# NetPassage WPE53G

## User Manual

# Table of Contents

# Overview the Product

## Introduction

NetPassage WPE53G is a high-performance and low-cost IEEE802.11b/g Access Point using the latest AR5007 technology. NetPassage WPE53G is also very small compared to other Access Points in the market. Using Atheros System-on-Chip (SoC) solution, WPE53G supports high-speed data transmission of up to 54Mbps or 108 Mbps. Moreover, Power-over-Ethernet support enables NetPassage WPE53G to be used even in areas without readily-available power outlets.

NetPassage WPE53G complements devices supporting multiple virtual AP connections by directing each to a separate secure virtual LAN. Each VLAN can be secured with different wireless encryption methods, providing the security connections necessary for enterprise networks.

NetPassage WPE53G also incorporates features that are useful to system integrators, such as Antenna Alignment for adjusting your antenna to optimize performance, Syslog for event logging, as well as Telnet/SSH for easy device management.

# Features and Benefits

- **Compact Form Factor**

Small in dimension; light in weight. You can bring it with you anywhere.

- **Multiple-SSID Supporting VLAN Segmentation.**

Up to 4 virtual access points (VAP) with unique BSSIDs is supported and if required, traffic from each VAP can be tagged to a specific VLAN and bridged. The security mode for each VLAN can be configured separately.

- **Long Range Support**

Our proprietary Long Distance Algorithm for ACK and CTS Timeout adjustment support opens up the potential for long range wireless deployment. Recommended values are provided for the parameters that can also be fine-tuned for optimal performance.

- **Bandwidth Control**

In Routing Mode, Bandwidth Control allows the administrator to manage the bandwidth of subscribers to prevent massive data transfer from slowing down the Internet access of other users. The Upload/Download bandwidth at WAN/LAN ports of specific IP or MAC addresses can be specifically limited.

- **Wireless Distribution System 2**

WDS connects access points using MAC address / ESSID to create a wider network so mobile users can roam while remaining connected to network resources.

- **Spanning Tree Protocol**

Provides redundancy and automatically reconfigures to changes in network topology.

- **Parallel Broadband**

In Gateway Mode, Load-Balancing and Fail-Over Redundancy provides scalable Internet bandwidth.

- **SNMP Trap**

SNMP traps logs and provides notification of significant events in the network.

- **Antenna Control and Alignment**

Allows the user to select the specific antenna to use, and also adjust it for optimal throughput.

- **DHCP Relay**

In Routing Mode, DHCP clients can get IP address from the central DHCP server even if they are on different subnets.

- **Remote Firmware Upgrade**

Even if they are physically distant from the access point, users can upgrade the firmware remotely through Telnet / SSH.

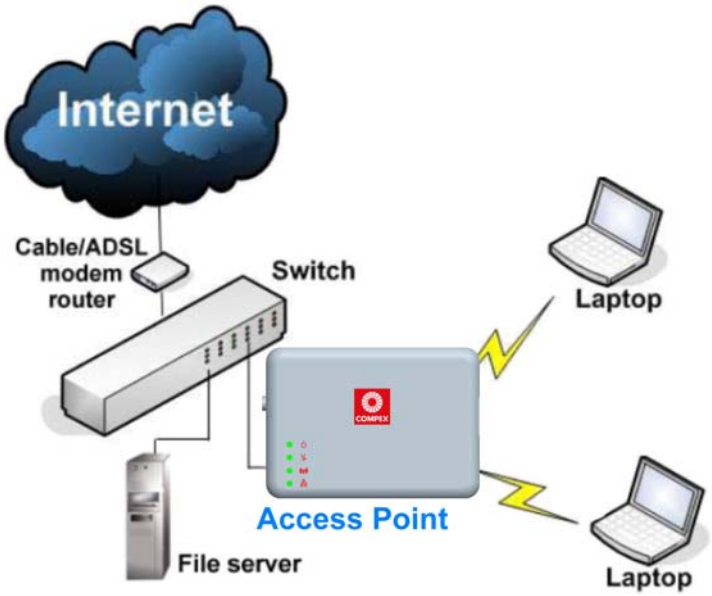
- **RIP 1 / 2**

In Routing Mode, Routing Information Protocol Version 1 / 2 is supported.

# When to Use Which Mode

## Access Point Mode

The Access Point Mode is the default mode of the access point and enables the bridging of wireless clients to access the wired network infrastructure and also enables their communication with each other. In this example the wireless users are able to access the file server connected to the switch, through the access point in Access Point Mode.



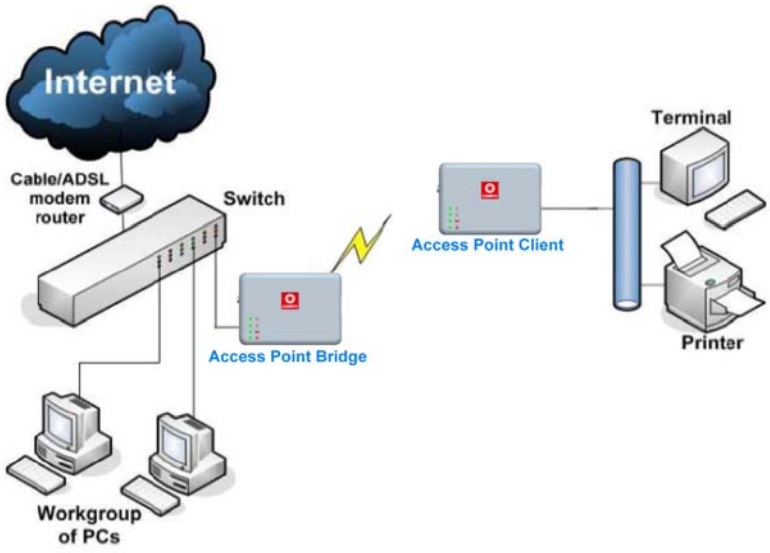
# Access Point Client Mode

In Access Point Client Mode the device acts as a wireless client. When connected to an access point, it creates a network link between the Ethernet network connected at this client device, and the wireless Ethernet network connected at the access point.

In this mode it can only connect with another access point. Other wireless clients cannot connect to it directly unless they are also connected to the same access point – allowing them to communicate with all devices connected to the Ethernet port of the access point.

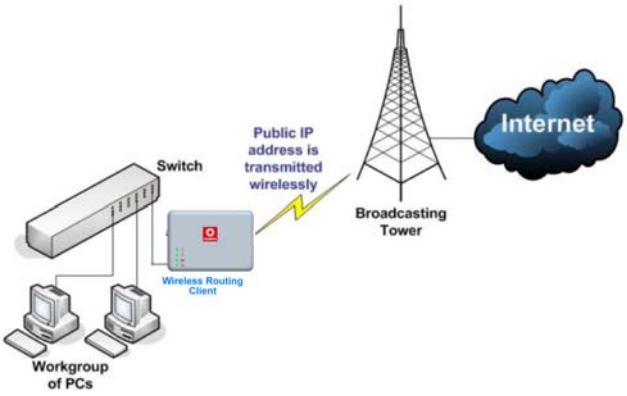
In this example the workgroup PCs can access the printer connected to the access point in Access Point Client Mode.

Optional additional feature:
Point-to-Point connection in this operation mode is also supported if you specifically wish to connect with an access point only.
Please refer to the Point-to-Point setup section.



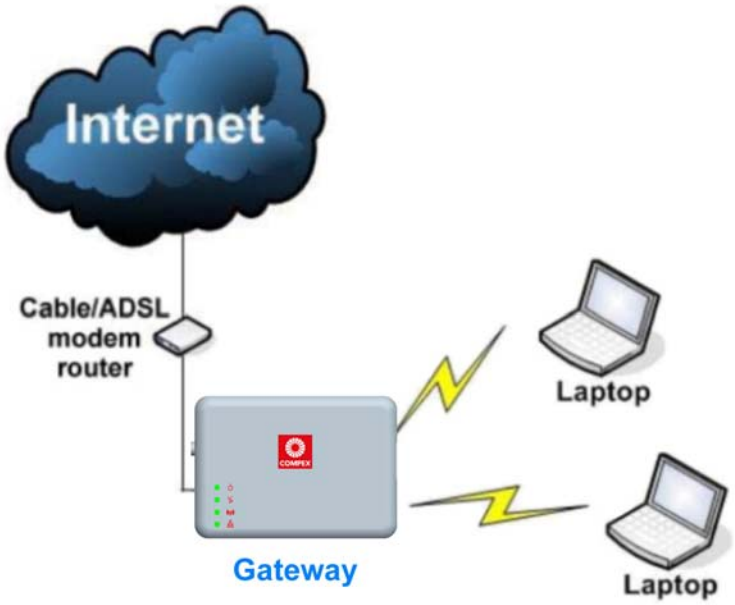
# Wireless Routing Client Mode

In Wireless Routing Client Mode the Ethernet port of the access point may be used to connect with other devices on the network while Internet access would be provided through wireless communication with a wireless ISP.



# Gateway Mode

In Gateway Mode, the access point supports several types of broadband connections in a wireless network after you have identified the type of broadband Internet access you are subscribed to.



Broadband Internet Access Type:

**Static IP Address**
Use Static IP Address if you have subscribed to a fixed IP address or to a range of fixed IP addresses from your ISP.

**Dynamic IP Address**
With Dynamic IP Address the access point requests for, and is automatically assigned an IP address by your ISP, for instance:

- Singapore Cable Vision
- @HOME Cable Services

**PPP over Ethernet (PPPoE)**
Use PPPoE if you are using ADSL services in a country utilizing standard PPPoE authentication, for instance:

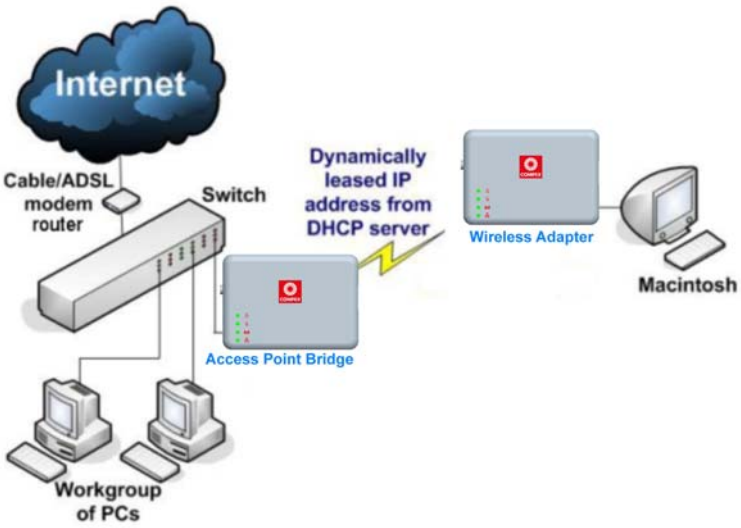
- Germany with T-1 Connection
- Singapore with SingNet Broadband or Pacific Internet Broadband

**PPTP**
Use PPTP if you are using ADSL services in a country utilizing PPTP connection and authentication.

# Wireless Adapter Mode

In Wireless Adapter Mode, the access point can communicate wirelessly with another access point to perform transparent bridging between 2 networks, like in the Access Point Client Mode. In this mode, however, the wireless adapter connects to a single workstation only. No client software or drivers are required to use this mode.

Optional additional feature:
Point-to-Point connection in this operation mode is also supported if you specifically wish to connect with an access point only.
Please refer to the Point-to-Point setup section.

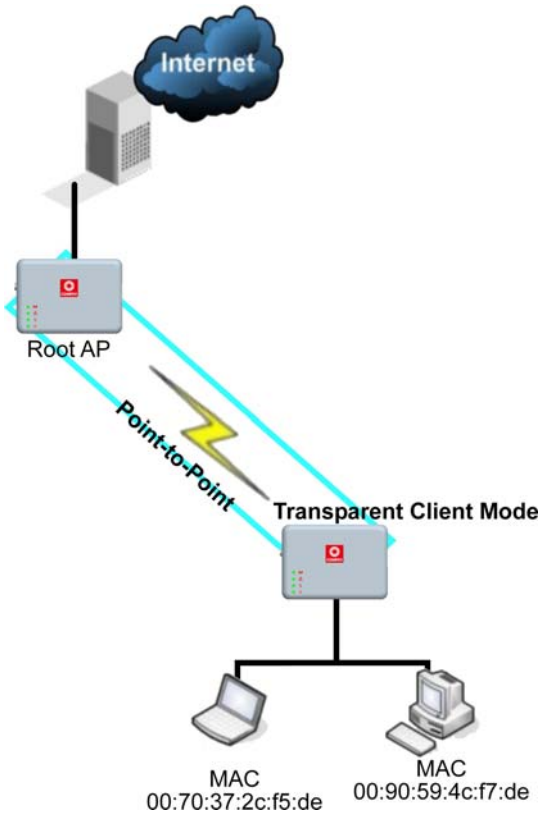


# Transparent Client Mode

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. |

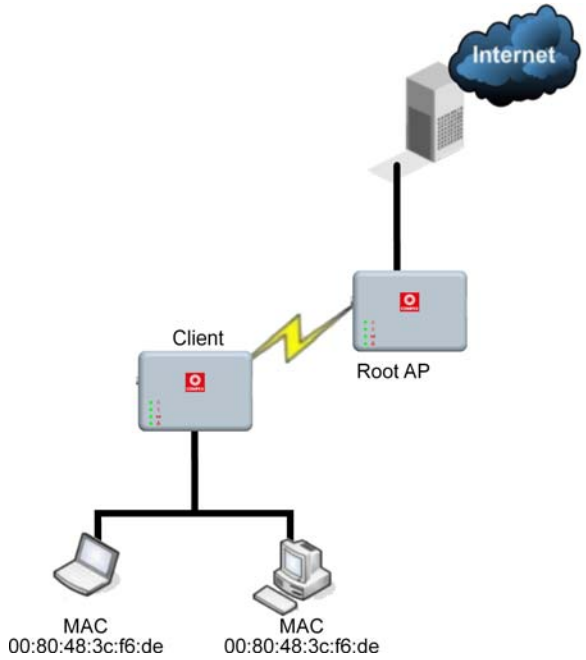
This mode is generally used for outdoor connections over long distances, or for indoor connections between local networks.




- Current Compex model that provide RootAP support are: WP54x series; WPP54x series; WP18; and NP18A. For newer models, please contact your Compex supplier or visit the Compex web site.

| 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 port use a common MAC address for communications with the AP. | Devices connected to the Ethernet port flow through freely and transparently without the MAC address restriction. |

The Transparent Client Mode is more transparent, making it more suitable for linking 2 networks together in a point-to-point, or point-to-multipoint network connection.

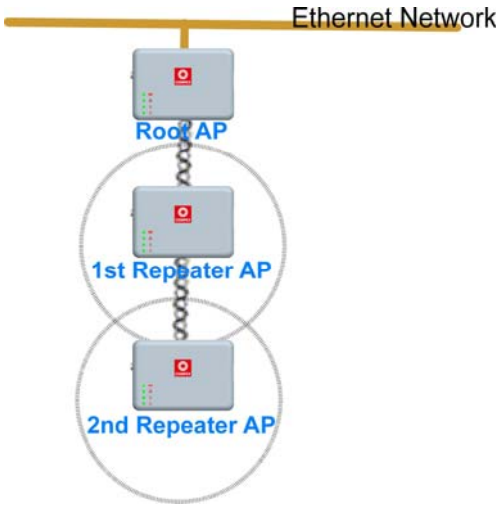


# Repeater Mode

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.



# Panel Views and Description

# Install the Hardware

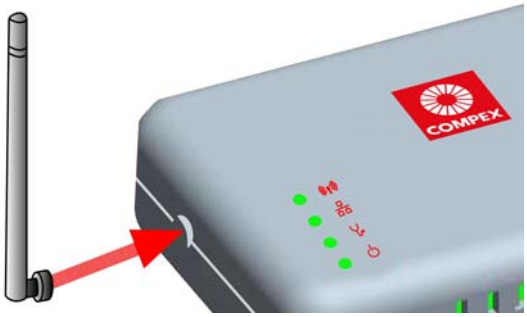
## Setup Requirements

- CAT5/5e Networking Cable.
- At least 1 computer installed with a web browser and a wired or wireless network interface adapter.
- All network nodes installed with TCP/IP and properly configured IP address parameters.

## Using power adapter to supply power to the unit

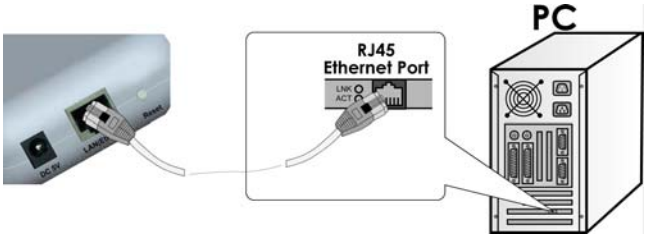
Step 1:

Connect the external antenna to the SMA connector of the access point.



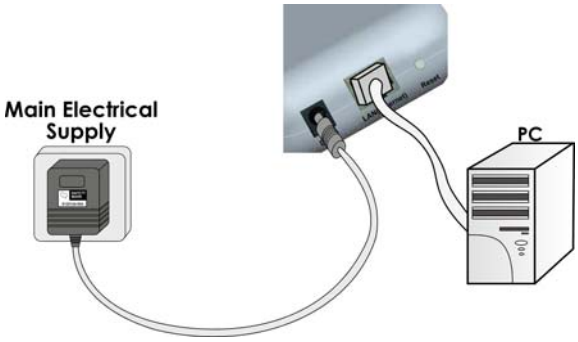
Step 2:

Insert one end of the Ethernet cable to the Ethernet port on your access point, and the other end of the cable to your PC's Ethernet network adapter.




Step 3:

Attach the power adapter to the main electrical supply, and connect the power plug into the socket of the access point.




Step 4:

Turn ON the power supply and power ON your PC. Notice that the LEDs: **Power** and Port **1** or **2** (depending on which port you have connected the RJ45 Ethernet cable to) have lighted up. This indicates that connection has been established successfully between your access point and your PC.

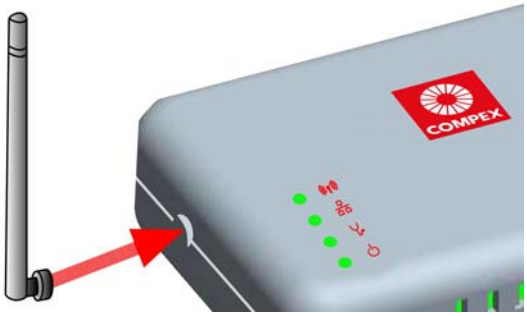
# Using PoE to supply power to the unit

PoE is fully compatible with your access point. This accessory supplies operational power to the wireless AP via the Ethernet cable connection.

Users who wish to use it to supply power to the access point may follow the installation procedures as shown below:

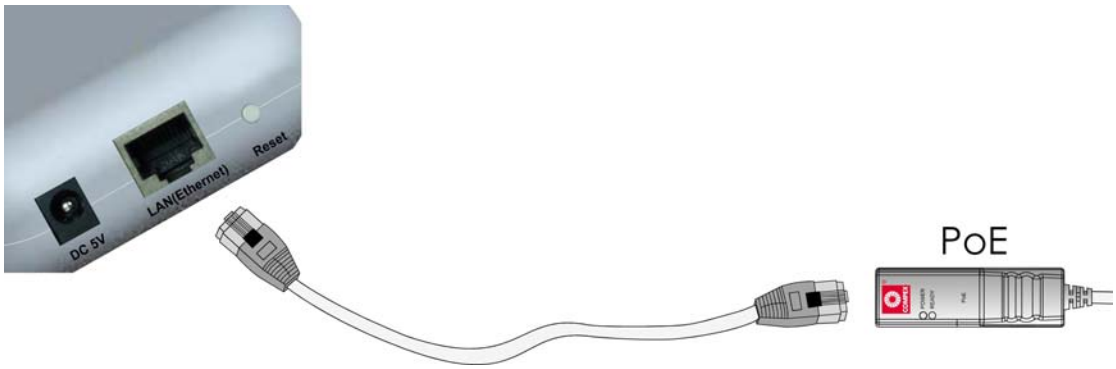
Step 1:

Connect the external antenna to the SMA connector of the access point.




Step 2:

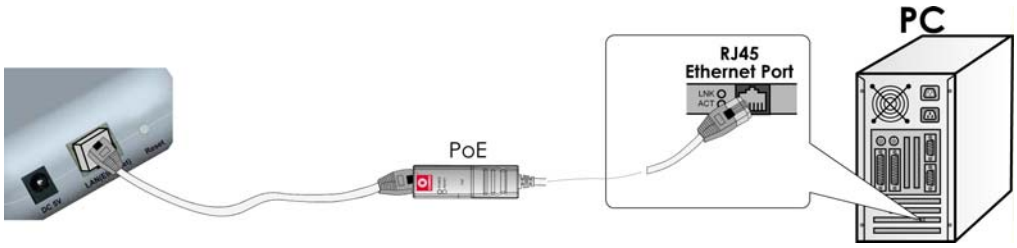
Use an RJ45 Ethernet cable to connect one end of the cable to the Ethernet socket of PoE and the other end to one of the Ethernet ports of the access point.



Step 3:

Next, connect the RJ45 Ethernet cable attached to PoE to your PC's Ethernet network adapter.

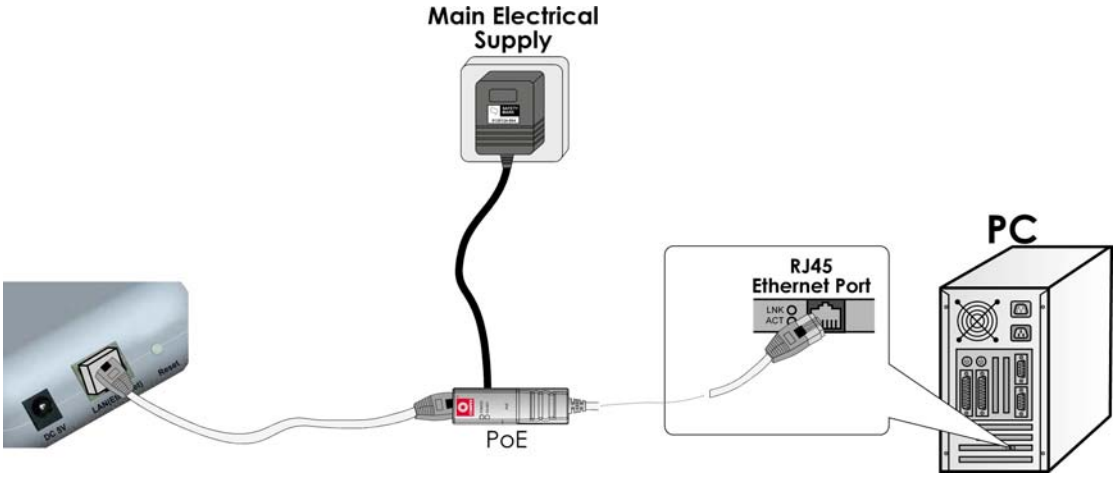
Once you have finished configuring your access point, you can connect the PoE RJ45 Ethernet cable to your network device, such as to a switch or hub.




Step 4:

Connect the power adapter supplied with PoE to the main electrical supply and the power plug into the socket of PoE.

**Note:**
The voltage and current supplied to the access point's power adapter and PoE power adapter are different. Do not interchange the power adapters.




Step 5:

Now, turn on your power supply. Notice that the LEDs have lighted up. This indicates that the access point is receiving power through PoE and that connection between the access point and your PC has been established.

# Setup for Windows XP/2000

Step 1:

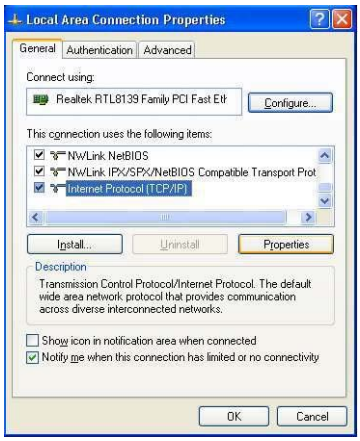
Go to your desktop, right-click on the **My Network Places** icon and select **Properties**.

Step 2:

Right-click the network adapter icon and select **Properties.**


Step 3:

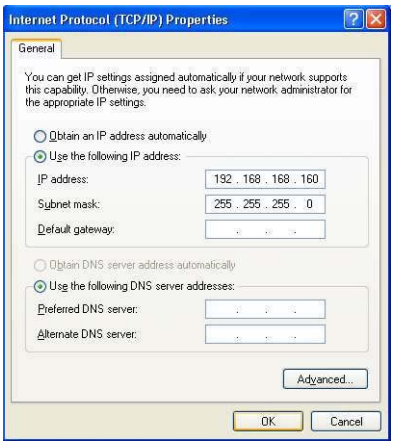
Highlight **Internet Protocol (TCP/IP)** and click on the **Properties** button.




Step 4:

Select the **Use the following IP address** radio button.

Set the IP address to 192.168.168.X and subnet mask to 255.255.255.0, where X can be any number from 2 to 254.

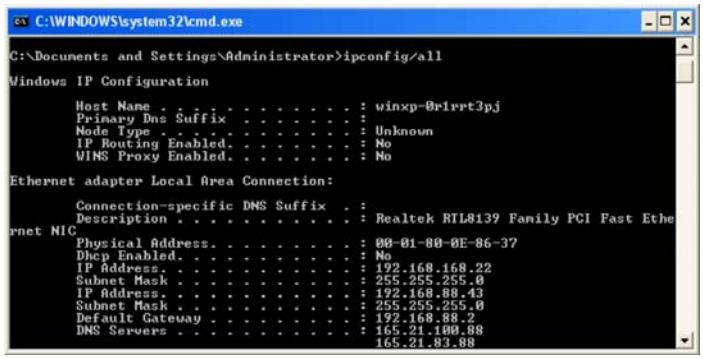


Step 5:

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

Step 6:

To verify that the IP address has been correctly assigned to your PC, go to the **Start** menu, **Accessories**, select **Command Prompt**, and type the command: *ipconfig/all*




Your PC is now ready to communicate with your access point.

# Access the Web Interface

## Access with uConfig

The UConfig utility provides direct access to the web interface.

Step 1:

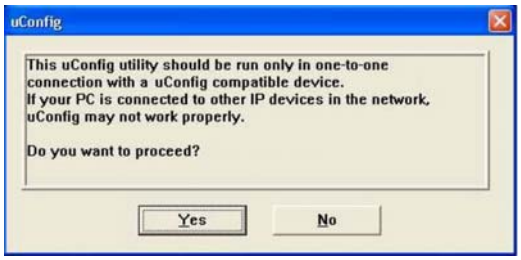
Insert the Product CD into your CD-ROM drive, the CD will autorun.

Step 2:

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

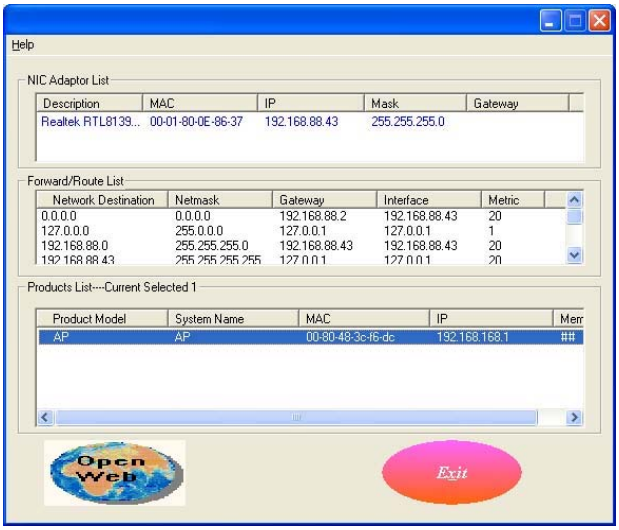
Step 3:

After installation double-click on the **uConfig** icon and click on the **Yes** button.



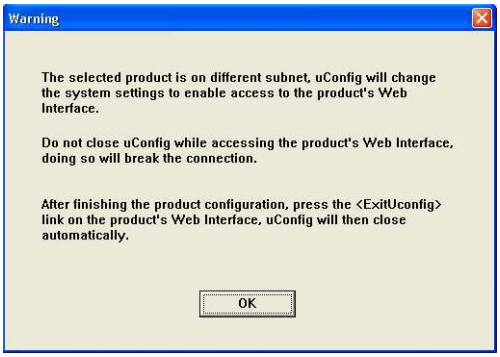
Step 6:

Select the access point from the products list and click on the **Open Web** button. To retrieve and display the latest device(s) in the list, click on the **Refresh** button.




Step 7:

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

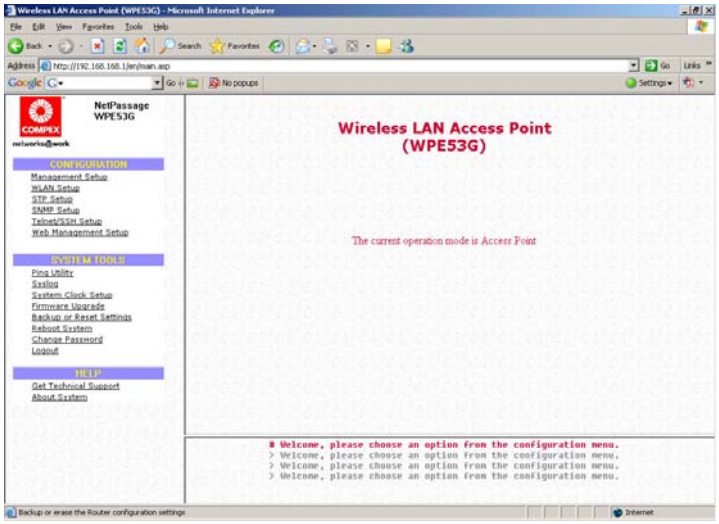


Step 8:

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


Step 9:

You will then reach the home page of the access point web-based interface.



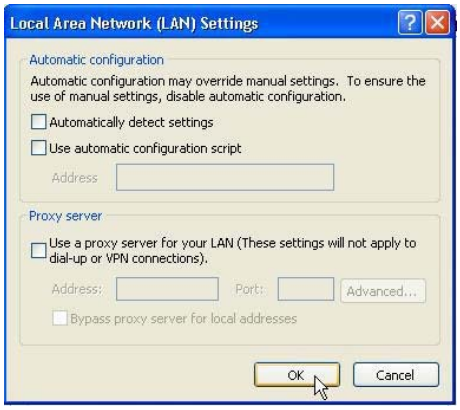
# Manual access with Internet Explorer

Step 1:

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


Step 2:

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



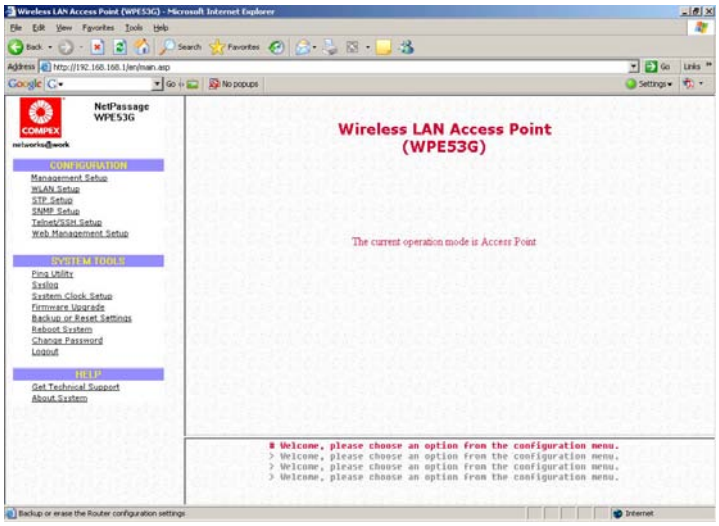
Step 3:

At the **Address** bar type in http://192.168.168.1 and press **Enter** on your keyboard.

Step 4:

At the login page, click on the **LOGIN!** Button.


You will then reach the home page of the access point web interface.



# Perform Basic Configuration

## Setup Management Port

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.

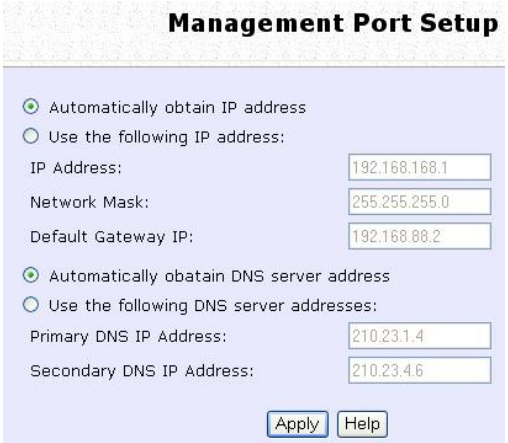
Step 2:

Select to **Automatically obtain IP address**.

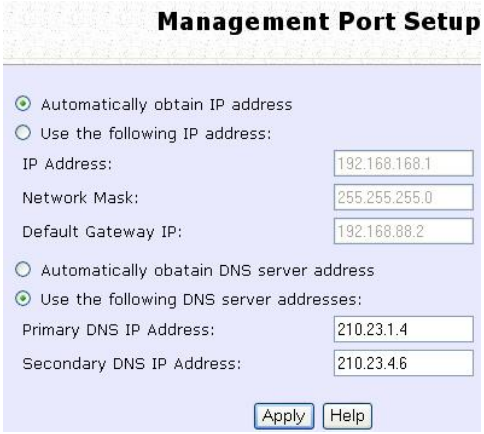
Step 3:

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.




If you choose to **Automatically obtain DNS server 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 |
|---|---|
| Primary DNS IP Address | Your ISP usually provides the IP address of the DNS server. |
| Secondary DNS IP Address | This optional field is reserved for the IP address of a secondary DNS server. |

Follow these steps to manually define the IP address.

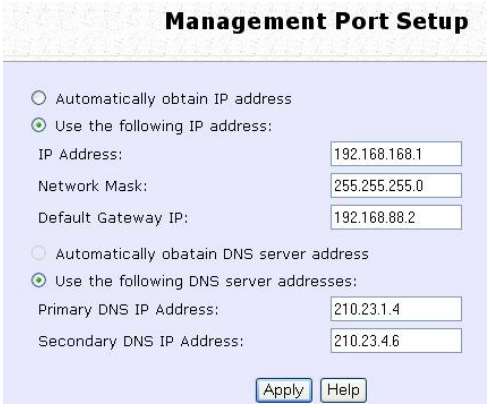
Step 1:

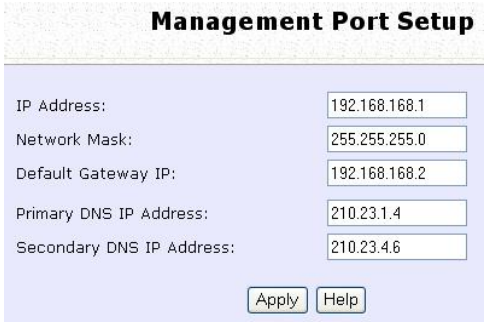
Click on **TCP/IP Settings** from **Management Setup** from the **CONFIGURATION** menu.

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.




The parameters are the same in routing mode.

Step 3:

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.

| Parameters | Description |
|---|---|
| IP Address | When the DHCP server of the access point is enabled (unless you set a different DHCP Gateway IP Address), this LAN IP Address would be allocated as the Default Gateway of the DHCP client.<br><br>The IP address of your Access point is set by default to *192.168.168.1*. |
| Network Mask | The Network Mask serves to identify the subnet in which your Access point resides. The default network mask is *255.255.255.0*. |
| Default Gateway IP | (Optional) As a bridge Access Point, the access point does not usually communicate with devices on other IP subnets. However, the Default Gateway a PC allows 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.<br><br>The Default Gateway IP address of your access point is set to nil by default. |
| Primary DNS IP Address | Your ISP usually provides the IP address of the DNS server. |
| Secondary DNS IP Address | This optional field is reserved for the IP address of a secondary DNS server. |

# 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.

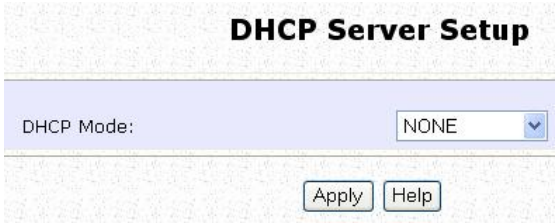
Follow these steps if you do not wish to use DHCP.

Step 1:

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

Step 2:

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




Step 3:

Click on the **Apply** button.

The following will guide you to setup the DHCP Server.

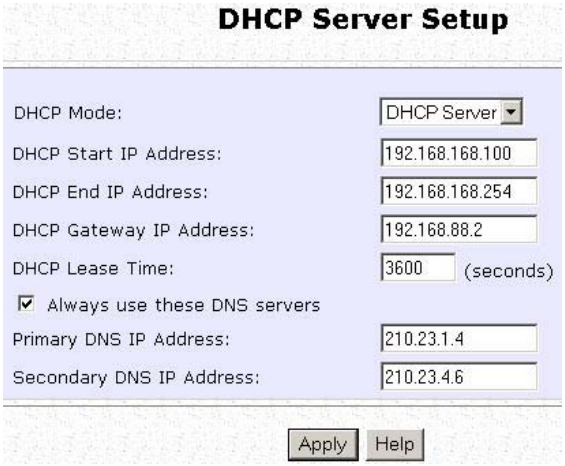
Step 1:

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.




Step 3:

Click on the **Apply** button.

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. | |
| DHCP Start IP Address | This is the first IP address that the DHCP server will assign and should belong to the same subnet as the access point. For example if the access point IP address is 192.168.168.1 and the network mask is 192.168.168.1 and 255.255.255.0, the DHCP Start IP Address should be 192.168.168.X, where X can be any number from 2 to 254. It is pre-set to *192.168.168.100*. |
| DHCP End IP Address | This is the last IP address that the DHCP server can assign and should also belong to the same subnet as your access point. For example if the access point IP address is 192.168.168.1 and the network mask is 192.168.168.1 and 255.255.255.0, the DHCP End IP Address should be 192.168.168.X, where X can be any number from 2 to 254. It is pre-set as *192.168.168.254*. |

| | |
|---|---|
| DHCP Gateway IP Address | Though the DHCP server usually also acts as the Default Gateway of the DHCP client, the access point allows you to define a different Gateway IP Address 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 the other LAN through the Default Gateway defined by the DHCP Gateway IP Address.<br><br>For instance if the access point in Access Point Client mode connects to an Internet gateway X, a PC wired to the access point will be unable to obtain a dynamic IP address directly from X. But if you enable the DHCP server of the access point and set the IP address of X as the DHCP Gateway IP Address, the PC will obtain its IP address from the access point and access the Internet through X. |
| DHCP Lease Time | 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. |
| Always use these DNS servers | Select this option to always use the DNS servers specified. |
| Primary DNS IP Address | Your ISP usually provides the IP address of the DNS server. |
| Secondary DNS IP Address | This optional setting is the IP address of a secondary DNS server. |

The following will guide you to setup the DHCP Relay.
(Available in Client and Wireless Routing Client modes)

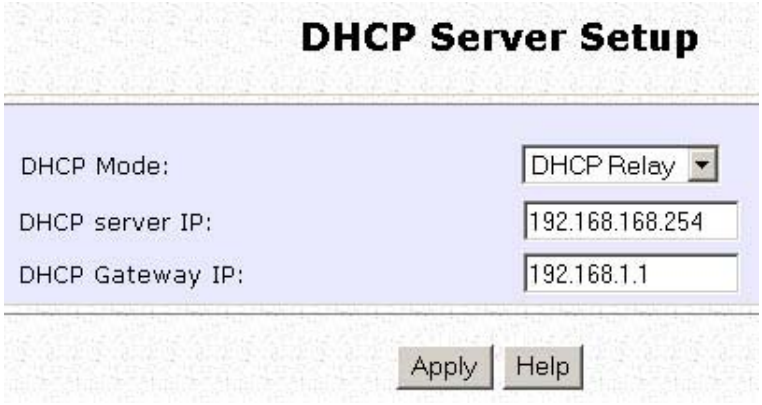
Step 1:

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.




Step 3:

Click on the **Apply** button.

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

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

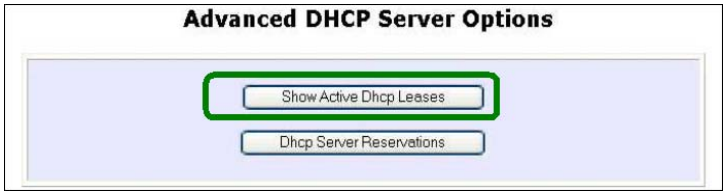
# View Active DHCP Leases

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**

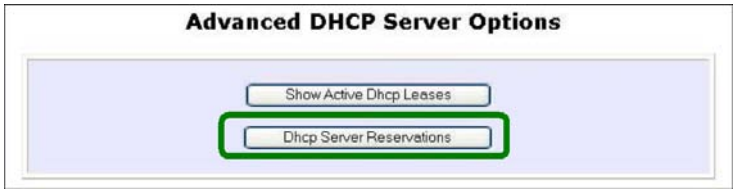
Invalid date and time displayed in the **Lease Expired Time** column indicates that the clock of the access point has not been set properly.

# 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 or 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.



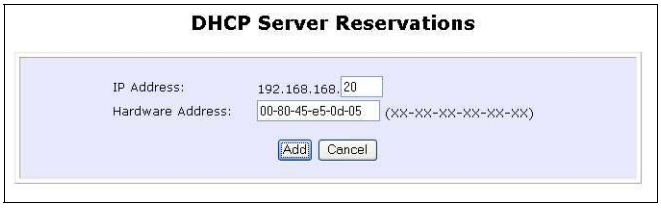

Step 2:

Click on the **Add** button.

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.




The **DHCP Server Reservations** page refreshes to display the currently reserved IP addresses.

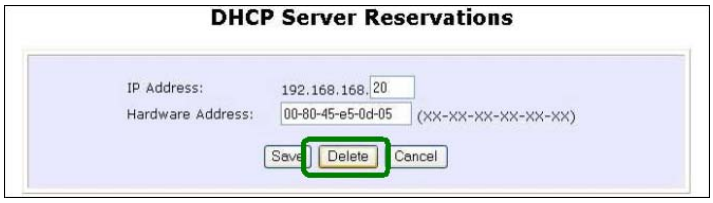
# Delete DHCP Server Reservation

Step 1:

Select the reserved IP address to delete.


Step 2:

Click on the **Delete** button.



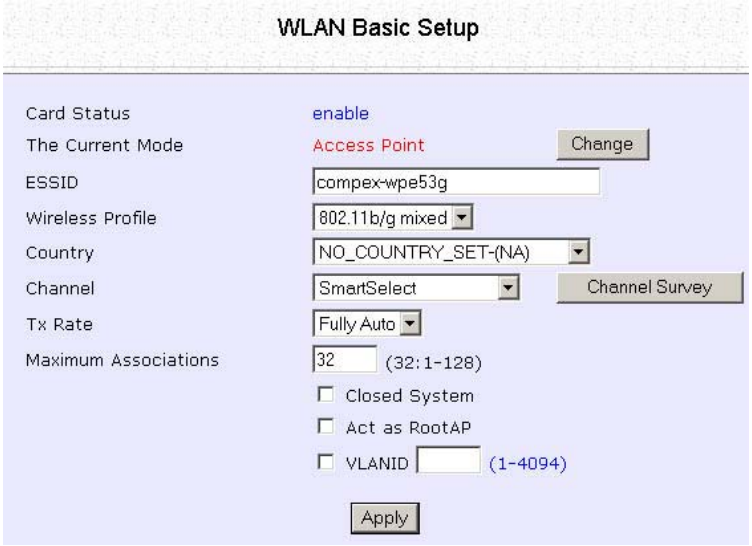

The **DHCP Server Reservations** table refreshes to display your changes.

# Setup WLAN

## Configure the Basic Setup of the Wireless Mode

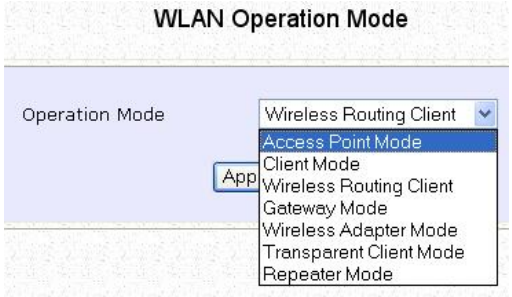
Step 1:

Select **WLAN Setup** from the **CONFIGURATION** menu and you will see the sub menus expanded under **WLAN Setup**, select **Basic**.
The default operating mode of the access point is the **Access Point** mode.




Step 2: (Optional: Change Current mode)

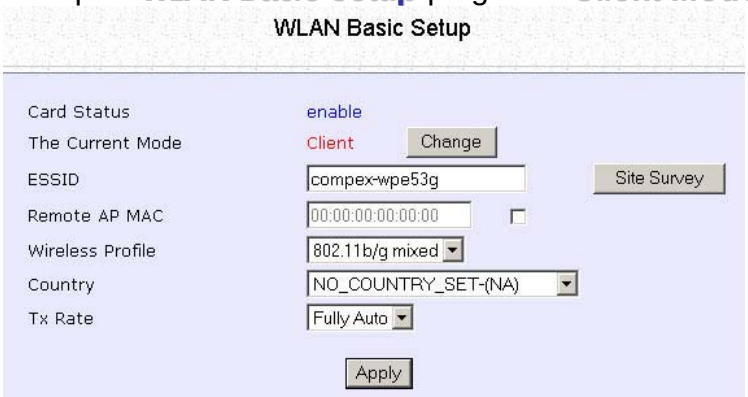
To change the current mode of the access point click on **Change**, select the **Operation Mode**, and click on the **Apply** button to access the setup page of the selected mode. You will be prompted to reboot the access point to effect the mode setting.



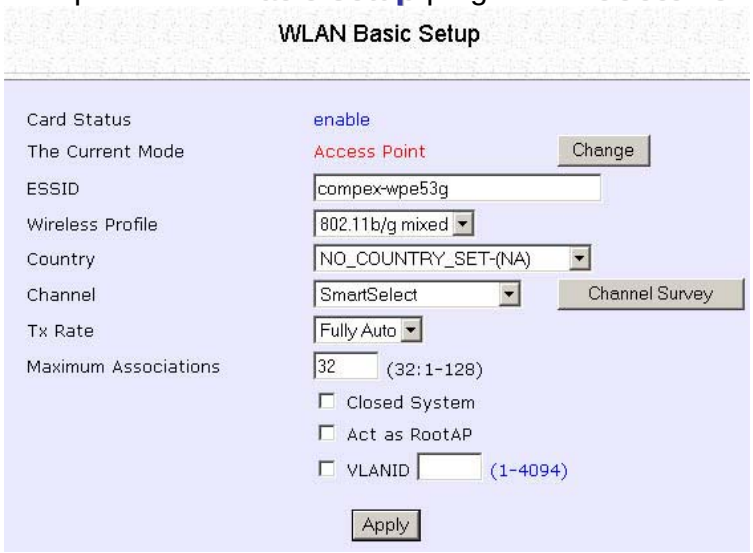
Step 3:
Enter the parameters in their respective fields, click on the **Apply** button and reboot your device to let your changes take effect.

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

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




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



| WLAN Basic Setup page Parameters | Description |
|---|---|
| **The Current Mode** | The default operating mode is the **Access Point** mode. Operating modes:<br><br>• Access Point Mode<br>• Client Mode<br>• Wireless Routing Client<br>• Gateway Mode<br>• Wireless Adapter Mode<br>• Transparent Client Mode<br>• Repeater Mode<br><br>You can toggle the modes by clicking on the **Change** button. |
| **ESSID** | Enter a preferred name for the wireless network. Your wireless clients must be configured with the same ESSID.<br>This case-sensitive entry can consist of a maximum of 32 characters. |
| **Site Survey** | 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.<br>This feature is supported by the Access Point Client and Wireless Routing Client modes. |

| | |
|---|---|
| **Wireless Profile** | A selection of network environment types in which to operate the access point:<br><br>• **802.11b only**<br>Supports wireless B clients with data rates of up to 11Mbps in the frequency range of 2.4GHz.<br><br>• **802.11b/g mixed**<br>Supports both wireless B and G clients.<br><br>• **802.11g only**<br>Supports wireless-G clients that offer transmission rates of up to 54Mbps in the 2.4GHz frequency band.<br><br>• **superG**<br>Supports wireless superG clients that offer transmission rates of up to 108Mbps in the 5GHz frequency band. |
| **Country** | Choose the **Country** where you are located. |
| **Channel** | This option allows you to select a frequency channel for the wireless communication and is only available in the Access Point, Point to Point and Point to Multiple Point modes.<br>Select SmartSelect to automatically scan and recommend the best channel that the access point can utilize. |
| **Tx Rate** | Allows you to choose the rate of data transmission ranging from **1Mbps** to **Fully Auto**. |
| **Closed System** | The access point will not broadcast its **WLAN name (ESSID)** when **Closed system** is enabled. By default **Closed system** is disabled. |

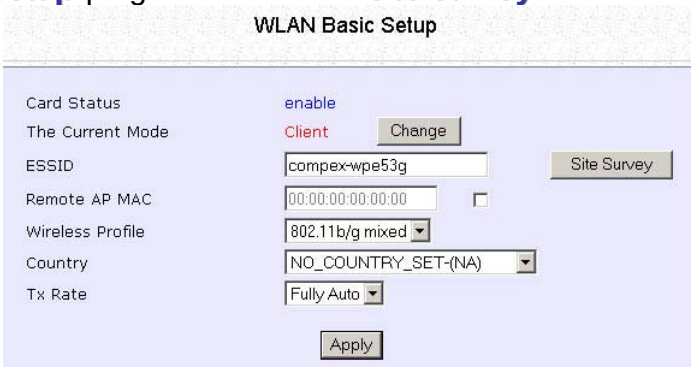
| | |
|---|---|
| **Act as RootAP** | The access point will connect with 1, or multiple clients to create a point-to-point and point-to-multi-point connection network with 2 or more access points.<br><br>This connection mode is fully compliant with 802.1h standards. |
| **VLAN ID** | This is the number that identifies the different virtual network segments to which the network devices are grouped.<br><br>This can be any number from 1 to 4094. |
| **Channel Survey** | 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.<br><br>The Access Point and Gateway modes support this feature. |

# Scan for Site Survey

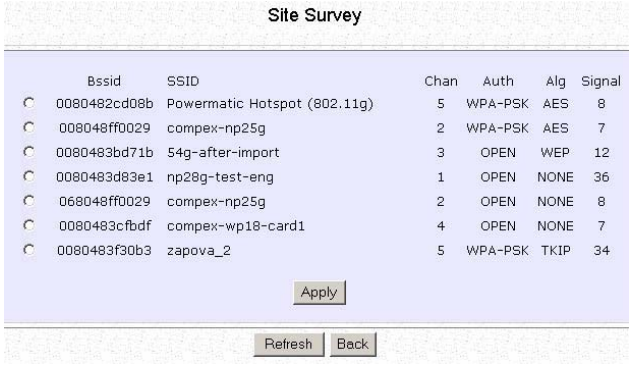
(Available in Client and Wireless Routing Client modes)

Step 1:

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




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




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.

| Read-Only Parameters of Neighbouring Access Points Viewable from Site Survey page | Description |
|---|---|
| **Bssid** | Wireless MAC address of the access point in a wireless network infrastructure. |
| **SSID** | Network name that uniquely identifies the network to which the access point is connected. |
| **Chan** | Channel being used for transmission. |
| **Auth** | Types of authentication, such as WPA, WPA-Personal, etc being used by the access point. |
| **Alg** | Types of algorithm, such as WEP, TKIP, etc being used by the access point. |
| **Signal** | Strength of the signal received in percentage. |

NOTE

**NOTE**

**Site Survey** is used 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 with 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.

# View Link Information

(Available in Client and Wireless Routing Client modes)

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


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 |

| Parameters Viewable from Link Information page | Description |
|---|---|
| **State** | Displays whether the **State** is **Scanning** or **Associated**, and MAC address of the access point to which the client is connected. |
| **Current Channel** | Channel presently being used for transmission. |
| **Tx Rate** | Rate of data transmission in Mbps. |
| **Signal Strength** | Intensity of the signal received, in percentage. |

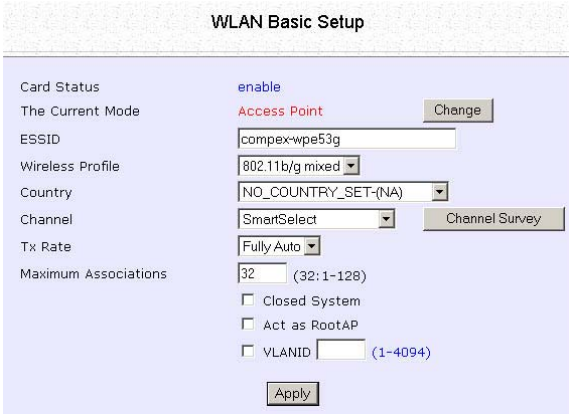
# Scan for Channel Survey

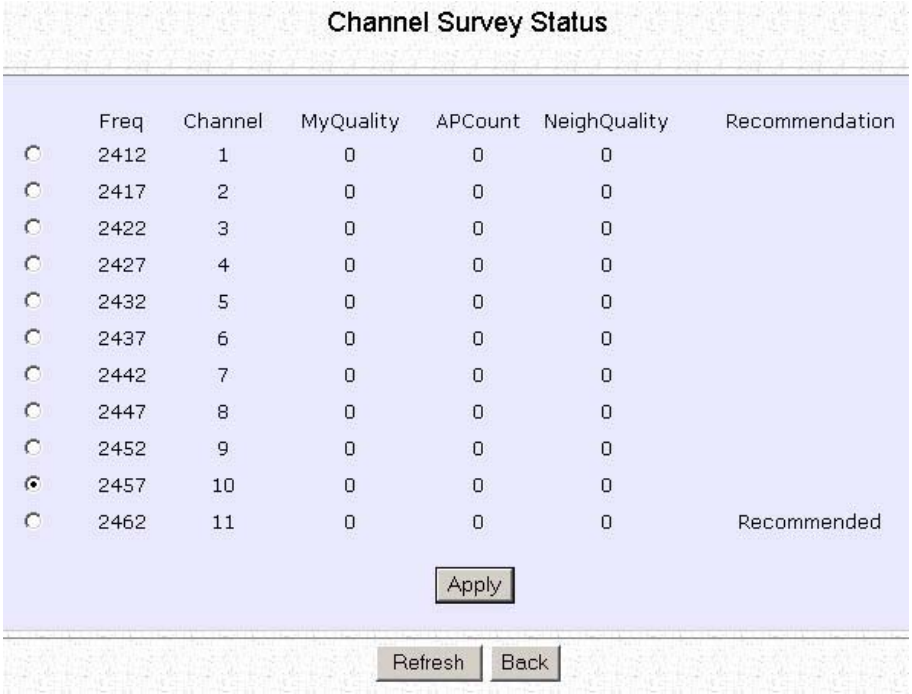
(Available in Access Point and Gateway modes)

Channel Survey displays a list of all the channels supported by the access point, shows the relative interference of all the channels, and recommends the least congested channel.

Step 1:

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





Channel Survey Status

| | Freq | Channel | MyQuality | APCount | NeighQuality | Recommendation |
|---|---|---|---|---|---|---|
| ○ | 2412 | 1 | 0 | 0 | 0 | |
| ○ | 2417 | 2 | 0 | 0 | 0 | |
| ○ | 2422 | 3 | 0 | 0 | 0 | |
| ○ | 2427 | 4 | 0 | 0 | 0 | |
| ○ | 2432 | 5 | 0 | 0 | 0 | |
| ○ | 2437 | 6 | 0 | 0 | 0 | |
| ○ | 2442 | 7 | 0 | 0 | 0 | |
| ○ | 2447 | 8 | 0 | 0 | 0 | |
| ○ | 2452 | 9 | 0 | 0 | 0 | |
| ◉ | 2457 | 10 | 0 | 0 | 0 | |
| ○ | 2462 | 11 | 0 | 0 | 0 | Recommended |

Apply

Refresh Back

Step 2:

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

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.

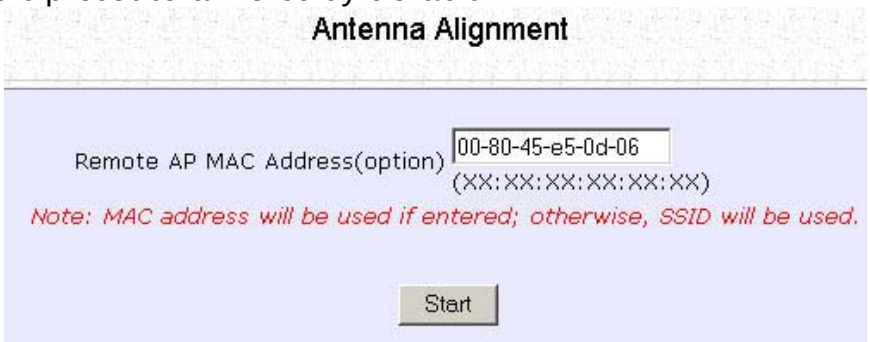
| Read-Only Parameters of All Channels Viewable from Channel Survey page | Description |
|---|---|
| **Freq** | Frequency of the channel at which your access point is operating. |
| **Channel** | Channel of the access point being used for transmission depending on its origin of country. |
| **MyQuality** | 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. |
| **APCount** | Total number of access points operating at the current channel. |
| **NeighQuality** | 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. |
| **Recommendation** | Best channel for the device to use in its current environment. |

# Align the Antenna

Antenna Alignment precisely aligns the antenna over long distances for higher signal strength to improve the connection between the access point and another access point.

Step 1:

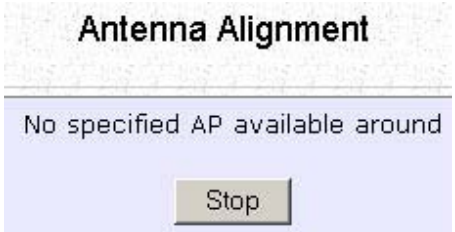
Select **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Antenna Alignment**. The **Antenna Alignment** page can act as a diagnostic tool to check the communication with a remote device. The remote AP MAC Address is preset to all zeros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




Step 2:

If you wish to specify the MAC address of the remote AP, edit 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 access point with the specified MAC address, this screen will display. To abort or to key in the MAC address of another available remote access point, click on the **Stop** button.



**NOTE**
If no MAC address is entered, the **Antenna Alignment** tool will make use of the SSID to align the antenna. Please ensure that the correct SSID is entered. If more than one access point share the same SSID, the access point with the strongest signal will be shown.

| Signal Strength (RSSI Value) Indicated by DIAG LED | 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.

# Configure the Advanced Setup of the Wireless Mode

Step 1:

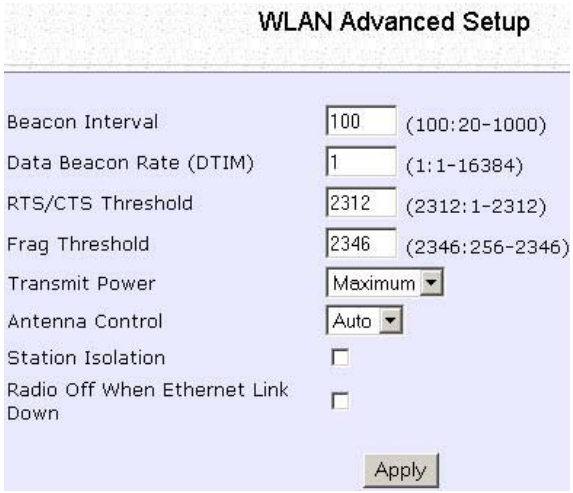
Select **WLAN Setup** from the **CONFIGURATION** menu to expand four sub-menus. From here, select **Advanced**.

Step 2:

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

Step 3:

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



| Advanced Setup Parameters | Description |
|---|---|
| **Beacon Interval (Only in Access Point mode)** | 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. |
| **Data Beacon Rate (DTIM) (Only in Access Point mode)** | How often the beacon contains a delivery traffic indication message (DTIM). The DTIM identifies which clients have data waiting to be delivered to them.<br><br>If the beacon period is set at the default value of 100, and the data beacon rate is set at the default value of 1, the access point will send a beacon containing a DTIM every 100 kilomicrosecond (1 kilomicrosecond equals 1,024 microsecond) |
| **RTS/CTS Threshold** | Minimum size of a packet in bytes that will trigger the RTS/CTS mechanism.<br><br>This value extends from 1 to 2312 bytes. |
| **Frag Threshold** | Maximum size that a packet can reach without being fragmented; represented in bytes.<br><br>This value extends from 256 to 2346 bytes, where a value of 0 indicates that all packets should be transmitted using RTS. |
| **Transmit Power** | Drop-down list of a range of transmission power. |
| **Radio Off When Ethernet Link Down** | Disables the radio card automatically when the Ethernet link is down. |

NOTE

**NOTE**
The values illustrated in the example are suggested values for their respective parameters.

# 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. The sub-menus under **WLAN Setup** expand, select **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 Connection List**

| ID | MAC Address | RSSI | TxRate |
|---|---|---|---|
| AP | 00:80:48:ff:00:2c | 0 | 0Mbps |

Refresh Back

Step 3:

To check the details on an individual wireless client, click on the corresponding MAC Address in the WLAN Station List.
The statistics of the selected wireless client displays.

**00:80:48:ff:00:2c Statistics**

| Authentication Type | Encryption |
|---|---|
| Open | No |

| Authentication | Deauthentication | Association | Disassociation | Reassociation |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |

| | MSDU | Data | Multicast | Management | Control | Errors |
|---|---|---|---|---|---|---|
| Receive | 0 | 0 | 0 | 14794 | 0 | 0 |
| Transmit | 0 | 0 | 0 | 10998 | 0 | 0 |

Back

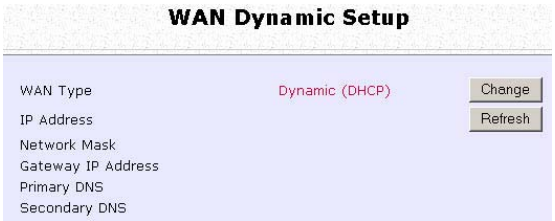
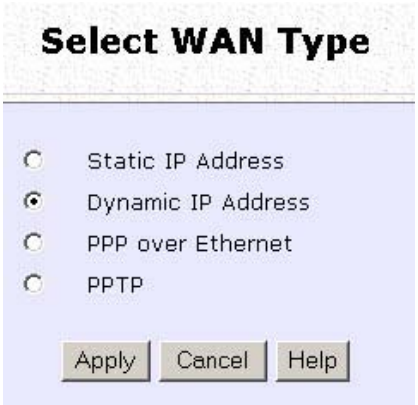
In **Client** mode you are not allowed to view the information of other wireless clients, to do that you need to change to the Access Point mode.

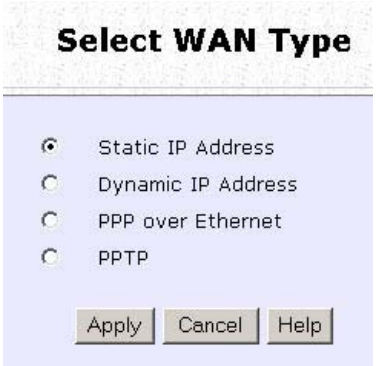
# Setup Your WAN

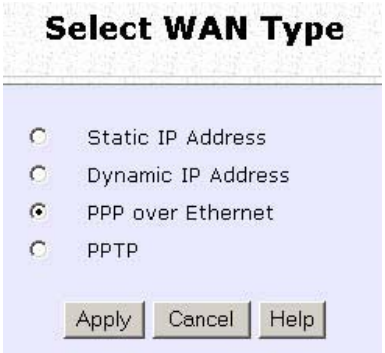
(Available in Wireless Routing Client and Gateway modes)

| | |
|---|---|
| NOTE | **NOTE:**<br>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:<br>Under **CONFIGURATION** on the command menu, select **WAN Setup**. |
| Step 2:<br>On the **WAN Dynamic Setup** screen, verify that the **WAN Type** is **Dynamic (DHCP)**. Otherwise, click on the **Change** button.<br>  <br> |
| Step 3:<br>Select **Dynamic IP Address** and hit the **Apply** button.<br>Reboot to let the settings take effect.<br>  <br> |

| Setup your WAN for cable internet whereby fixed WAN IP address is assigned by ISP |
|---|
| WAN Setup Parameters Example:<br>• IP Address: 203.120.12.240<br>• Network Mask: 255.255.255.0<br>• Gateway IP Address: 203.120.12.2 |
| Step 1:<br>Under **CONFIGURATION** on the command menu, select **WAN Setup**. |
| Step 2:<br>Access the **Select WAN Type** page and select **Static IP Address** before clicking the **Apply** button.<br>  <br> |
| Step 3:<br>Fill in the information provided by your ISP in the **IP Address**, **Network Mask** and **Gateway IP Address** fields, and click the **Apply** button.<br>Select **Reboot System** under **SYSTEM TOOLS** and click the **Reboot** button to effect the settings.<br>  <br> |

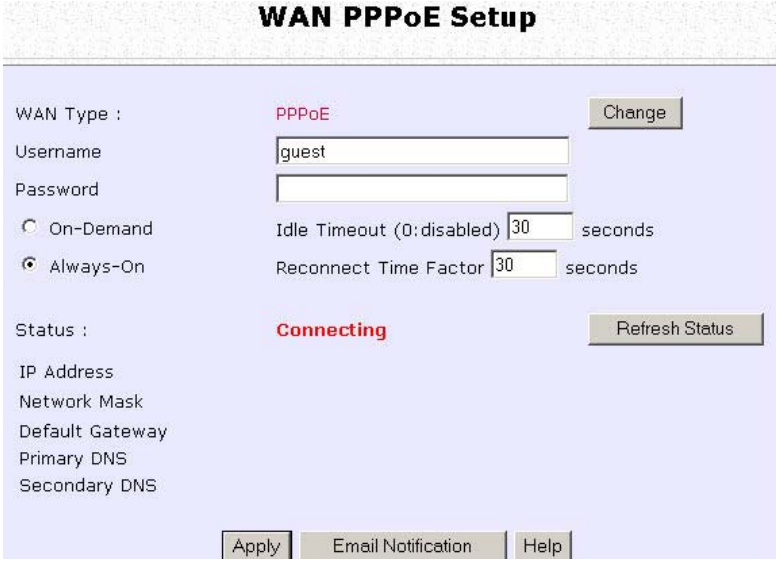
| Setup your WAN for ADSL Internet using PPP over Ethernet |
| --- |
| If you subscribe to an ADSL service using PPP over Ethernet (PPPoE) authentication, you can set up your access point's WAN type as follows. For example, you may configure an account whose username is 'guest' as described below: |
| Step 1:<br>Under **CONFIGURATION** on the command menu, click on **WAN Setup**. |
| Step 2:<br>Access the **Select WAN Type** page and choose **PPP over Ethernet** before clicking the **Apply** button.<br>  <br> |

Step 3:

Enter your account name assigned by your ISP (Example: guest) in the field for **Username**, followed by your account **Password**.

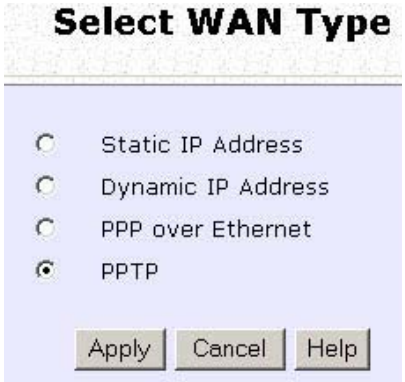
Select **Always-On** if you want your access point to always maintain a connection with the ISP. Otherwise select **On-Demand** for the access point to connect to the ISP automatically when it receives Internet requests from the PCs in your network.

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



You can limit the maximum size a packet can be in a network by setting the **MTU** (Maximum Transmissible Unit).
Click the **MTU** Button in **Advanced WAN Options**.


The **MTU Value** has a range of 1 to 1492.
Enter the **MTU Value** and click **Apply**.

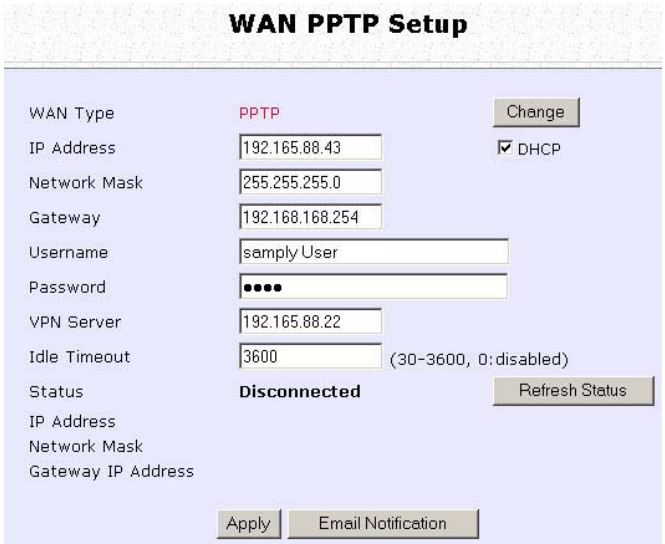
| Setup your WAN for ADSL Internet using Point-to-Point Tunneling Protocol (PPTP) |
| --- |
| WAN Setup Parameters Example:<br>• IP Address: 203.120.12.47<br>• Network Mask: 255.255.255.0<br>• VPN Server: 203.120.12.15 |
| Step 1:<br>Under **CONFIGURATION** on the command menu, click on **WAN Setup**. |
| Step 2:<br>Access the **Select WAN Type** page and select **PPTP** before clicking the **Apply** button.<br>  <br> |

Step 3:

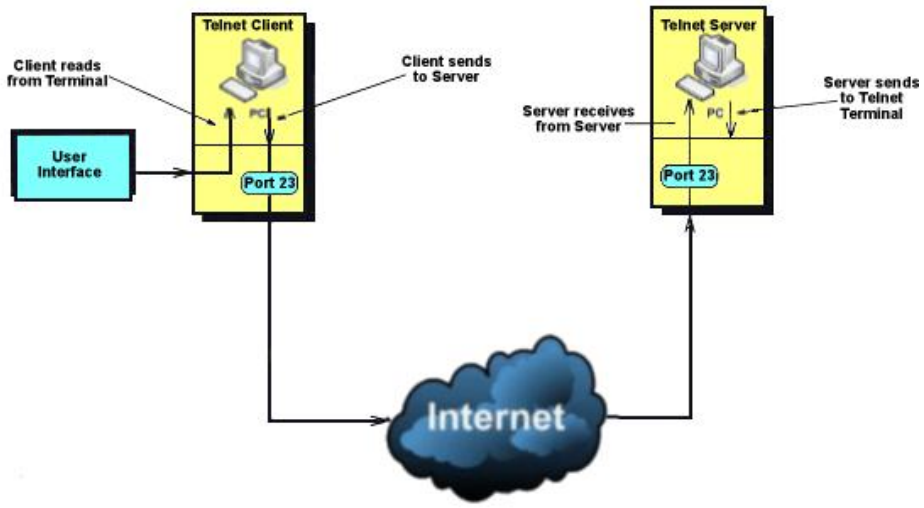
Fill in the information provided by your ISP in the **IP Address**, **Network Mask**, **Gateway,** and **VPN Server** fields; select whether to enable **DHCP**; and click the **Apply** button.

Select **Reboot System** under **SYSTEM TOOLS** and click the **Reboot** button to effect the settings

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



# 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.

Step 3:

To add user:

1. Click the **Add** button.


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.


To Delete User:

1. Select which user to Delete.

2. Click the **Delete** button.

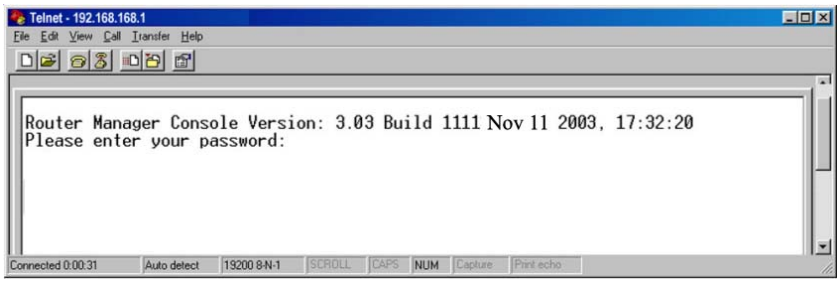

To Refresh User Management list click the **Refresh** button.

# 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.

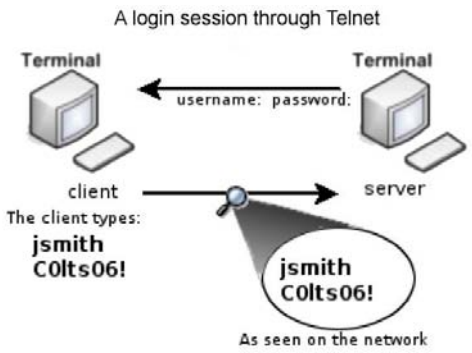
2. At the login prompt, type in the default password "password" and press enter. You will then login to the CLI.

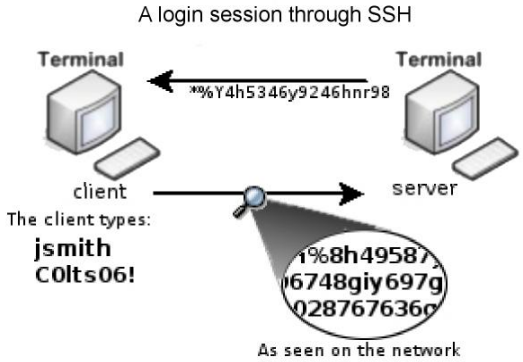


# Access the Secure Shell Host Command Line Interface

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.

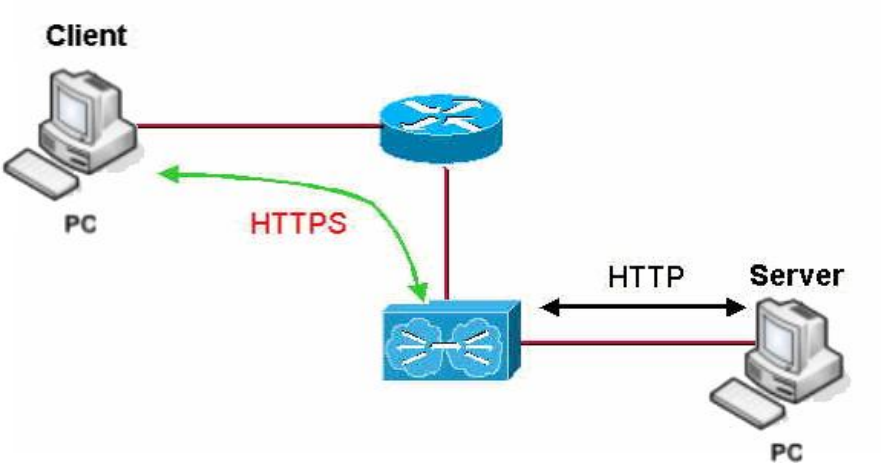



SSH CLI has a command line interface.

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

Step 2:

1. Select whether to set web server to **HTTP** or **HTTPS (SSL)** mode.
2. Specify the **Login Timeout** (time of inactivity in seconds before user is automatically logged out).
3. Click **Apply**.

Changes will be effected after reboot.

# Setup SNMP

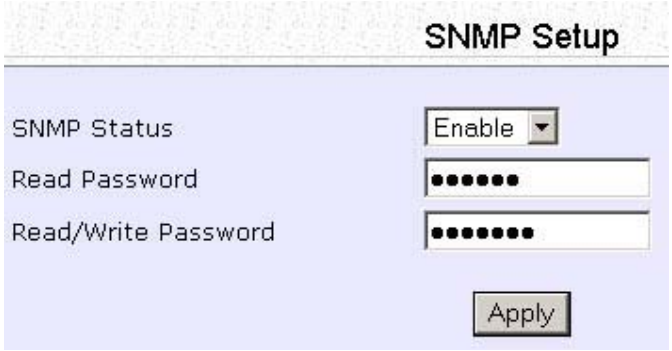
The Simple Network Management Protocol (SNMP) is a set of communication protocols that separates the management software architecture from the hardware device architecture.

Step 1:
Select **SNMP Setup** from the **CONFIGURATION** menu.

Step 2:
Select **Enable** from the **SNMP State** drop-down list.

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

Step 3:
Click on the **Apply** button.



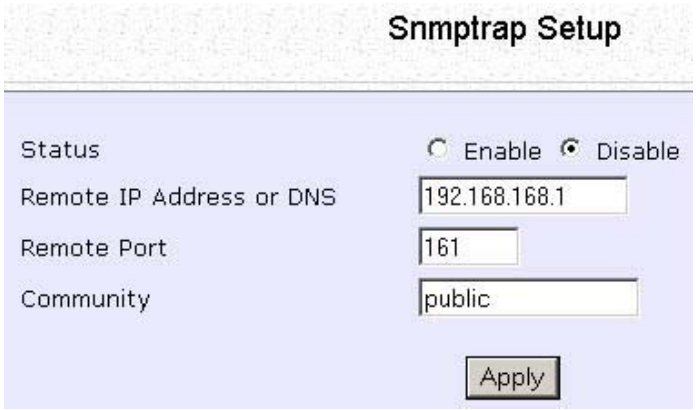
# Setup SNMP Trap

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.

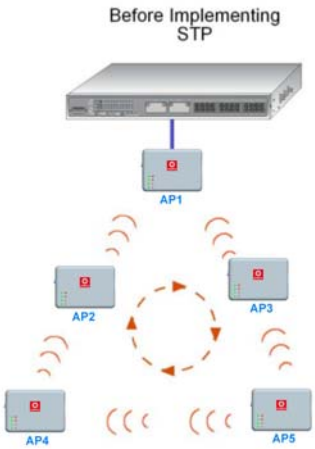
Step 2:

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.

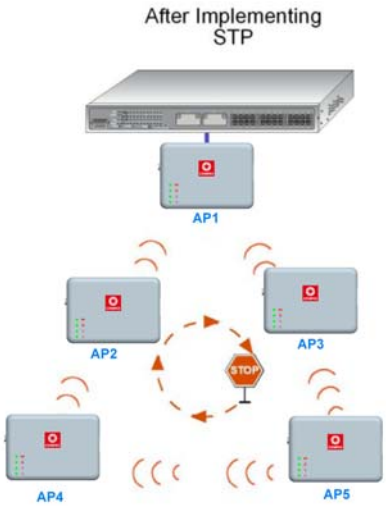


# Setup STP

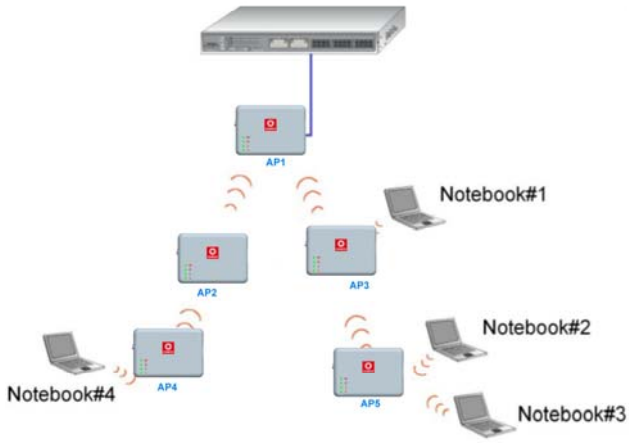
(Available in Access Point, Transparent Client, and Repeater modes)



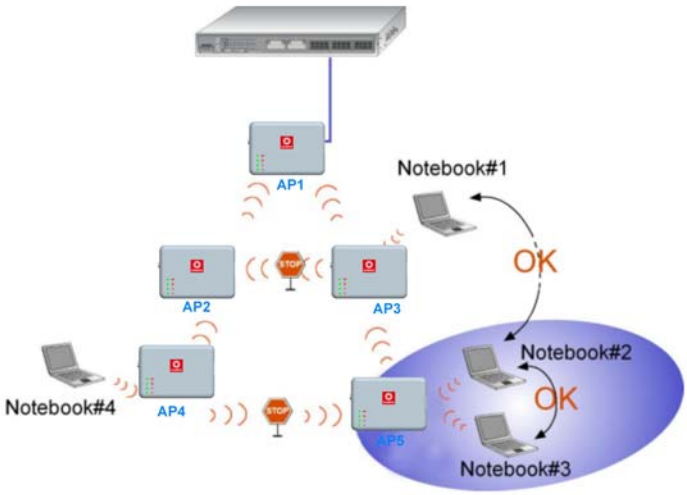

Spanning Tree Protocol (STP) prevents broadcast storms when there are redundant paths in the network. STP creates a tree that spans all devices in an extended network, forcing redundant paths into a standby state, but establishing the redundant links as backup in case the active link should fail. If 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. The path with the smallest cost will be used and extra redundant paths will be disabled.



**<u>Scenario #1</u> – (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.




**<u>Scenario #2</u> – (With STP)**
With STP, extra redundant network paths between access points will be disabled, hence preventing multiple active network paths in between any 2 access points. If one of the access points 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 associated to the access points that are in the same zone.



Step 1:

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

Step 2:

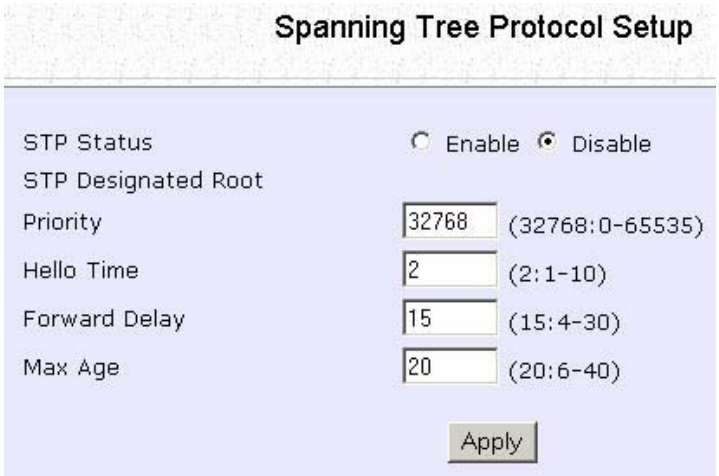
Select the **STP Status Enable** radio button, fill in the fields, and click on the **Apply** button to update the changes.

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.



# 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.

# Add a MAC Address to the MAC Address List

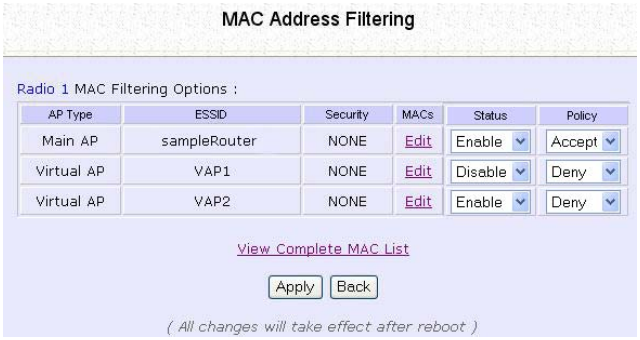
Step 1:

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.

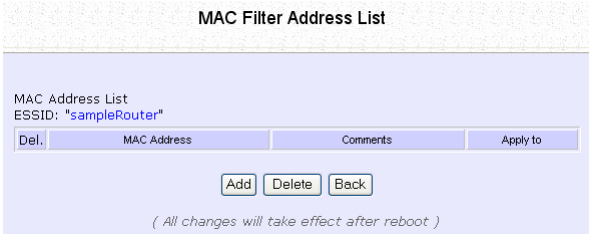
| | |
|---|---|
| Status: Enable / Policy: Accept | MAC Filtering set to **Enable** with Policy to **Accept** only the MAC addresses in the MAC Filter Address List and deny all other MAC addresses. |
| Status: Enable / Policy: Deny | MAC Filtering set to **Enable** with Policy to **Deny** all the MAC addresses in the MAC Filter Address List and accept all other MAC addresses. |
| Status: Disable / Policy: Accept | MAC Filtering set to **Disable**. Whether Policy is set to **Enable** or **Deny** does not matter. |
| Status: Disable / Policy: Deny | MAC Filtering set to **Disable**. Whether Policy is set to **Enable** or **Deny** does not matter. |

Click the **Edit** button.



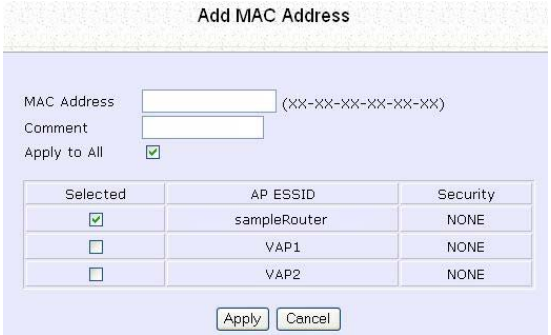
Step 2:

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




Step 3:

The Add MAC Address page displays.

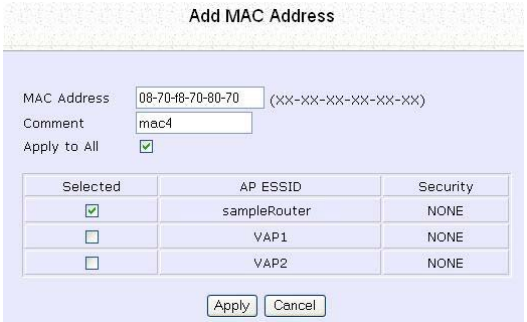



Step 4:

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.



Step 5:

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


**NOTE**

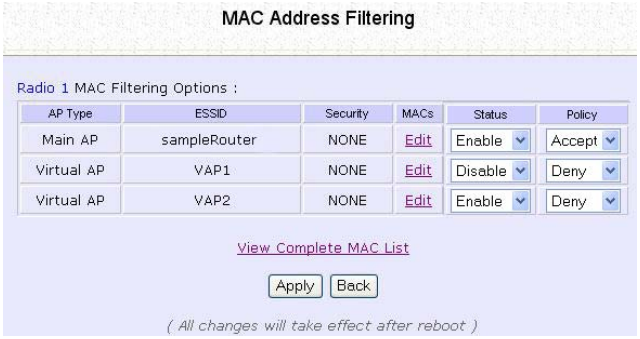
Please reboot to effect all changes and new MAC address entries.

# 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**.



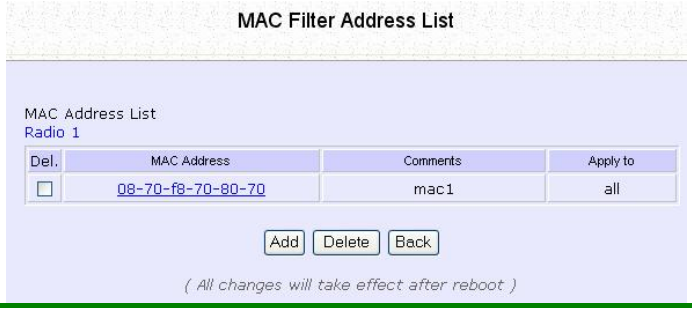

Step 2:

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

Click the **Delete** button.

Step 3:

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

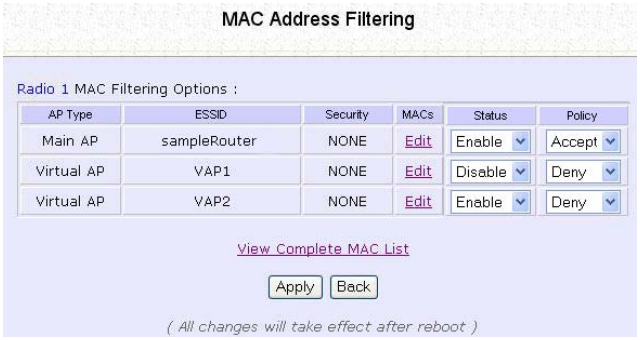


# Delete a MAC Address from Individual Access Point

Step 1:

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

Select **Edit** for the corresponding access point.




Step 2:

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

Click the **Delete** button.

Step 3:

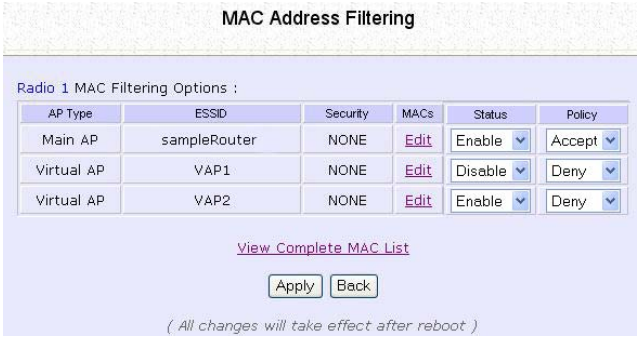
The MAC Filter Address List page displays with updated MAC Address List.

# Edit MAC Address from the MAC Address List

Step 1:

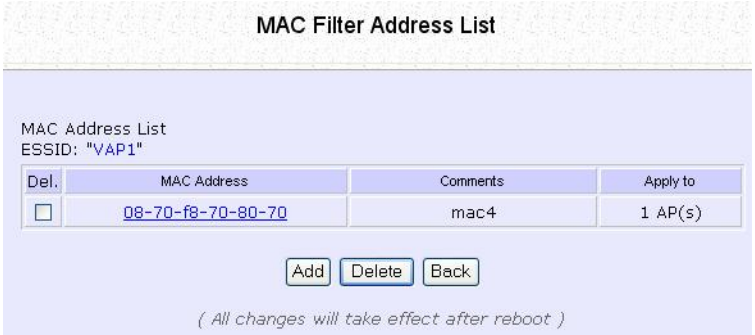
Select **MAC Filtering** from **WLAN Setup**.
The MAC Address Filtering page displays.

Select **Edit**.




Step 2:

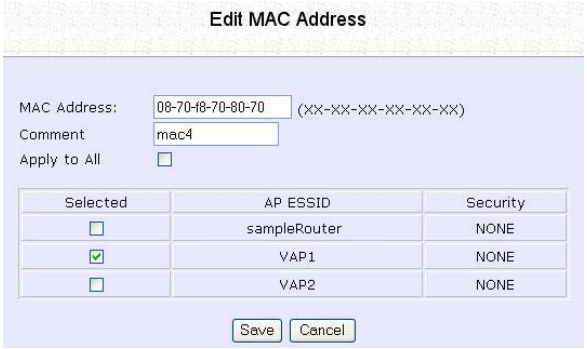
MAC Filter Address List page displays.
Select the MAC address to edit.



Step 3:

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

Click the **Save** button.




Step 4:

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

# Perform Advanced Configuration

## Setup Routing

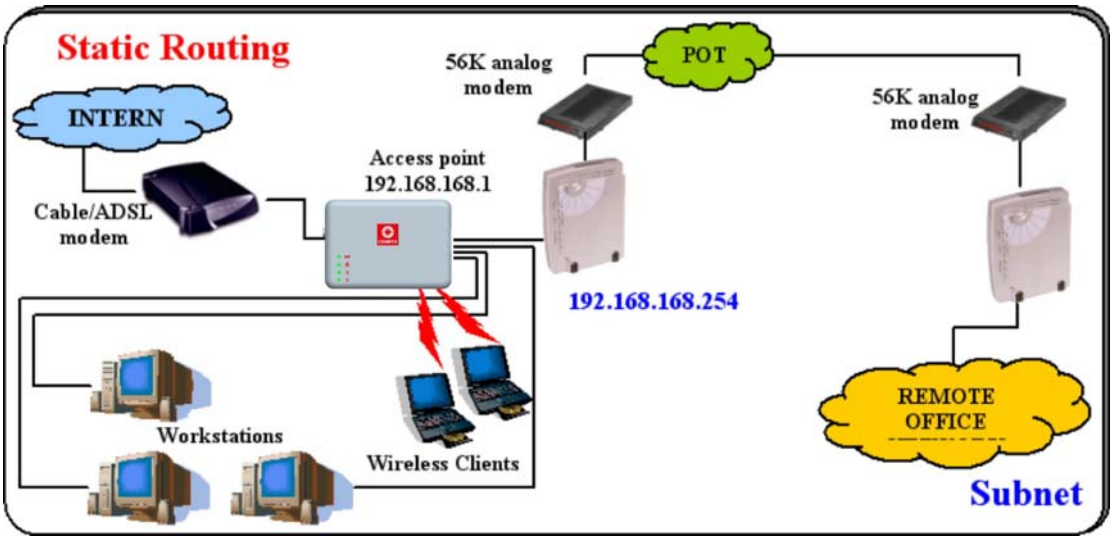
(Available in Wireless Routing Client and Gateway modes)

The access point allows you to add a static routing entry into its routing table to re-route IP packets to another access point. This is useful if your network has 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. The wrong routing configuration might cause the access point to function improperly.

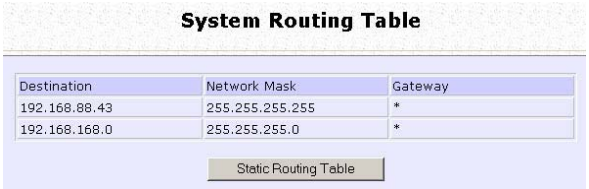
In this network, the main office of subnet 192.168.168.0 contains two routers: the office is connected to the Internet via the access point (192.168.168.1) and to the remote office via 192.168.168.254 The remote office resides on subnet 192.168.100.0

You can add a static routing entry into the access point routing table 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 the router, which acts as the gateway to that subnet.



# Configure Static Routing

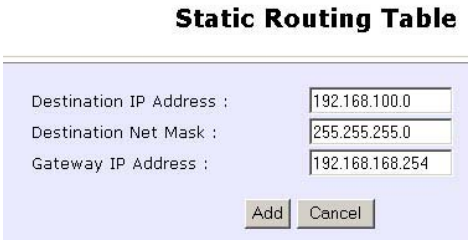
Step 1:
Select **Routing** from the **CONFIGURATION** command menu. The **System Routing Table** page displays. Initially the table contains the default routing entries of the access point.




Step 2:
Click on the **Static Routing Table** button, and then click the **Add** button.


Step 3:
Enter the **Destination IP Address**, **Destination Net Mask**, and **Gateway IP Address**, and click the **Add** button.

The **Static Routing Table** reflects the entry.



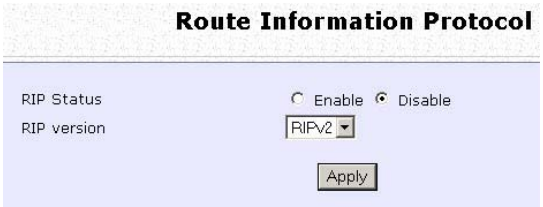

# Use Routing Information Protocol

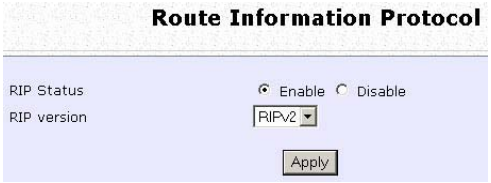
(Available in Wireless Routing Client and Gateway modes)

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**.




Step 2:
Select to **Enable RIP Status**.

Select either RIPv1 or RIPv2.

On this page, click the **Apply** button.

# Use Network Address Translation

(Available in Wireless Routing Client and Gateway modes)

NAT (Network Address Translation) allows multiple PCs in a private network to share a single public IP address by using different TCP ports to identify requests coming from different PCs, and is enabled by default. Computers in the private LAN behind the access point will not be directly accessible from the Internet. However, employing virtual servers allows the hosting of Internet servers by using IP/ Port Forwarding and De-Militarized Zone hosting.

Step 1:
Select **NAT** from the **CONFIGURATION** command menu. To disable it, select the **Disable** radio button.]

Step 2:
Click the **Apply** button to effect the setting.


NOTE

**Important:**
NAT provides for effective broadband Internet sharing; do NOT disable NAT unless it is absolutely necessary.

# Configure Virtual Servers Based on DMZ Host

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

With NAT, the access point keeps track of which client is using which port number and forwards Internet replies to the client according to the port number in the reply packet. Reply packets with unrecognized port numbers are discarded, but with DMZ, these packets are forwarded to the DMZ-enabled PC instead.


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

Step 2:
Click on the **DMZ** button in **Advanced NAT Options**.

Step 3:
Enter the **Private IP Address** of the DMZ host on the **NAT DMZ IP Address** page.

To disable DMZ, enter **0.0.0.0**

Click the **Apply** button.


**NOTE**

1. DMZ may not function properly if the DMZ host IP address is changed due to DHCP, therefore, Static IP Address configuration is recommended for the DMZ host.

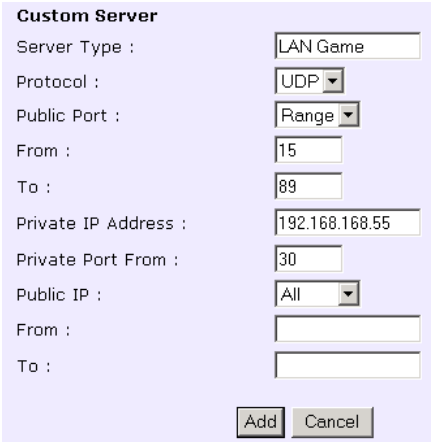
2. Please note that the DMZ host is susceptible to malicious attacks as ALL of its ports are exposed to the Internet.

# Configure Virtual Servers Based on Port Forwarding

| Virtual Server based on Port Forwarding forwards Internet requests arriving at the access point WAN interface to specific PCs in the private network based on their ports. |
|---|
| Step 1:<br>Select **NAT** from the **CONFIGURATION** command menu.<br><br>Step 2:<br>Click the **Port Forwarding** button in **Advanced NAT Options**.<br>  <br> |
| Step 2:<br>Click the **Add** button on the **Port Forward Entries** page.<br>  <br> |

Step 3:

In the **Add Port Forward Entry** page, 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**.

| | | |
|---|---|---|
| **Known Server** | | |
| **Server Type** | : | Select from the drop-down list of known server types:<br>• HTTP<br>• FTP<br>• POP3<br>• Netmeeting |
| **Private IP Address** | : | Specify the LAN IP address of the server PC running within the private network. |
| **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. |
| **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 the 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. |

For example to set up a web server on a PC with IP address 192.168.168.55, set the **Server Type** as HTTP and set the **Private IP Address** as **192.168.168.55**, then click on the **Add** button.

**Port Forward Entries**

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

Add Back

# Configure Virtual Servers based on IP Forwarding

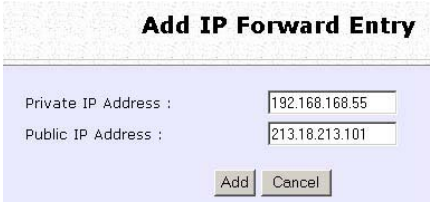
If you are subscribed to more than one IP address from your ISP, virtual servers based on IP forwarding can forward all Internet requests regardless of the port number to defined computers in the private network.


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

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.




**NOTE**
Please ensure that you are subscribed to the **Public IP Address** you intend to forward from.

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


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

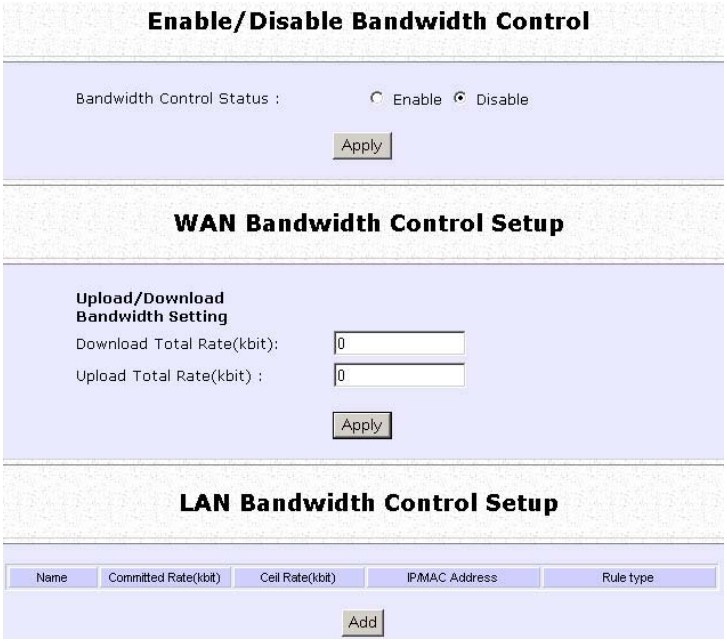
# Control the Bandwidth Available

(Available in Wireless Routing Client and Gateway modes)

Keep in control of your LAN network in router operation. Bandwidth access to the Internet on both the wireless LAN connection in Gateway mode and the Ethernet connection in Wireless Routing Client Mode can be managed.

## Enable Bandwidth Control

Step 1:
Select **Bandwidth Control** from the **CONFIGURATION** command menu.




Step 2:
**Bandwidth Control** is disabled by default, select **Enable**, and click the **Apply** button.

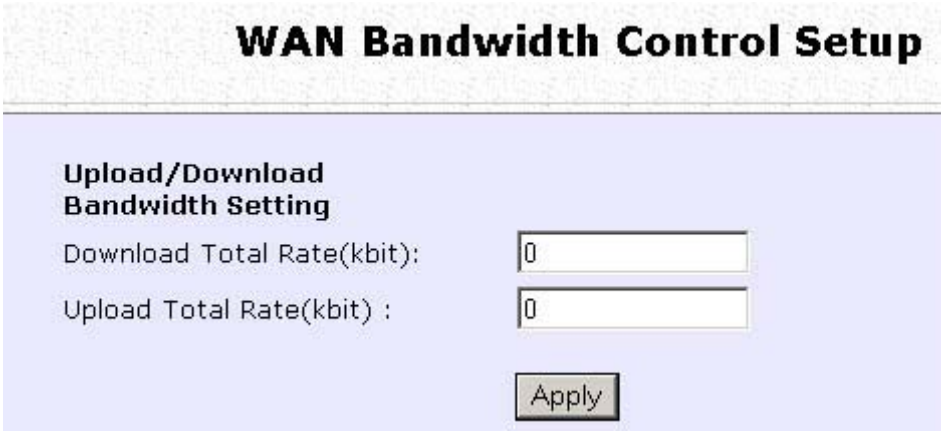
# Configure WAN Bandwidth Control

The **Upload / Download Bandwidth Setting** can limit throughput to the defined rates regardless of the number of connections.

Step 1:
Select **WAN Bandwidth Control Setup** from the **Bandwidth Control** sub-menu from the **CONFIGURATION** command menu.

Step 2:
Enter the **Download Total Rate** and **Upload Total Rate**.
The default values are 0, which indicates that there is no bandwidth limit.

Click the **Apply** button.



# Configure LAN Bandwidth Control

**Bandwidth Control** can also limit LAN users' throughput.

Step 1:
Select **LAN Bandwidth Control Setup** from the **Bandwidth Control** sub-menu from the **CONFIGURATION** command menu.

Step 2:
Click the **Add** button to create the bandwidth rule for LAN user.