLI (Command Line Interface) via a TELNET session to the default IP **192.168.168.1** Microsoft TELNET command is shown here but any TELNET client can be used.

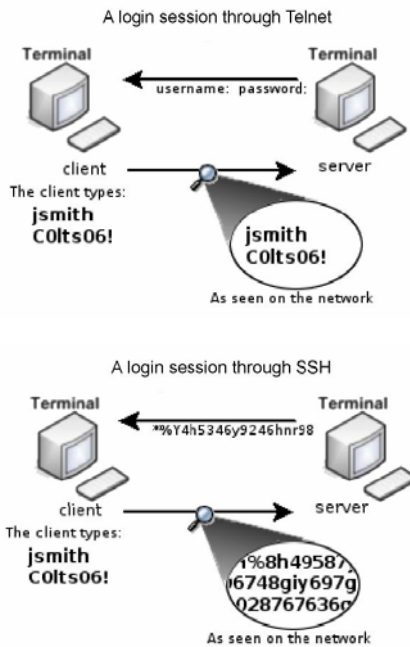
1. Enter C:\WINDOWS\TELNET 192.168.168.1 at DOS prompt and the TELNET application will launch and connect.
2. At the login prompt, type in the default password "password" and press enter. You will then login to the CLI.



### ACCESS THE SECURE SHELL HOST COMMAND LINE INTERFACE

SSH provides the best remote access security using different forms of encryption and ciphers to encrypt sessions, and providing better authentication facilities and features that increase the security of other protocols.

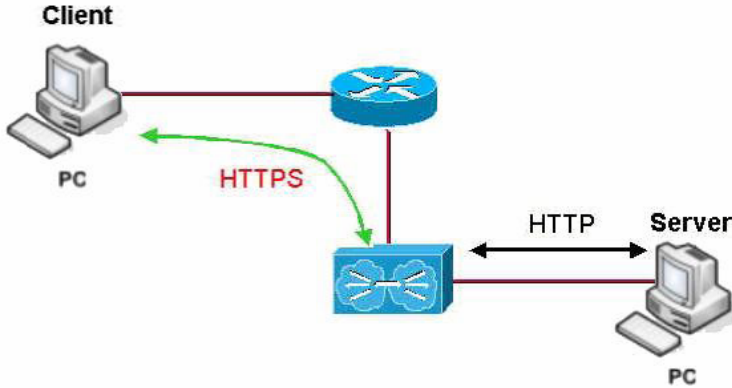
An encrypted connection like SSH is not viewable on the network. The Server can still read the information, but only after negotiating the encrypted session with the client.



SSH CLI has a command line interface.

```
Generating public/private dsa key pair.  
Enter file in which to save the key (/home/localuser/.ssh/id_dsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/localuser/.ssh/id_dsa.  
Your public key has been saved in /home/localuser/.ssh/id_dsa.pub.  
The key fingerprint is:  
93:58:20:56:72:d7:bd:14:86:9f:42:aa:82:3d:f8:e5 localuser@mybox.home.com
```

## SET THE WEB MODE



The access point supports HTTPS (SSL) featuring additional authentication and encryption for secure communication, in addition to the standard HTTP.

Step 1:

Select **Web Server Setup** from the **CONFIGURATION** menu.

Step 2:

1. Select whether to set web server to HTTP or HTTPS (SSL) mode.
2. Click **Apply**.

Changes will be effected after reboot.

### Web Server Setup

Mode	<input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS (SSL)
Login Timeout	<input type="text" value="300"/> ( Seconds )
<input type="button" value="Apply"/>	



## Common Configuration

### SNMP SETUP

Simple Network Management Protocol (SNMP) is a set of communication protocols that separates the management architecture from the architecture of the hardware devices.

#### Step 1:

Click on **SNMP** from the **CONFIGURATION** menu.



The screenshot shows a window titled "SNMP Setup". Inside the window, there are three fields: "SNMP State" with a dropdown menu showing "Enable", "Read Password" with a text input field containing "\*\*\*\*\*", and "Read/Write Password" with a text input field containing "\*\*\*\*\*". Below these fields is an "Apply" button with a mouse cursor pointing to it.

#### Step 2:

Select **Enable** from the **SNMP State** drop-down list.

The default **Read Password** is set to *public* while the default **Read/Write Password** is *private*.

#### Step 3:

Click on the **Apply** button.

### SETUP SNMP TRAP

The SNMP Trap saves network resources through eliminating the need for unnecessary SNMP requests by providing notification of significant network events with unsolicited SNMP messages.

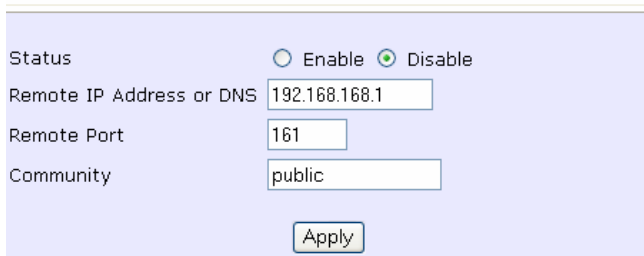
#### Step 1:

Select **SNMP Setup** from the **CONFIGURATION** menu.

#### Step 2:

1. Select whether to **Enable** or **Disable** the SNMP Trap.
2. Enter the **Remote IP Address or DNS**.
3. Enter the **Remote Port**.  
This is the port number of the SNMP manager.
4. Enter the **Community**.  
This is used to authenticate message, and is included in every packet that is transmitted between the SNMP manager and agent.
5. Click on the **Apply** button.

#### Snmpttrap Setup

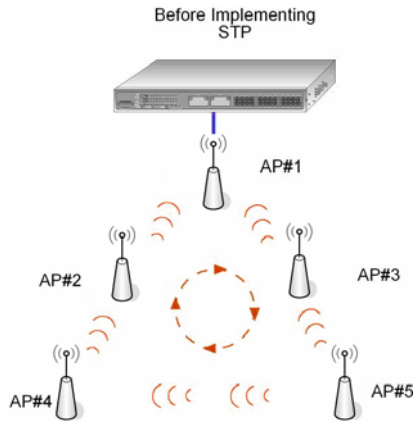


The screenshot shows a configuration window titled "Snmpttrap Setup" with a light blue background. It contains the following fields and controls:

- Status:** Two radio buttons, "Enable" (unselected) and "Disable" (selected).
- Remote IP Address or DNS:** A text input field containing "192.168.168.1".
- Remote Port:** A text input field containing "161".
- Community:** A text input field containing "public".
- Apply:** A button located at the bottom center of the form.

### STP SETUP (ONLY AVAILABLE IN ACCESS POINT, TRANSPARENT CLIENT AND REPEATER MODES)

Spanning Tree Protocol (STP) is a link management protocol that helps to prevent undesirable loops occurs in the network. For an Ethernet network to function properly, only one active path can exist between two stations. If a loop exists in the network topology, duplication of messages will occur and this might confuse the forwarding algorithm and allow duplicate frames to be forwarded.

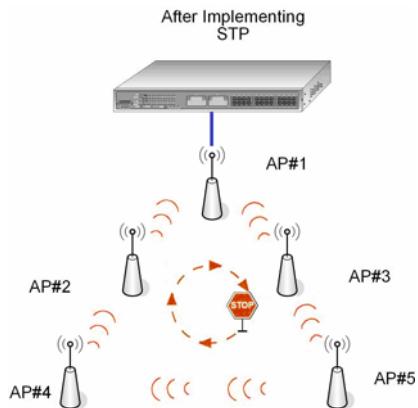


## Common Configuration

In short, the main purpose of activating STP is to prevent looping when you have redundant paths in the network. Without activating STP, redundant topology will cause broadcast storming.

To establish path redundancy, STP creates a tree that spans all of the devices in an extended network, forcing redundant paths into a standby, or blocked, state, but establishing the redundant links as a backup in case the active link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and re-establishes the connection by activating the standby path. Without spanning tree in place, it is possible that more than one connection may be simultaneously live, which could result in an endless loop of traffic on the LAN.

Spanning-Tree Protocol operation is transparent to end stations, which are unaware whether they are connected to a single LAN segment or a switched LAN of multiple segments.

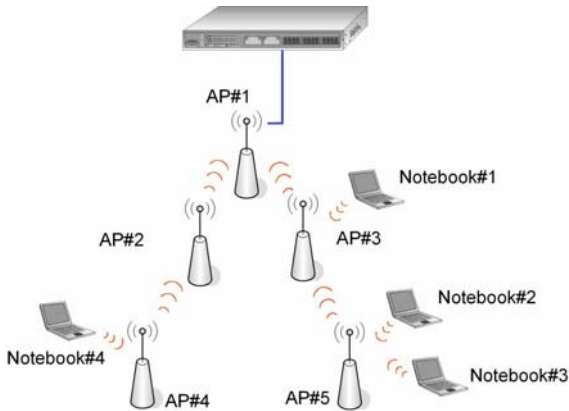


The path with the smallest cost will be used and extra redundant paths will be disabled.

## Common Configuration

### Scenario #1 – (No STP)

With no STP, all clients (Notebook#1, #2, #3, #4) can access one another, resulting in low data security. Due to the redundant paths, broadcast packets will be duplicated and forwarded endlessly, resulting in a broadcast storm.



### Scenario #2 – (With STP)

When STP is enabled, extra redundant network paths between APs will be disabled, hence preventing multiple active network paths in-between any two APs. If one of the APs is down, the STP algorithm will reactivate one of the redundant paths so that the network connection will not be lost. All wireless users will be able to communicate with each other if they are in the same WDS zone.



## Common Configuration

### Step 1:

Click on **STP Setup** from the **CONFIGURATION** menu

### Step 2:

Select the **STP Status Enable** radio button, fill in the fields, and click on the **Apply** button to update the changes.

Priority: (Default: 32768, Range: 0 – 65535)

This is the relative priority.

The lowest priority will be elected as the root.

Hello Time: (Default: 2, Range: 1 – 10)

This is the time interval in seconds whereby a hello packet is sent out. Hello packets are used to communicate information about the topology throughout the entire STP network.

Forward Delay: (Default: 15, Range: 4 – 30)

This is the time that is spent in the listening and learning state.

Max Age: (Default: 20, Range: 6 – 40)

The max age timer controls the maximum length of time that passes before a port saves its configuration information.

**Spanning Tree Protocol Setup**

STP Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
STP Designated Root	32768 00:80:40:3d:0f:80
Priority	<input type="text" value="32768"/> (32768:0-65535)
Hello Time	<input type="text" value="2"/> (2:1-10)
Forward Delay	<input type="text" value="15"/> (15:4-30)
Max Age	<input type="text" value="20"/> (20:6-40)

### USE MAC FILTERING

MAC Filtering acts as a security measure by restricting user network access according to MAC address. Each WLAN or radio card supports up to 16 virtual access points and has its own MAC address listing.



**NOTE**

MAC Filtering will not filter any MAC address from the Ethernet port.

---

# Common Configuration

## ADD A MAC ADDRESS TO THE MAC ADDRESS LIST

### Step 1:

Select **MAC Filtering** from **WLAN Setup**.  
The MAC Address Filtering page displays.

In this page you may also set the MAC Filtering Status to **Enable** or **Disable** for access points and set the Policy to either **Accept** or **Deny** MAC addresses.

<table border="1"><tr><th>Status</th><th>Policy</th></tr><tr><td>Enable</td><td>Accept</td></tr></table>	Status	Policy	Enable	Accept	MAC Filtering set to <b>Enable</b> with Policy to <b>Accept</b> only the MAC addresses in the MAC Filter Address List and deny all other MAC addresses.
Status	Policy				
Enable	Accept				

<table border="1"><tr><th>Status</th><th>Policy</th></tr><tr><td>Enable</td><td>Deny</td></tr></table>	Status	Policy	Enable	Deny	MAC Filtering set to <b>Enable</b> with Policy to <b>Deny</b> all the MAC addresses in the MAC Filter Address List and accept all other MAC addresses.
Status	Policy				
Enable	Deny				

<table border="1"><tr><th>Status</th><th>Policy</th></tr><tr><td>Disable</td><td>Accept</td></tr></table>	Status	Policy	Disable	Accept	MAC Filtering set to <b>Disable</b> . Whether Policy is set to <b>Enable</b> or <b>Deny</b> does not matter.
Status	Policy				
Disable	Accept				

<table border="1"><tr><th>Status</th><th>Policy</th></tr><tr><td>Disable</td><td>Deny</td></tr></table>	Status	Policy	Disable	Deny	MAC Filtering set to <b>Disable</b> . Whether Policy is set to <b>Enable</b> or <b>Deny</b> does not matter.
Status	Policy				
Disable	Deny				

Click the **Edit** button.

**MAC Address Filtering**

Radio 1 MAC Filtering Options :

AP Type	ESSID	Security	MACs	Status	Policy
Main AP	sampleRouter	NONE	<a href="#">Edit</a>	Enable	Accept
Virtual AP	VAP1	NONE	<a href="#">Edit</a>	Disable	Deny
Virtual AP	VAP2	NONE	<a href="#">Edit</a>	Enable	Deny

[View Complete MAC List](#)

*( All changes will take effect after reboot )*



## Common Configuration

### Step 2:

MAC Filter Address List page displays.  
Click the **Add** button.

MAC Filter Address List

MAC Address List  
ESSID: \*sampleRouter\*

Del.	MAC Address	Comments	Apply to
------	-------------	----------	----------

( All changes will take effect after reboot )

### Step 3:

The Add MAC Address page displays.

Add MAC Address

MAC Address  (xx-xx-xx-xx-xx-xx)

Comment

Apply to All

Selected	AP ESSID	Security
<input checked="" type="checkbox"/>	sampleRouter	NONE
<input type="checkbox"/>	VAP1	NONE
<input type="checkbox"/>	VAP2	NONE

### Step 4:

Enter the MAC Address of the client in the format **xx-xx-xx-xx-xx-xx**, where x can take any value from 0 to 9 or a to f.  
Enter the Comment. This describes the MAC Address you have entered.

To apply to all virtual access points, check **Apply to All**.  
To apply to specific virtual access point, select the checkbox of the corresponding access point.  
Click the **Apply** button.

Add MAC Address

MAC Address  (xx-xx-xx-xx-xx-xx)

Comment

Apply to All

Selected	AP ESSID	Security
<input checked="" type="checkbox"/>	sampleRouter	NONE
<input type="checkbox"/>	VAP1	NONE
<input type="checkbox"/>	VAP2	NONE

## Common Configuration

### Step 5:

MAC Filter Address List page displays with updated MAC Address List.

MAC Filter Address List

MAC Address List  
ESSID: \*sampleRouter\*

Del.	MAC Address	Comments	Apply to
<input type="checkbox"/>	08-70-f8-70-80-70	mac4	all

*( All changes will take effect after reboot. )*



### NOTE

Please reboot to effect all changes and new MAC address entries.

# Common Configuration

## DELETE A MAC ADDRESS FROM ALL ACCESS POINTS

### Step 1:

Select **MAC Filtering** from **WLAN Setup**.  
The MAC Address Filtering page displays.

Select **View Complete MAC List**.

AP Type	ESSID	Security	MACs	Status	Policy
Main AP	sampleRouter	NONE	<a href="#">Edit</a>	Enable	Accept
Virtual AP	VAP1	NONE	<a href="#">Edit</a>	Disable	Deny
Virtual AP	VAP2	NONE	<a href="#">Edit</a>	Enable	Deny

[View Complete MAC List](#)

*( All changes will take effect after reboot )*

### Step 2:

The MAC Filter Address List page displays.  
Select the checkbox of the MAC address you wish to delete.

Click the **Delete** button.

Del.	MAC Address	Comments	Apply to
<input type="checkbox"/>	<a href="#">08-70-f8-70-80-70</a>	mac1	all
<input checked="" type="checkbox"/>	<a href="#">00-b0-d0-86-bb-f7</a>	mac3	1 AP(s)

*( All changes will take effect after reboot )*

## Common Configuration

### Step 3:

The MAC Filter Address List page displays with updated MAC Address List.

**MAC Filter Address List**

MAC Address List  
Radio 1

Del.	MAC Address	Comments	Apply to
<input type="checkbox"/>	<a href="#">08-70-f8-70-80-70</a>	mac1	all

*( All changes will take effect after reboot )*

# Common Configuration

## DELETE A MAC ADDRESS FROM INDIVIDUAL ACCESS POINTS

### Step 1:

Select **MAC Filtering** from **WLAN Setup**.  
The MAC Address Filtering page displays.

Select **Edit** for the corresponding Access Point.

AP Type	ESSID	Security	MACs	Status	Policy
Main AP	sampleRouter	NONE	<a href="#">Edit</a>	Enable	Accept
Virtual AP	VAP1	NONE	<a href="#">Edit</a>	Disable	Deny
Virtual AP	VAP2	NONE	<a href="#">Edit</a>	Enable	Deny

[View Complete MAC List](#)

*( All changes will take effect after reboot )*

### Step 2:

The MAC Filter Address List page displays.  
Select the checkbox of the MAC address you wish to delete.

Click the **Delete** button.

Del.	MAC Address	Comments	Apply to
<input type="checkbox"/>	<a href="#">08-70-f8-70-80-70</a>	mac1	all
<input checked="" type="checkbox"/>	<a href="#">09-70-f8-70-80-70</a>	mac2	all
<input type="checkbox"/>	<a href="#">00-b0-d0-86-bb-f7</a>	mac3	1 AP(s)

*( All changes will take effect after reboot )*

## Common Configuration

### Step 3:

The MAC Filter Address List page displays with updated MAC Address List.

**MAC Filter Address List**

MAC Address List  
ESSID: "sampleRouter"

Del.	MAC Address	Comments	Apply to
<input type="checkbox"/>	<a href="#">08-70-f8-70-80-70</a>	mac1	all
<input type="checkbox"/>	<a href="#">00-b0-d0-86-bb-f7</a>	mac3	1 AP(s)

*( All changes will take effect after reboot )*

# Common Configuration

## EDIT MAC ADDRESS FROM THE MAC ADDRESS LIST

### Step 1:

Select **MAC Filtering** from **WLAN Setup**.  
The MAC Address Filtering page displays.

Select **Edit**.

AP Type	ESSID	Security	MACs	Status	Policy
Main AP	sampleRouter	NONE	<a href="#">Edit</a>	Enable	Accept
Virtual AP	VAP1	NONE	<a href="#">Edit</a>	Disable	Deny
Virtual AP	VAP2	NONE	<a href="#">Edit</a>	Enable	Deny

[View Complete MAC List](#)

( All changes will take effect after reboot )

### Step 2:

The MAC Filter Address List page displays.  
Select the MAC Address to edit.

Del.	MAC Address	Comments	Apply to
<input type="checkbox"/>	<a href="#">08-7U-fb-7U-8U-7U</a>	mac4	1 AP(s)

( All changes will take effect after reboot )

## Common Configuration

### Step 3:

The Edit MAC Address page displays.  
Edit the MAC address settings accordingly.

Click the **Save** button.

**Edit MAC Address**

MAC Address:  (XX-XX-XX-XX-XX-XX)  
Comment   
Apply to All

Selected	AP ESSID	Security
<input type="checkbox"/>	multipleSSID	NONE
<input checked="" type="checkbox"/>	APV1	NONE
<input type="checkbox"/>	APV2	NONE

### Step 4:

The MAC Filter Address List page displays with updated MAC Address List.

**MAC Filter Address List**

MAC Address List  
ESSID: "APV1"

Del.	MAC Address	Comments	Apply to
<input type="checkbox"/>	<u>08-70-f8-70-80-70</u>	mac4	all

*( All changes will take effect after reboot )*



# Chapter 5: Advanced Configuration

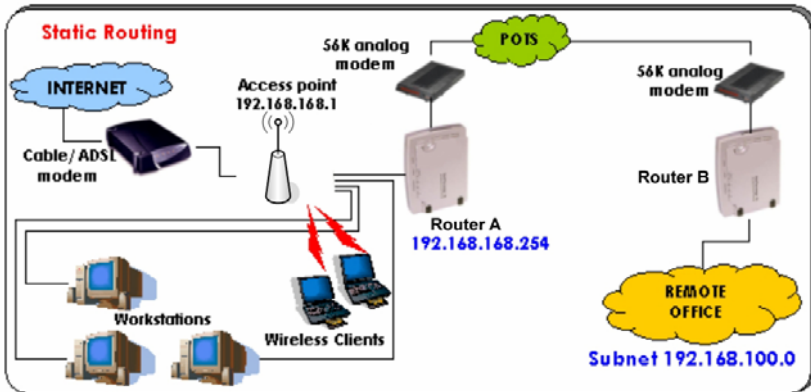
## SETUP ROUTING (ONLY SUPPORTED BY WIRELESS ROUTING CLIENT AND GATEWAY)

The access point allows the network administrator to add a static routing entry into its routing table so that the access point can re-route IP packets to another network access point. This feature is very useful for a network with more than one access point.



### Important:

You do NOT need to set any routing information if you are simply configuring the access point for broadband Internet sharing. Improper routing configuration will cause the access point to function improperly.



In this network, the main office of subnet 192.168.168.0 contains two routers: the office is connected to the Internet via the access point (192.168.168.1) and the remote office via Router A (192.168.168.254). The remote office resides on a subnet 192.168.100.0.

You can add a static routing entry into the access point routing tables so that IP packets from the clients in the main office with a destination IP address of 192.168.100.X (where X is any number from 2 to 254) will be re-routed to Router B, which acts as the gateway to that subnet.

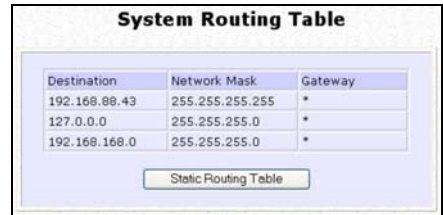
# Advanced Configuration

## CONFIGURE STATIC ROUTING

With an understanding of how adding a static routing entry can facilitate a network setup such as the one described above, here is how you may configure the access point:

### Step 1:

Under the **CONFIGURATION** command menu, click on **Routing** to be brought to the **System Routing Table** shown (on the right). Initially, the table will contain the default routing entries built into Access point.



**System Routing Table**

Destination	Network Mask	Gateway
192.168.88.43	255.255.255.255	*
127.0.0.0	255.255.255.0	*
192.168.168.0	255.255.255.0	*

Static Routing Table



**Static Routing Table**

Destination	Network Mask	Gateway
-------------	--------------	---------

Add Back

### Step 2:

Click on the **Static Routing Table** button, and then click the **Add** button.



**Static Routing Table**

Destination IP Address :

Destination Net Mask :

Gateway IP Address :

Add Cancel

### Step 3:

Enter the **Destination IP Address**, **Destination Net Mask**, and **Gateway IP Address** here. For this example, they are 192.168.100.0, 255.255.255.0 and 192.168.168.254 respectively. Hit the **Add** button to finish.



**Static Routing Table**

Destination	Network Mask	Gateway
192.168.100.0	255.255.255.0	192.168.168.254

Add Back

When the entry is added, it is reflected in the **Static Routing Table**.

# Advanced Configuration

## USING ROUTING INFORMATION PROTOCOL-RIP

(Available in Wireless Routing Client and Gateway modes)

RIP (Routing Information Protocol) allows information to be exchanged within a set of routers under the same administration.

RIPv1 bases the path used to pass traffic between routers on the fewest number of hops between the source and destination IP addresses within a packet. Routers broadcast RIPv1 information on all router interfaces every 30 seconds and process the information from other routers to determine if a better path is available. RIPv2 is more secure, and performs broadcasting and the assignment of IP address more efficiently.

### Step 1:

Under the **CONFIGURATION** command menu, click on **Routing** to be brought to **Route Information Protocol**.

#### Route Information Protocol



RIP Status  Enable  Disable  
RIP version

#### Route Information Protocol



RIP Status  Enable  Disable  
RIP version

### Step 2:

Select to Enable RIP Status.

Select either RIPv1 or RIPv2.

On this page, click the Apply button.

## Advanced Configuration

### NAT – NETWORK ADDRESS TRANSLATION (ONLY SUPPORTED BY WIRELESS ROUTING CLIENT AND GATEWAY)

The basic purpose of NAT is to share a single public IP address when there are multiple PCs in the private network by using different TCP ports to identify requests coming from different PCs. NAT is enabled by default.

Due to NAT, computers in the private LAN behind the access point will not be directly accessible from the Internet. However, employing virtual Servers lets you host Internet servers behind the NAT by way of IP/Port Forwarding as well as De-Militarized Zone hosting.

#### Step 1:

Under the **CONFIGURATION** command menu, click on **NAT**. NAT is enabled by default. To disable it, click **Disable**.



#### Step 2:

Click **Apply** to effect the setting.



#### Important:

Do NOT disable NAT unless absolutely necessary. Disabling NAT will disable broadband Internet sharing effectively.

## Advanced Configuration

---

### CONFIGURE VIRTUAL SERVERS BASED ON DE-MILITARIZED ZONE (DMZ) HOST

DMZ (De-Militarized Zone) makes specific PCs in a NAT-enabled network directly accessible from the Internet.

When NAT is enabled, an Internet request from a client within the private network first goes to the access point receiving a request, the access point keeps track of which client is using which port number. Since any reply from Internet goes to the access point first, the access point (from the port number in the reply packet) knows to which client to forward the reply. If the access point does not recognize the port number, it will discard the reply.

When using DMZ on a PC, any reply not recognized by the access point will be forwarded to the DMZ-enabled PC instead.



#### Step 1:

Under the **CONFIGURATION** command menu, click on **NAT**. You will find the **Advanced NAT Options** available near the bottom of the page.

#### Step 2:

Click the **DMZ** button to configure Virtual Servers based on De-Militarized Zone host.

## Advanced Configuration

### Step 3:

On the **NAT DMZ IP Address** page, you have to define the **Private IP Address** of the DMZ host. In this example, we keyed in the private IP address for the PC we wish to place within the DMZ : 192.168.168.55

(Enter **0.0.0.0** as the **Private IP Address** and it will disable DMZ).

Remember to click the **Apply** button.



**NAT DMZ IP Address**

Private IP Address : 192.168.168.55

Apply Back



### NOTE

1. When you enable DMZ, the Static IP Address configuration is recommended for the DMZ host. Otherwise, if the address is allocated by DHCP, it may change and DMZ will not function properly.
2. DMZ allows the host to expose ALL of its parts to the Internet. The DMZ host is thus susceptible to malicious attacks from the Internet.

## CONFIGURE VIRTUAL SERVERS BASED ON PORT FORWARDING

Virtual Server based on Port Forwarding is implemented to forward Internet requests arriving at the access point's WAN interface, based on their TCP ports, to specific PCs in the private network.



### Step 1:

Under the **CONFIGURATION** command menu, click on **NAT**. You will find the **Advanced NAT Options** available near the bottom of the page.

### Step 2:

Click the **Port Forwarding** button to configure Virtual Servers based on Port Forwarding.

### Step 3:

Hit the **Add** button on the **Port Forward Entries** page.



# Advanced Configuration

## Add Port Forward Entry

### Known Server

Server Type :

Private IP Address :

### Custom Server

Server Type :

Protocol :

Public Port :

From :

To :

Private IP Address :

Private Port From :

As an example, if you want to set up a web server on a PC with IP address of 192.168.168.55, select HTTP as **Server Type** and enter **192.168.168.55** as the **Private IP Address**. Click on the **Add** button. You will see the entry reflected as on the right.

## Step 4:

On the following **Add Port Forward Entry** screen, you can set up a Virtual Server for a **Known Server** type by selecting from a drop-down menu OR you can define a **Custom Server**.

## Port Forward Entries

Server Type	Protocol	Public Port	Private IP	Private Port
HTTP	TCP	80	192.168.168.55	80



## Advanced Configuration

### Known Server

- Server Type** : Select from the drop-down list of known server types: (HTTP, FTP, POP3 or Netmeeting).
- Private IP Address** : Specify the LAN IP address of your server PC running within the private network.
- Public IP From** : Select **All**, **Single**, or **Range** from the dropdown list.
- To** : Enter the beginning of the range.
- To** : Enter the end of the range.

### Custom Server


- Server Type** : Define a name for the server type you wish to configure.
- Protocol** : Select either **TCP** or **UDP** protocol type from the dropdown list.
- Public Port** : Select whether to define a single port or a range of public port numbers to accept.
- From** : Starting public port number.
- To** : Ending public port number. If the Public Port type is Single, this field will be ignored.
- Private IP Address** : Specify the IP address of your server PC running within the private network.
- Private Port From** : Starting private port number. The ending private port number will be calculated automatically according to the public port range.
- Public IP** : Select **All**, **Single**, or **Range** from the dropdown list.
- From** : Enter the beginning of the range.
- To** : Enter the end of the range.

## Advanced Configuration

### CONFIGURE VIRTUAL SERVERS BASED ON IP FORWARDING

When you have subscribed for more than one IP address from your ISP, you may define Virtual Servers based on IP Forwarding for which all Internet requests, regardless of ports, are forwarded to defined computers in the private network. Here are the steps to set it up:

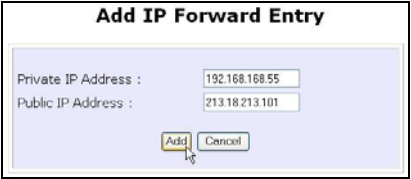
**Step 1:**  
Select **NAT** from the **CONFIGURATION** command menu.



The screenshot shows a window titled "Advanced NAT Options" with three buttons: "DMZ", "Port Forwarding", and "IP Forwarding". The "IP Forwarding" button is highlighted with a mouse cursor.

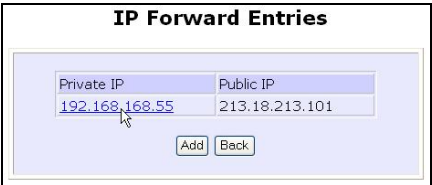
**Step 2:**  
Click the **IP Forwarding** button in Advanced NAT Options.

**Step 3:**  
In the **Add IP Forward Entry** page, enter the **Private IP Address** and **Public IP Address**. In this example, we would like all requests for 213.18.213.101 to be forwarded to a PC with **Private IP Address** 192.168.168.55.



The screenshot shows a form titled "Add IP Forward Entry". It has two input fields: "Private IP Address" with the value "192.168.168.55" and "Public IP Address" with the value "213.18.213.101". There are "Add" and "Cancel" buttons at the bottom.

**Step 4:**  
Click the **Add** button to continue.



The screenshot shows a table titled "IP Forward Entries". The table has two columns: "Private IP" and "Public IP". The "Private IP" column contains the value "192.168.168.55" and the "Public IP" column contains the value "213.18.213.101". There are "Add" and "Back" buttons below the table.

**Step 5:**  
The **IP Forward Entries** page will reflect your new addition.



#### NOTE

For step 3 above, please ensure that you have subscribed to the Public IP Address you intend to forward from.

### BANDWIDTH CONTROL (ONLY SUPPORTED BY WIRELESS ROUTING CLIENT AND GATEWAY)

The access point is designed to support simple bandwidth management that makes use of the **Bandwidth Control**. This feature gives the administrator the choice to manage the bandwidth control of subscribers in case of massive data transfer which causes slowdown problems when surfing the Internet.

#### TO ENABLE OR DISABLE BANDWIDTH CONTROL

Only two simple steps are required to enable or disable bandwidth control for the access point.

##### Step 1:

Under the **CONFIGURATION** command menu, click on **Bandwidth Control**.

**Enable/Disable Bandwidth Control**

Bandwidth Control Status :  Enable  Disable

Apply

**WAN Bandwidth Control Setup**

**Upload/Download Bandwidth Setting**

Download Total Rate(kbit) :

Upload Total Rate(kbit) :

Apply

**LAN Bandwidth Control Setup**

Name	Committed Rate (Kbit)	Cel Rate(Kbit)	IP/MAC Address	Rate type
------	-----------------------	----------------	----------------	-----------

##### Step 2:

By default, **Bandwidth Control** is disabled. Select **Enable**, followed by clicking the **Apply** button.

**Enable/Disable Bandwidth Control**

Bandwidth Control Status :  Enable  Disable

Apply

# Advanced Configuration

## TO CONFIGURE WAN BANDWIDTH CONTROL SETTING

The access point can allow you to limit the entire throughput by configuring the **Upload / Download Bandwidth Setting** option. These values should be set to a positive integer indicating the maximum number of kilobytes transferred per second that will be allowed. The value of zero means unlimited.

For example, if you configure the **Upload Total Rate** to be 640kb/sec (80KB/sec), then the access point will send out packets by this speed no matter how many clients/users are connected to it.

### Step 1:

Under the **CONFIGURATION** command menu, click on **Bandwidth Control** to select **WAN Bandwidth Control Setup**.

### Step 2:

The values for the **Download Total Rate** and **Upload Total Rate Bandwidth Control** are preset to zero. The value of zero indicates no limit and is the default. Key in the desired values, followed by clicking the **Apply** button.



The screenshot shows a web interface titled "WAN Bandwidth Control Setup". Under the heading "Upload/Download Bandwidth Setting", there are two input fields: "Download Total Rate(kbit):" and "Upload Total Rate(kbit):", both containing the value "0". Below these fields is an "Apply" button.

# Advanced Configuration

## TO CONFIGURE LAN BANDWIDTH CONTROL SETTING

The access point can allow you to limit the LAN user's throughput by configuring the **Bandwidth Control Rule**.

### Step 1:

Under the **CONFIGURATION** command menu, click on **Bandwidth Control** to select **LAN Bandwidth Control Setup**.

### Step 2:

Click **Add** to create the bandwidth rule for LAN user.



The screenshot shows the 'LAN Bandwidth Control Setup' window. It features a table with five columns: 'Name', 'Committed Rate (kbit)', 'Cell Rate(kbit)', 'IP/MAC Address', and 'Rule type'. Below the table is an 'Add' button.

Name	Committed Rate (kbit)	Cell Rate(kbit)	IP/MAC Address	Rule type
------	-----------------------	-----------------	----------------	-----------

### Step 3:

Click **Add** to create the rule for LAN user's bandwidth control.



The screenshot shows the 'Add Bandwidth Control Entry' window. It contains the following fields and controls:

- Bandwidth Control Rule**
- Rule Name :
- Committed Rate(kbit) :
- Cell Rate(kbit) :
- Rule type :  (dropdown menu)
- IP/MAC Address :
-

## Advanced Configuration

This table describes the parameters that can be modified in the **Add Bandwidth Control Entry** page.

Parameters	Description
<b>Rule Name</b>	The rule describes the type of bandwidth traffic to be controlled and of a specification of what action to take when that bandwidth traffic is encountered.
<b>Committed Rate (kbit)</b>	This is the minimum bandwidth rate at which a user can get the throughput.
<b>Ceiling Rate (kbit)</b>	This is the capped bandwidth rate to limit a user's throughput.
<b>Rule Type</b>	This is the type of rule depending on which IP or MAC address to use to download or upload a user's throughput.
<b>IP/MAC Address</b>	This is the type of address to be chosen depending on the rule type. For instance, if you may want to limit an entire machine address or a user by his router's MAC address, you can specify the MAC address using that field in the same way that you can limit by IP address.

### Step 4:

After you have completed the parameters, click **Add** so that the new rule is added in the entry list shown in **Step 1**. To add more new bandwidth rules, repeat Step 1 through 3.



#### NOTE

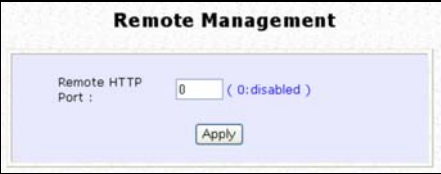
The sum of **Committed Rate** of the rules should never exceed the corresponding **Total Rate**.

### REMOTE MANAGEMENT (ONLY SUPPORTED BY WIRELESS ROUTING CLIENT AND GATEWAY)

The advanced network administrator will be delighted to know that remote management is supported on the access point. With this feature enabled, you will be able to access the access point's web-based configuration pages from anywhere on the Internet and manage your home/office network remotely.

#### TO SET UP REMOTE MANAGEMENT

Only two simple steps are required to set up remote management for the access point.



**Remote Management**

Remote HTTP Port :  ( 0: disabled )

Step 1:

Under the **CONFIGURATION** command menu, click on **Remote Management**, and you will be brought to the following screen.

Step 2:

By default, **Remote Management** is disabled. (To disable Remote Management, just enter 0 for **Remote Http Port**).

To enable **Remote Management**, enter a port number which is not being used by other applications in the network. Please take note that it is recommended to use a different port number other than port 80 because some ISP block port number 80.



#### NOTE

In view of preventing unauthorized management from a remote location, please remember to replace the default password with a new one.

You are also advised to change this password from time to time to guard against malicious attackers.

---

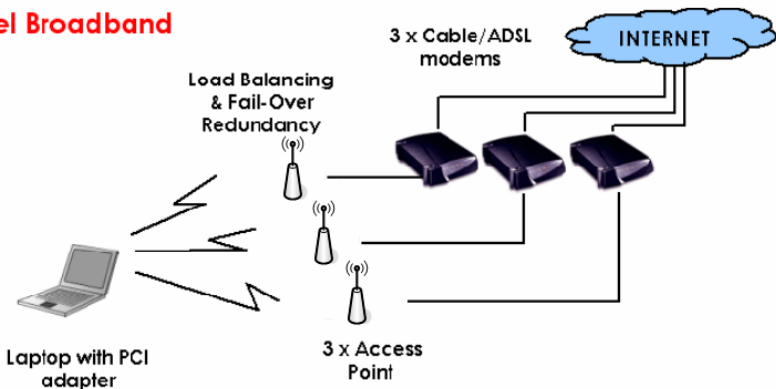
### PARALLEL BROADBAND (ONLY SUPPORTED BY GATEWAY MODE)

Parallel Broadband provides scalable Internet bandwidth with Load Balancing and Fail-Over Redundancy.

Load Balancing is provided by balancing the aggregate bandwidth of multiple broadband connections across the traffic demands of your private network. With Parallel Broadband, if a particular broadband connection fails, the access point will use the remaining functional broadband connections, thus providing Fail-Over Redundancy.

Implementing Parallel Broadband requires the installation of 2 or more access points in the network, each connected to separate broadband Internet service accounts. As there is no restriction to the type of broadband Internet they are connected to, be it cable or ADSL, you may thus have one access point connected to cable Internet, and another to an ADSL line. The access points have to be operating in Gateway mode with Parallel Broadband and set to the same ESSID.

#### Parallel Broadband





# Advanced Configuration

## ENABLE PARALLEL BROADBAND ON THE ACCESS POINT

Before you begin, ensure that each of the access point within the network is properly configured to connect to its individual broadband Internet account. Then ensure that either:

- each access point is connected to an Ethernet port in the network as illustrated above or
- Or
- the access points are wired to each other.

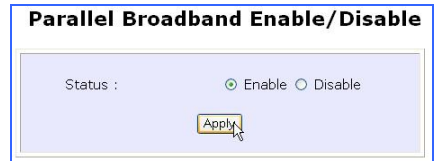
Finally, you are ready to access the web-based configuration of each of your access point to enable the Parallel Broadband feature. You will have to enable all the DHCP servers in all access points before enabling Parallel Broadband. Please note that you need to interconnect all access points

### Step 1:

Under the **CONFIGURATION** command menu, click on **Parallel Broadband**.

### Step 2:

Next simply select **Enable** and click the **Apply** button to make the changes effective.



### Step 3:

Repeat this for the other access points in your network

New users will then be assigned to the access point with the smallest load, ensuring that each access point has approximately the same number of users.



### Important:

If you have only one unit of the access point, you DO NOT need to implement the Parallel Broadband feature for broadband Internet sharing.

# Advanced Configuration

## EMAIL NOTIFICATION

The access point provides this feature to notify you by email when there is a change in the WAN IP address that was supplied to you earlier.

**WAN PPPoE Setup**

WAN Type : **PPPoE**

Username :

Password :

On-Demand    Idle Timeout (0:disabled)  seconds

Always-On    Reconnect Time Factor  seconds

Status : **Connecting**

IP Address  
Network Mask  
Default Gateway  
Primary DNS  
Secondary DNS

Step 1:

Under the **CONFIGURATION** command menu, click on **WAN PPPoE Setup** or **WAN PPTP Setup**, and you will be brought to the following screen.

Step 2:

Click on the **Email Notification** button.

**Email Notification**

Email Notification:  Enable  Disable

Email address of Receiver:

IP address of Mail Server :   Needs Authentication

User Name :

Password :

Email address of Sender:

Status :

Step 3:

Click on the **Enable** button and key in the following fields as described below:

## Advanced Configuration

---

- **Email address of Receiver:**

This is the email address of the receiver to whom the message would be sent.

- **IP address of Email Server:**

This is the IP address of the SMTP server through which the message would be sent out. (Take note that you are encouraged to use your ISP's SMTP server).

- **User Name:**

This is the mail account user's name that should be entered if authentication is required.

- **Password:**

This is the mail account user's password that should be entered if authentication is required.

- **Email address of Sender:**

This is the email address of the sender from whom the message will appear to come.

### Step 4:

By default, the checkbox next to **Needs Authentication** is not ticked. This option allows you to specify whether the SMTP server requires authentication.

### Step 5:

Then click on the **Apply** button.

### STATIC ADDRESS TRANSLATION (ONLY SUPPORTED BY WIRELESS ROUTING CLIENT AND GATEWAY)

If you use a notebook for work in the office, you most probably bring it home to connect to the Internet as well. Since it is most likely that your office network and home network broadband-sharing network subnets are configured differently, you would have the hassle of reconfiguring your TCP/IP settings every time you use the notebook in a different place. Static Address Translation allows you to bypass this hassle.

With SAT, if you try to access the Internet on your notebook from home but with your office TCP/IP settings, the notebook will try to contact the IP address of your office gateway to the Internet. When the access point finds that the notebook is trying to contact a device lying on a different subnet from that of the home network, it would inform the notebook that the gateway to the Internet is in fact the access point itself. From then the notebook would contact the access point for access to the Internet without any change to the TCP/IP settings.



#### NOTE

For SAT to function properly:

1. The IP address of the notebook should belong to a different subnet from the LAN IP address of your access point.

The <Default Gateway> in the TCP/IP settings of your notebook should NOT be left blank.

#### Step 1:

Under the **Home User Features** command menu, click on **Static Address Translation**.

#### Step 2:

You may then choose to **Enable** or **Disable** Static Address Translation here, followed by clicking the **Apply** button. (Note: SAT is disabled by default)



### **DNS REDIRECTION (ONLY SUPPORTED BY WIRELESS ROUTING CLIENT AND GATEWAY)**

When you enter a URL in your Internet browser, the browser requests for a name-to-IP address translation from the Domain Name System (DNS) servers to be able to locate the web server

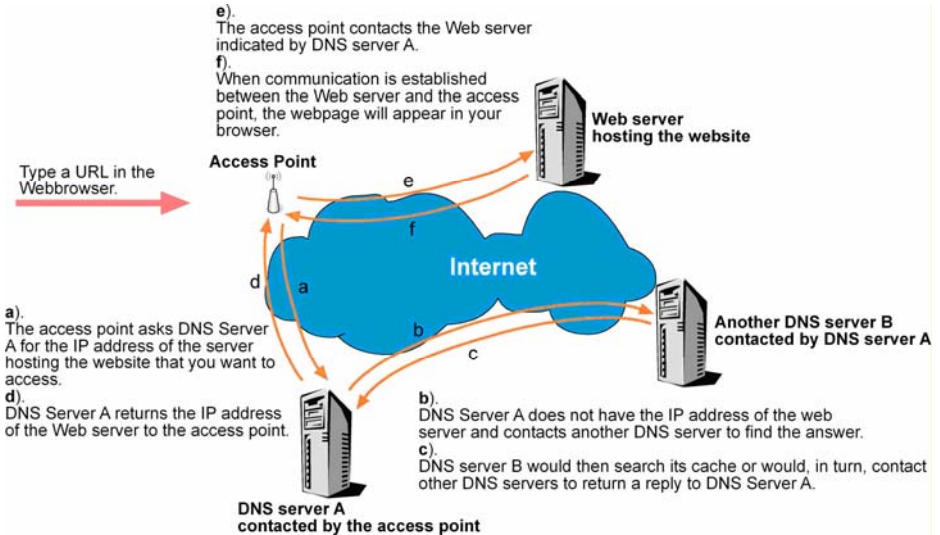
The DNS server, in turn, looks for the answer in its local cache and if an appropriate entry is found, sends back this cached IP address to the browser. Otherwise, it would have to contact other DNS servers until the query can be resolved.

When you enable the DNS Redirection feature, DNS requests from the LAN clients will be processed by Access point. Unless in the access point's LAN Setup you have already assigned a specific DNS server which should always be used, the access point would contact the DNS server allocated by your ISP to resolve DNS requests.

When DNS Redirection is enabled, the DNS server used by the access point would override the one defined in the TCP/IP settings of the LAN clients. This allows the access point to direct DNS requests from the LAN to a local or to a closer DNS server it knows of, thus improving response time.

DNS Redirection also provides more control to the network administrator. In the event that there is a change in DNS servers, he can simply indicate the actual DNS server IP address in the access point LAN Setup and enable DNS Redirection, without having to reconfigure the DNS settings of every LAN client.

# Advanced Configuration



## NOTE

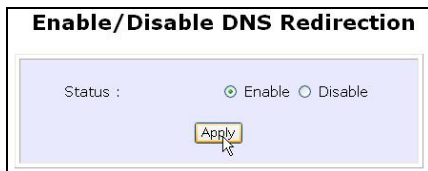
An entry for the DNS Server field in the PC TCP/IP Properties is required for Internet access.

If the exact DNS IP address is unavailable, simple key in any valid IP address, for example: 10.10.10.10

## TO ENABLE/DISABLE DNS REDIRECTION

### Step 1:

Under the **Home User Features** command menu, click on **DNS Redirection**.



### Step 2:

Simply choose **Enable** or **Disable** for the **Status** of **DNS Redirection**.

### Step 3:

Complete the setup by clicking the **Apply** button.

## Advanced Configuration

### DYNAMIC DNS SETUP

It is difficult to remember the IP addresses used by computers to communicate on the Internet. It gets even more complicated when ISPs change your public IP address regularly, as is the case when the Internet connection type is Dynamic IP or PPPoE with Dynamic IP.

If you are doing some web hosting on your computer and are using Dynamic IP, Internet users would have to keep up with the changing IP address before being able to access your computer.

When you sign up for an account with a Dynamic Domain Name Service (DDNS) provider, the latter will register your unchanging domain name, e.g. **MyName.Domain.com**. You can configure your access point to automatically contact your DDNS provider whenever the access point detects that its public IP address has changed. The access point would then log on to your account and update it with its latest public IP address.

If a user enters your address: **MyName.Domain.com** into their web browser, this request would go to the DDNS provider which will then redirect the request to your computer, regardless of the IP address it is currently assigned by your ISP.

### TO ENABLE/DISABLE DYNAMIC DNS SETUP

#### Step 1:

Under the **Home User Features** command menu, click on **Dynamic DNS Setup**.



#### Step 2:

You may then choose to **Enable** or **Disable** Dynamic DNS here, followed by clicking the **Apply** button. (Note: Dynamic DNS is disabled by default)



## Advanced Configuration


### TO MANAGE DYNAMIC DNS LIST (DDNS)

#### Step 1:

Under the **Home User Features** command menu, click on **Dynamic DNS Setup**.

#### Step 2:

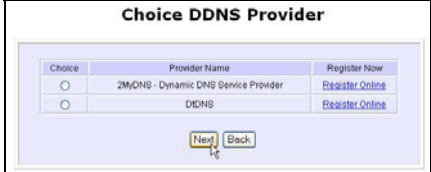
If you have already created a list earlier, click on the **Refresh** button to update the list.



The screenshot shows a web interface titled "Dynamic DNS List". It features two input fields: "Domain Name" and "Update Status". Below these fields are two buttons: "Add" and "Refresh".

#### Step 3:

To add a new Dynamic DNS to the list, click on the Add button and you will see the **Choice DDNS Provider** page appear. There are two default providers which you can use. The following parameters are explained below:



The screenshot shows a web interface titled "Choice DDNS Provider". It contains a table with two columns: "Choice" and "Provider Name". There are two rows of providers. The first row is "2M/DNS - Dynamic DNS Service Provider" and the second is "DIDNS". Each row has a radio button in the "Choice" column and a "Register Now" link in the "Provider Name" column. Below the table are "Next" and "Back" buttons.

Choice	Provider Name	Register Now
<input type="radio"/>	2M/DNS - Dynamic DNS Service Provider	<a href="#">Register Online</a>
<input type="radio"/>	DIDNS	<a href="#">Register Online</a>

- **Choice :**

This allows you to check the radio button of your preferred DDNS provider.

- **Provider Name :**

This is the name of your preferred DDNS provider.

- **Register Now :**

This allows you to go to the website of your preferred DDNS provider where you can register your account.



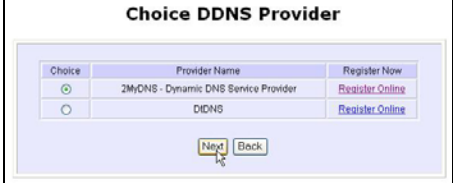
## Advanced Configuration

There are two DDNS providers that are pre-defined for you. Please note that you need to be connected to the Internet to register your DDNS account.

To select **2MyDNS – Dynamic DNS Service Provider** as DDNS Service Provider

### Step 1:

Under the **Choice** column in the **Choice DDNS Provider** check the radio button next to the **2MyDNS – Dynamic DNS Service Provider**. Then click on the **Next** button to proceed.



Choice	Provider Name	Register Now
<input checked="" type="radio"/>	2MyDNS - Dynamic DNS Service Provider	<a href="#">Register Online</a>
<input type="radio"/>	DIDNS	<a href="#">Register Online</a>

### Step 2:


Enter your **Domain Name**.

### Step 3:

The **Auto Detect** checkbox is selected by default. The **WAN IP** entry box is blank by default. These default settings should be applied if the dynamic WAN IP connection is used.

For instance,

If your ISP connection service uses the dynamic WAN IP, tick the **Auto Detect** checkbox to let the DDNS server learn your current WAN IP address. Enter your DDNS account **Username** and **Password**.



Provider: **2MyDNS - Dynamic DNS Service Provider**

Domain Name:  .2mydns.net

WAN IP:   Auto Detect

Username:

Password:

Wildcard:  YES  NO

Mail Exchanger:

Backup Mail Exchanger:  YES  NO

However, if you are using a fixed WAN IP connection, enter the IP address in the **WAN IP** field. Then, un-tick the **Auto Detect** checkbox. Then the access point will update the DDNS server using that WAN IP entered in its field.

## Advanced Configuration

### Step 4:

(Optional) If you enable the wildcard service, your hostname would be allowed multiple identities.

For example, if you register:

**mydomain.2mydns.net**, users looking

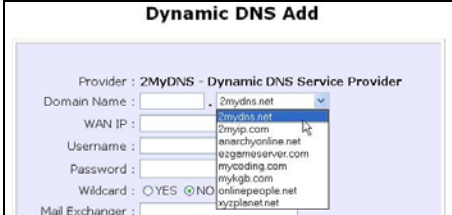
for [www.mydomain.2mydns.net](http://www.mydomain.2mydns.net) or

[ftp.mydomain.2mydns.net](http://ftp.mydomain.2mydns.net) can still

reach your hostname.

### Step 5:

(Optional) In the Mail Exchanger field, enter the Static WAN IP address of the mail server configured to handle email for your domain. Select **Backup Mail Exchanger** to enable this service.



**Dynamic DNS Add**

Provider : 2MyDNS - Dynamic DNS Service Provider

Domain Name :

WAN IP :

Username :

Password :

Wildcard :  YES  NO

Mail Exchanger :

The screenshot shows a web form titled "Dynamic DNS Add". It has several input fields: "Domain Name" with a dropdown menu showing "2mydns.net", "WAN IP" with "2mydns.net", "Username" with "anarchyonline.net", "Password" with "mycoding.com", "Wildcard" with radio buttons for "YES" and "NO" (where "NO" is selected), and "Mail Exchanger" with "onlinepeople.net".

### Step 6:

Click on the Add button to save the new addition.

### Step 7:

The new domain is added to the Dynamic DNS list table.



**Dynamic DNS List**


Domain Name	Update Status
<a href="#">Mr Codina.mrcodina.com</a>	
<a href="#">people.onlinepeople.net</a>	

The screenshot shows a web page titled "Dynamic DNS List". It contains a table with two columns: "Domain Name" and "Update Status". There are two rows of data: "Mr Codina.mrcodina.com" and "people.onlinepeople.net". Below the table are two buttons: "Add" and "Refresh".

## Advanced Configuration

### Step 8:

It will appear as a hyperlink which you can click to go back to the Dynamic DNS Edit page. From this page, you can update any of the parameters, delete the domain name or reset all parameters to be blank again.



**Dynamic DNS Edit**

Provider : 2MyDNS - Dynamic DNS Service Provider  
Domain Name : **people . onlinepeople.net**

WAN IP :   Auto Detect

Username :

Password :

Wildcard :  YES  NO

Mail Exchanger :

Backup Mail Exchanger :  YES  NO

## Advanced Configuration

Select **DtDNS** as DDNS Service Provider

### Step 1:

Under the **Choice** column in the table of **Choice DDNS Provider** check the radio button next to the **DtDNS**. Then click on the **Next** button to proceed.

Choice	Provider Name	Register Now
<input type="radio"/>	2MyDNS - Dynamic DNS Service Provider	<a href="#">Register Now</a>
<input checked="" type="radio"/>	DtDNS	<a href="#">Register Now</a>

### Step 2:

Enter your **Domain Name**.

### Step 3:

The **Auto Detect** checkbox is ticked by default. The **WAN IP** entry box is blank by default. These default settings should be applied if the dynamic WAN IP connection is used.

Provider : DtDNS  
Domain Name :  3d-igame.com  
WAN IP :   Auto Detect  
Password :

For instance,

If your ISP connection service uses the dynamic WAN IP, tick the **Auto Detect** checkbox to let the DtDNS server learn your current WAN IP address. Enter your DtDNS account **Username** and **Password**.

However, if you are using a fixed WAN IP connection, enter the IP address in the **WAN IP** field. Then, un-tick the **Auto Detect** checkbox. Then the access point will update the DtDNS server using that WAN IP entered in its field.

## Advanced Configuration

### Step 4:

Then click on the **Add** button.

### Step 5:

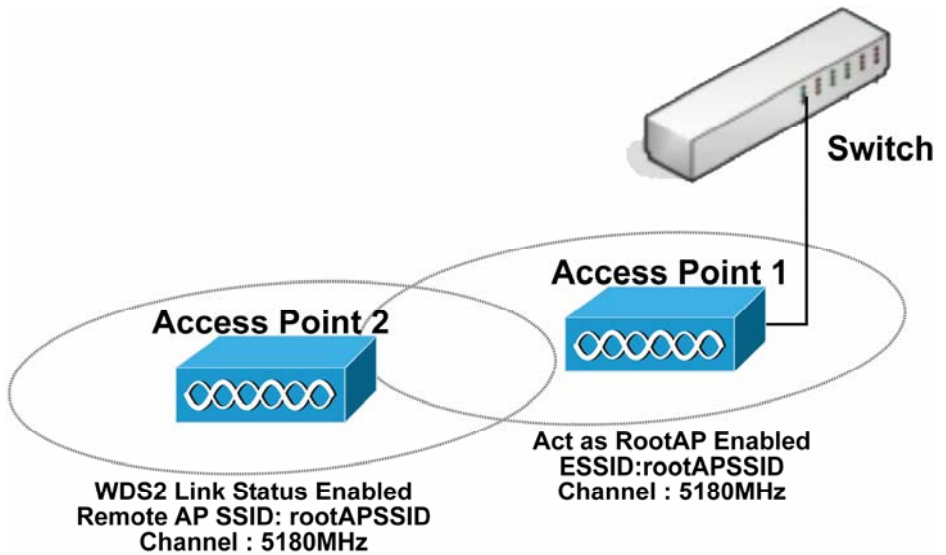
In our example, while the new domain name, **cool.3d-game.com** is being added to the list, the message 'Waiting in queue...' will be displayed under the **Update Status** column of the **Dynamic DNS List** table.



# Chapter 6: Wireless Extended Features

## SETUP WDS2

WDS2 (Wireless Distributed System 2) links up access points to create a wider network in which mobile users can roam while still staying connected to available network resources. The wireless client and root access point has to be set up with the same channel frequency. This allows them to connect even when the link is lost, as the channel frequency setting is preserved.



In this example, there are 2 access points: Access Point 1 and Access Point 2, with Access Point 1 as the root access point.

# Wireless Extended Features

Follow these steps to change the setup of the root access point.

Setup access point 1:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Basic**.

Ensure that **The Current Mode** is set to **Access Point**.

To change **The Current Mode**, please refer to: Common Configuration – WLAN Setup - To Configure the Basic Setup of the Wireless Mode.

Select **Act as RootAP**.

Select the **Channel** common to both access point 1 and access point 2.

## WLAN Basic Setup

Card Status	enable
The Current Mode	Access Point <input type="button" value="Change"/>
ESSID	<input type="text" value="rootAPSSID"/>
Wireless Profile	802.11a <input type="button" value="v"/>
Country	NO_COUNTRY_SET-(NA) <input type="button" value="v"/>
Channel	5805MHz (Channel 161) <input type="button" value="v"/> <input type="button" value="Channel Survey"/>
Tx Rate	Fully Auto <input type="button" value="v"/>
Maximum Associations	<input type="text" value="32"/> (32: 1-128)
	<input type="checkbox"/> Closed System
	<input checked="" type="checkbox"/> Act as RootAP
	<input type="checkbox"/> VLANID <input type="text"/>
	<input type="button" value="Apply"/>

## Wireless Extended Features

Follow these settings to setup access point 2.

Setup access point 2:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Basic**.

Select the **Channel** common to both access point 1 and access point 2.

### WLAN Basic Setup

Card Status	<b>enable</b>	
The Current Mode	<b>Access Point</b>	<input type="button" value="Change"/>
ESSID	<input type="text" value="accesspoint2"/>	
Wireless Profile	<input type="text" value="802.11a"/>	
Country	<input type="text" value="NO_COUNTRY_SET-(NA)"/>	
Channel	<input type="text" value="5805MHz (Channel 161)"/>	<input type="button" value="Channel Survey"/>
Tx Rate	<input type="text" value="Fully Auto"/>	
Maximum Associations	<input type="text" value="32"/> (32: 1-128)	
	<input type="checkbox"/> Closed System	
	<input type="checkbox"/> Act as RootAP	
	<input type="checkbox"/> VLANID <input type="text"/>	
		<input type="button" value="Apply"/>



# Wireless Extended Features

Configure WDS2 link:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menu expanded under **WLAN Setup**. Click on **Advanced**.

## Extended Features

Long Distance Parameters

WMM Settings

WDS2 Settings

Under **Extended Features**, click on the **WDS2 Settings** button. Set **WDS2 Link Status** to **Enable**.

Options for configuring WDS2 link:

- By Remote AP MAC – Enter the Remote AP MAC

### WDS2 Link Configuration

WDS2 Link Status:	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Remote AP SSID:	<input type="text" value="default"/>	
Remote AP MAC:	<input type="text" value="08:00:69:02:01:FC"/>	<input checked="" type="checkbox"/>
Cur. Security Mode:	NONE	

Apply

OR

- By Remote AP SSID – Uncheck the Remote AP MAC checkbox and enter the Remote AP SSID

### WDS2 Link Configuration

WDS2 Link Status:	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Remote AP SSID:	<input type="text" value="RootAPSSID"/>	
Remote AP MAC:	<input type="text" value="08:00:69:02:01:FC"/>	<input type="checkbox"/>
Cur. Security Mode:	NONE	

Apply

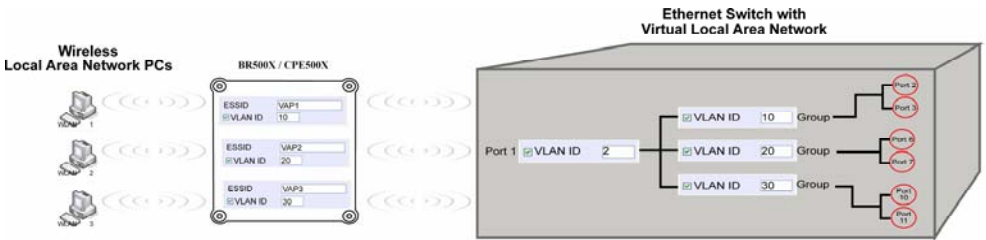
Click **Apply**.

# Wireless Extended Features

## SET VIRTUAL AP (MULTIPLE SSID)

Virtual AP implements mSSID (Multi-SSID) whereby a single wireless card can be setup with up to 16 virtual AP connections with different SSIDs or BSSID (Basic Service Set Identifier) and security modes.

Virtual AP delivers multiple services by VLAN segmentation: making the network think there are many SSIDs available and channeling each connection through different VLANs to the respective virtual network segments on the Ethernet network.



### How it Works

When WLAN PC 1 connects to VAP 1 its packets are channeled to VLAN 10 group where only services connected to Port 2 and Port 3 are available to this wireless connection.

It is similar for WLAN PC 2 and WLAN PC 3. Although they connect to the same radio card as WLAN PC 1, WLAN PC 2 can only access the services available at Port 6 and Port 7 and WLAN PC 3 can only access the services available at Port 10 and Port 11.

For more information on Virtual AP (Multiple SSID) please refer to Appendix: Virtual AP (Multiple SSID) FAQ.

# Wireless Extended Features

Follow these steps to setup Virtual AP.

## Virtual AP

### Step 1:

Click on **WLAN Setup** from the **CONFIGURATION** menu.  
Select **Virtual AP**.

### Step 2:

Virtual AP List page displays.

Virtual AP List

En	ESSID	BSSID	Statistics	Security	
<input checked="" type="checkbox"/>	Main	XX-XX-XX-XX-XX-XX	<a href="#">View</a>	NONE	<a href="#">Delete</a>
<input checked="" type="checkbox"/>	Sub	XX-XX-XX-XX-XX-XX	<a href="#">View</a>	NONE	<a href="#">Delete</a>

*( All changes will take effect after reboot )*

- Click **Apply** to register changes.
- Click **Clear** to clear Virtual AP List.
- Click **Back** to return to WLAN Basic Setup page.
- Select the **Delete** option beside any Virtual APs you wish to delete.

Click **Add** to goto add Virtual AP page.

## Virtual AP

ESSID	<input type="text" value="samplevirtualAP"/>
Max Associations	<input type="text" value="32"/> (32:1-128)
<input checked="" type="checkbox"/> VLAN ID	<input type="text" value="1"/>
<input checked="" type="checkbox"/> Closed System	
<input checked="" type="checkbox"/> RootAP	
Security Mode:	<input type="text" value="NONE"/> ▼
<input type="button" value="Apply"/> <input type="button" value="Back"/>	

### Step 3:

1. Enter ESSID name.
2. Settings:
  - VLAN ID
  - Closed System
  - RootAP
3. Select Security Mode.
4. Click **Apply** to make changes or click **Back** to return to Virtual AP List page.

## SET PREFERRED APs (AVAILABLE IN CLIENT MODE)

When there is more than one AP with the same SSID, the Preferred APs function allows you define the MAC address of the APs in order of preference.

The MAC address at the top of the Preferred APs list has the highest connection preference, and the MAC address at the bottom has the lowest connection preference.

Follow these steps to specify your preferred APs.

### Preferred APs

**Step 1:**

1. Click on **WLAN Setup** from the **CONFIGURATION** menu.
2. Select Preferred APs.

**Step 2:**

1. Enter the MAC addresses of the preferred APs.
2. Click Apply to effect the settings.

**Preferred Access Point MAC Address**

Access Point 1	<input type="text" value="09:10:4A:B9:E2:A4"/>	(XX:XX:XX:XX:XX:XX)
Access Point 2	<input type="text" value="08:00:07:A9:2B:FC"/>	(XX:XX:XX:XX:XX:XX)
Access Point 3	<input type="text"/>	(XX:XX:XX:XX:XX:XX)
Access Point 4	<input type="text"/>	(XX:XX:XX:XX:XX:XX)

# Wireless Extended Features

## LONG DISTANCE PARAMETERS

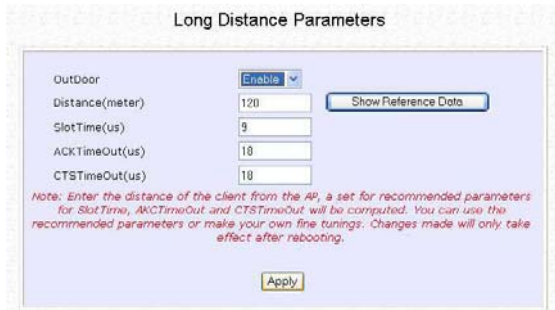
The access point can calculate and display suggested values for certain parameters to use to ensure that efficient wireless communication between physically distant access points.

Select **Advanced** from **WLAN Setup** under **Configuration**.

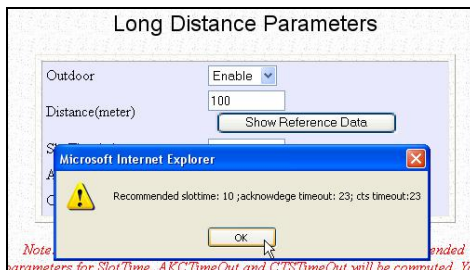
Click on the **Long Distance Parameters** button under the **Extended Features** section.



Select to **Enable** the **Outdoor** function.



The access point can automatically calculate the values of the parameters to input based on the distance between your access point and the other wireless device. Enter the distance in meters and click on the **Show Reference Data** button.



You can enter the parameters based on the recommended values in the popup window, click on the **Apply** button to update the changes.

## Wireless Extended Features

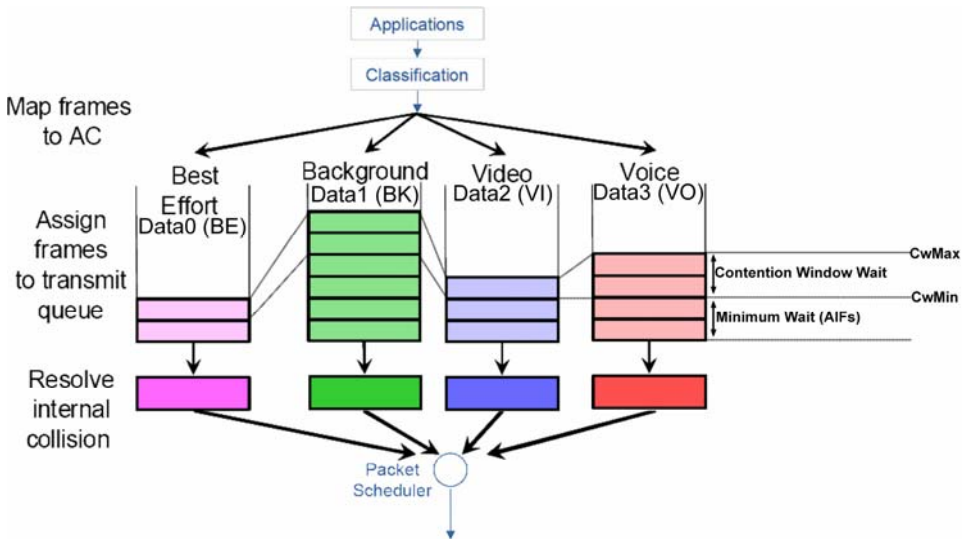
---

This table describes the parameters that can be modified in the **Long Distance Parameters** page.

Parameters	Description
<b>Outdoor</b>	The Outdoor parameter is disabled by default. If set to Enable, the Outdoor parameters will be configured for outdoor communication over short or long distances as specified.
<b>Distance</b>	This parameter determines the distance between your access point and the remote access point. It should be entered in meters.
<b>Slot Time</b>	Time is slotted and each unit of time is called one slot time.
<b>ACK Timeout</b>	This parameter determines the timeout allowed for the sending client to receive the acknowledgment response from the receiving client. If no acknowledgment packet is received within this period, the sender will assume the receiver has not received the packet and will attempt to re-send.
<b>CTS Timeout</b>	This Clear-to-Send time is the time the wireless sender will wait for a CTS packet signaling that the channel is idle and it can start data transmission. If no CTS packet is received within this period, the sender will assume the channel is busy and will wait before trying to send again.

## SET WIRELESS MULTIMEDIA

Wireless Multimedia (WMM) is a QoS (Quality of Service) standard in IEEE802.11E that we have adopted to improve and support the user experience for multimedia, video, and voice applications by prioritizing data traffic. QoS can be realized through 4 different Access Categories (AC). Each AC type consists of an independent transmit queue, and a channel access function with its own parameters.



# Wireless Extended Features

Follow these steps to change the setup Wireless Multimedia on your access point.

## Step 1:

1. Click on **WLAN Setup** from the **CONFIGURATION** menu.
2. Select Advanced.

## Step 2:

Click on the **WMM Settings** button.



## Step 3:

Select to Enable **Wireless Multimedia (WMM)**

Enter the desired WMM parameters. Using the default parameters is recommended.

Click **Apply** to apply the WMM settings, click **Default** to reset all parameters to default, or click **Back** to discard any changes and return to WLAN Basic Setup page.

Wireless Multimedia (WMM)  Enable  Disable

AP WMM Parameters:

	AIFs	cwMin	cwMax	TxOp limit	NoAck
Data0 (BE)	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="63"/>	<input type="text" value="0"/>	<input type="checkbox"/>
Data1 (BK)	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>
Data2 (VI)	<input type="text" value="1"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="3008"/>	<input type="checkbox"/>
Data3 (VO)	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="1504"/>	<input type="checkbox"/>

Station WMM Parameters:

	AIFs	cwMin	cwMax	TxOp limit	ACM
Data0 (BE)	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>
Data1 (BK)	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>
Data2 (VI)	<input type="text" value="2"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="3008"/>	<input type="checkbox"/>
Data3 (VO)	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="1504"/>	<input type="checkbox"/>

*( All changes will take effect after reboot )*



## Wireless Extended Features

<b>WMM Parameters (for advanced users)</b>	
<b>AIFs (Arbitrary Inter-Frame Spacce)</b>	Arbitrary Inter-Frame Space is the minimum wait time interval between the wireless medium becoming idle and the start of transmission of a frame over the network.
<b>Cwmin (Contention Window Minimum)</b>	Contention Window Minimum is the minimum random wait time drawn from this interval or window for the backoff mechanism on the network.
<b>CwMax (Contention Window Maximum)</b>	Contention Window Maximum is the maximum random wait time drawn from this interval or window for the backoff mechanism on the network.
<b>TxOP limit (Transmit Opportunity Limit)</b>	Transmit Opportunity limit specifies the minimum duration that an end-user device can transmit data traffic after obtaining a transmit opportunity. TxOp limit can be used to give data traffic longer and shorter access.
<b>NoAck (No Acknowledgement)</b>	No Acknowledgement provides control of the reliability of traffic flow. Usually an acknowledge packet is returned for every packet received, increasing traffic load and decreasing performance. Enabling No Acknowledgement cancels the acknowledgement. This is useful for data traffic where speed of transmission is important.
<b>ACM (Admission Control Mandatory)</b>	Admission Control Mandatory enables WMM on the radio interface. When ACM is enabled, associated clients must complete the WMM admission control procedure before access.
<b>BE (Best Effort)</b>	Parameters for Data0 Best Effort. Best Effort data traffic has no prioritization and applications equally share available bandwidth.

## Wireless Extended Features

---

<b>BK (Background)</b>	Parameters for Data1 Background. Background data traffic is de-prioritized and is mostly for backup applications, or background transfers like backup applications or background transfers like bulk copies that do not impact ongoing traffic like Internet downloads.
<b>VI (Video)</b>	Parameters for video data traffic.
<b>VO (Voice)</b>	Parameters for voice data traffic.

## SETUP POINT-TO-POINT & POINT-TO-MULTIPOINT CONNECTION

You can implement Point-to-Point connection by simply setting one access point as RootAP in Access Point mode and setting the other access points to Transparent Client mode.

You can set a root access point and a transparent client to allow point-to-point communication between different buildings and enable you to bridge wireless clients that are kilometres apart while unifying the networks. Or you can set a root access point and multiple transparent clients to allow point-to-multiple-point communication between the access point located at a facility and several other access points installed in any direction from that facility.

### Follow these steps to setup RootAP

#### RootAP Step 1:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**.

Click on **Basic**.

Ensure that **The Current Mode** is set to **Access Point**.

To change **The Current Mode**, please refer to: Common Configuration - WLAN Setup - To Configure the Basic Setup of the Wireless Mode.

#### WLAN Basic Setup

Card Status	enable
The Current Mode	Access Point <input type="button" value="Change"/>
ESSID	sampleRouter
Wireless Profile	802.11a
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect <input type="button" value="Channel Survey"/>
Tx Rate	Fully Auto
Maximum Associations	32 (32:1-128)
	<input type="checkbox"/> Closed System
	<input type="checkbox"/> Act as RootAP
	<input type="checkbox"/> VLANID <input type="text"/>
	<input type="button" value="Apply"/>

## Wireless Extended Features

### RootAP Step 2:

Select **Act as RootAP**, click on the **Apply** button and reboot your device to let your changes take effect.

**WLAN Basic Setup**

Card Status	enable
The Current Mode	Access Point <input type="button" value="Change"/>
ESSID	<input type="text" value="sampleRouter"/>
Wireless Profile	802.11a <input type="button" value="v"/>
Country	NO_COUNTRY_SET-(NA) <input type="button" value="v"/>
Channel	SmartSelect <input type="button" value="v"/> <input type="button" value="Channel Survey"/>
Tx Rate	Fully Auto <input type="button" value="v"/>
Maximum Associations	<input type="text" value="32"/> (32: 1-128)
	<input type="checkbox"/> Closed System
	<input checked="" type="checkbox"/> Act as RootAP
	<input type="checkbox"/> VLANID <input type="text"/>
	<input type="button" value="Apply"/>

# Wireless Extended Features

Follow these steps to setup Transparent Client/s.

## Transparent Client Step 1:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**.  
Click on **Basic**.

Ensure that **The Current Mode** is set to **Transparent Client**.

To change **The Current Mode**, please refer to: Common Configuration – WLAN Setup - To Configure the Basic Setup of the Wireless Mode.

**WLAN Basic Setup**

Card Status	enable
The Current Mode	Transparent Client <input type="button" value="Change"/>
ESSID	sampleRouter <input type="button" value="Site Survey"/>
Remote AP MAC	00:00:00:00:00:00 <input type="checkbox"/>
Wireless Profile	802.11a
Country	NO_COUNTRY_SET-(NA)
Tx Rate	Fully Auto
<input type="button" value="Apply"/>	

## Transparent Client Step 2:

Select the **Remote AP MAC** checkbox.

Enter the **Remote AP MAC**.

**WLAN Basic Setup**

Card Status	enable
The Current Mode	Transparent Client <input type="button" value="Change"/>
ESSID	sampleRouter <input type="button" value="Site Survey"/>
Remote AP MAC	09:00:2B:23:00:00 <input checked="" type="checkbox"/>
Wireless Profile	802.11a
Country	NO_COUNTRY_SET-(NA)
Tx Rate	Fully Auto
<input type="button" value="Apply"/>	

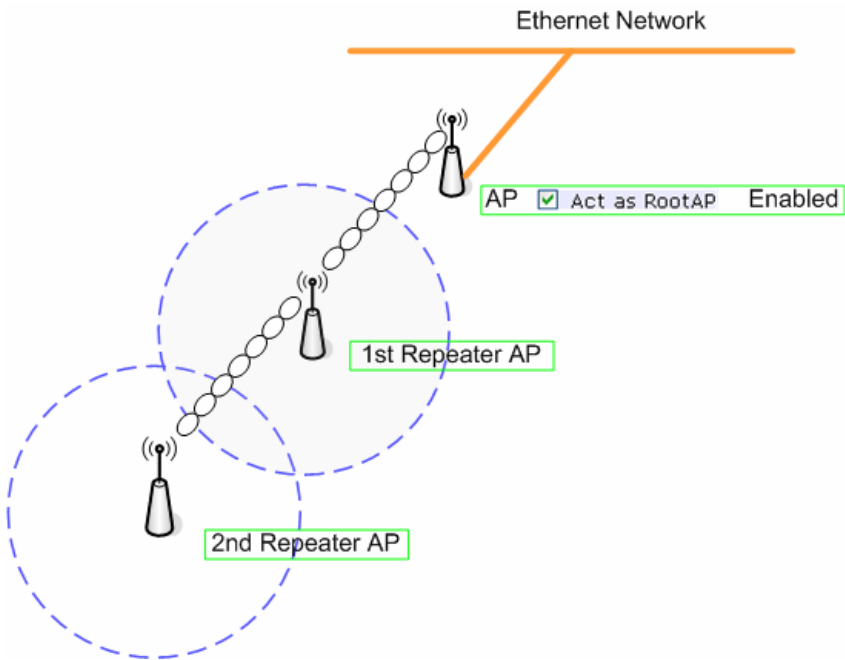
Note:

When using **Remote AP MAC**, the **ESSID** name must also match the AP's ESSID name, especially when Closed System is enabled on the AP.

Repeat Transparent Client step to add more points to the Point-to- MultiPoint connection.

## SETUP REPEATER

A Repeater AP can connect to an AP only if the option **Act as RootAP** is set or checked in the AP setup.



### NOTE

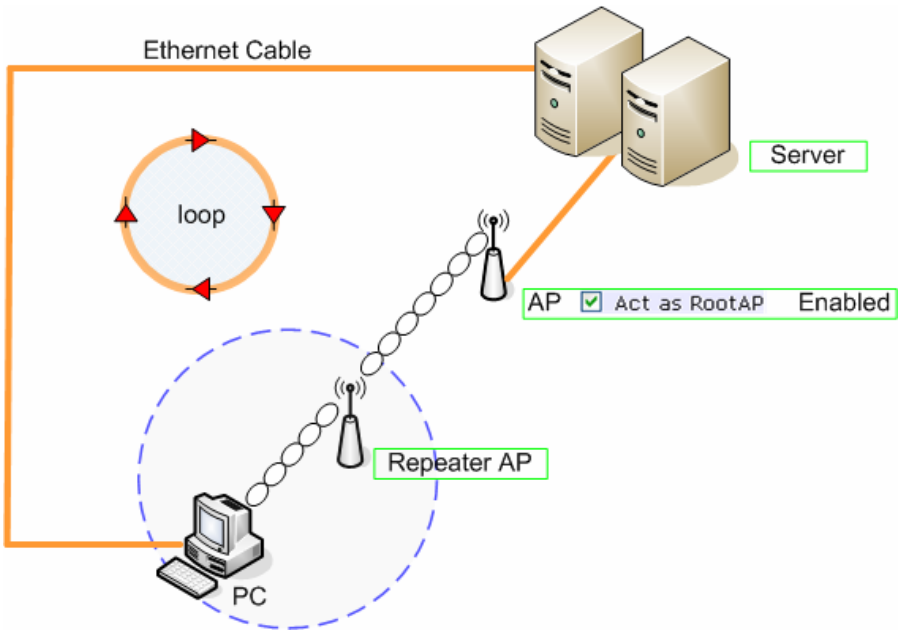
As bandwidth degrades with every repeater hop it is recommended that a limit of **4 hops** is not exceeded.

## Wireless Extended Features

### NOTE

#### NOTE

DO NOT physically connect your PC to the server via Ethernet cable in addition to the wireless connection, as doing so will create a loop that is not prevented by wireless loop preventing feature.



# Wireless Extended Features

Follow these settings to setup the root AP.

Root AP Settings:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**.

Click on **Basic**.

Ensure that **The Current Mode** is set to **Access Point**.

To change **The Current Mode**, please refer to: Common Configuration - WLAN Setup - To Configure the Basic Setup of the Wireless Mode.

Select **Act as RootAP**.

**WLAN Basic Setup**

Card Status	enable
The Current Mode	Access Point <input type="button" value="Change"/>
ESSID	<input type="text" value="rootSSID"/>
Wireless Profile	802.11a <input type="button" value="v"/>
Country	NO_COUNTRY_SET-(NA) <input type="button" value="v"/>
Channel	SmartSelect <input type="button" value="v"/> <input type="button" value="Channel Survey"/>
Tx Rate	Fully Auto <input type="button" value="v"/>
Maximum Associations	<input type="text" value="32"/> (32:1-128)
	<input type="checkbox"/> Closed System
	<input checked="" type="checkbox"/> Act as RootAP
	<input type="checkbox"/> VLANID <input type="text"/>
	<input type="button" value="Apply"/>

Click **Apply**.



## Wireless Extended Features

Follow these settings to setup the repeater.

Repeater Settings:

Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**.

Click on **Basic**.

Ensure that **The Current Mode** is set to **Repeater**.

To change **The Current Mode**, please refer to: Common Configuration - WLAN Setup - To Configure the Basic Setup of the Wireless Mode.

### Repeater Basic Setup

Card Status	enable	
The Current Mode	Repeater	<input type="button" value="Change"/>
ESSID	<input type="text" value="repeaterSSID"/>	
Remote ESSID	<input type="text" value="default"/>	<input type="button" value="Site Survey"/>
Remote BSSID	<input type="text" value="00:00:00:00:00:00"/>	<input type="checkbox"/>
Wireless Profile	<input type="text" value="802.11a"/>	<input type="button" value="v"/>
Country	<input type="text" value="NO_COUNTRY_SET-(NA)"/>	<input type="button" value="v"/>
Tx Rate	<input type="text" value="Fully Auto"/>	<input type="button" value="v"/>
	<input type="checkbox"/> Closed System	
		<input type="button" value="Apply"/>

Click **Apply**.

## Wireless Extended Features

Options for defining the root AP:

- Accept the default **Remote ESSID** (root AP's SSID)

Remote ESSID	<input type="text" value="default"/>
Remote BSSID	<input type="text" value="00:00:00:00:00:00"/> <input type="checkbox"/>

OR

- Enter the **Remote ESSID**.

Remote ESSID	<input type="text" value="rootSSID"/>
Remote BSSID	<input type="text" value="00:00:00:00:00:00"/> <input type="checkbox"/>

OR

- Check and enter the **Remote BSSID** (root AP's MAC address)

Remote ESSID	<input type="text" value="default"/>
Remote BSSID	<input type="text" value="00:80:48:3d:0f:81"/> <input checked="" type="checkbox"/>

Click **Apply**.

# Chapter 7: WLAN Security

This section illustrates how to make your WLAN more secure. All the nodes in your network MUST share the same wireless settings to be able to communicate.

We will illustrate how to configure each type of security mode individually.

To start with, follow the common preliminary steps described below to select the most appropriate security approach for protecting your wireless communications.

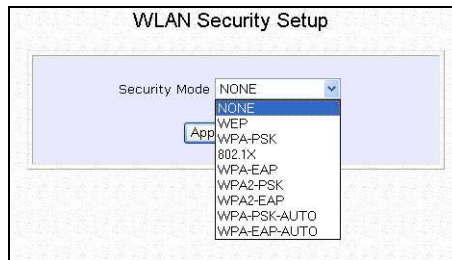
## Step 1:

Click on **WLAN Setup** from the **CONFIGURATION** menu to select **Security**.

## Step 2:

Make a selection from the **Security Mode** drop down list. The **Security Mode** is set to **NONE** by default.

Click on the **Apply** button.



## NOTE

All nodes in your network must share the same wireless settings in order to communicate.

## HOW TO SET UP WEP

The guidelines below will help you to set up your access point for using WEP.

At the **WEP Setup** page,

The screenshot shows the 'WEP Setup' configuration interface. It includes a 'Key String Type' section with radio buttons for 'Hex' (selected) and 'Ascii'. Below that is a 'Transmission Key' dropdown menu with 'Key 1' selected. There are four key configuration sections, each with a radio button for '64Bit' (selected) and '128Bit', a text input field, and a 'Reset' button. An 'Apply' button is located at the bottom right of the form.

### Step 1:

Specify the **key entry type**, by selecting either:

- **Use Hexadecimal:**
- **Use ASCII**

### Step 2:

Select the **Transmission Key** from the pull down menu:

- **Key 1**
- **Key 2**
- **Key 3**
- **Key 4**

The access point lets you define up to four different transmission keys. It defines a set of shared keys for network security. You must enter at least one WEP key to enable security using a shared key.

### Step 3:

Select the **length** of each encryption key:

- **64-bit WEP**  
10 hexadecimal or 5 ASCII Text
- **128-bit WEP**  
26 hexadecimal or 13 ASCII Text

To clear the values that you had entered in the field, click on the **Reset** button.

Click on the **Apply** button and reboot your access point.

### HOW TO SET UP WPA-PERSONAL (ONLY AVAILABLE IN ACCESS POINT MODE)

The guidelines below will help you to set up the access point for using WPA-PSK. Please follow the steps below if you have activated **WPA-PSK**, **WPA2-PSK** or **WPA-PSK-AUTO** security modes.

At the **WPA1/2-PSK Setup** page,

WPA1/2-PSK Setup

Key String Type:  
 Hexadecimal(64 hex digits)  
 Passphrase(8~63 ascii characters)

WPA-PSK: 11111111

Cipher Type:   
TKIP  
AES  
AUTO

GTK Update(seconds):  (60~9999)

#### Step 1:

Specify the **key entry type**, by selecting either:

- **Passphrase (Alphanumeric characters)**
- **Hexadecimal**

#### Step 2:

Fill in the **WPA-PSK** (Pre-Shared network Key):

If you are using the **Passphrase** format, your entry can consist of a minimum of 8 alphanumeric characters or a maximum of 63 alphanumeric characters.

Otherwise, when using the **Hexadecimal** format, your entry MUST consist of 64 hexadecimal characters.

### Step 3:

#### For WPA-PSK

Set the **Cipher Type** to **TKIP**.

WPA replaces WEP with a strong encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC).

#### For WPA2-PSK

Set the **Cipher Type** to **AES**.

**Advanced Encryption Standard (AES)** is a stronger symmetric 128-bit block data encryption technique. AES is a requirement of WPA2 under the IEEE 802.11i standard.

#### For WPA-PSK-AUTO

Set the **Cipher Type** to **Auto** to allow the access point to automatically detect the cipher type to use.

### Step 4:

Enter the **GTK (Group Transient Key) Updates**.

This is the length of time after which the access point will automatically generate a new shared key to secure multicast/broadcast traffic among all stations that are communicating with it. By default, the value is 600 seconds.

### Step 5:

Press the **Apply** button and reboot your system, after which your settings will become effective.

### HOW TO SET UP 802.1X/RADIUS (ONLY AVAILABLE IN ACCESS POINT MODE)

The guidelines below will help you to set up the access point for using 802.1x/RADIUS.

At the IEEE 802.1x Setup page,

IEEE 802.1X Setup

Primary RADIUS Server IP	<input type="text" value="0.0.0.0"/>
Secondary RADIUS Server IP	<input type="text" value="0.0.0.0"/>
Authentication Port	<input type="text" value="1812"/>
Accounting Port	<input type="text" value="1813"/>
Shared Secret Key	<input type="password" value="....."/>
Broadcast Key Rotation(seconds)	<input type="text" value="600"/> (60~9999)
Key Length	<input type="button" value="64 bits"/> <input type="button" value="128 bits"/> <input type="button" value="256 bits"/>

#### Step 1:

Key in the IP address of the **Primary RADIUS Server** in your WLAN. You can optionally add in the IP address of a **Secondary RADIUS Server**, if any.

The RADIUS authentication server MUST be in the same subnet as the access point.

#### Step 2:

By default, the value for **Authentication Port** number is **1812**. You can leave this value as it is. This value must be set to be the same as the one in the RADIUS server.

#### Step 3:

By default, the value for **Accounting Port** number is **1813**. You can leave this value as it is. This value must be set to be the same as the one in the RADIUS server.

### Step 4:

Enter the **Shared Secret Key** in the field provided.

### Step 5:

By default, the **Broadcast Key Rotation** is set as **600** seconds. You may leave this value as its default setting.

### Step 6:

Select the **length** of each encryption key:

- **64-bit**  
10 hexadecimal or 5 ASCII Text
- **128-bit**  
26 hexadecimal or 13 ASCII Text

### Step 7:

Press the **Apply** button and reboot your system, after which your settings will become effective.



# HOW TO SET UP WPA ENTERPRISE (ONLY ACCESS POINT MODE SUPPORTS WPA2-EAP AND WPA-EAP-AUTO)

The guidelines below will help you to set up the access point for using WPA-EAP. Please follow the steps below if you have selected the WPA or WPA1-EAP, WPA2-EAP or WPA-EAP-AUTO.

At the **WPA1/2-EAP Setup** page,

**WPA1/2-EAP Setup**

Primary RADIUS Server IP	<input type="text" value="0.0.0.0"/>
Secondary RADIUS Server IP	<input type="text" value="0.0.0.0"/>
Authentication Port	<input type="text" value="1812"/>
Accounting Port	<input type="text" value="1813"/>
Shared Secret Key	<input type="password" value="....."/>
Cipher Type:	<input type="button" value="AUTO"/> <input type="button" value="TKIP"/> <input type="button" value="AES"/>
GTK update(seconds):	<input type="text" value=""/> (60~9999)

### Step 1:

Key in the IP address of the **Primary RADIUS Server** in your WLAN.

You can optionally add in the IP address of a **Secondary RADIUS Server**, if any. The RADIUS authentication server MUST be in the same subnet as the access point.

### Step 2:

By default, the value for **Authentication Port** number is **1812**. You can either leave this value as it is or key in a different Authentication Port but it MUST match the corresponding port of the RADIUS server.

### Step 3:

By default, the value for **Accounting Port** is **1813**. You can leave this value as it is. This value must be set to be the same as the one in the RADIUS server.

## WLAN Security

### Step 4:

Enter the **Shared Secret Key** used to validate client-server RADIUS communications.

### Step 5:

Select the **length** of each encryption key:

- **64-bit**  
10 hexadecimal or 5 ASCII Text
- **128-bit**  
26 hexadecimal or 13 ASCII Text

### Step 6:

#### For WPA-EAP

Set the **Cipher Type** to **TKIP**.

WPA replaces WEP with a strong encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC).

#### For WPA2-EAP (Only in Access Point mode)

Set the **Cipher Type** to **AES**.

**Advanced Encryption Standard (AES)** is a symmetric 128-bit block data encryption technique. It is a requirement of WPA2 under the IEEE 802.11i standard.

#### For WPA-EAP-AUTO (Only in Access Point mode)

Set the **Cipher Type** to **Auto** to allow the access point to automatically detect the cipher type to use.

### Step 7:

Enter the **GTK (Group Transient Key) Updates**.

This is the length of time after which the access point will automatically generate a new shared key to secure multicast/broadcast traffic among all stations that are communicating with it. By default, the value is 600 seconds.

### Step 8:

Press the **Apply** button and reboot your system, after which your settings will become effective.

# Chapter 8: Security Configuration

This chapter describes the security configuration mainly found in the **Wireless Routing Client** and **Gateway** modes.

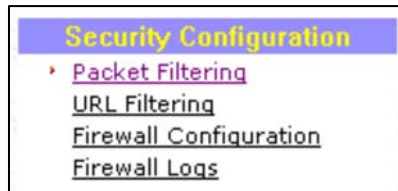
## PACKET FILTERING

As part of the comprehensive security package found on the access point, you may perform IP packet filtering to selectively allow/disallow certain applications from connecting to the Internet.

### CONFIGURE PACKET FILTERING

Step 1:

Under the **Security Configuration** command menu, click on **Packet Filtering**.

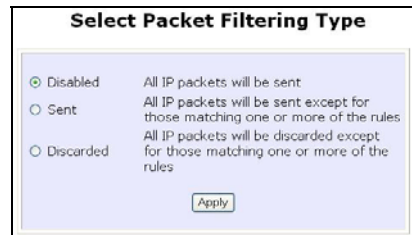


Step 2:

You must first choose the **Packet Filter Type** by clicking on the **Change** button.

Step 3:

Select from three choices: **Disabled**, **Sent**, **Discarded**, then click on the **Apply** button. The default is **Disabled**, which allows all packets to be sent.



# Security Configuration

### Packet Filter Configuration

Packet Filter Type : **Sent**

Rule Name	IP Address(es)	Destination Port(s)	Day of the week	Time of the Day
<input type="button" value="Add"/>				

### Add a new Packet Filter rule

Rule Name :

IP Address : **Any**   
From : 192.168.168.   
To : 192.168.168.

Destination Port : **Any**   
From :   
To :

Day of the Week : **Any**   
From : **Mon**   
To : **Fri**

Time of the Day : **Any** (hh: 00-23, mm: 00-59)   
From :  (hh:mm)  
To :  (hh:mm)

## Step 4:

Click on the **Add** button and you will be able to define the details of your **Packet Filter Rule** from the screen on the right.

4a). Enter **Rule Name** for this new packet filtering rule. For example, *BlockCS*

Rule Name :

4b). From the **IP Address** drop down list, select whether to apply the rule to:

- A **Range** of IP addresses  
In this case, you will have to define (**From**) which IP address (**To**) which IP address, your range extends.

IP Address : **Range**   
From : 192.168.168.  25  
To : 192.168.168.  75

- A **Single** IP address  
Here, you need only specify the source IP address in the (**From**) field.

IP Address : **Single**   
From : 192.168.168.  25  
To : 192.168.168.

- **Any** IP address  
You may here, leave both, the (**From**) as well as the (**To**) fields, blank. Here, the rule will apply to all IP addresses.

IP Address : **Any**   
From : 192.168.168.   
To : 192.168.168.

4c). At the **Destination Port** drop down list, select either:

Destination Port : **Range**   
From :  21  
To :  81

Destination Port : **Single**   
From :  25  
To :

## Security Configuration

- A **Range** of TCP ports

In this case, you will have to define **(From)** which port **(To)** which port, your rule applies.



Destination Port : Any ▾  
From :   
To :

- A **Single** TCP port

Here, you need only specify the source port in the **(From)** field.

- **Any** IP port

You may here, leave both, the **(From)** as well as the **(To)** fields, blank. Here, the rule will apply to all ports.

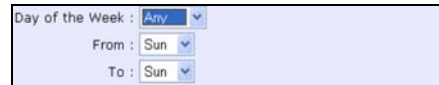


Day of the Week : Range ▾  
From : Wed ▾  
To : Fri ▾

- 4d). From the **Day of the Week** drop down list, select whether the rule should apply to:

- A **Range** of days

Here, you will have to select **(From)** which day **(To)** which day



Day of the Week : Any ▾  
From : Sun ▾  
To : Sun ▾

- **Any** day

In this case, you may skip both the **(From)** as well as the **(To)** drop down fields.

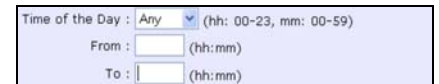


Time of the Day : Range ▾ (hh: 00-23, mm: 00-59)  
From : 08:00 (hh:mm)  
To : 21:30 (hh:mm)

- 4e). At the **Time of the Day** drop down list, you may also choose to apply the rule to:

- A **Range** of time

In which case, you have to specify the time in the format **HH:MM**, where **HH** may take any value from 00 to 23 and **MM**, any value from 00 to 59.



Time of the Day : Any ▾ (hh: 00-23, mm: 00-59)  
From :  (hh:mm)  
To :  (hh:mm)

- **Any** time

## Security Configuration

Here, you may leave both **(From)** and **(To)** fields blank.

### Step 5:

Click on the **Apply** button to make the new rule effective.

The **Filtering Configuration** table will then be updated.



The screenshot shows a dialog box titled "Add a new Packet Filter rule" with the following configuration:

- Rule Name: BlockCS
- IP Address: Any
- From: 192.168.168. (blank)
- To: 192.168.168. (blank)
- Destination Port: Single
- From: 27015
- To: 27015
- Day of the Week: Range
- From: Mon
- To: Fri
- Time of the Day: Range (hh: 00-23, mm: 00-59)
- From: 07:00 (hh:mm)
- To: 18:00 (hh:mm)

Buttons: Add, Cancel, Help

### Step 6:

In this example, let us say we would like to block an application called CS from all PCs (any IP address within the network) from Monday to Friday 7am to 6pm, and this application is using the port number 27015.

Therefore, for a rule we name BlockCS, and add the entries depicted on the left. Clicking on the **Add** button will make your packet filter rule effective.

# Security Configuration

## URL FILTERING

The access point supports URL Filtering which allows you to easily set up rules to block objectionable web sites from your LAN users.

### TO CONFIGURE URL FILTERING

Step 1:

Under the **Security Configuration** command menu, click on **URL Filtering**.



Step 2:

You may now define the **URL Filter Type** by clicking the **Change** button.

Step 3:

Select **Block** or **Allow**, and then click on the **Apply** button. The default is **Disabled**, which allows all websites to be accessed.



When you will be returned to the page shown above, then click the **Add** button.



Step 4:

For the **Host Name** field, input the web site address that you wish to block. Then click the **Add** button to complete your setup.

## FIREWALL CONFIGURATION

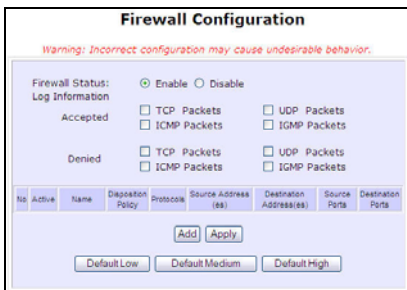
More than just a “NAT” firewall, there is a powerful Stateful Packet Inspection (SPI) firewall option that can be activated on the access point. Stateful inspection compares certain key parts of the packet to a database of trusted information before allowing it through. Common hacker attacks like IP Spoofing, Port Scanning, Ping of Death and SynFlood can be easily thwarted with the access point’s SPI firewall.

### TO CONFIGURE SPI FIREWALL

The following steps explain the configuration of the access point’s SPI firewall. As incorrect configuration to the firewall can result in undesirable network behavior, you are advised to carefully plan your firewall security rules.

#### Step 1:

Under the **Security Configuration** command menu, click on **Firewall Configuration**.



#### Step 2:

First, enable the firewall. You can choose among the **Default Low**, **Default Medium** or **Default High** security options for convenient setup.

#### Step 3:

Then you may choose the type of network activity information you wish to log for reference. Data activity arising from different types of protocol can be recorded.



# Security Configuration

The packet types that you have selected in the **Accepted** section will be displayed in the firewall log if they are detected by the firewall. This also applies to the **Denied** section.

## Step 4:

You may add more firewall rules for specific security purposes. Click on the **Add** radio button at the screen shown above, followed by the **Edit** button and the screen on the left will appear.

- Rule Name** : Enter a unique name to identify this firewall rule.
- Disposition Policy** : This parameter determines whether the packets obeying the rule should be accepted or denied by the firewall. Choose between Accept or Deny.
- Protocols** : Users are allowed to select the type of data packet from: TCP, UDP, ICMP, IGMP or ALL.

Note: If users select either ICMP or IGMP, they are required to make further selection in the ICMP Types or IGMP Types respectively.

## Security Configuration

**ICMP Types** : This IP protocol is used to report errors in IP packet routing. ICMP serves as a form of flow control, although ICMP messages are neither guaranteed to be received or transmitted.

ICMP Packet Type	Description
Echo request	Determines whether an IP node (a host or a router) is available on the network.
Echo reply	Replies to an ICMP echo request.
Destination unreachable	Informs the host that a datagram cannot be delivered.
Source quench	Informs the host to lower the rate at which it sends datagrams because of congestion.
Redirect	Informs the host of a preferred route.
Time exceeded	Indicates that the Time-to-Live (TTL) of an IP datagram has expired.
Parameter Problem	Informs that host that there is a problem in one the ICMP parameter.
Timestamp Request	Information that is from the ICMP data packet.
Information Request	Information that is from the ICMP data packet.
Information Reply	Information that is from the ICMP data packet.

**IGMP Types** : This IP protocol is used to establish host memberships in particular multicast groups on a single network. The mechanisms of the protocol allow a host to inform its local router, using Host Membership Reports.

Host Membership Report	Information that is from the IGMP data packet.
Host Membership Query	Information that is from the IGMP data packet.
Leave Host Message	Information that is from the ICMP data packet.

**Source IP** : This parameter allows you to specify workstation(s) generating the data packets. Users can either set a single IP address or set a range

## Security Configuration

of IP addresses.

**Destination IP** : This parameter lets you specify the set of workstations that receive the data packets. Users can either set a single IP address or set a range of IP addresses.

**Source Port** : You can control requests for using a specific application by entering its port number here. Users can either set a single port number or a range of port numbers.

**Destination Port** : This parameter determines the application from the specified destination port. Users can either set a single port number or a range of port numbers.

**Check Options** : This parameter refers to the options in the packet header. The available selection options are abbreviated as follows:

- SEC – Security
- LSRR – Loose Source Routing
- Timestamp – Timestamp
- RR – Record Route
- SID – Stream Identifier
- SSRR – Strict Source Routing
- RA – Router Alert

**Check TTL** : This parameter would let you screen packets according to their Time-To-Live (TTL) value available options are:

1. Equal
2. Less than
3. Greater than
4. Not equal

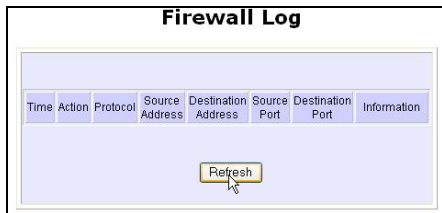
## FIREWALL LOGS

When the access point's SPI firewall is in operation, valuable traffic patterns in your network will be captured and stored into the Firewall Logs. From these logs, you can extract detailed information about the type of data traffic, the time, the source and destination address/port as well as the action taken by the SPI firewall. You can choose which type of packets to log from the **Firewall Configuration**.

### TO VIEW FIREWALL LOGS

#### Step 1:

Under the **SECURITY CONFIGURATION** command menu, click on **Firewall Logs**.



#### Step 2:

Click the **Refresh** button to see new information captured in the log.

# Chapter 9: System Utilities

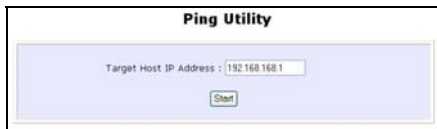
## USING THE SYSTEM TOOLS MENU

### PING UTILITY

This feature lets you determine whether your access point can communicate (ping) with another network host. This feature is available only for the **Wireless Routing Client** and **Gateway** modes.

#### Step 1:

Select **Ping Utility** under the **SYSTEM TOOLS** command menu.

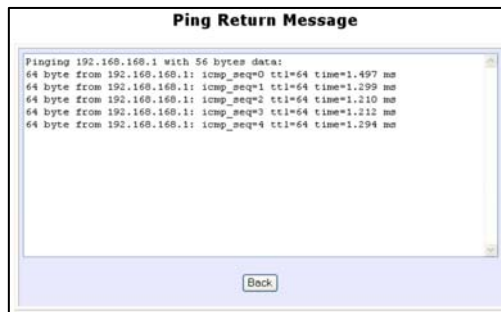


#### Step 2:

Enter the IP address of the target host where the target host you want the access point to ping to.

#### Step 3:

To ping the access point, click **Start**.



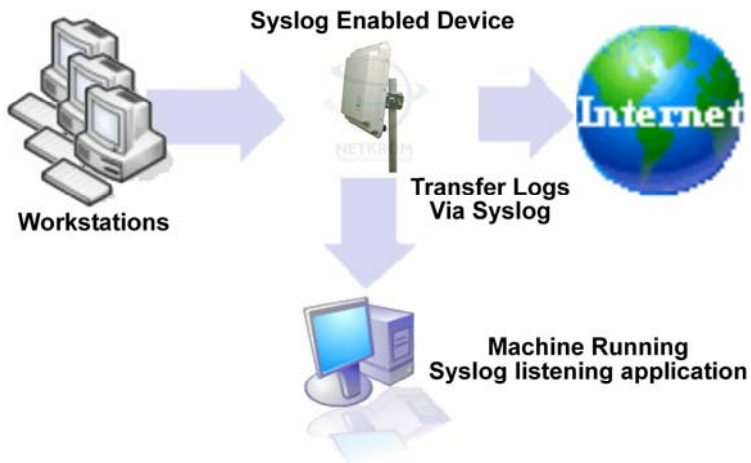
#### Step 4:

The Ping messages will be displayed.

### USE SYSLOG

**Syslog** forwards system log messages in a network to a machine running a Syslog listening application. It is used to help in managing the computer system and increase security on the network.

Freeware supporting Syslog is widely available for download from the Internet.



This section shows how to:

- Setup Syslog.
- View logged information.

The System Log Setup page allows the user to:

- Enable or Disable system logging.
- Set the Remote IP Address or Domain Name and Remote Port for the router to send the system log messages to.

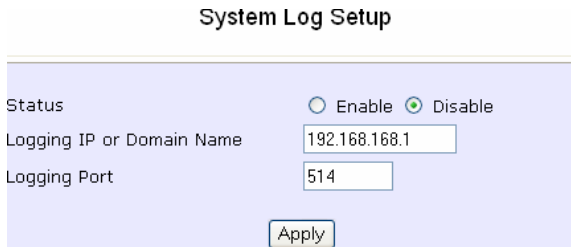
## System Utilities

Follow these steps to setup Syslog:

Step 1:

Click on **Syslog** from the **SYSTEM TOOLS** menu.

Step 2:



The screenshot shows a dialog box titled "System Log Setup". It contains three fields: "Status" with radio buttons for "Enable" and "Disable" (where "Disable" is selected), "Logging IP or Domain Name" with a text box containing "192.168.168.1", and "Logging Port" with a text box containing "514". An "Apply" button is located at the bottom center of the dialog.

Select to **Enable** Syslog.

Enter the **Logging IP or Domain Name**

Enter the **Logging Port**

Click **Apply** to make the changes.

# System Utilities

Follow these sample steps to view logged information:

## Step 1:

Search for a Syslog listening application.

Web [Images](#) [Groups](#) [News](#) [more »](#)

syslog

Search

Search:  the web  pages from Singapore

## Step 2:

Select a Syslog listening application.

### Web

[Syslog Daemon for Windows, Free Syslog Server, Firewall logging ...](#)

Windows **Syslog** Daemon: receives, filters, logs, displays and forwards **Syslog** messages and SNMP traps. Freeware and service versions available.

## Step 3:

Download Syslog listening application.

Download Now

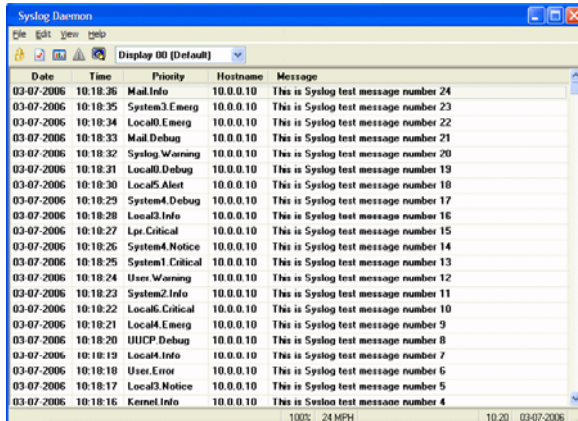
## Step 4:

Install Syslog listening application.



## Step 5:

View logged information on Syslog listening application.



Date	Time	Priority	Hostname	Message
03-07-2006	10:18:36	Mail.Info	10.0.0.10	This is Syslog test message number 24
03-07-2006	10:18:35	System3.Emerg	10.0.0.10	This is Syslog test message number 23
03-07-2006	10:18:34	Local0.Emerg	10.0.0.10	This is Syslog test message number 22
03-07-2006	10:18:33	Mail.Debug	10.0.0.10	This is Syslog test message number 21
03-07-2006	10:18:32	Syslog.Warning	10.0.0.10	This is Syslog test message number 20
03-07-2006	10:18:31	Local0.Debug	10.0.0.10	This is Syslog test message number 19
03-07-2006	10:18:30	Local5.Alert	10.0.0.10	This is Syslog test message number 18
03-07-2006	10:18:29	System4.Debug	10.0.0.10	This is Syslog test message number 17
03-07-2006	10:18:28	Local3.Info	10.0.0.10	This is Syslog test message number 16
03-07-2006	10:18:27	Lpr.Critical	10.0.0.10	This is Syslog test message number 15
03-07-2006	10:18:26	System4.Notice	10.0.0.10	This is Syslog test message number 14
03-07-2006	10:18:25	System1.Critical	10.0.0.10	This is Syslog test message number 13
03-07-2006	10:18:24	User.Warning	10.0.0.10	This is Syslog test message number 12
03-07-2006	10:18:23	System2.Info	10.0.0.10	This is Syslog test message number 11
03-07-2006	10:18:22	Local6.Critical	10.0.0.10	This is Syslog test message number 10
03-07-2006	10:18:21	Local4.Emerg	10.0.0.10	This is Syslog test message number 9
03-07-2006	10:18:20	UIUCP.Debug	10.0.0.10	This is Syslog test message number 8
03-07-2006	10:18:19	Local4.Info	10.0.0.10	This is Syslog test message number 7
03-07-2006	10:18:18	User.Error	10.0.0.10	This is Syslog test message number 6
03-07-2006	10:18:17	Local3.Notice	10.0.0.10	This is Syslog test message number 5
03-07-2006	10:18:16	Kernel.Info	10.0.0.10	This is Syslog test message number 4



## System Utilities

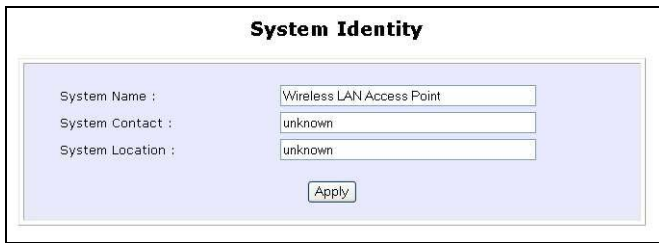
### SYSTEM IDENTITY

If your network operates with several access points, you would find it useful to have a means of identifying each individual device.

You can define the **System Identity** of your access point to be uniquely identifiable as follows:

#### Step 1:

Click on **System Identity** from the **SYSTEM TOOLS** menu.



The screenshot shows a window titled "System Identity" with a light blue background. It contains three text input fields and an "Apply" button. The fields are labeled "System Name :", "System Contact :", and "System Location :". The values entered in the fields are "Wireless LAN Access Point", "unknown", and "unknown" respectively. The "Apply" button is located at the bottom center of the form area.

#### Step 2:

Enter a unique name in the **System Name** field.

#### Step 3:

Fill in the name of a person to contact in the **System Contact** field.

#### Step 4:

Fill up the **System Location** field. If there are multiple devices in your network or building, this entry might help to identify the device location.

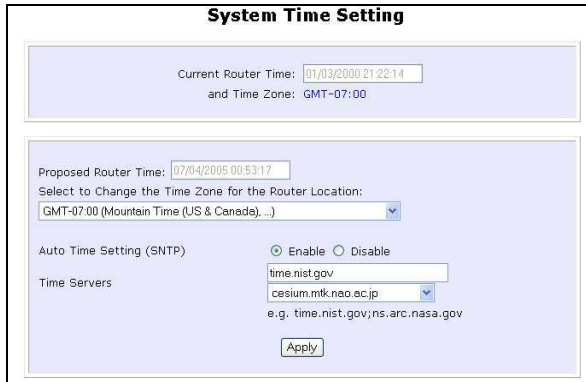
#### Step 5:

Click on the **Apply** button to effect the changes.

## SET SYSTEM'S CLOCK

### Step 1:

Click on **Set System's Clock** from the **SYSTEM TOOLS** menu.



The screenshot shows a web interface titled "System Time Setting". It contains the following elements:

- Current Router Time:** 01/03/2000 21:22:14
- and Time Zone:** GMT-07:00
- Proposed Router Time:** 07/04/2005 00:53:17
- Select to Change the Time Zone for the Router Location:** A drop-down menu currently showing "GMT-07:00 (Mountain Time (US & Canada) ...)".
- Auto Time Setting (SNTP):** Two radio buttons, "Enable" (which is selected) and "Disable".
- Time Servers:** A text input field containing "time.nist.gov" and a drop-down menu showing "cesium.mtk.nao.ac.jp". Below this, there is a small text example: "e.g. time.nist.gov;ns.arc.nasa.gov".
- Apply:** A button at the bottom center.

### Step 2:

Select the appropriate time zone from the **Select to Change the Time Zone for the Router Location** drop-down list.

### Step 3:

**Enable** the Auto Time Setting (SNTP) radio button. **SNTP** stands for Simple Network Time Protocol and is used to synchronise computer clocks.

### Step 4:

Fill in the **Time Servers** field and click on the **Apply** button to effect the changes.

## System Utilities

### FIRMWARE UPGRADE

You can check the types and version of your firmware by clicking on **About System** from the **HELP** menu.

To begin with, ensure that you have downloaded the latest firmware onto your local hard disk drive.

#### Step 1:

Click on **Firmware Upgrade** from the **SYSTEM TOOLS** menu.



#### Step 2:

Click on the **Browse** button to locate the file.

#### Step 3:

Click on the **Upgrade** button.

Follow the instructions given during the upgrading process.



Step 4:

You need to reboot the system after the firmware upgrade.



## NOTE

The firmware upgrade process must NOT be interrupted otherwise the device might become unusable.

## BACKUP OR RESET SETTINGS

You may choose to save the current configuration profile, to make a backup of it onto your hard disk, to restore an earlier profile saved on file or to reset the access point back to its default settings.

### RESET YOUR SETTINGS

#### Step 1:

Click on **Backup or Reset Settings** from the **SYSTEM TOOLS** menu.

#### Step 2:

To discard ALL the configuration you have made and restore the access point to its initial factory settings, click on **Reset** button.

**Backup or Reset Settings**

Erase the Machine's configuration, restore its factory default settings ==>

Backup the Machine's configuration ==>

Restore the Machine's configuration (path and file name)

#### Step 3:

The system will prompt you to reboot your device. Click on the **Reboot** button to proceed.

# System Utilities

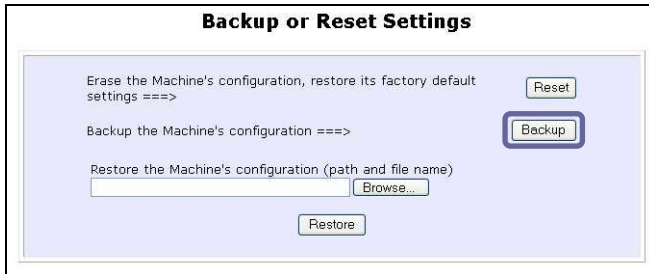
## BACKUP YOUR SETTINGS

### Step 1:

Click on **Backup or Reset Settings** from the **SYSTEM TOOLS** menu.

### Step 2:

If you want to back up the current settings of your access point onto your hard disk drive, click on the **Backup** button.



### Step 3:

Next, save your configuration file to your local disk.



# System Utilities

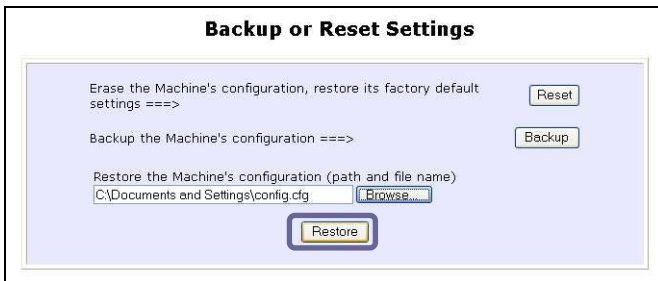
## RESTORE YOUR SETTINGS

### Step 1:

Click on **Backup or Reset Settings** from the **SYSTEM TOOLS** menu.

### Step 2:

If you want to store back the settings that you had previously saved, click on the **Browse...** button. Proceed to the folder where you saved your configuration file.



Click on the **Restore** button and the system will prompt you to reboot your device.

### REBOOT SYSTEM

Most of the changes you make to the system's settings require a system reboot before the new parameters can take effect.

#### Step 1:

Click on **Reboot System** from the **SYSTEM TOOLS** menu.

#### Step 2:

Click on the **Reboot** button.



#### Step 3:

Wait for the system to reboot and the login page will be displayed.





## CHANGE PASSWORD

It is recommended that you change the default login password, which is case sensitive and is set by default, to **password**.

### Step 1:

Click on **Change Password** from the **SYSTEM TOOLS** menu.

### Step 2:

Key in the **Current Password**. The factory default is *password*.

Enter the **new password** in the **New Password** field as well as in the **Confirm Password** field.

### Step 3:

Click on the **Apply** button to update the changes.



The screenshot shows a dialog box titled "Change Password". It contains three input fields: "Current Password:", "New Password:", and "Confirm Password:". Each field is filled with a series of dots, indicating that the text is masked. Below the input fields is a yellow "Apply" button.

### LOGOUT

To exit the Web interface, follow the next few steps.

#### Step 1:

Click on **Logout** from the **SYSTEM TOOLS** menu.

#### Step 2:

Click the **LOGIN!** button to access your access point's configuration interface again.



**Wireless-G Access Point Management**

Please enter your password:

[ Forgot your password? - see the User's Guide for instructions ]

## USING THE HELP MENU

### ABOUT SYSTEM

The **About System** page displays a summary of your system configuration information. Support technicians might require specific information about your system data when they are troubleshooting your configuration. You can use the information displayed in this page to quickly find the data they need to resolve your system problem.

#### Step 1:

Click on **About System** from the **HELP** menu.

The **System Information** page will supply information concerning your access point's configuration settings.

<b>System Information</b>	
<b>Device:</b>	
System Up Time :	0 Days 00:24:54
BIOS/Loader Version :	2.0 (build 0027)
Firmware Version :	1.00 (build 0706)
NetWork Mode :	Inherent Bridge
<b>Wireless:</b>	
Hardware Address :	00-80-45-37-86-dd
WLAN name (ESSID):	Wireless-G AP
Operating frequency :	2457MHz
Operating Channel :	10
Security mode :	WPA-PSK-AUTO
<b>Management Port:</b>	
Hardware Address :	00-80-45-37-86-dc
IP Address :	192.168.168.1
Network Mask :	255.255.255.0
DHCP Server :	Disable

# Appendix I: Firmware Recovery

This section demonstrates how to reload the firmware to the access point should the system fail to launch properly. In such cases, the access point will automatically switch to loader mode and the diagnostic LED will light up and remain ON.

The table below illustrates the behavior of the diagnostic LED (Y).

Access point State	Diagnostic LED (Y) State
Corrupted firmware – access point automatically switches to loader mode	Blinks very fast
Recovery in progress	ON
Successful recovery	Blinks very slowly

Before starting, check the status of the diagnostic LED against the table above to confirm whether firmware failure has occurred.

## Step 1:

Power the access point off and disconnect it from the network.

## Step 2:

Use a MDI cable to connect the LAN port of the access point to the LAN port of your computer.

## Step 3:

Power the access point on, and then start up your computer. You are recommended to set your computer's IP address to 192.168.168.100 and its network mask to 255.255.255.0.

## Step 4:

Insert the Product CD into the CD drive of your computer.

## Firmware Recovery

---

### Step 5:

From the **Start** menu, click **Run** and type **cmd**. When the command prompt window appears, type in the following command:

**X:\recovery\TFTP -i 192.168.168.1 PUT image\_name.IMG**, where **X** refers to your CD drive and **image\_name.IMG** to the firmware filename found in the Recovery folder of the Product CD.

### Step 6:

If you have downloaded a newer firmware and have saved it in your local hard disk as: **C:\EP54G1A\541Axxx.IMG**, then replace the command with this new path and firmware name. In our example:

**C:\ EP54G1A \TFTP -i 192.168.168.1 PUT 541Axxx.img**

The recovery process will now take place. You can check the diagnostic LED to monitor the progress of the recovery process.

When firmware restoration has completed, reboot the access point and it will be ready to operate.

## Appendix II: TCP/IP Configuration

Once the hardware has been set up, you need to assign an IP address to your PC so that it will be in the same subnet as the access point. By default, the access point's IP address is 192.168.168.1; and its subnet mask is 255.255.255.0. You need to configure your PC's IP address to 192.168.168.xxx; and its subnet mask is 255.255.255.0, where xxx can be any number from 2 to 254 excluding 1. Simply follow the procedures stated below to configure the TCP/IP settings of your PC.

### FOR WINDOWS 95/98/98SE/ME/NT

Please note the following instructions are based on Windows 98.

#### Step 1:

From your desktop, click on **Network Neighborhood** icon and select **Properties**.

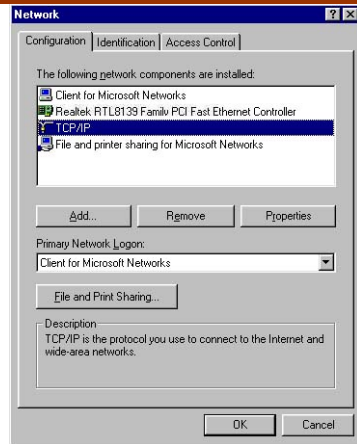
#### Step 2:

Choose the network adapter that you are using; right click and select **Properties**.

#### Step 3:

Highlight the **TCP/IP** and click on **Properties** button.

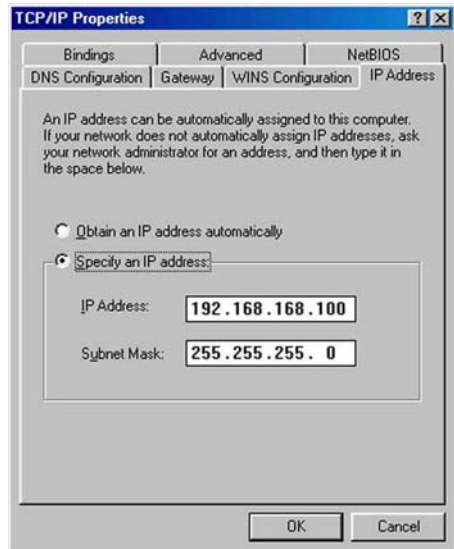
# TCP/IP Configuration



## Step 4:

Select the radio button for **Specify an IP address**.

Enter the IP Address and Subnet Mask as 192.168.168.X and 255.255.255.0, where X can be any number from 2 to 254, except for 1. In this example, we are using 192.168.168.100 as the static IP Address.



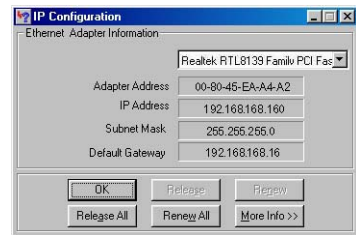
## TCP/IP Configuration

### Step 5:

In order to check if the IP address has been assigned correctly to your PC, simply go to the **Start** menu, select **Run**, and enter the command *winipcfg*.

Select your respective Ethernet Adapter from the drop down list and click **OK**.

Now, your PC is now ready to communicate with your access point.





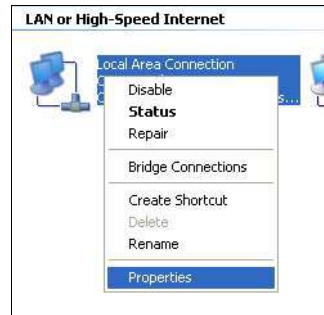
## FOR WINDOWS XP/2000

### Step 1:

Go to your desktop, right-click on **My Network Places** icon and select **Properties**.

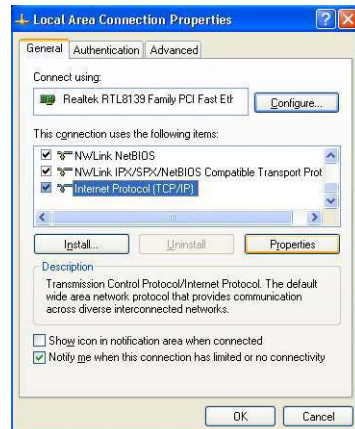
### Step 2:

Go to your network adapter icon, right click and select to **Properties**.



### Step 3:

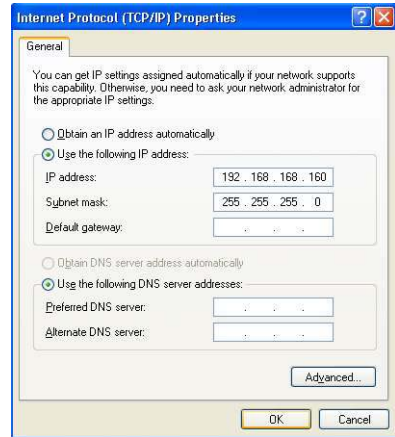
Highlight **Internet Protocol (TCP/IP)** and click on **Properties** button.



## TCP/IP Configuration

### Step 4:

Select the radio button for **Use the following IP address**. Enter the IP Address and Subnet Mask as 192.168.168.X and 255.255.255.0, where X can be any number from 2 to 254, except for 1. In this example, we are using 192.168.168.160 as the static IP Address.

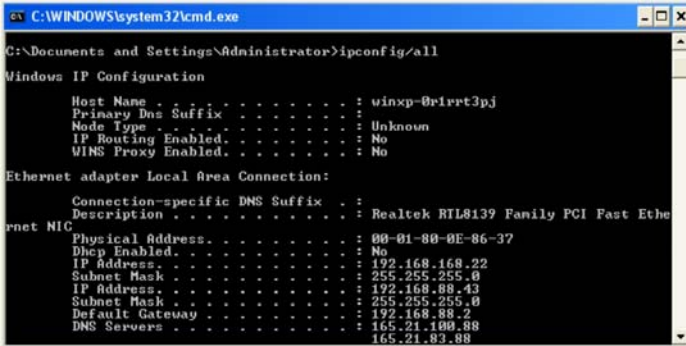


### Step 5:

Click on **OK** to close all windows.

### Step 6:

Next, in order to check if the IP address has been correctly assigned to your PC, go to **Start** menu, **Accessories**, select **Command Prompt** and type the command *ipconfig/all*.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig/all

Windows IP Configuration

   Host Name . . . . . : winxp-0e1ret3pj
   Primary Dns Suffix . . . . . :
   Node Type . . . . . : Unknown
   IP Routing Enabled . . . . . : No
   WINS Proxy Enabled . . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix . :
   Description . . . . . : Realtek RTL8139 Family PCI Fast Eth
   Physical NIC
   Physical Address. . . . . : 00-01-80-0E-86-37
   Dhcp Enabled. . . . . : No
   IP Address. . . . . : 192.168.168.22
   Subnet Mask . . . . . : 255.255.255.0
   IP Address. . . . . : 192.168.88.43
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 192.168.88.2
   DNS Servers . . . . . : 165.21.199.88
   . . . . . : 165.21.83.88
```

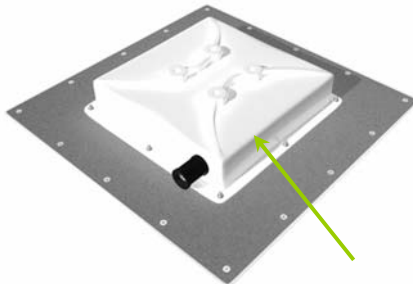
Your PC is now ready to communicate with your access point.

## Appendix III: Panel Views & Descriptions

Front View of AIRNET Outdoor Bridge



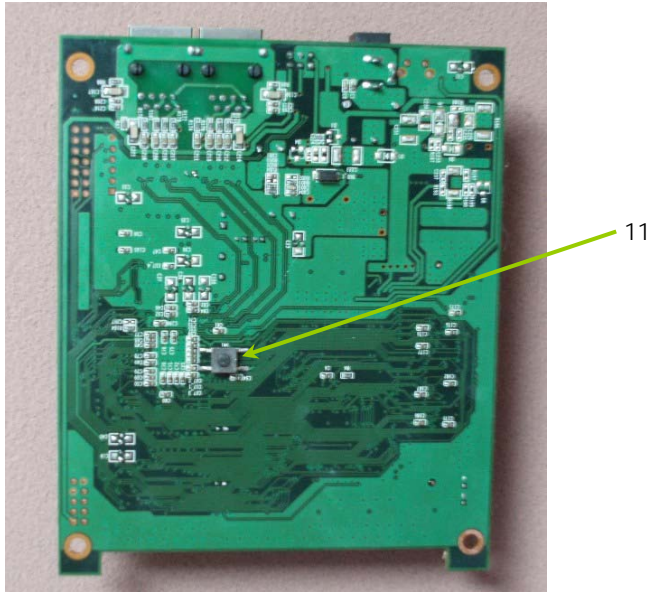
Back View of AIRNET Outdoor Bridge



Waterproof RJ45 Connector

# Panel View & Descriptions

## Bottom View of AIRNET Outdoor Bridge's Board



	Name	Description
11	Reset Push button	<p>To reboot, press once.</p> <p>To reset password, press and hold the button for 5 seconds. The DIAG light will flash fast for about 5 flashes/sec before releasing the button.</p> <p>To restore the factory default settings, press and hold the button for more than 10 seconds. The DIAG light will flash slowly for about 10 flashes/sec before releasing the button.</p>

# Appendix IV: Virtual AP (Multi-SSID) FAQ

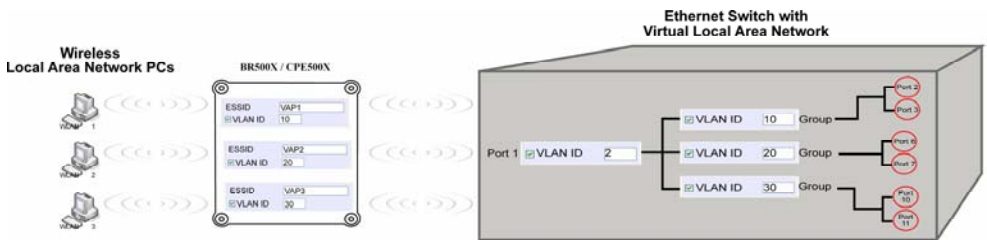
Q1) What is mSSID?

Multi-SSID (mSSID) as the name suggest, allows an access point (AP) with a single radio card to support more than one SSID.

Q2) What can you do with mSSID connection?

The application of mSSID is to provide better security with multiple network path connections from a single AP, to multiple VLAN network segments of the switch on the local area network.

A network setup application is illustrated below.



E.g.

Virtual AP with SSID: VAP1, VLAN ID: 10, and WPA-PSK wireless security enabled will be channeled to Port 2 and Port 3 where the internetsharing router is connected.

Virtual AP with SSID: VPA2, VLAN ID: 20, WPA-EAP enabled, and connected to a radius server, will be channeled to Port 5 and Port 6, which are connected to the firewall of the internal local area network.

---

Q3) Can I update my access point to this mSSID firmware? **(See Appendix V)**

Yes. You can retain your access point configuration when you update to the mSSID firmware if the current firmware running is v1.3x and above.

If AP is running the following configuration setup, updating to the mSSID firmware will affect the configuration.

If AP is running as PtP (Point-To-Point) or PtMP (Point-To-MultiPoint) mode.

The reason it cannot retain the configuration is because mSSID uses a new PtP and PtMP connection setup method called: RootAP and Transparent Client. This method is compliant with IEEE 802.11h standard.

Q4) Can I update to mSSID firmware but setup only one SSID connection?

Yes, mSSID firmware operation is similar to previous single SSID firmware when setup with one SSID.

If the existing AP is running v1.3x firmware, after updating to mSSID it will retain and continue to run the previous configuration. No reconfiguration is needed.

Q5) I have a MAC Filtering table set from a previous firmware. Will updating to mSSID cause the MAC table to be lost?

No, if your firmware is v1.3x and higher, updating to mSSID firmware will retain all entries in the MAC table.

However, if you switch back from mSSID to the previous sSSID firmware, the MAC table will be lost.

---

Q6) I have Pseudo VLAN for Per Group enabled. Will updating to mSSID firmware still support wireless clients with MAC addresses listed in Per Group?

The mSSID firmware replaces Pseudo VLAN and integrates it into VAP (Virtual AP) and MAC Filtering.

Thus, Pseudo VLAN with its VLAN ID and MAC listing will be lost after updating to mSSID firmware.

Refer to the user manual on how to create new VAP with VLAN ID and MAC Filtering.

Similarly, Per Node (control to isolate wireless station in AP) being part of Pseudo VLAN will also be lost.

This option can be enabled again with the option "Station Isolation" in VAP setup page.

Q7) I have WDS setup in my network. Will mSSID still support this?

WDS has the limitation that it can only support WEP security key.

To support higher wireless security it is replaced with Repeater mode in mSSID firmware.

Thus, updating to mSSID will disconnect the WDS links and connections with the rest of the APs.

It is recommended to connect directly to each AP to update the firmware, then set to Repeater mode and configure it before updating the next AP. This way you can build back the connections.

Refer to the user manual for more details instructions on the setup.

Updating to the mSSID firmware is not necessary if you do not need the higher wireless security support.

---

Q8) I have 2 of the access point units installed at a site about 2km from each other running PtP modes.

Should I update to mSSID firmware? Can I do it from one location to update the firmware like I do with the current single SSID firmware?

The setup for PtP and PtMP for mSSID firmware is different the current sSSID firmware.

After mSSID firmware starts up, the link between the 2 APs will be lost.

The recommended method is to setup 2 similar model units in the office. Load the mSSID firmware and create the new PtP / PtMP configuration using the actual parameters of the 2 units on site that you will update.

After testing the connection to be working in the office, backup the configuration file for each unit.

Go to the first site to update the mSSID firmware and restore the configuration for the site, then go to the next site and do the same.

When both APs are up again, the network at both sides should be connected with the new PtP setup.

\*\* Note: If existing PtP connection is running well, it is not necessary to update to the mSSID firmware.

Unless you have the following concerns:

Current firmware PtP is not compliant with IEEE 802.11h standard and the respective country authority requires it to be changed.

Current firmware PtP wireless security only supports WEP key and you are very concerned about the vulnerability to being hacked.

