Wireless Access Point

networks@work

USER'S MANUAL

Wireless Classic

802.11a/b/g

RoHS compliant

Trademark Information

Compex® is a registered trademark of Compex, Inc. Microsoft Windows and the Windows logo are the trademarks of Microsoft Corp. NetWare is the registered trademark of Novell Inc. WMM and WPA are the registered trademarks of Wi-Fi Alliance. All other brand and product names are trademarks or registered trademarks of their respective owners.

Manual Revision by wentao
Version 1.23c May 2010

Disclaimer

Compex, Inc. provides this manual without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Compex, Inc. may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Compex, Inc will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

FCC NOTICE

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this device does cause harmful interference to radio or television reception, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Connect the computer into an outlet on a circuit different from that to which the receiver is connected.
- Increase the separation between the computer and receiver.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

FCC Compliance Statement: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
This device may not cause harmful interference, and
This device must accept any interference received, including interference that may cause undesired operation.

RF Exposure warning
The equipment complies with FCC RF exposure limits set forth for an uncontrolled environment.
The equipment must not be co-located or operating in conjunction with any other antenna or transmitter.

ICES 003 Statement
This Class B digital apparatus complies with Canadian ICES-003.

Declaration of Conformity

Compex, Inc. declares the following:
Product Name: Wireless Access Point with PoE
Model No.: WP543 conforms to the following Product Standards:
This device complies with the Electromagnetic Compatibility Directive (89/336/EEC) issued by the Commission of the European Community. Compliance with this directive implies conformity to the following European Norms (in brackets are the equivalent international standards.)
Electromagnetic Interference (Conduction and Radiation): EN 55022 (CISPR 22)
Electromagnetic Immunity: EN 55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11)
Low Voltage Directive: EN 60 950: 1992+A1: 1993+A2: 1993+A3: 1995+A4: 1996+A11: 1997.
Therefore, this product is in conformity with the following regional standards: **FCC Class B:** following the provisions of FCC Part 15 directive, **CE Mark:** following the provisions of the EC directive.

Compex, Inc. also declares that:
The wireless card in this product complies with the R&TTE Directive (1999/5/EC) issued by the Commission of the European Community. Compliance with this directive implies conformity to the following:
EMC Standards: FCC: 47 CFR Part 15, Subpart B, 47 CFR Part 15, Subpart C (Section 15.247); CE: EN 300 328-2, EN 300 826 (EN 301 489-17)
Therefore, this product is in conformity with the following regional standards: **FCC Class B**: following the provisions of FCC Part 15 directive, **CE Mark:** following the provisions of the EC directive.

Firmware

This manual is written based on Firmware version 1

Table of Contents

Overview the Product

Introduction

The high-performance Wireless Network Access Point (AP) is designed for enterprise and public access applications. Embedded with the Atheros chipset, it boasts network robustness, stability and wider network coverage. Based on 802.11, the access point supports high-speed data transmission of up to 54Mbps.

The access point is capable of operating in different modes, which makes it suitable for a wide variety of wireless applications, including long-distance deployments.

Designed with two externals SMA connector offering excellent electrical performance and compatible with SMA antennas, the access point can be used for a wide variety of wireless applications and allows you to position the wireless antenna in a better signal-broadcasting location for improved wireless coverage and signal strength or simply in a more convenient location.

Moreover, its integrated Power over Ethernet (PoE) allows the access point to be used in areas where power outlets are not readily available.

To protect your security and privacy, the access point is armed with many enhanced wireless security features such as WPA, WPA2 (with Advanced Encryption Standard encryption) MAC Address Filtering, IEEE 802.1x Authentication and 64/128-bit WEP (Wired Equivalent Privacy) to ensure privacy for the heterogeneous mix of users within the same wireless network.

The access point also incorporates a unique set of advanced features such as: Virtual AP to deliver multiple services; Long-Range parameter fine-tuning which provide the access point with the ability to auto-calculate parameters such as slot time, ACK time-out and CTS time-out to achieve a longer range.

Depending on the model, some model will have less hardware features. All the software functions are the same.

Features and Benefits

- **Point-to-Point & Point-to-MultiPoint Support**
  Point-to-Point and Point-to-MultiPoint communication between different buildings enables you to bridge wireless clients that are kilometres apart while unifying the networks.

- **Virtual AP (Multiple SSID)**
  Virtual AP implements mSSID (Multi-SSID)
  This allows a single wireless card to be set up with multiple virtual AP connections with different SSIDs or BSSID (Basic Service Set Identifier) and security modes.

- **Highly Secured Wireless Network**
  The access point supports the highest available wireless security standard: WPA2. WPA2 has two different modes: WPA2-Personal for SOHO users and WPA2-Enterprise for Enterprise users. The access point also supports IEEE 802.1x for secure and centralized user-based authentication. Wireless clients are thus required to authenticate through highly secure methods like EAP-TLS, EAP-TTLS, and EAP-PEAP, in order to obtain access to the network.

- **Smart Select**
  This feature will automatically scan and recommend the best channel that the access point can utilize.

- **uConfig Utility**
  The exclusive **uConfig** utility allows users to access the user-friendly Web configuration interface of the access point without having to change the TCP/IP setup of the workstation.

- **STP**

  Spanning-Tree Protocol provides path redundancy while preventing undesirable loops in the network. It forces certain redundant data paths into a standby (blocked) state. If one network segment in the Spanning-Tree Protocol becomes unreachable, or if Spanning-Tree Protocol costs change, the spanning-tree algorithm reconfigures the spanning-tree topology and re-establishes the link by activating the standby path.

- **HTTPS**

  The access point supports HTTPS (SSL) in addition to the standard HTTP.

  HTTPS (SSL) features additional authentication and encryption for secure communication.

- **Telnet**

  Telnet allows a computer to remotely connect to the access point CLI (Command Line Interface) for control and monitoring.

- **SSH**

  SSH (Secure Shell Host) establishes a secure host connection to the access point CLI for control and monitoring.

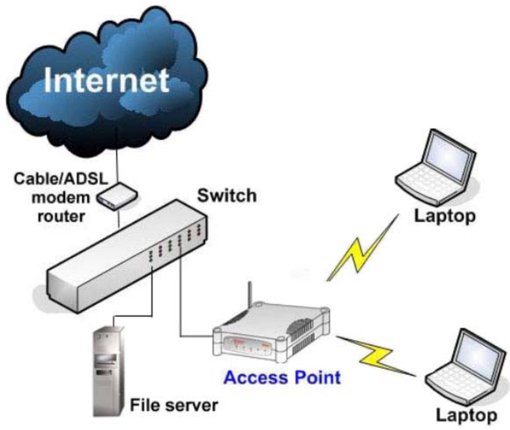
- **WDS2**

  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.

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.



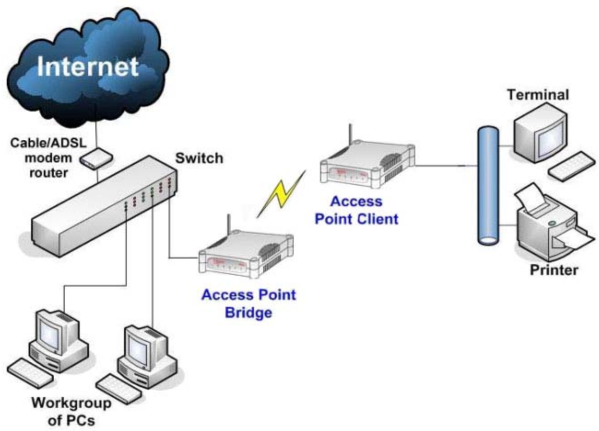
Access Point Client Mode

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.

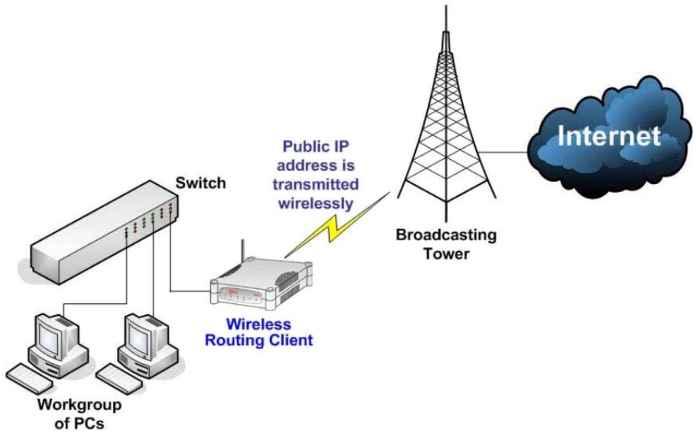
In this example the workgroup PCs can access the printer connected to the access point in Access Point Client Mode.

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.



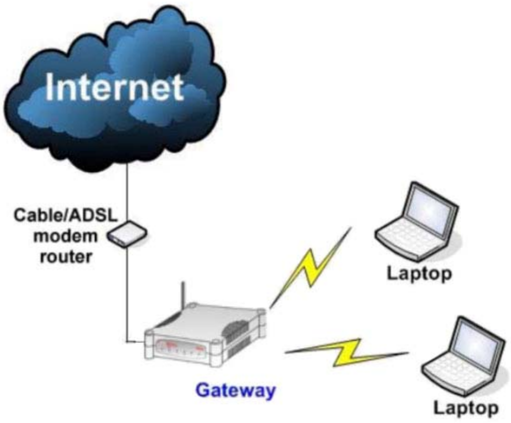
Wireless Routing Client Mode

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

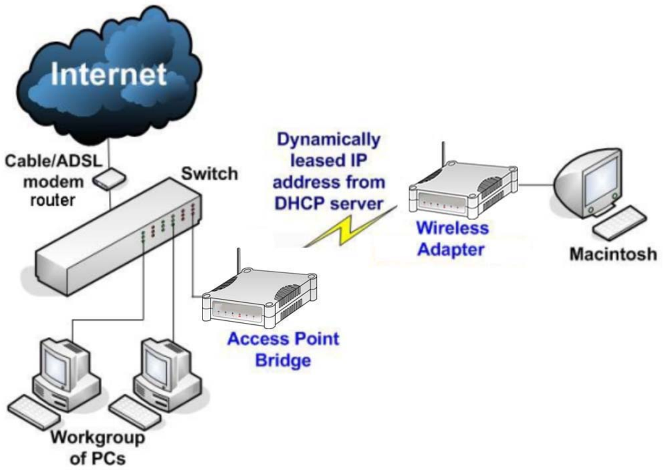
PPTP
Use PPTP if you are using ADSL services in a country utilizing PPTP connection and authentication.

Layer Two Tunneling Protocol (L2TP)
L2TP enables ISPs to operate Virtual Private Networks (VPNs)

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.

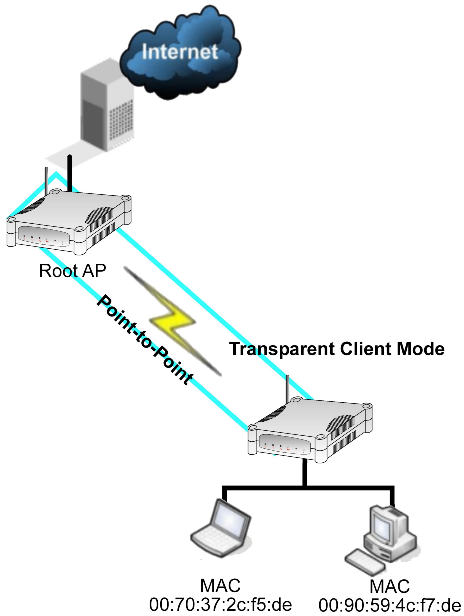


Transparent Client Mode

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.

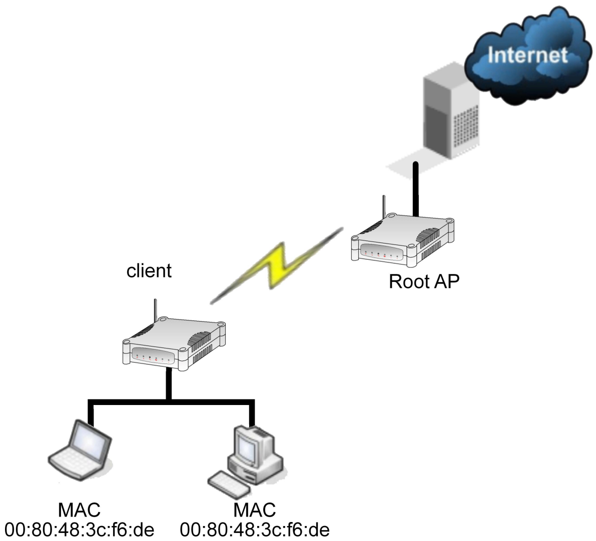
This mode is generally used for outdoor connections over long distances, or for indoor connections between local networks.



- 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 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.

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.

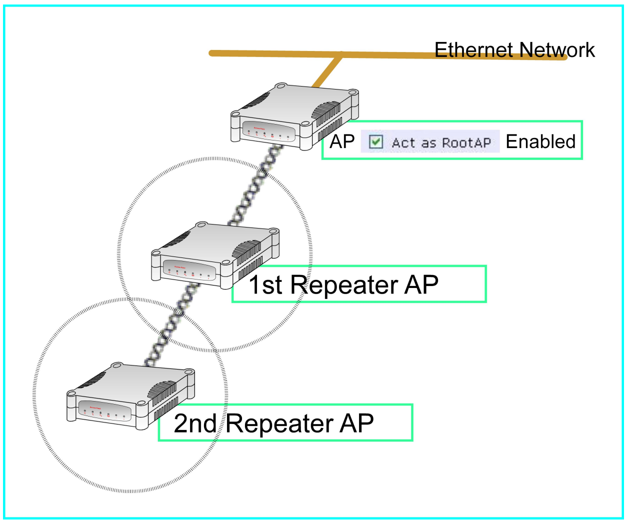


Repeater Mode

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.

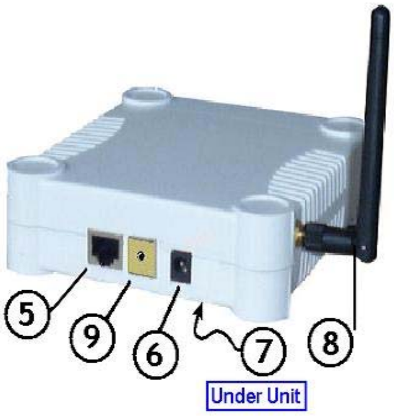
In Repeater Mode, the access point acts as a relay for network signals on the network by regenerating the signals it receives, and retransmitting them to extend the range of the existing network infrastructure.

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



Panel Views and Description

Figure1: Front Panel Light Indicator **Figure2: Back Panel View**



	Features	Status and Indications
1	**Power LED**	Static Light: Power is being supplied to the device. Off: Power is not being supplied to the device.
2	**Diagnostic LED**	Flashing Light: This indicateds the flash during power-up and will go off after the diagnostic is passed.
3	**WAN Link/Act LED**	Steady Light: WAN connection is established.
4, 5	**WLAN Link/Act LED**	Steady Light: Wireless interface running and ready for operation. Flashing Light: Wireless network is active.
6	**Ethernet Port LED**	Steady Light: Connection has been established between the device and the network. Flash Light: network is active. Off: No network connection.
7	**Ethernet and PoE Port**	10/100Mbps Ethernet port Passive PoE : 24V~48V 802.11af PoE : 48V~56V
8	**DC Jack**	For power input. 24V – 48V DC.
9	**Reset Button**	• To reboot, press once. • To reset password, press and hold the button for 5 seconds before releasing it. • To restore the factory default settings, press and hold the button for 8 seconds before releasing it.
10	**Antenna**	External SMA Antenna. For antenna mode setup, please refer to the “Antenna Mode Setup” section in the user manual.

Install the Hardware

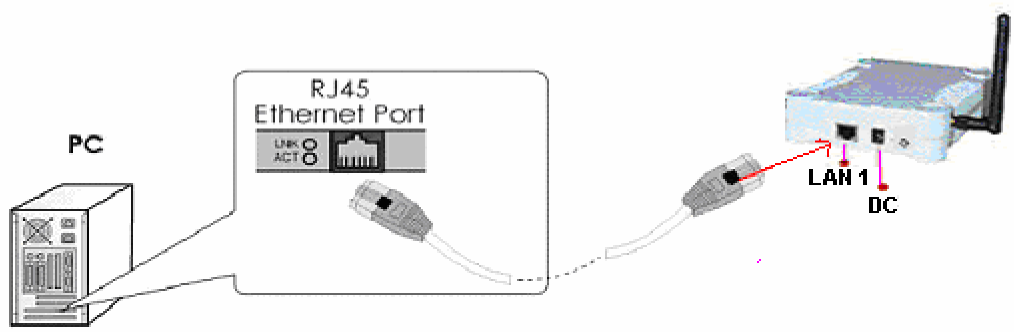
Setup Requirements

- 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

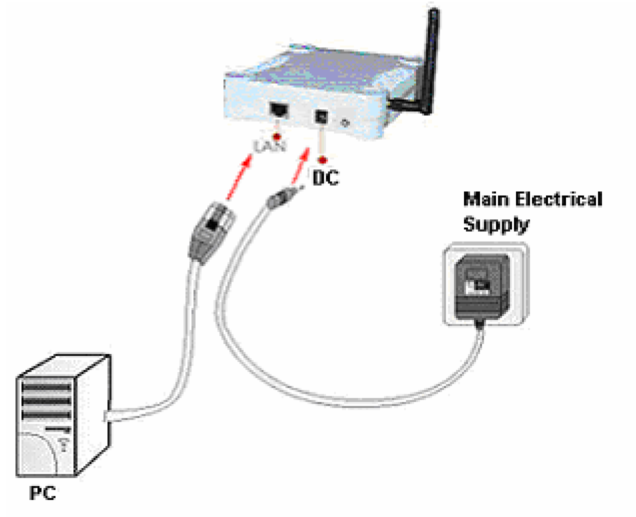
Step 1:

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 2:

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



Step 3:

Turn ON the power supply and power ON your PC. Notice that the LEDs: Power and Port have lighted up. This indicates that connection has been established successfully between your access point and your PC.

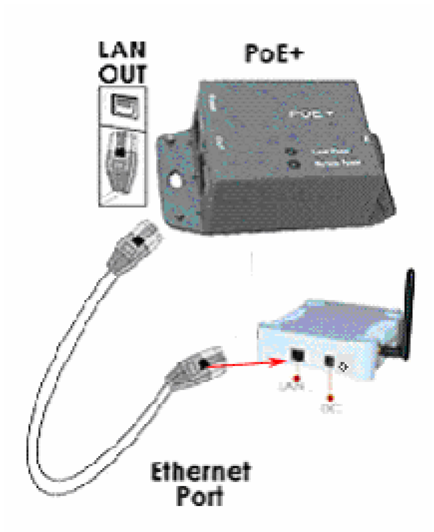
Using PoE+ to supply power to the unit

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

Users who have already purchased PoE+ and who wish to use it to supply power to the access point may follow the installation procedures shown below:

Step 1:

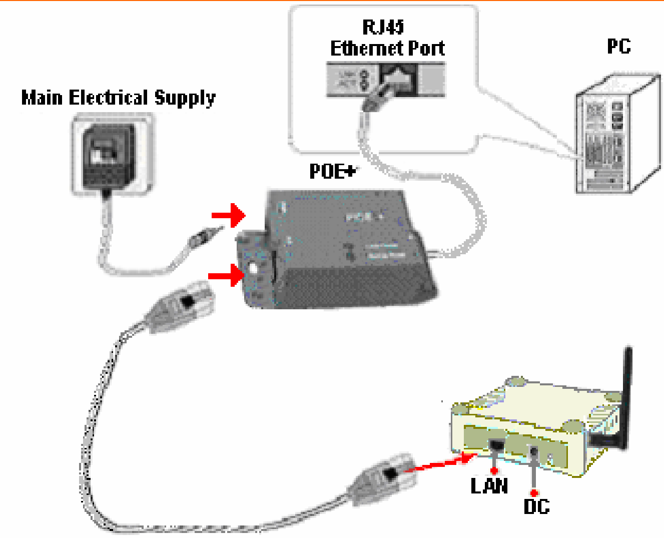
Use an RJ45 Ethernet cable to connect one end of the cable to the LAN OUT port of PoE+ and the other end to Ethernet port of the access point.



Step 2:

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

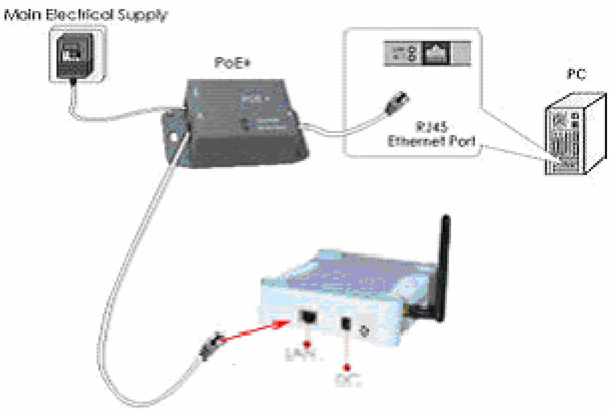
Once you have finished configuring your access point, you can connect the PoE+'s RJ45 Ethernet cable to your network device, such as to a switch or hub.



Step 3:

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

Note:
The voltage and current supplied to the power adapter and the PoE+ power adapter are different. Do not interchange the power adapters.



Step 4:

Turn on your power supply. Notice that the **Power** LED has lighted up. This indicates that the access point is receiving power through PoE+. Notice also that the corresponding port LEDs have lighted up. This indicates that connection between your access point and your PC has been established.

Configure the IP Address

After setting up the hardware you need to assign an IP address to your PC so that it is in the same subnet as the access point.

For Windows 95/98/98SE/ME/NT

Step 1:

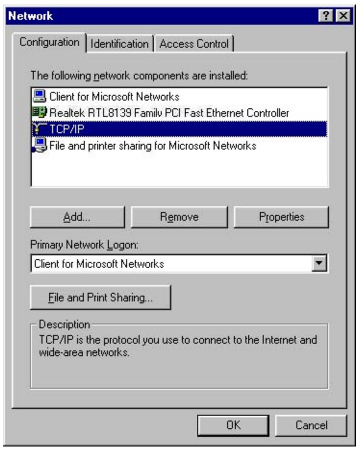
From your desktop, right-click the **Network Neighborhood** icon and select **Properties**.

Step 2:

Select the network adapter that you are using, then right-click and select **Properties**.

Step 3:

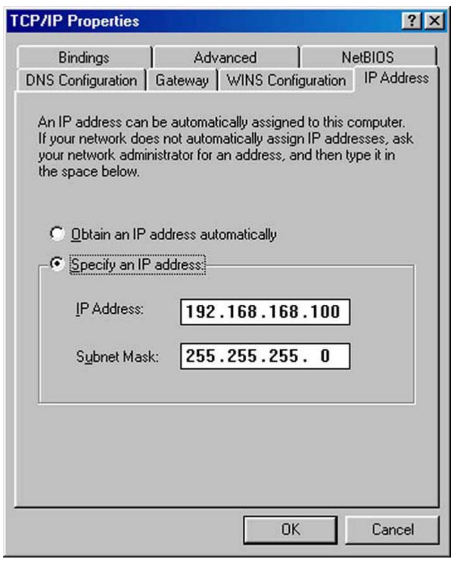
Highlight **TCP/IP** and click on the **Properties** button.



Step 4:

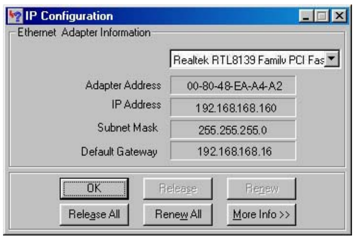
Select the **Specify an IP address** radio button.

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:

To verify that the IP address has been correctly assigned to your PC, go to the **Start** menu, select **Run**, and enter the command: *winipcfg*.



Select the Ethernet adapter from the drop-down list and click **OK**.

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

For Windows XP/2000

Step 1:

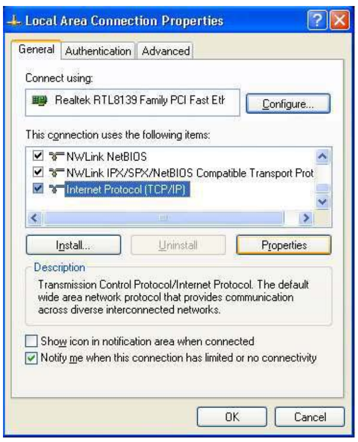
Go to your desktop, right-click on the **My Network Places** icon and select **Properties**.

Step 2:

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

Step 3:

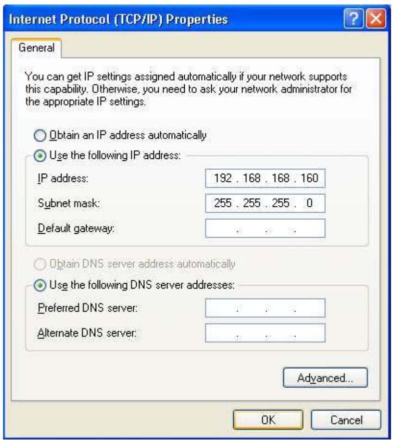
Highlight **Internet Protocol (TCP/IP)** and click on the **Properties** button.



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.

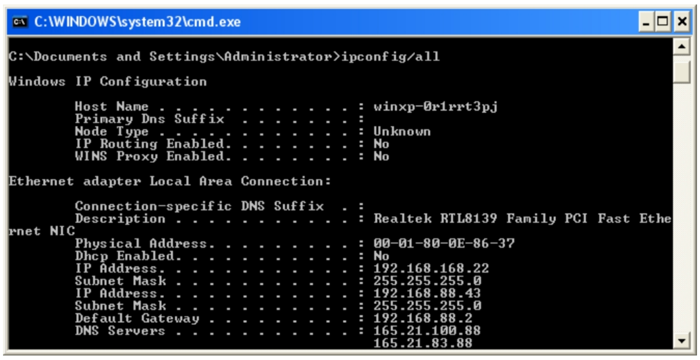


Step 5:

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

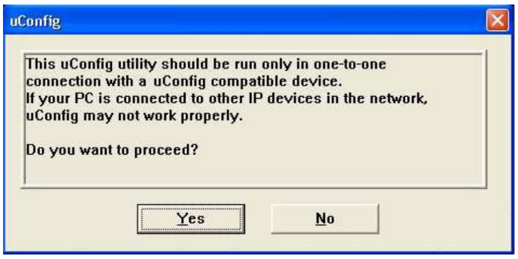
The UConfig utility provides direct access to the web interface. This utility can be downloaded from our website at www.compex.com.sg

Step 1:

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

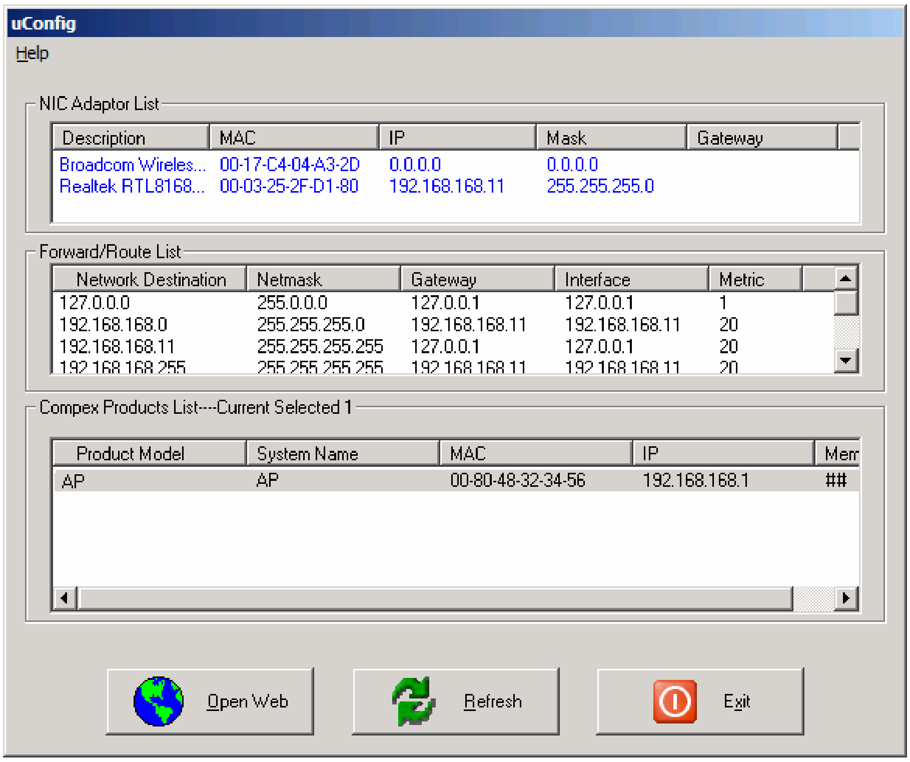
Step 2:

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



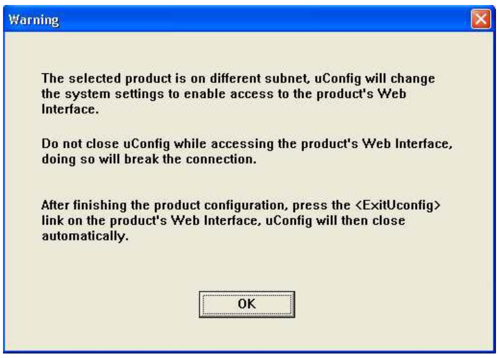
Step 3:

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.



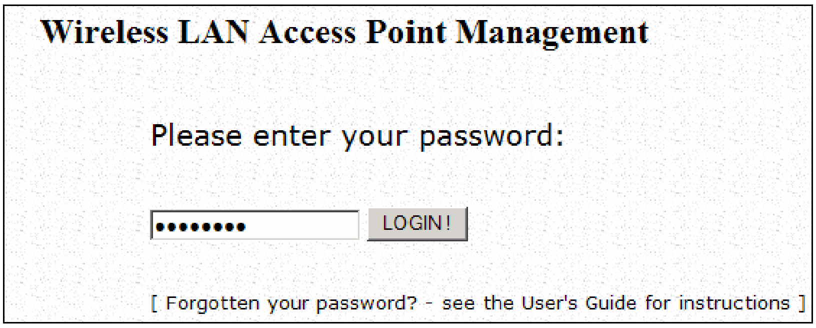
Step 4:

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.



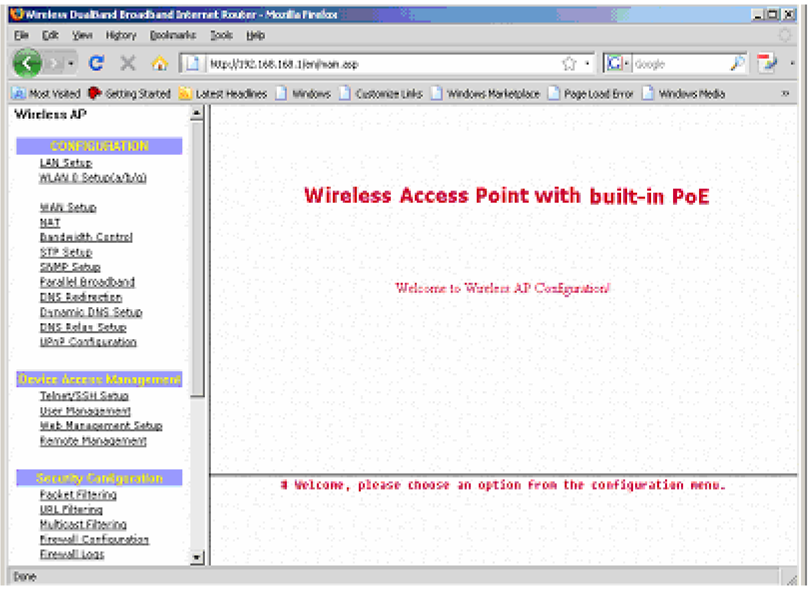
Step 5:

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



Step 6:

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



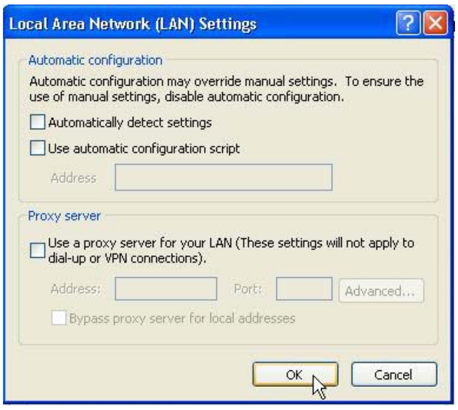
Manual access with Internet Explorer

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.



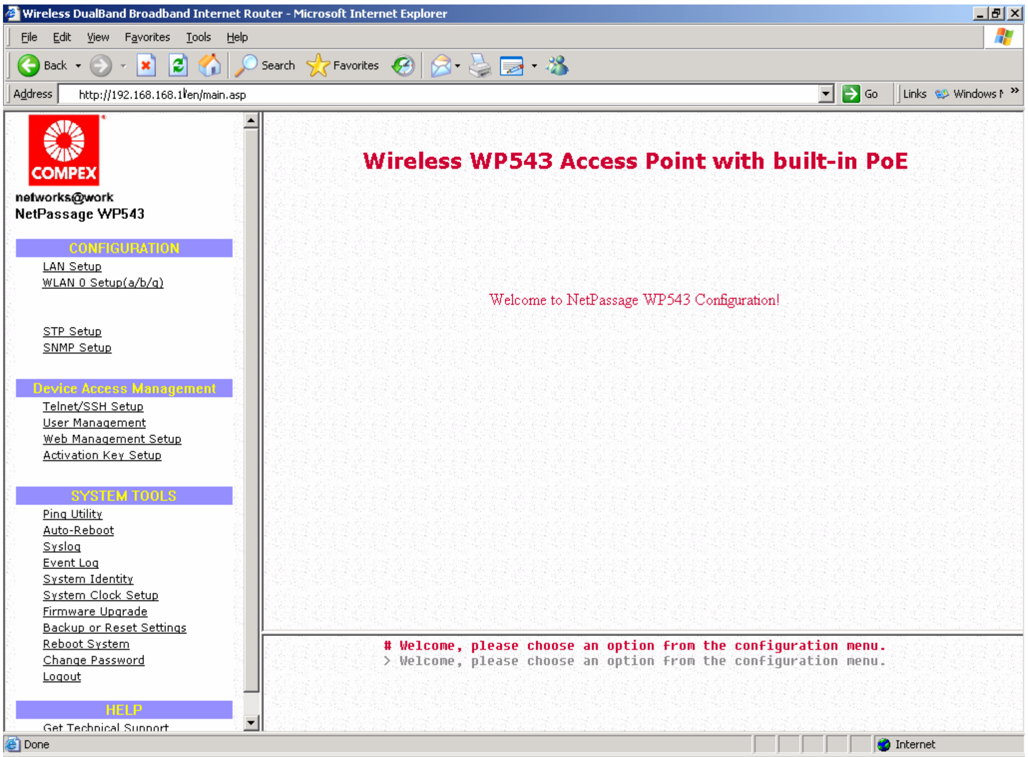
Step 3:

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.

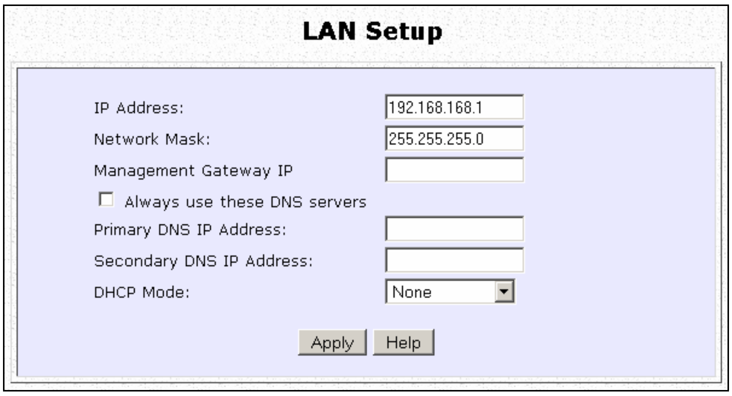
You will then reach the home page of the access point web interface.



Perform Basic Configuration

LAN Setup

You will note that **192.168.168.1** is the default IP address assigned to the router, with a **Network Mask** of 255.255.255.0. You may leave them as they are. (The router's subnet is 192.168.168.0)



The following table lists out the parameters relevant to your LAN setup. You can replace the default settings with appropriate values to suit the needs of your LAN.

LAN Parameters	Description
IP Address	The IP address of your router is set by default to 192.168.168.1.
Network Mask	The Network Mask serves to identify the subnet in which your router resides. The default network mask is 255.255.255.0.
Management Gateway IP	(Optional) As a bridge Access Point, the access point does not usually communicate with devices on other IP subnets. However, the Gateway 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 Management Gateway IP field. The Management Gateway IP address of your access point is set to nil by default.
Always use these DNS servers	Enable this checkbox if you want the router to only use the DNS server you have specified below.
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.

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 **LAN 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.

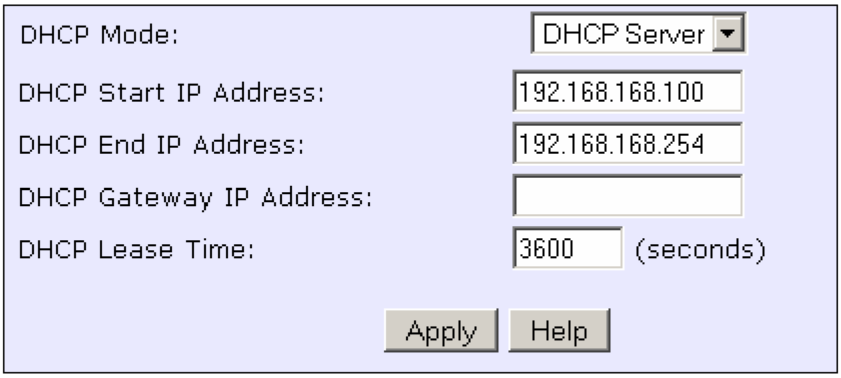
Step 1:

Click on **LAN 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. 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.

The following will guide you to setup the DHCP Relay.

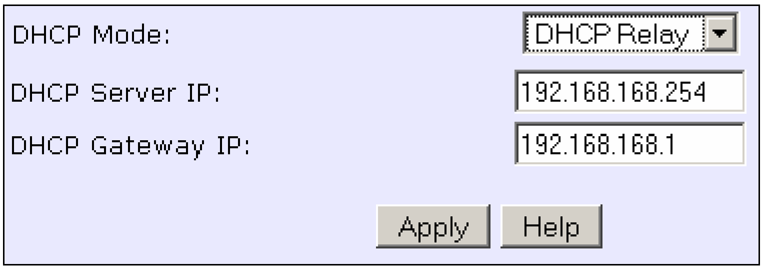
Step 1:

Click on **LAN 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. 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.

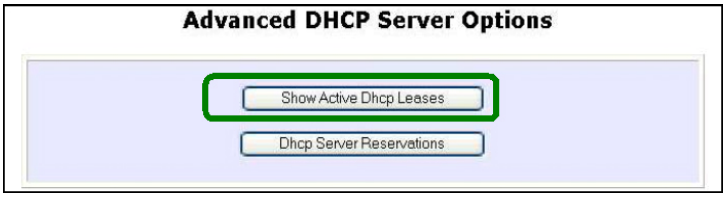
View Active DHCP Leases

Step 1:

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

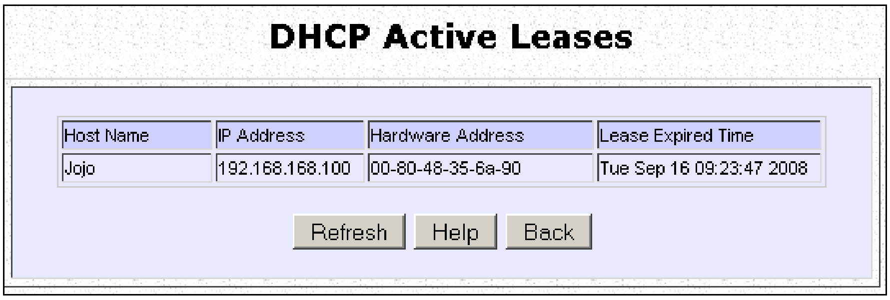
Step 2:

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.**


DHCP Active Leases

Host Name	IP Address	Hardware Address	Lease Expired Time
Jojo	192.168.168.100	00-80-48-35-6a-90	Tue Sep 16 09:23:47 2008

Refresh Help Back

NOTE

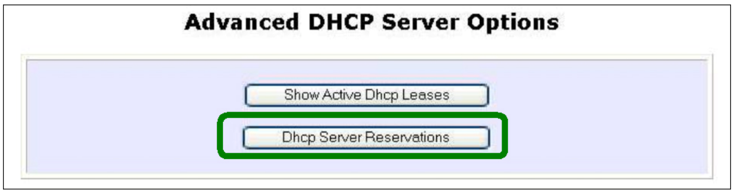
Invalid date and time displayed in the **Lease Expired Time** column indicates that the clock of the access point has not been set properly.

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.



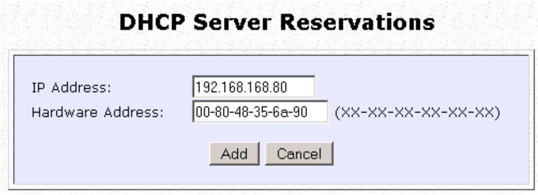
Step 2:

Click on the **Add** button.

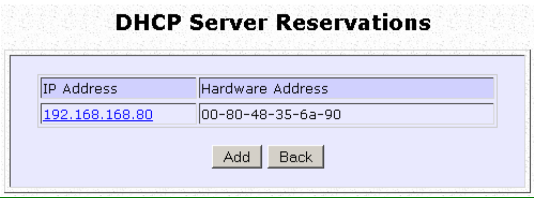
Step 3:

Fill in:
Type in the **IP Address** to be reserved.
The **Hardware Address**, in pairs of two hexadecimal values.

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



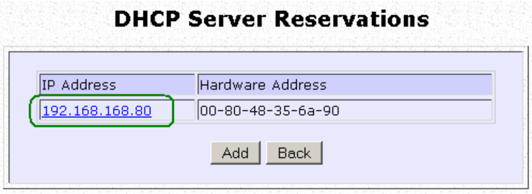
The **DHCP Server Reservations** page refreshes to display the currently reserved IP addresses.



Delete DHCP Server Reservation

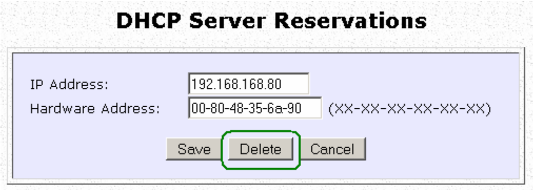
Step 1:

Select the reserved IP address to delete.



Step 2:

Click on the **Delete** button.



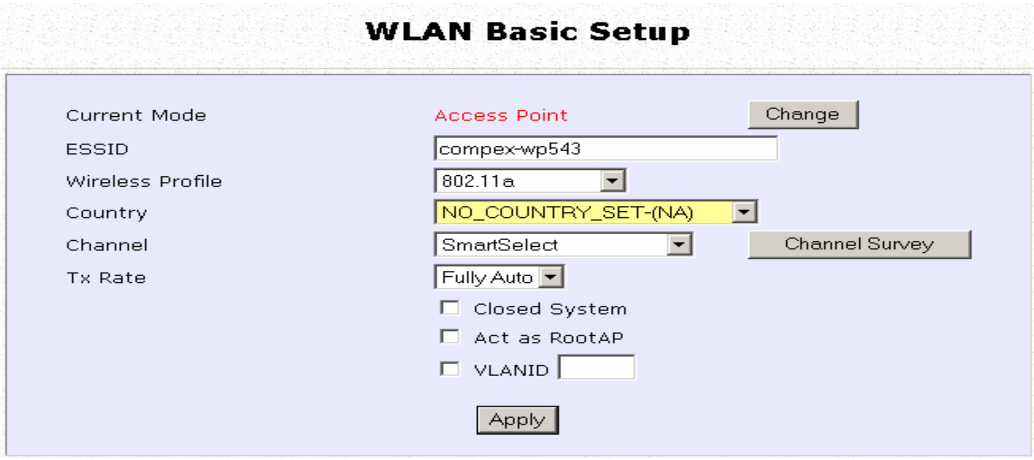
The **DHCP Server Reservations** table refreshes to display your changes.

Setup WLAN

Configure the Basic Setup of the Wireless Mode

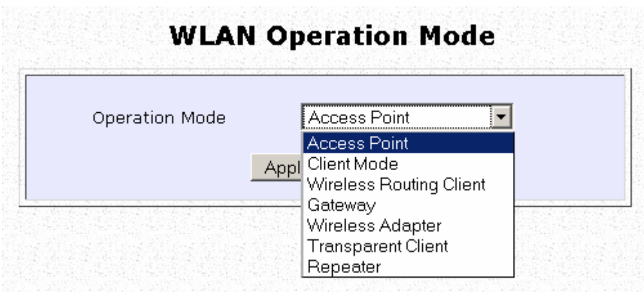
Step 1:

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)

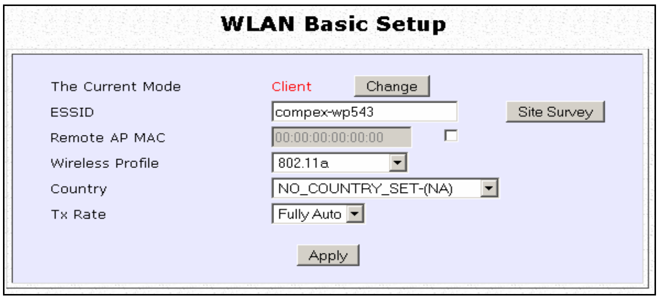
To change the current mode of the access point click on **Change**, select the **Operation Mode**, and click on the **Apply** button to access the setup page of the selected mode. You will be prompted to reboot the access point to effect the mode setting.



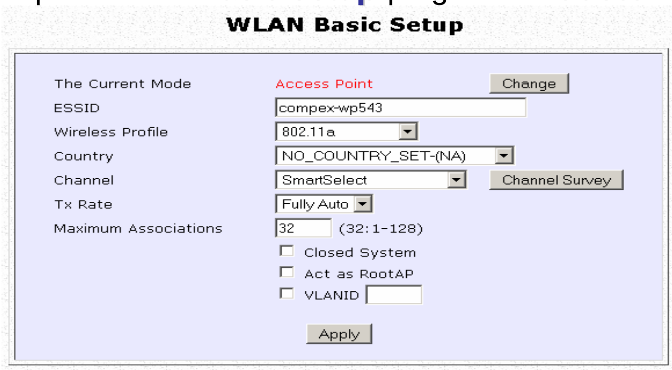
Step 3:
Enter the parameters in their respective fields, click on the **Apply** button and reboot your device to let your changes take effect.

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**



*** Note: For antenna mode setup, please refer to the "Antenna Mode Setup" section in the user manual.**

WLAN Basic Setup page Parameters	Description
The Current Mode	The default operating mode is the **Access Point** mode. Operating modes: • Access point • Client Mode • Wireless Routing Client • Gateway • Wireless Adapter • Transparent Client • Repeater You can toggle the modes by clicking on the **Change** button.
ESSID	ESSID is a connection name this device will broadcast for wireless client to connect. The minimum length is 1 character and maximum length is 32 characters. * Note: In Repeater mode, this name is automatically set to be the same as Remote ESSID.
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. This feature is supported by the Access Point Client, Wireless Routing Client, Wireless Adapter, Transparent Client and Repeater.
Wireless Profile	A selection of network environment types in which to operate the access point: • **802.11a only (Version AG)** Supports wireless A clients with data rates of up to 54Mbps in the frequency range of 5.4GHz. • **802.11b only** Supports wireless B clients with data rates of up to 11Mbps in the frequency range of 2.4GHz. • **802.11b/g mixed** Supports both wireless B and G clients. • **802.11g only** Supports wireless-G clients that offer transmission rates of up to 54Mbps in the 2.4GHz frequency band.

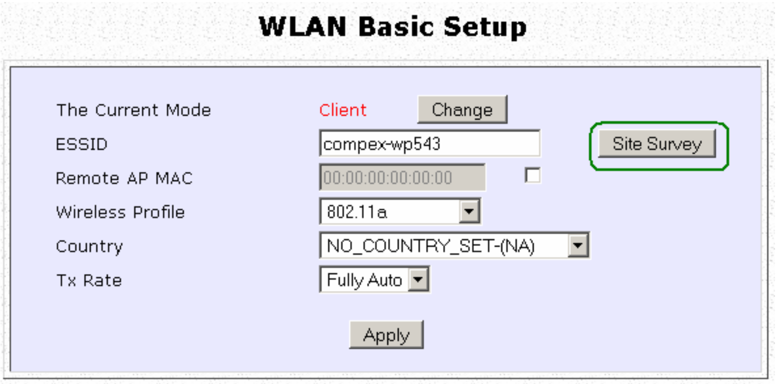
Country	Choose the **Country** where you are located.
Channel	This option allows you to select a frequency channel for the wireless communication. Default is SmartSelect. It automatically scan and set to the best channel to use during initial device power up. To use a specific channel, click the down arrow at the side-bar for a list of available channels. Just click on the channel number to select. * Note: Different country has different channel list. You should first select the conntry before select the channel.
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	If device setup as access point (AP), You need to check this option before AP can communicate with another device. Running Repeater or Transparent Client. This option does not affect standard or normal PC wireless client.
VLAN ID	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.
Channel Survey	A list of channels that are detected by your access point in the WLAN. Information such as frequency, channel, MyQuality, APCount, NeighQuality and Recommendation can be found in the listing. 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:

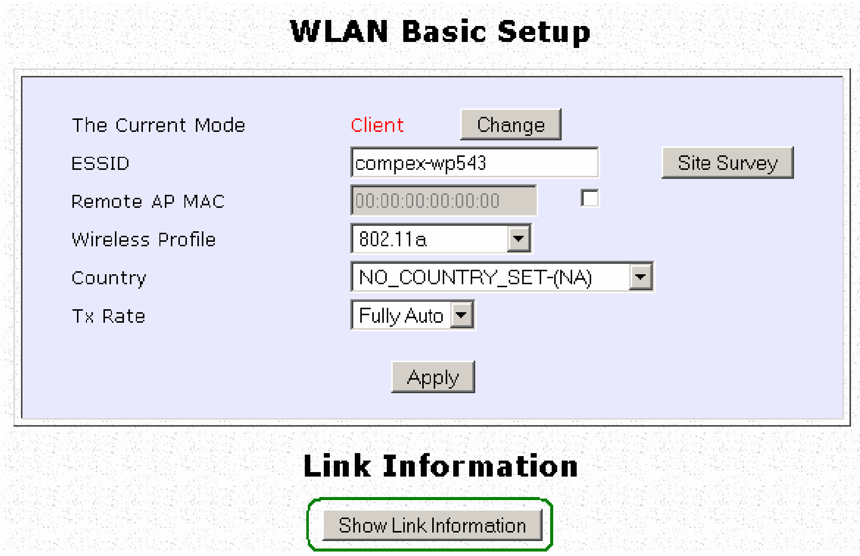
Click on the **Refresh** button to update the screen.

Read-Only Parameters of Neighbouring Access Points Viewable from Site Survey page	Description
Bssid	Wireless MAC address of the access point in an 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.

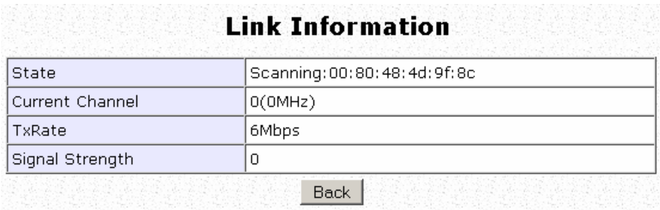
View Link Information

(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:



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.

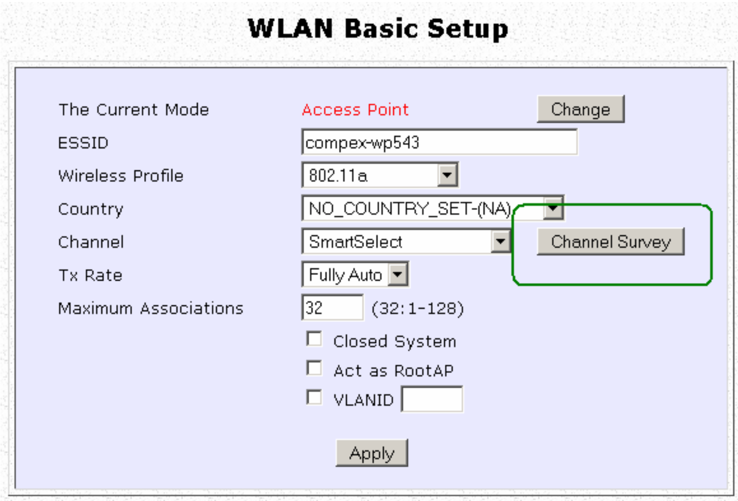
Scan for Channel Survey

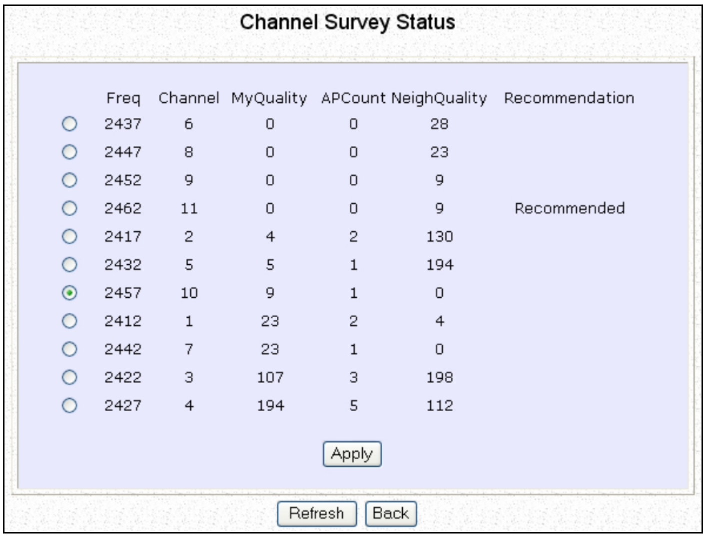
(Available in Access Point and Gateway modes)

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.





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.

Configure the Advanced Setup of the Wireless Mode

Step 1:

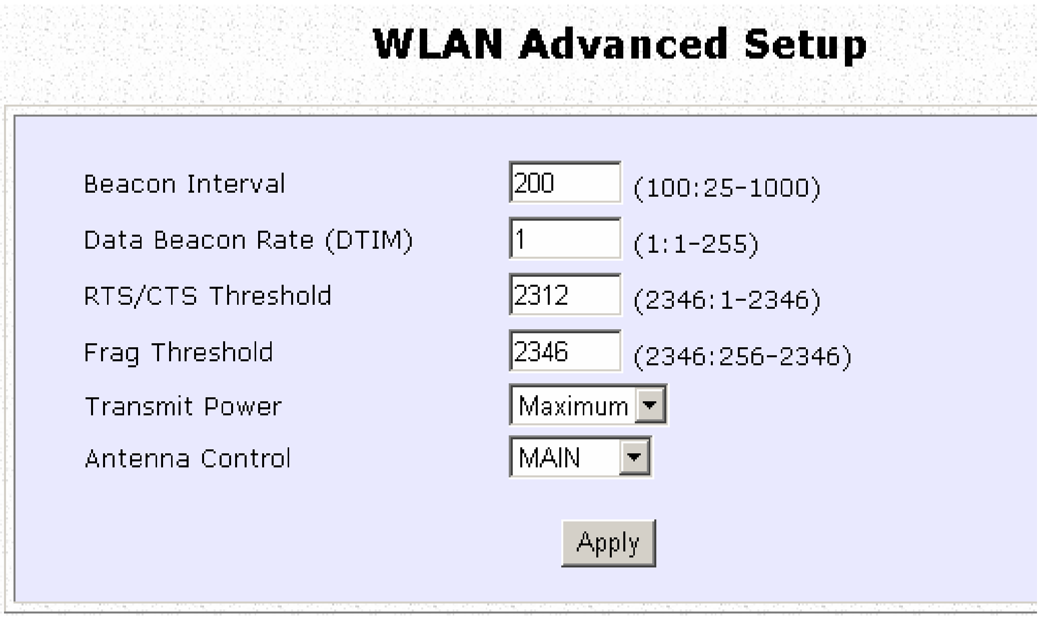
Select **WLAN Setup** from the **CONFIGURATION** menu to expand four sub-menus. From here, select **Advanced**.

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. 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. This value extends from 1 to 2312 bytes.
Frag Threshold	Maximum size that a packet can reach without being fragmented, represented in bytes. 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.
Antenna Control	Drop-down list of antenna mode selection. There are three modes available to choose: Main; AUX; and Auto.

NOTE

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

Antenna Mode Setup

Step 1:

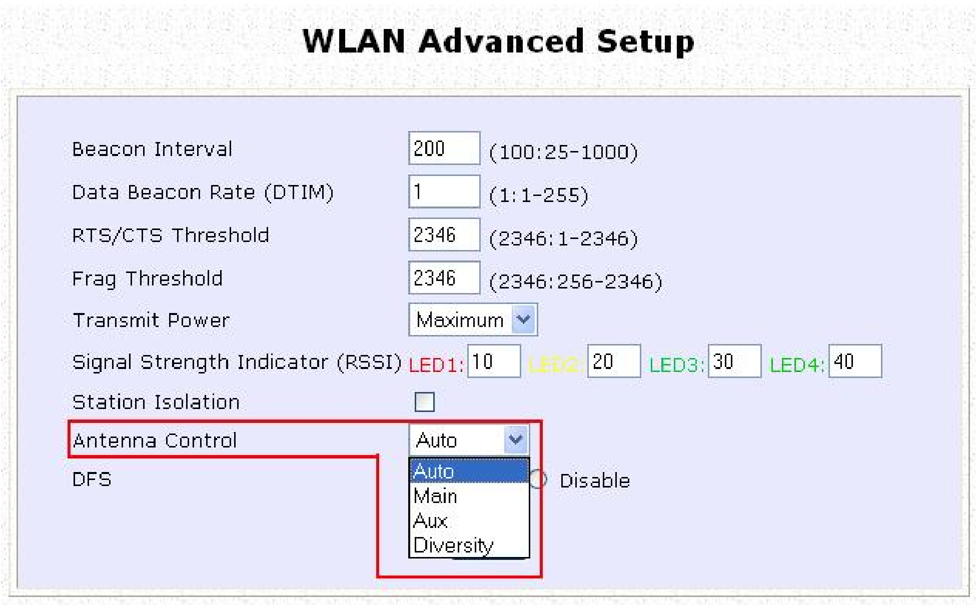
Select **WLAN Setup** from the **CONFIGURATION** menu to expand four sub-menus. From here, select **Advanced**.

Step 2:

Chose the antenna mode from the **Antenna Control** list page.

Step 3:

The default setup is "**Auto**".
To change, select one from list, click **Apply** button to update.



View the Statistics

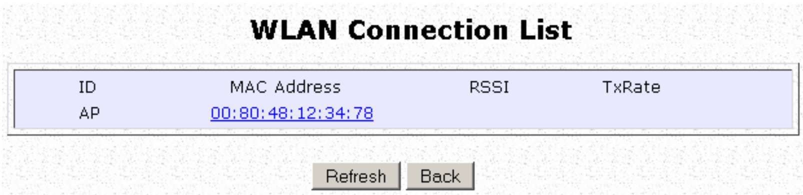
The Statistics feature reveals information on the wireless device connected to the WLAN.

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 Connection List.

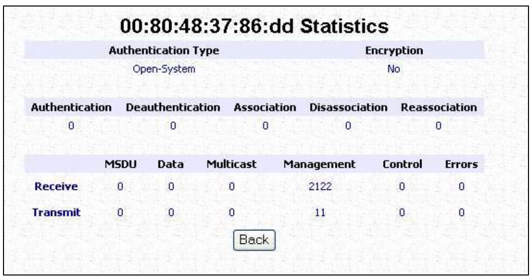
Step 2:

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



Step 3:

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



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.

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

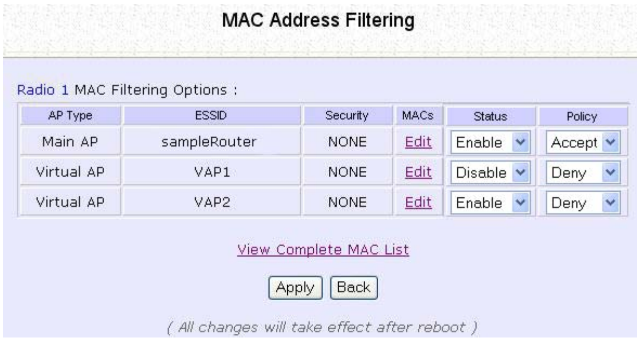
Add a MAC Address to the MAC Address List

Step 1:

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

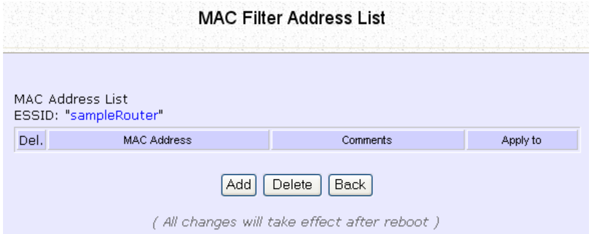
In this page you may also set the MAC Filtering Status to **Enable** or **Disable** for access points and set the Policy to either **Accept** or **Deny** MAC addresses.	
	MAC Filtering set to **Enable** with Policy to **Accept** only the MAC addresses in the MAC Filter Address List and deny all other MAC addresses.
	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.
	MAC Filtering set to **Disable**. Whether Policy is set to **Enable** or **Deny** does not matter.
	MAC Filtering set to **Disable**. Whether Policy is set to **Enable** or **Deny** does not matter.

Click the **Edit** button.



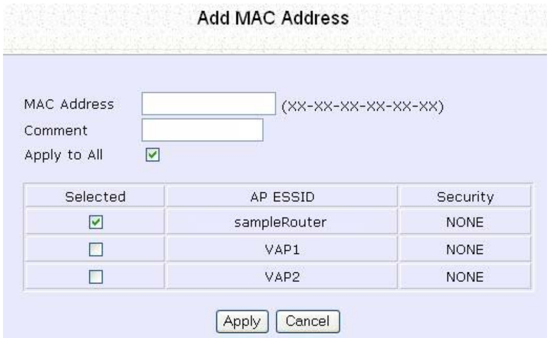
Step 2:

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



Step 3:

The Add MAC Address page displays.

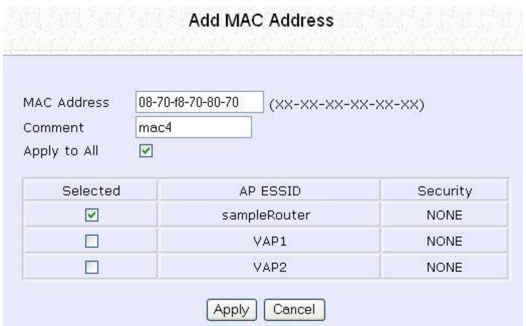


Step 4:

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

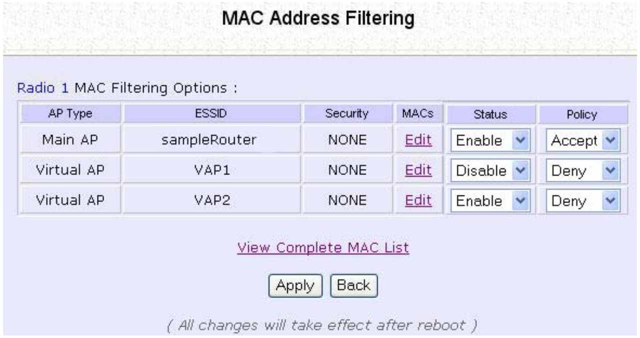
Please reboot to effect all changes and new MAC address entries.

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:

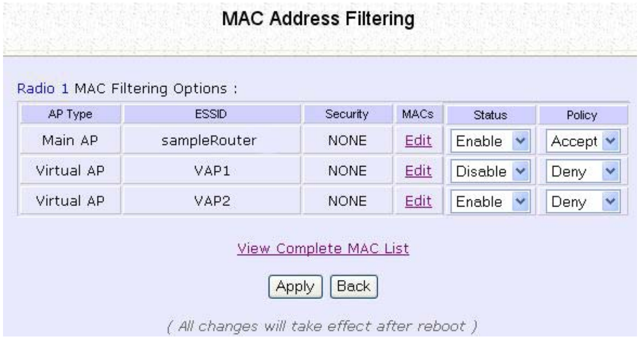
The MAC Filter Address List page displays with updated MAC Address List.

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:

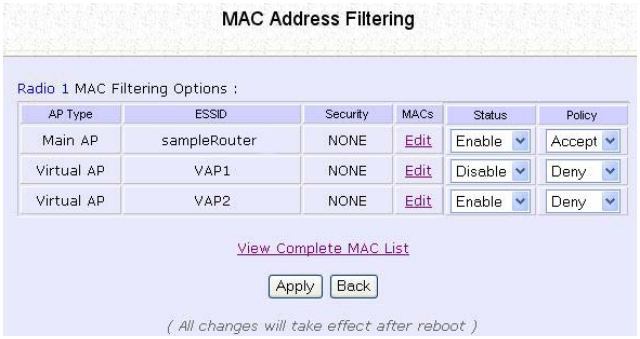
The MAC Filter Address List page displays with updated MAC Address List.

Edit MAC Address from the MAC Address List

Step 1:

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

Select **Edit**.



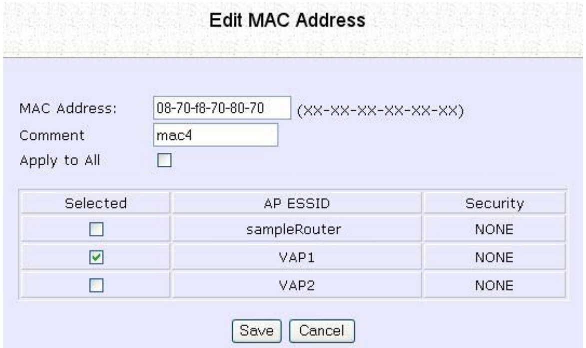
Step 2:

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:

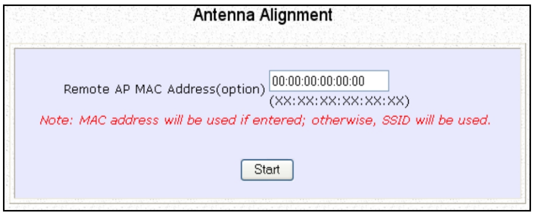
The MAC Filter Address List page displays with updated MAC Address List.

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:

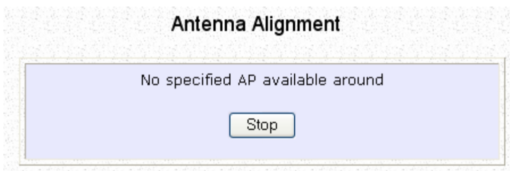
Select **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Antenna Alignment**. The **Antenna Alignment** page can act as a diagnostic tool to check the communication with a remote device. The remote AP MAC Address is preset to all zeros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

NOTE
Outdoor long distance connection should preferably have a 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.

Setup your WAN

(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

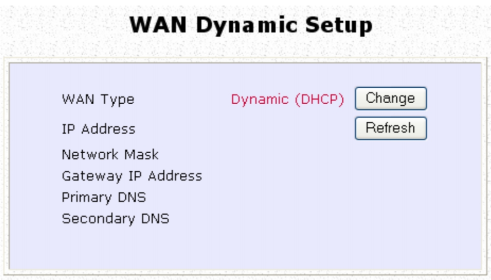
The access point is pre-configured to support this WAN type. However, you may verify the WAN settings with the following steps:

Step 1:

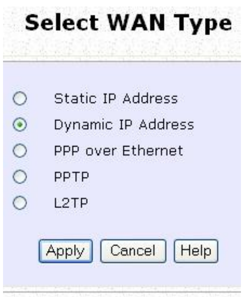
Under **CONFIGURATION** on the command menu, select **WAN Setup**.

Step 2:

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



Step 3:
Select **Dynamic IP Address** and hit the **Apply** button.
Reboot to let the settings take effect.

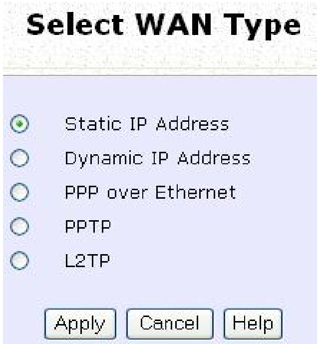
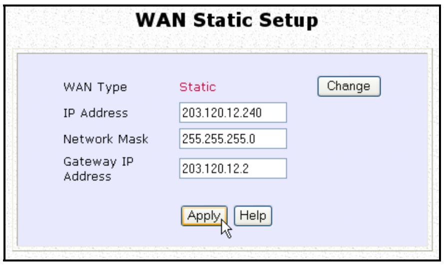


Note:
Additional configuration might be required before your ISP will allocate an IP address to the access point.
Certain ISPs require authentication through a DHCP Client ID before releasing a public IP address to you. The access point uses the System Name in the System Identity as the DHCP Client ID.
Therefore if this is the case, refer to your ISP for the correct DHCP Client ID to be set and follow **steps 4 - 5** to accomplish the setup.

Step 4:

Steps 4 - 5 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.
Select **System Identity** under the **SYSTEM TOOLS** command menu.

Step 5:
Enter the DHCP Client ID assigned by your ISP for the **System Name**. You may also enter in a preferred **System Contact** person and the **System Location** of the access point. Click the **Apply** button.
Select **Reboot System** under **SYSTEM TOOLS** and click the **Reboot** button to effect the settings.

Setup your WAN for cable internet whereby fixed WAN IP address is assigned by ISP
WAN Setup Parameters Example: • 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, select **WAN Setup**.
Step 2: Access the **Select WAN Type** page and select **Static IP Address** before clicking the **Apply** button. 
Step 3: Fill in the information provided by your ISP in the **IP Address, Network Mask** and **Gateway IP Address** fields, and click the **Apply** button. Select **Reboot System** under **SYSTEM TOOLS** and click the **Reboot** button to effect the settings. 

Setup your WAN for ADSL Internet using PPP over Ethernet

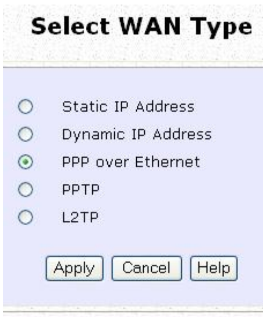
If you subscribe to an ADSL service using PPP over Ethernet (PPPoE) authentication, you can set up your access point’s WAN type as follows. For example, you may configure an account whose username is ‘guest’ as described below:

Step 1:

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.

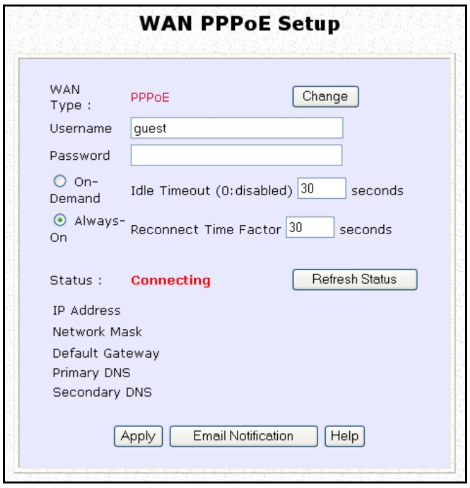


Step 3:

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

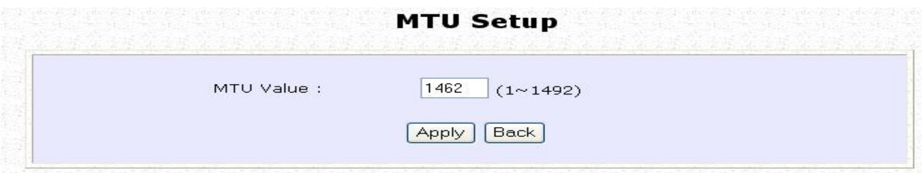
Select **Always-On** if you want your access point to always maintain a connection with the ISP. Otherwise select **On-Demand** for the access point to connect to the ISP automatically when it receives Internet requests from the PCs in your network.

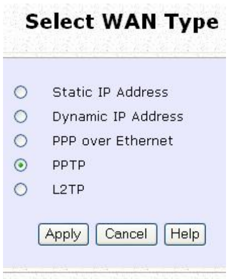
Idle Timeout is associated with the **On-Demand** option, allowing you to specify the value in seconds after the last Internet activity by which the access point will disconnect from the ISP. A value of "0" will disable idle timeout. **Reconnect Time Factor** is also associated with the **Always-on** 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**.



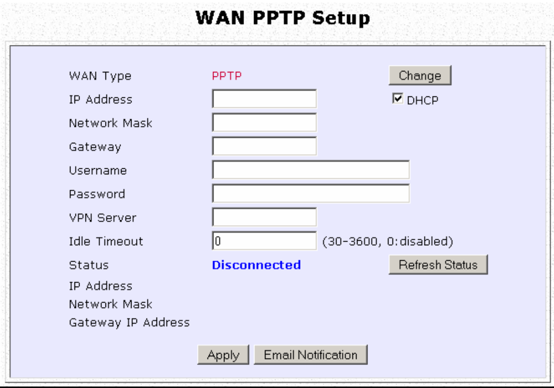
Setup your WAN for ADSL Internet using Point-to-Point Tunneling Protocol (PPTP)
WAN Setup Parameters Example: • IP Address: 203.120.12.47 • Network Mask: 255.255.255.0 • VPN Server: 203.120.12.15
Step 1: Under **CONFIGURATION** on the command menu, click on **WAN Setup**.
Step 2: Access the **Select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

Step 3:

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

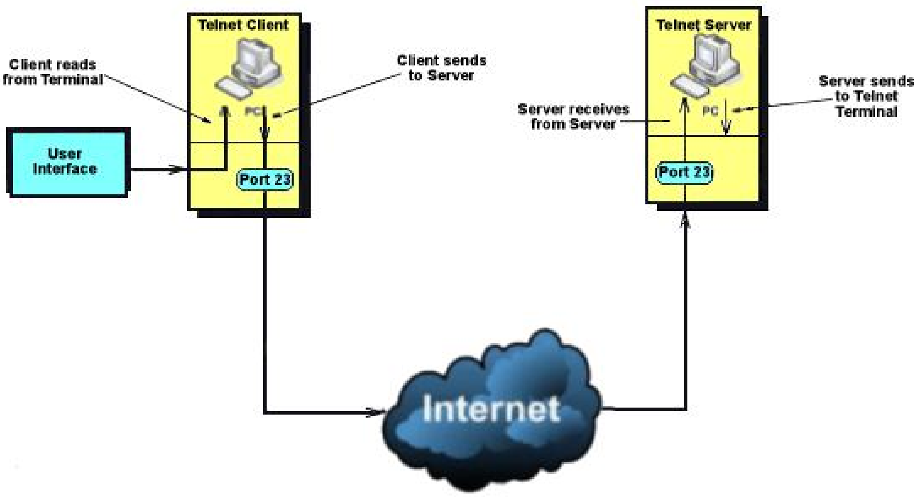
Select **Reboot System** under **SYSTEM TOOLS** and click the **Reboot** button to effect the settings

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.



Device Access Management

Telnet / SSH Setup



Telnet allows a computer to remotely connect to the access point CLI (Command Line Interface) for control and monitoring.

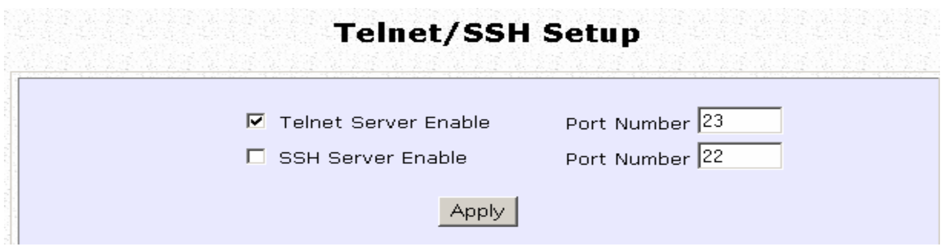
SSH (Secure Shell Host) establishes a secure host connection to the access point CLI for control and monitoring.

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.
3. Click the **Apply** button.

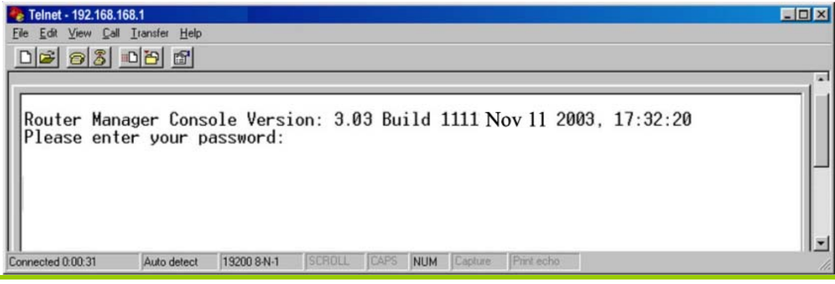


Access the TELNET Command Line Interface

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.

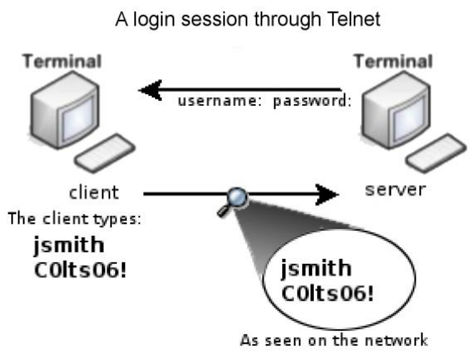
2. At the login prompt, type in the default password "password" and press enter. You will then login to the CLI.

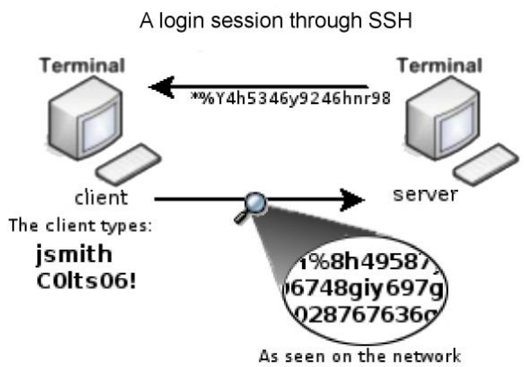


Access the Secure Shell Host Command Line Interface

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.

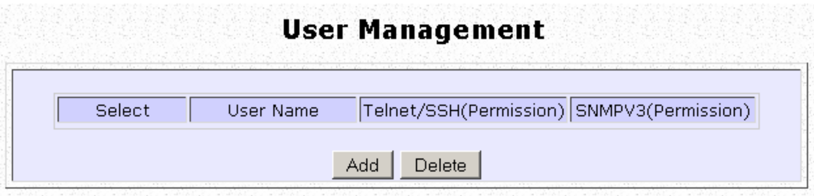
```
Generating public/private dsa key pair.
Enter file in which to save the key (/home/localuser/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/localuser/.ssh/id_dsa.
Your public key has been saved in /home/localuser/.ssh/id_dsa.pub.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

User Management

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.

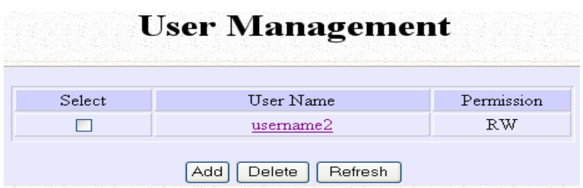
3. Click the **Apply** button.

To Delete User:

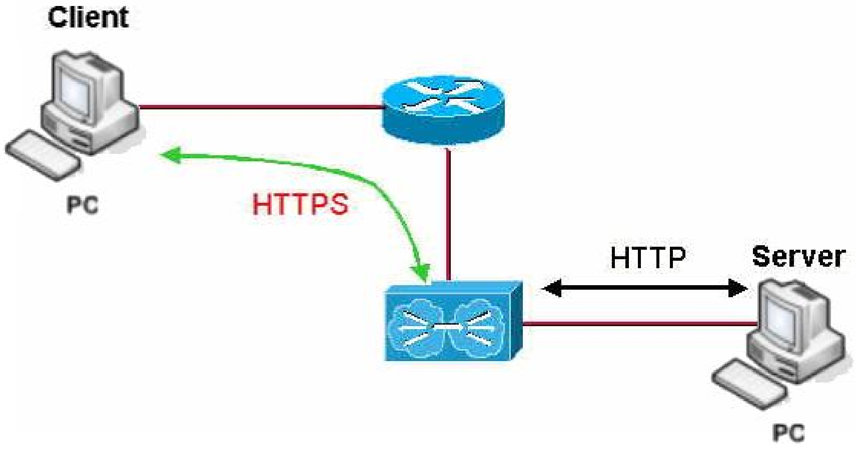
1. Select which user to Delete.

2. Click the **Delete** button.

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



Web Management Setup



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

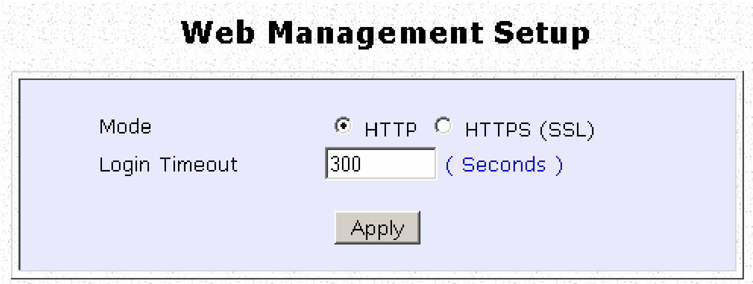
Step 1:

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

Step 2:

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

Changes will be effected after reboot.

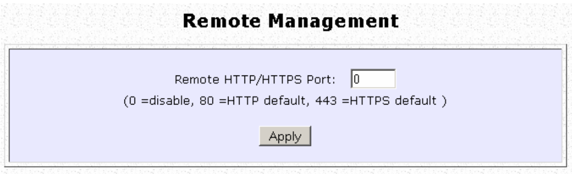


Perform Remote Management

(Available in Wireless Routing Client and Gateway modes)

You can use the access point web-based interface from the Internet to manage your network remotely.

Setup Remote Management



Step 1:
Select **Remote Management** from the **CONFIGURATION** command menu.

Step 2:
To disable Remote Management, set **Remote Http Port** to 0

To enable Remote Management, set **Remote Http Port** to an unused port number. It is recommended that you avoid using port number 80 as it is blocked by some ISPs.

In Gateway mode, **Remote Management** is disabled and the Ethernet port becomes a WAN port. To continue using it, enter the Remote Management with port 80 for example.
Example: For WAN IP 100.100.100.1 use http://100.100.100.1:80

NOTE
It is recommended that the default password is replaced with a new password changed periodically to prevent unauthorized access.

Perform Advanced Configuration

Setup Routing

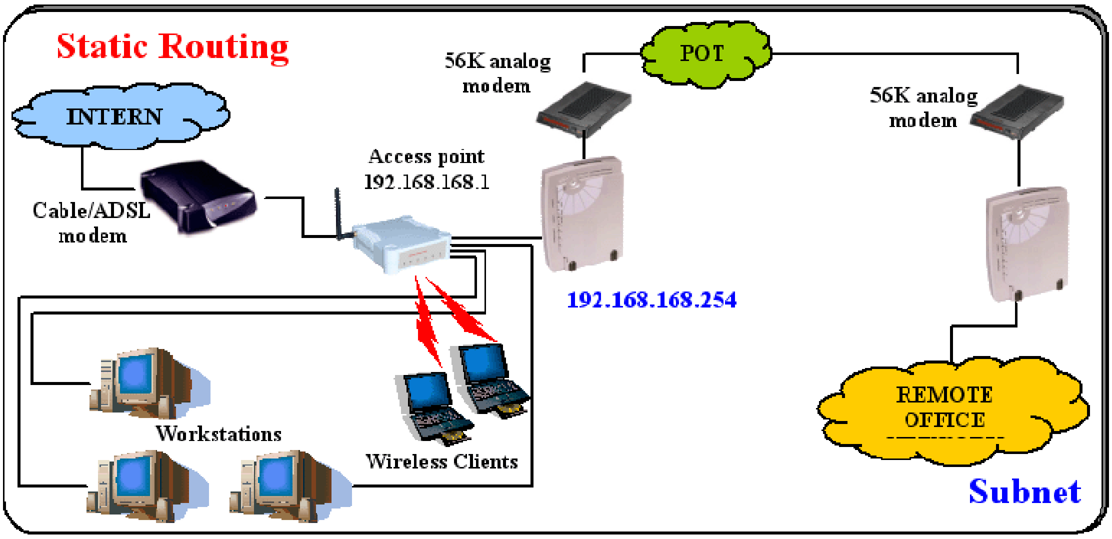
(Available in Wireless Routing Client and Gateway modes)

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.

NOTE	**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.

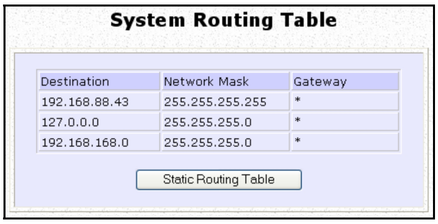
In this network, the main office of subnet 192.168.168.0 contains two routers: the office is connected to the Internet via the access point (192.168.168.1) and to the remote office via 192.168.168.254 The remote office resides on subnet 192.168.100.0

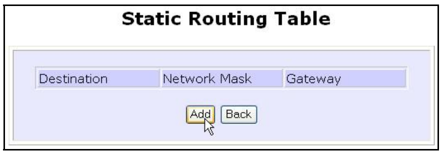
You can add a static routing entry into the access point routing table so that IP packets from the clients in the main office with a destination IP address of 192.168.100.X where X is any number from 2 to 254 will be re-routed to the router, which acts as the gateway to that subnet.



Configure Static Routing

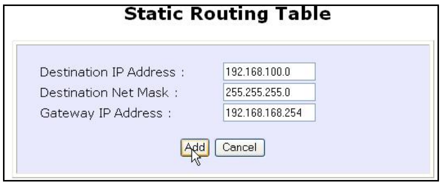
Step 1:
Select **Routing** from the **CONFIGURATION** command menu. The **System Routing Table** page displays. Initially the table contains the default routing entries of the access point.



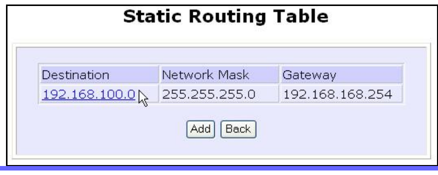


Step 2:
Click on the **Static Routing Table** button, then click the **Add** button.

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.

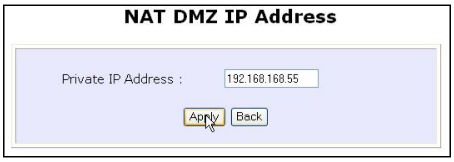
Step 1:
Select **NAT** from the **CONFIGURATION** command menu.

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.



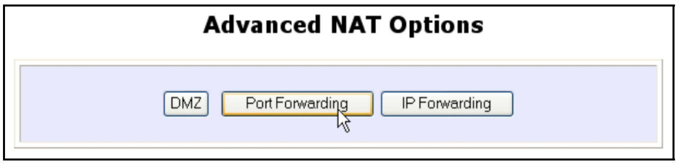
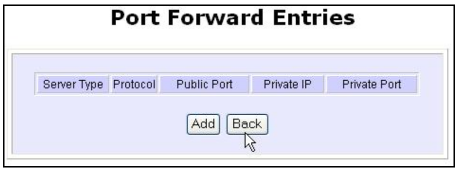
NOTE

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.

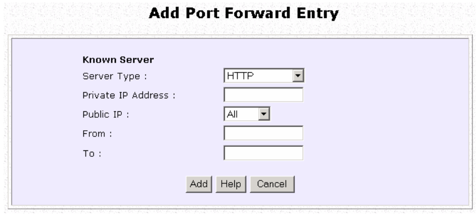
2. Please note that the DMZ host is susceptible to malicious attacks as ALL of its ports are exposed to the Internet.

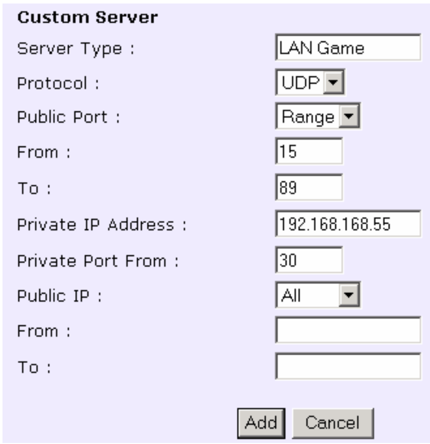
Configure Virtual Servers Based on Port Forwarding

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: Select **NAT** from the **CONFIGURATION** command menu.
Step 2: Click the **Port Forwarding** button in **Advanced NAT Options**. 
Step 2: Click the **Add** button on the **Port Forward Entries** page. 

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

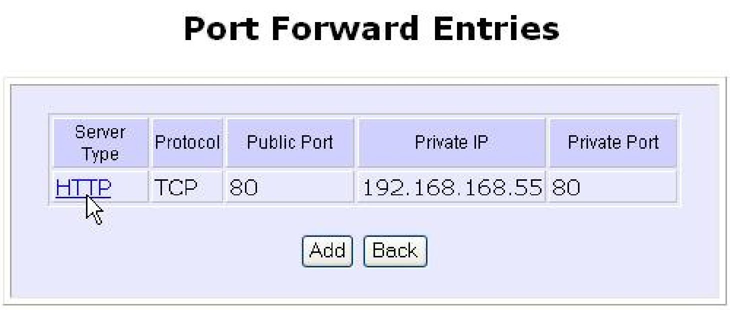
Server Type	:	Select from the drop-down list of known server types: • HTTP • FTP • POP3 • Netmeeting
Private IP Address	:	Specify the LAN IP address of the server PC running within the private network.
Public IP	:	Select **All**, **Single**, or **Range** from the dropdown list.
From	:	Enter the beginning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



Configure Virtual Servers based on IP Forwarding

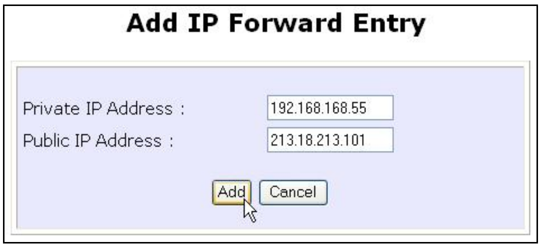
If you are subscribed to more than one IP address from your ISP, virtual servers based on IP forwarding can forward all Internet requests regardless of the port number to defined computers in the private network.

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

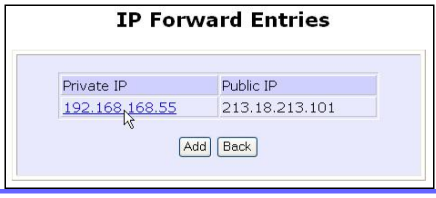
In this example, we would like all requests for 213.18.213.101 to be forwarded to a PC with **Private IP Address** 192.168.168.55.



NOTE

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.

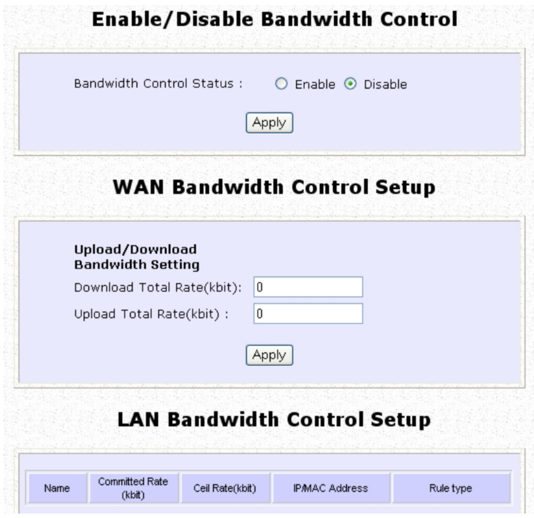
Control the Bandwidth Available

(Available in Wireless Routing Client and Gateway modes)

You can control the bandwidth available to subscribers to prevent the occurrence of massive data transfer that can slow down the network.

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.

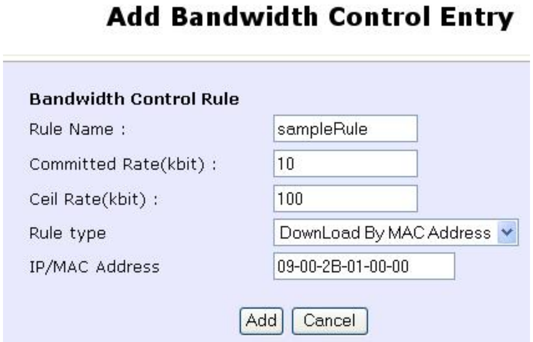
Configure LAN Bandwidth Control

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.

Step 3:
Click the **Add** button to create the rule for LAN user's bandwidth control.



Parameters	Description
Rule Name	You can set a name for the bandwidth control rule.
Committed Rate (kbit)	Minimum bandwidth rate of throughput. **NOTE:** The sum of the **Committed Rate** of all the rules should not exceed the total rate available.
Ceiling Rate (kbit)	Capped bandwidth rate of throughput.
Rule Type	This defines whether the bandwidth control rule works on downloads or uploads, and whether it works by IP address or MAC address.
IP/MAC Address	IP address or MAC address for the bandwidth control rule, corresponding to whether the Rule Type is defined by IP address or MAC address.

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

Repeat Steps 1 to Step 3 to add new bandwidth rule.

Setup SNMP

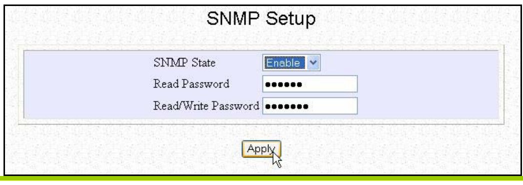
The Simple Network Management Protocol (SNMP) is a set of communication protocols that separates the management software architecture from the hardware device architecture.

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.

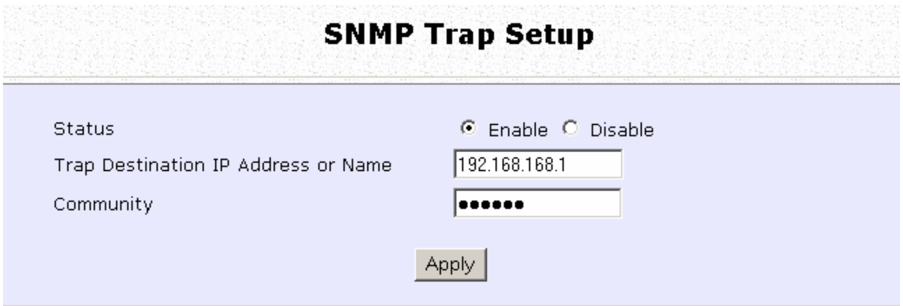
Step 2:

1. Select whether to **Enable** or **Disable** the SNMP Trap.

2. Enter the **Remote IP Address or DNS**.

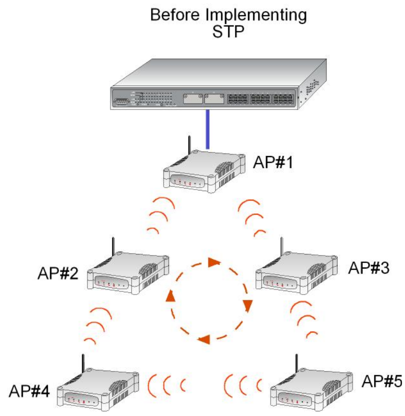
3. Enter the **Community**.
   This is used to authenticate message, and is included in every packet that is transmitted between the SNMP manager and agent.

4. Click on the **Apply** button.

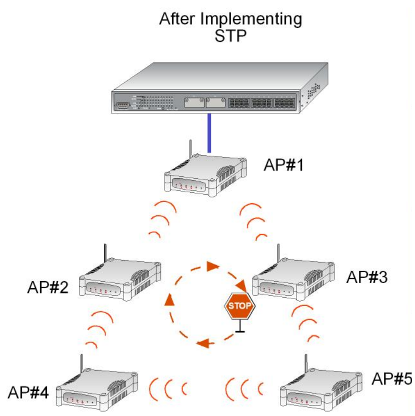


Setup STP

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

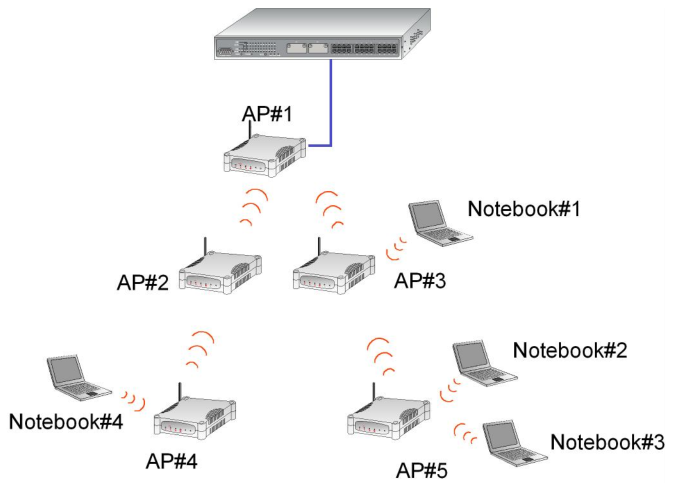


Spanning Tree Protocol (STP) prevents broadcast storms when there are redundant paths in the network. STP creates a tree that spans all devices in an extended network, forcing redundant paths into a standby state, but establishing the redundant links as backup in case the active link should fail. If 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.



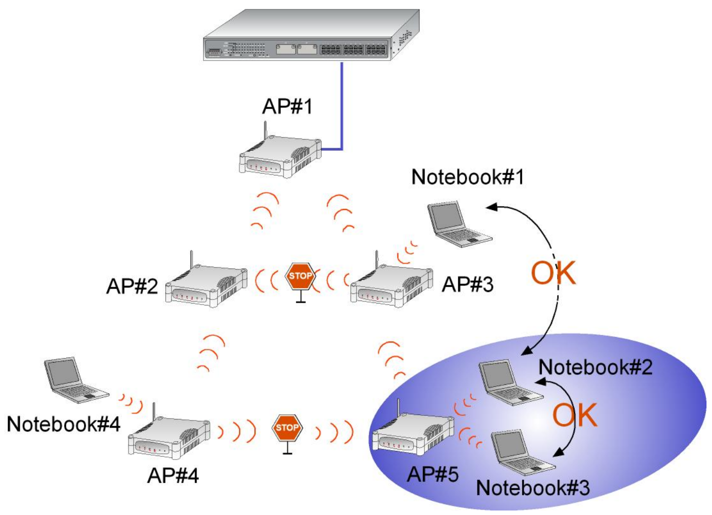
Scenario #1 – (No STP)

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)

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 2:

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

Step 2:

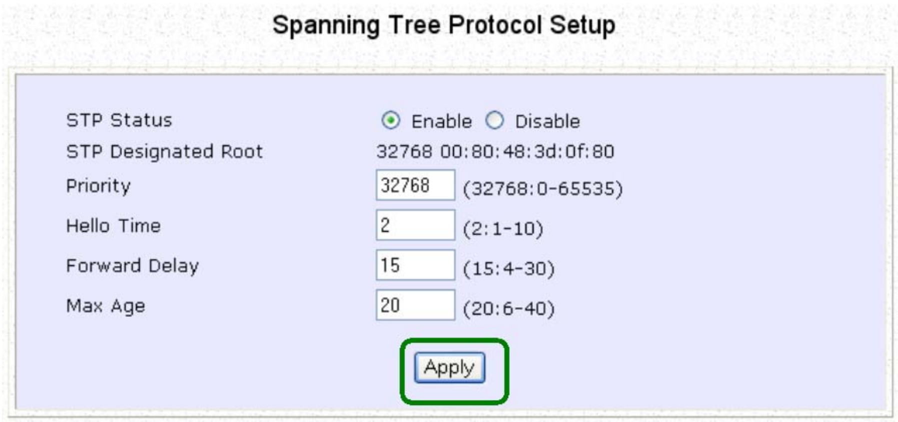
Select the **STP Status Enable** radio button, fill in the fields, and click on the **Apply** button to update the changes.

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.



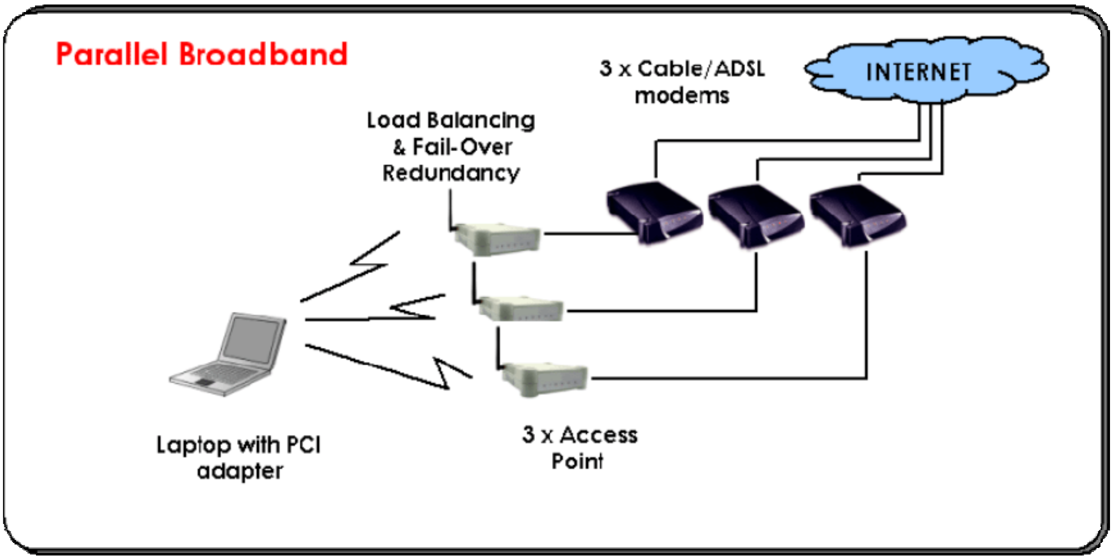
Use Parallel Broadband

(Available in 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 account. 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.



Enable Parallel Broadband

Begin by verifying that every access point in the network is properly configured to connect to its individual broadband Internet account.

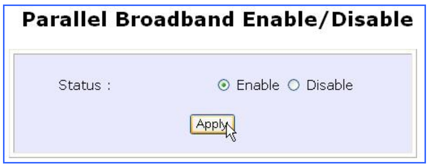
Secondly ensure that either:

- each access point is connected to an Ethernet port in the network OR
- the access points are wired to each other.

Then all the access points has to have the DHCP server, followed by the Parallel Broadband feature, enabled through the web-based configuration. Please note that all the access points need to be interconnected.

Step 1:
Select **Parallel Broadband** from the **CONFIGURATION** command menu.

Step 2:
Select **Enable** and click the **Apply** button.



Step 3:
Repeat Step 1 and Step 2 for the rest of the access points.

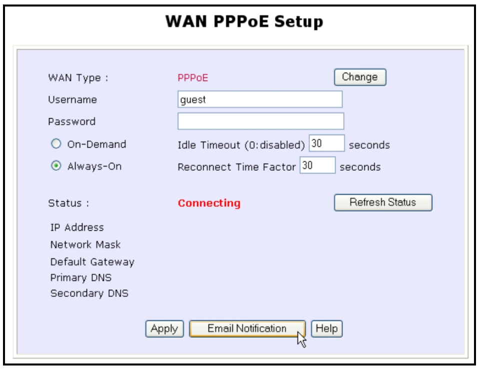
New users will then be assigned to the access point with the smallest load, ensuring that each access point has approximately the same number of users.

NOTE

Important:
Implementing Parallel Broadband is redundant if there is only 1 access point.

Email Notification

This feature notifies you by email if there is a change in the WAN IP address that was supplied to you.



Step 1:
Select **WAN PPPoE Setup** or **WAN PPTP Setup** from the **CONFIGURATION** command menu.

Step 2:
Click on the **Email Notification** button.

Step 3:
Select to **Enable** Email Notification and enter the following details:

- **Email address of Receiver:**
Email address of the receiver to whom the message would be sent.

- **IP address of Email Server:**
IP address of the SMTP server through which the message will be sent.
It is recommended that you use your ISP's SMTP server.

- **User Name:**
User Name for the specified email account.
This is necessary if authentication is required.

- **Password:**
Pass word for the specified email account.
This is necessary if authentication is required.

- **Email address of Sender:**
Email address to be displayed as the sender.

Step 4: Specify whether the SMTP server **Needs Authentication** or not by setting the checkbox accordingly. By default it is not selected.
Step 5: Click on the **Apply** button.

Using Static Address Translation

(Available in Wireless Routing Client and Gateway modes)

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:

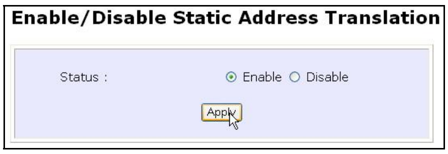
1. The IP address of the notebook should belong to a different subnet from the LAN IP address of your access point.

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

Step 1:
Select **Static Address Translation** from the **Home User Features** command menu.

Step 2:
Select whether to **Enable** or **Disable** SAT, and click the **Apply** button.

SAT is disabled by default.



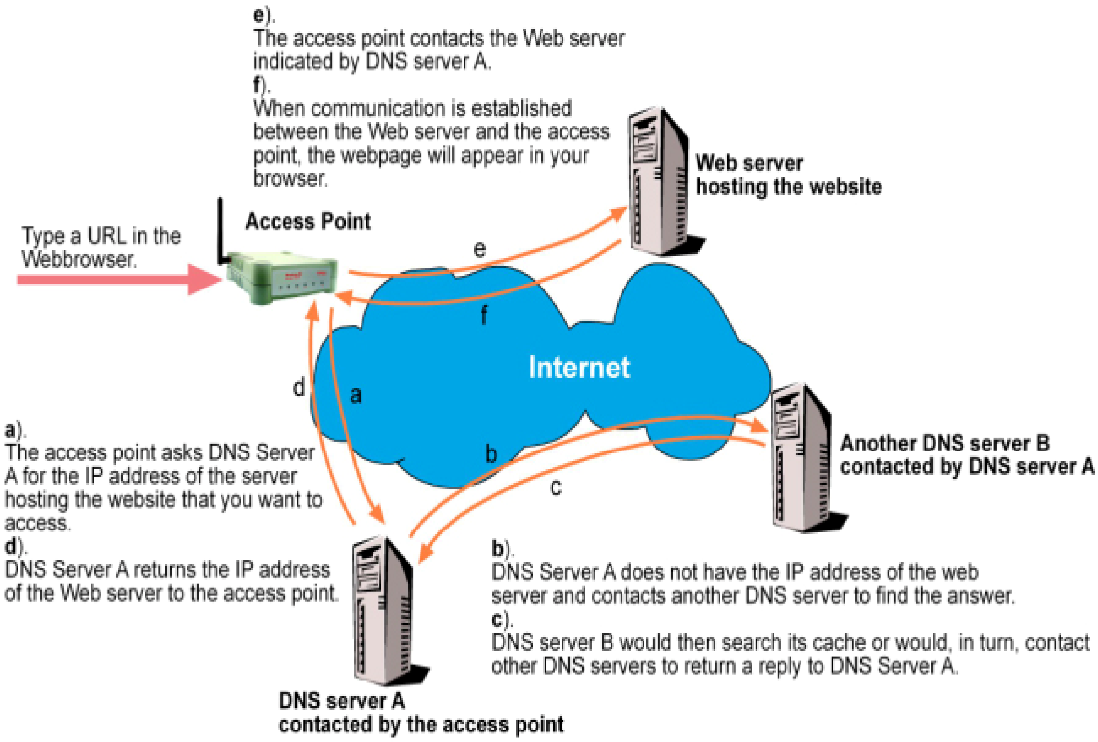
Use DNS Redirection

(Available in Wireless Routing Client and Gateway modes)

When you enter a URL into your Internet browser, it requests for a name-to-IP address translation from the Domain Name System (DNS) servers to locate the web server hosting the desired website. The DNS server searches its local cache for the answer, and if found, returns this cached IP address. Otherwise, it contacts other DNS servers until the query is answered.

With DNS Redirection, DNS requests from the LAN clients are processed by the access point. It contacts the DNS server allocated by your ISP to resolve these DNS requests unless you have already specified a default DNS server in the access point LAN Setup. This default DNS server overrides the one defined in the TCP/IP settings of the LAN clients, allowing the access point to direct DNS requests from the LAN to a local or to a closer DNS server that it is aware of, thus improving the 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 an the access point LAN Setup and enable DNS Redirection, without having to reconfigure the DNS settings of every LAN client.

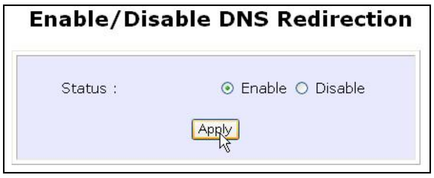


NOTE

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

Enable or Disable DNS Redirection

Step 1:
Select **DNS Redirection** from the **Home User Features** command menu.



Step 2:
Select to **Enable** or **Disable** DNS Redirection.

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

Dynamic DNS Setup

With Dynamic IP Internet connection, keeping track of your public IP address for Internet communication is complicated as it is changed regularly by the ISP. If you are doing some web hosting on your computer, Internet users will have to keep up with the changing IP address to access your computer.

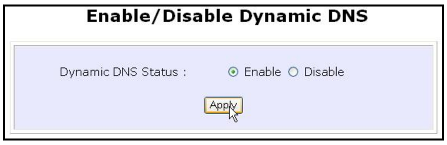
When you sign up for an account with a Dynamic Domain Name Service (DDNS) provider, it will register your permanent domain name, for example: **MyName.Domain.com** You can configure the access point to automatically contact your DDNS provider whenever it detects a change in its public IP address. The access point will then log on to update your account 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:
Select **Dynamic DNS Setup** from the **Home User Features** command menu.

Step 2:
Select to **Enable** or **Disable** Dynamic DNS.
Dynamic DNS is disabled by default.

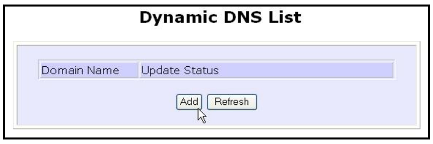


Click the **Apply** button.

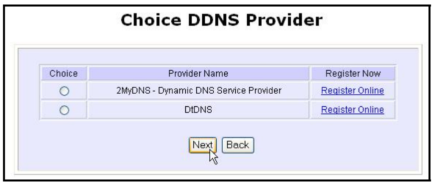
To manage Dynamic DNS List

Step 1:
Select **Dynamic DNS Setup** from the **Home User Features** command menu.

Step 2:
If you have created a list earlier, click on the **Refresh** button to update the list.



Step 3:
To add a new Dynamic DNS, click on the Add button.
The **Choice DDNS Provider** page appears.
There are two default providers that you can use.
The parameters are explained below:



- **Choice**:
Indicates your preferred DDNS provider.

- **Provider Name:**
Name of your preferred DDNS provider.

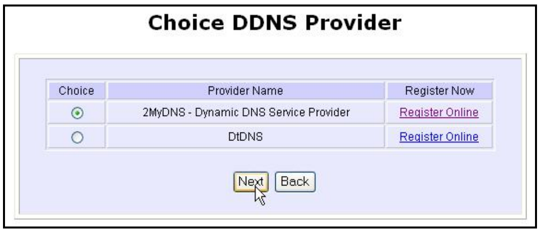
- **Register Now:**
Allows you to go to the website of your preferred DDNS provider where you can register your account.

2 DDNS providers are predefined for you. You need to be connected to the Internet to register your DDNS account.

Select **2MyDNS – Dynamic DNS Service Provider** as DDNS Service Provider:

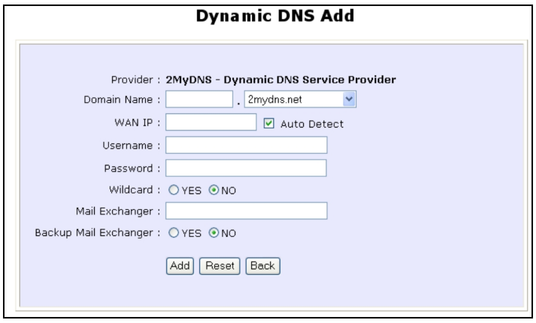
Step 1:
Under the **Choice** column in the **Choice DDNS Provider** list, check the radio button next to the **2MyDNS – DNS Service Provider** entry.

Click on the **Next** button.



Step 2:
Enter your **Domain Name**.

Step 3:
The **Auto Detect** checkbox is selected by default.
The **WAN IP** field is empty by default.
These default settings should be used if dynamic WAN IP connection is used.

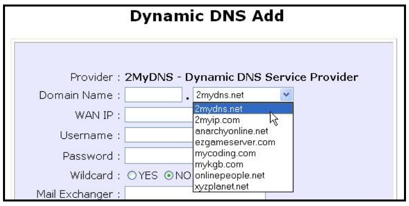


If your ISP connection uses dynamic WAN IP:
Select the **Auto Detect** checkbox to let the DDNS server learn your current WAN IP address.
Enter your DDNS account **Username** and **Password**.

If your ISP connection uses a fixed WAN IP:
Enter the IP address in the **WAN IP** field.
Deselect the **Auto Detect** checkbox.
The access point will update the DDNS server with the specified WAN IP.

Step 4: Optional
Your hostname will be allowed multiple identities if wildcard is enabled.
For example, if you register: **mydomain.2mydns.net**, users looking for www.mydomain.2mydns.net or ftp.mydomain.2mydns.net can still reach your hostname.

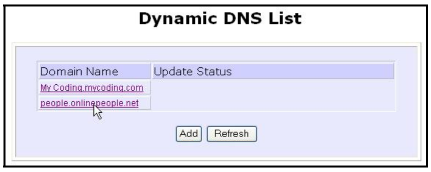
Step 5: Optional
In the Mail Exchanger field, enter the Static WAN IP address of the mail server configured to handle email for your domain.



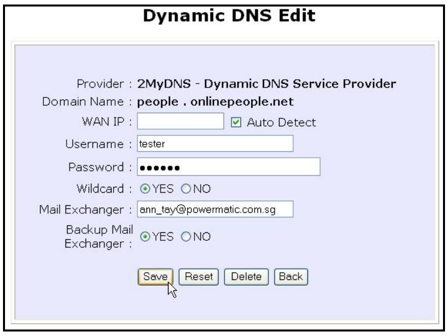
Select **Backup Mail Exchanger** to enable this service.

Step 6:
Click on the Add button.

The new domain is added to the Dynamic DNS list table. It will appear as a hyperlink that you can click to go back to the Dynamic DNS Edit page.



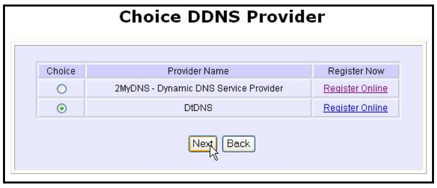
Step 7:
From the Dynamic DNS Edit page you can update or reset the parameters, or delete the domain name.



Select **DtDNS as** DDNS Service Provider:

Step 1:
Under the **Choice** column in the **Choice DDNS Provider** list, check the radio button next to the **DtDNS** entry.

Click on the **Next** button.



Step 2:
Enter your **Domain Name**.

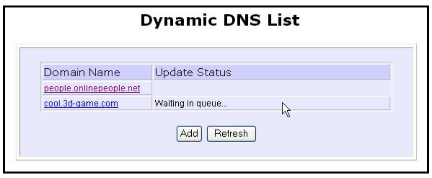
Step 3:
The **Auto Detect** checkbox is selected by default.
The **WAN IP** field is empty by default.
These default settings should be used if dynamic WAN IP connection is used.

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

If your ISP connection uses a fixed WAN IP:
Enter the IP address in the **WAN IP** field.
Deselect the **Auto Detect** checkbox.
The access point will update the DtDNS server with the specified WAN IP.

Step 4:
Then click on the **Add** button.

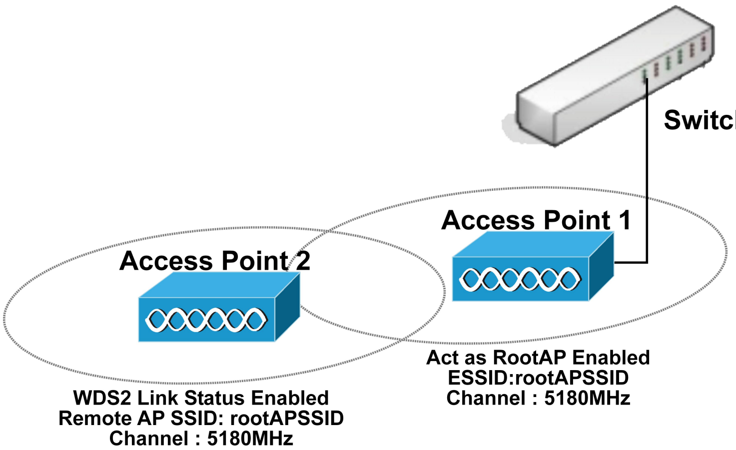
Step 5:
While the new domain name is being added to the list, the message 'Waiting in queue…" will be displayed under the **Update Status** column of the **Dynamic DNS List** table.



Use the 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.

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

Setup access point 1:

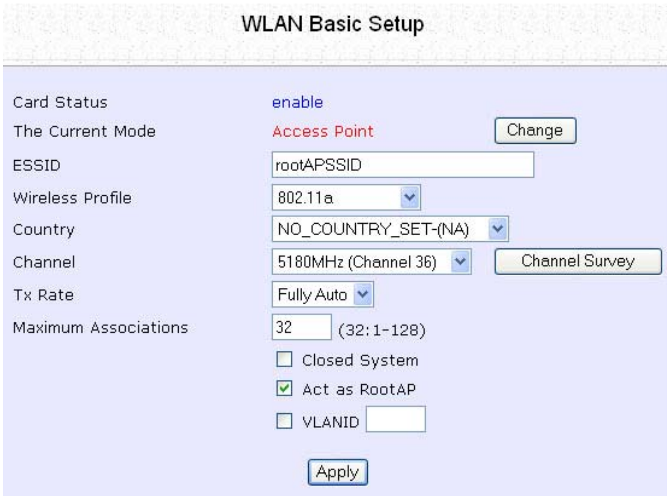
Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Basic**.

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.

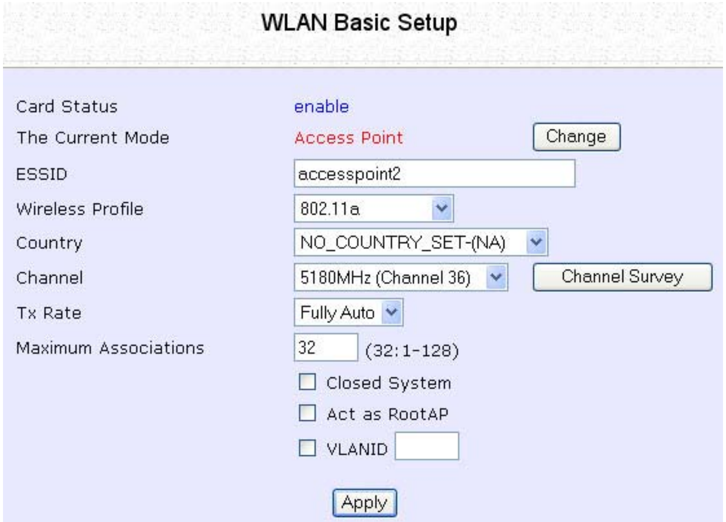


Follow these settings to setup access point 2.

Setup access point 2:

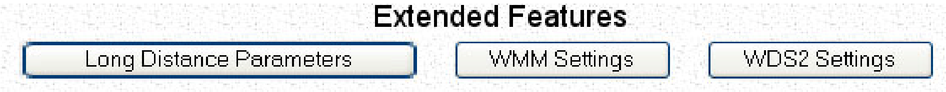
Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Basic**.

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



Configure WDS2 link:

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

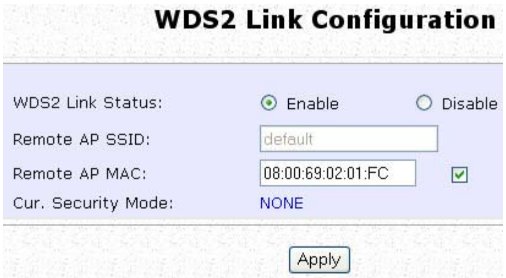


Under **Extended Features**, click on the **WDS2 Settings** button.

Set **WDS2 Link Status** to **Enable**.

Options for configuring WDS2 link:

- By Remote AP MAC – Enter the Remote AP MAC



OR

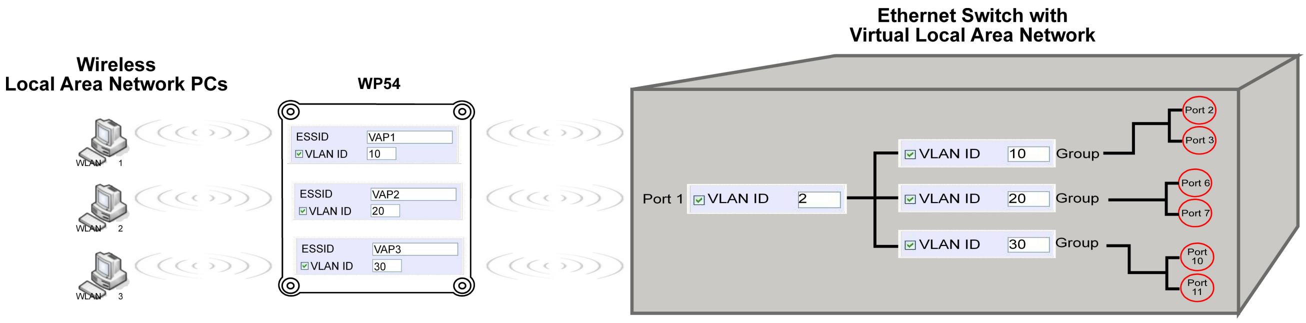
- By Remote AP SSID – Uncheck the Remote AP MAC checkbox and enter the Remote AP SSID.

Click **Apply**.

Set Virtual AP (Multiple SSID)

Virtual AP implements mSSID (Multi-SSID) whereby a single wireless card can be setup with up to 4 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.



<u>How it Works</u>

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.

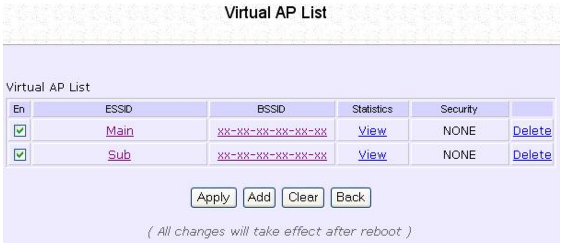
For more information on Virtual AP (Multiple SSID) please refer to Appendix: Virtual AP (Multiple SSID) FAQ.

Follow these steps to setup Virtual AP.

Virtual AP

1

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

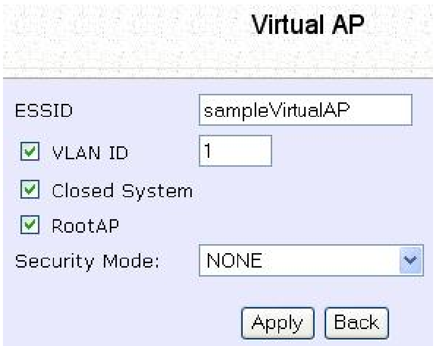


2

Virtual AP List page displays.

- 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.



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.

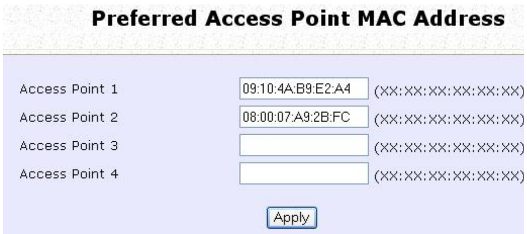
Follow these steps to specify your preferred APs.

Preferred APs

1

1. Click on WLAN Setup from the CONFIGURATION menu.

2. Select Preferred APs.



2

1. Enter the MAC addresses of the preferred APs.

2. Click Apply to effect the settings.

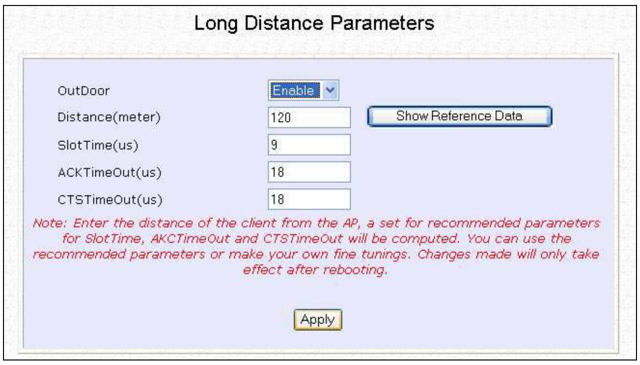
Get Long Distance Parameters

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.

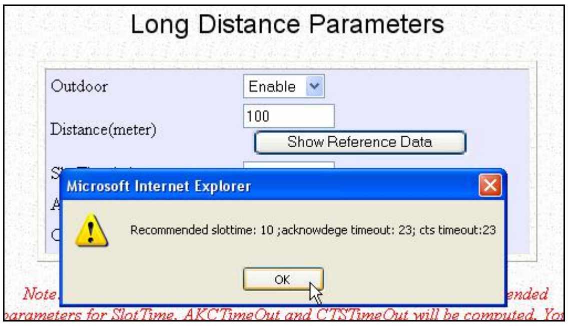
Select **Advanced** from **WLAN Setup** under **Configuration**.

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.

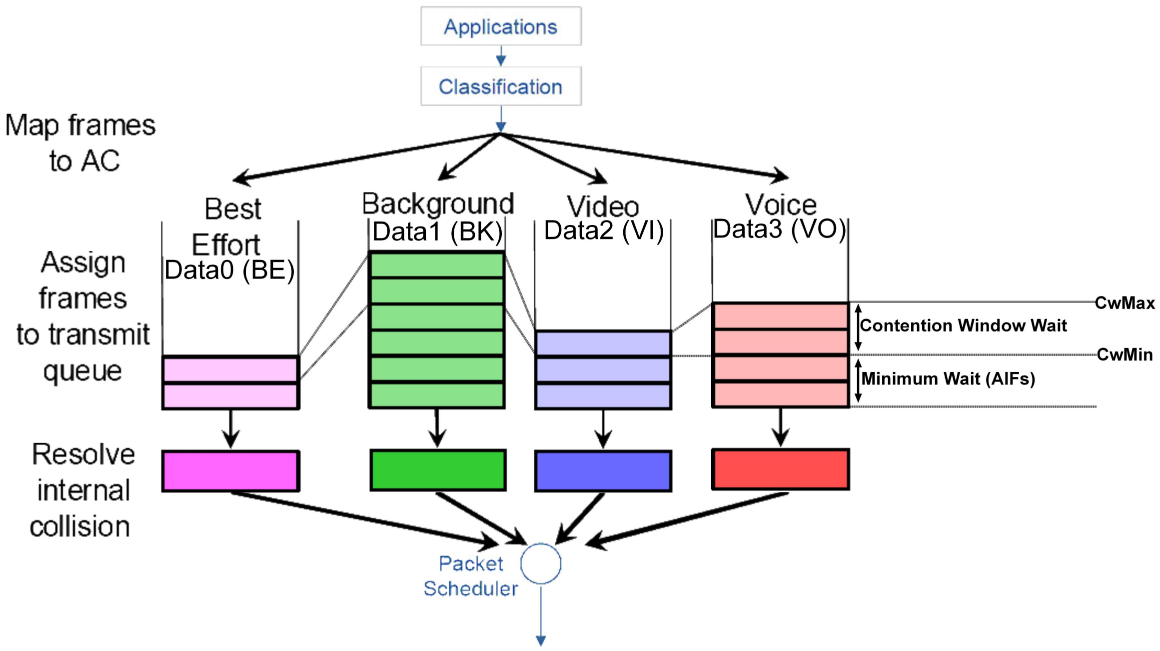


You can enter the parameters based on the recommended values in the pop-up window, click on the **Apply** button to update the changes.

Long Distance Parameters	Description
Outdoor	If set to Enable, the Outdoor parameters will be configured for outdoor communication over short or long distances as specified, it is disabled by default.
Distance	Determines the distance between your access point and the remote access point in meters.
Slot Time	The amount of time is divided and each unit of time is called one slot time.
ACK Timeout	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 resend.
CTS Timeout	Clear-to-Send Timeout 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 (WMM)

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.



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.

WMM Parameters (for advanced users)	
AIFs (Arbitrary Inter-Frame Space)	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.
Cwmin (Contention Window Minimum)	Contention Window Minimum is the minimum random wait time drawn from this interval or window for the backoff mechanism on the network.
CwMax (Contention Window Maximum)	Contention Window Maximum is the maximum random wait time drawn from this interval or window for the backoff mechanism on the network.
TxOp limit (Transmit Opportunity Limit)	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.
NoAck (No Acknowledgement)	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.
ACM (Admission Control Mandatory)	Admission Control Mandatory enables WMM on the radio interface. When ACM is enabled, associated clients must complete the WMM admission control procedure before access.
BE (Best Effort)	Parameters for Data0 Best Effort. Best Effort data traffic has no prioritization and applications equally share available bandwidth.
BK (Background)	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.
VI (Video)	Parameters for video data traffic.
VO (Voice)	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.

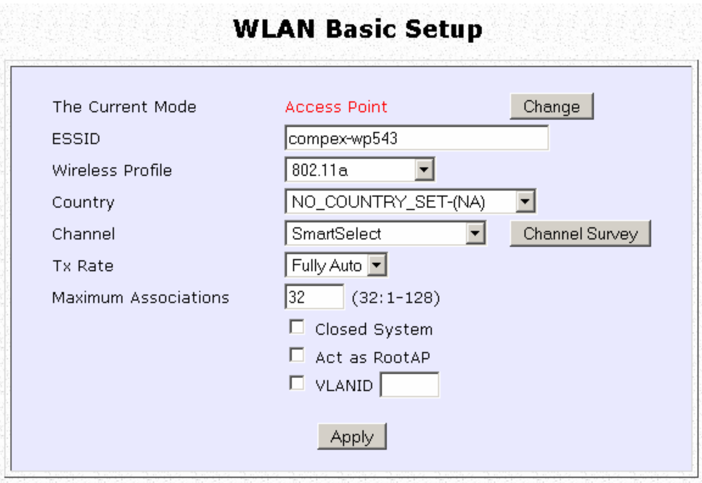
Follow these steps to setup RootAP

RootAP Step 1:

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

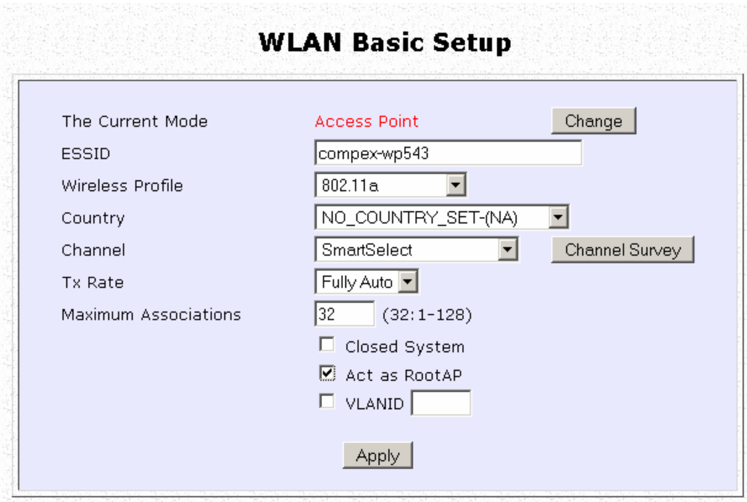
Ensure that **The Current Mode** is set to **Access Point**.

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



RootAP Step 2:

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



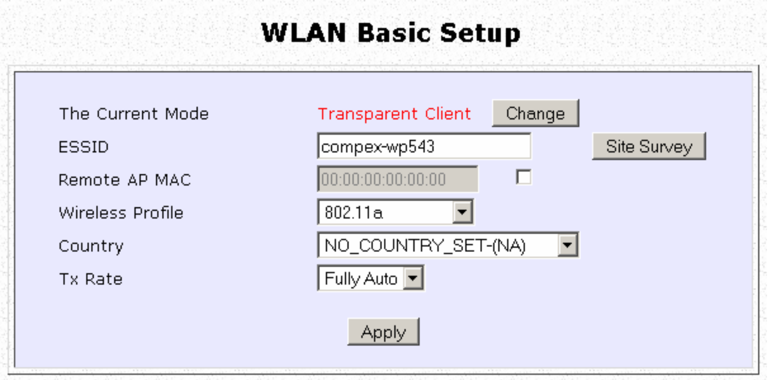
Follow these steps to setup Transparent Client/s.

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**.

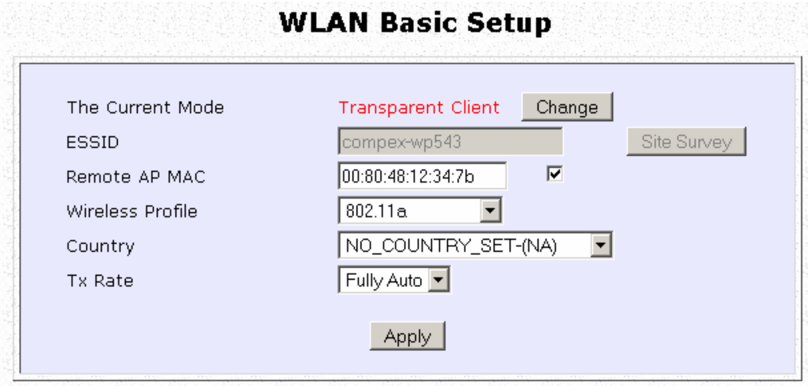
To change **The Current Mode**, please refer to: Common Configuration – WLAN Setup - To Configure the Basic Setup of the Wireless Mode.



Transparent Client Step 2:

Select the **Remote AP MAC** checkbox.

Enter the **Remote AP MAC**.

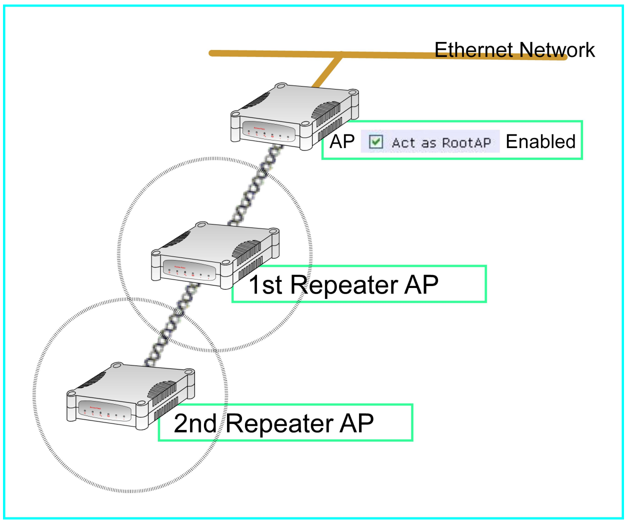


Note:
When using **Remote AP MAC**, the **ESSID** name must also match the AP's ESSID name, especially when Closed System is enabled on the AP.

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.

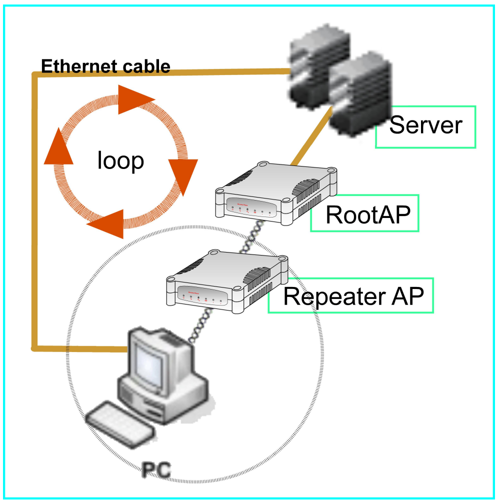


Example: Network diagram with 2 repeater hops.

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

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.



Follow these settings to setup the root AP.

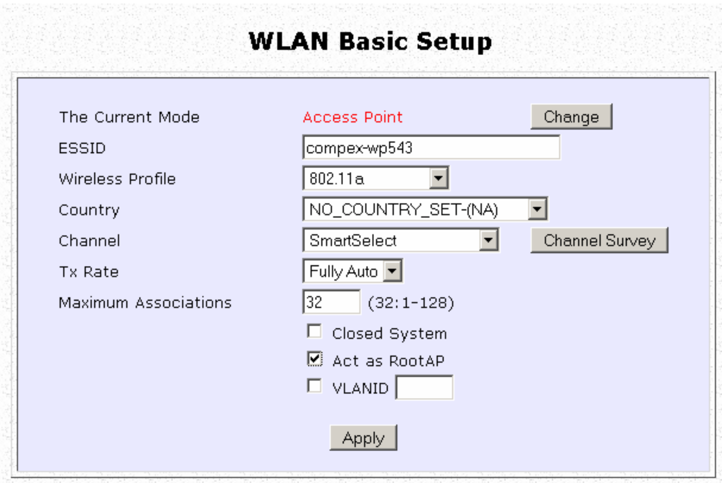
Root AP Settings:

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**.



Click **Apply**.

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**.

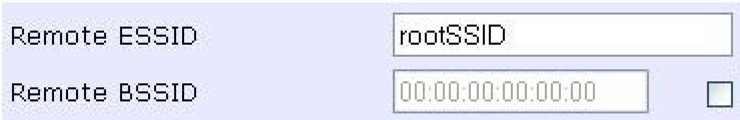
To change **The Current Mode**, please refer to: Common Configuration – WLAN Setup - To Configure the Basic Setup of the Wireless Mode.

Options for defining the root AP:

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

OR

- Enter the **Remote ESSID**.



OR

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

Click **Apply**.

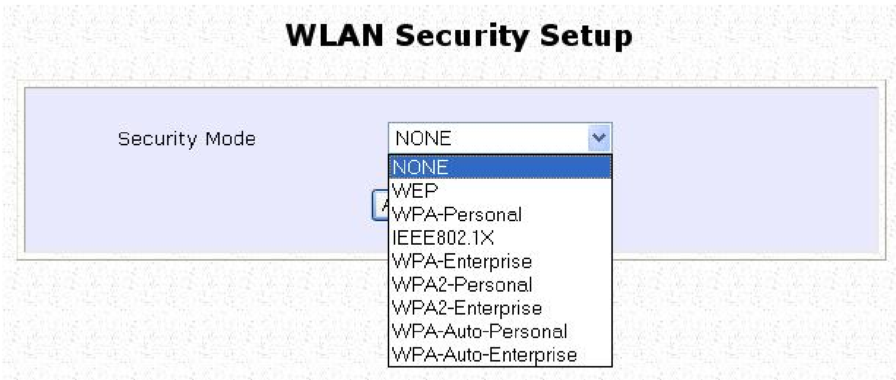
Secure your Wireless LAN

Step 1:
Select **Security** from **WLAN Setup** under the **CONFIGURATION** menu.

Step 2:

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

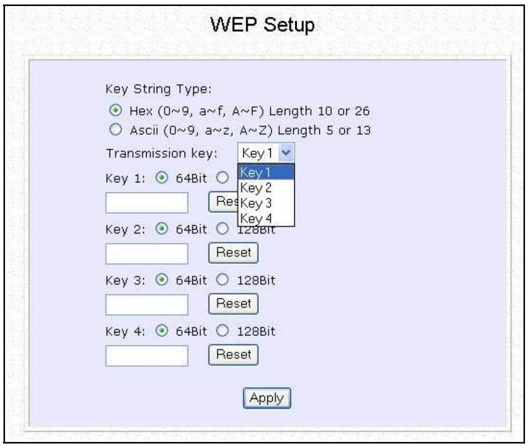
Click on the **Apply** button.



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

Setup WEP

At the **WEP Setup** page,



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 2:

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 have entered in the field, click on the **Reset** button.

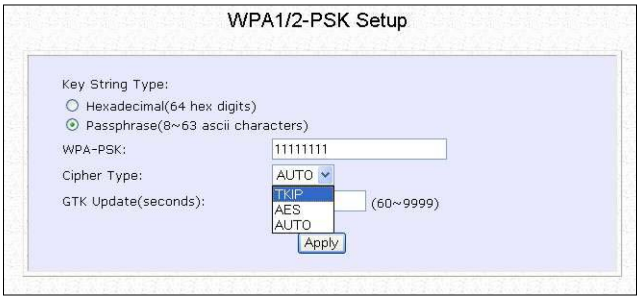
Click on the **Apply** button and reboot your access point.

Setup WPA-Personal

(Available in Access Point mode)

Follow these steps if you have activated the **WPA-Personal**, **WPA2-Personal** or **WPA-Personal-AUTO** security modes.

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



Step 1:

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

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

Step 2:

Fill in the 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-Personal
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-Personal
Set the **Cipher Type** to **AES**.
Advanced **E**ncryption **S**tandard (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-Personal-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.

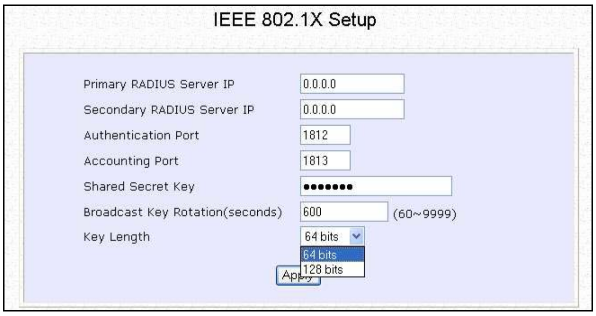
Step 5:

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

Setup 802.1x/RADIUS

(Available in Access Point mode)

At the IEEE 802.1x Setup page,



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:

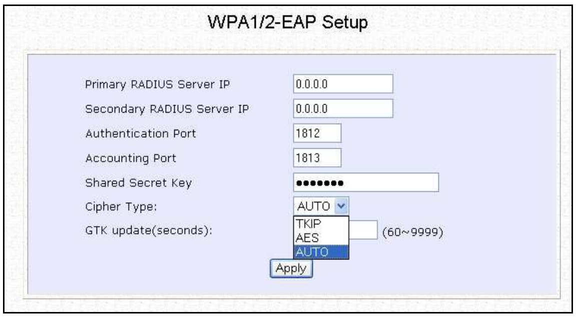
Click the **Apply** button and reboot your system, after which your settings will become effective.

Setup WPA Enterprise

(Available in Access Point mode)

Follow these steps if you have selected the **WPA**, **WPA1-Enterprise**, **WPA2-Enterprise**, or **WPA-Enterprise-AUTO** security modes.

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



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.

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-Enterprise
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- Enterprise
Set the **Cipher Type** to **AES**.
Advanced **E**ncryption **S**tandard (AES) is a symmetric 128-bit block data encryption technique. It is a requirement of WPA2 under the IEEE 802.11i standard.

For WPA- Enterprise -AUTO
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:

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

Configure the Security Features

Use Packet Filtering

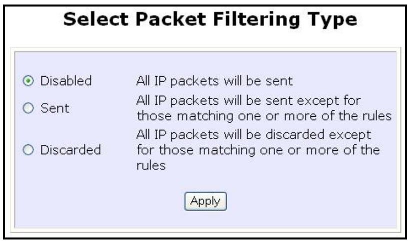
Packet filtering selectively allows /disallows applications from Internet connection.

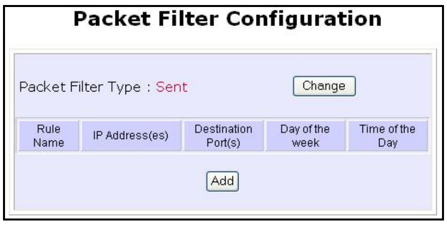
Configure Packet Filtering

Step 1:
Select **Packet Filtering** from the **Security Configuration** command menu.

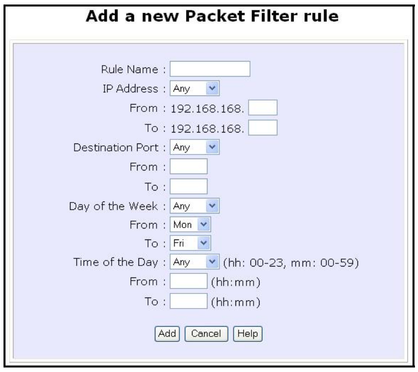
Step 2:
Select the **Packet Filter Type** by clicking on the **Change** button.

Step 3:
Select from three choices: **Disabled**, **Sent**, **Discarded**, and then click on the **Apply** button. The default is **Disabled**, which allows all packets to be sent.





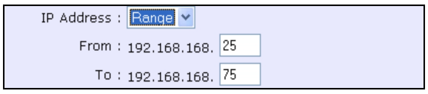
Step 4:
Click on the **Add** button and you will be able to define the details of your **Packet Filter Rule** from the screen on the right.



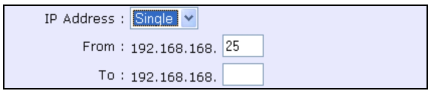
4a). Enter **Rule Name** for this new packet filtering rule. For example, *BlockCS*

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

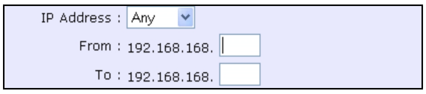
- A **Range** of IP addresses
  In this case, you will have to define **(From)** which IP address **(To)** which IP address, your range extends.



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

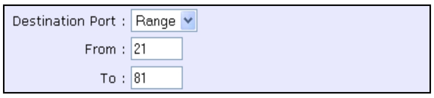


- **Any** IP address
  You may here, leave both, the **(From)** as well as the **(To)** fields, blank. Here, the rule will apply to all IP addresses.

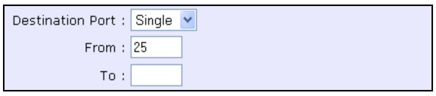


4c). At the **Destination Port** drop down list, select either:

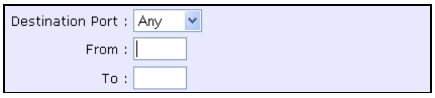
- A **Range** of TCP ports
  In this case, you will have to define **(From)** which port **(To)** which port, your rule applies.



- 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.



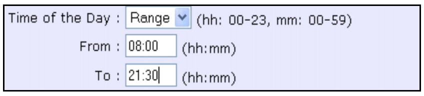
4d). From the **Day of the Week** drop down list, select whether the rule should apply to:

- A **Range** of days
  Here, you will have to select **(From)** which day **(To)** which day

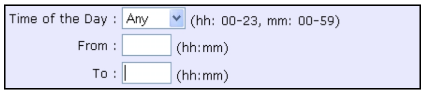
- **Any** day
  In this case, you may skip both the **(From)** as well as the **(To)** drop down fields.

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.

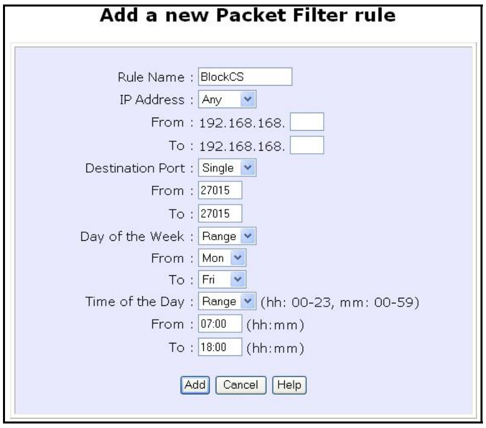


- **Any** time
  Here, you may leave both **(From)** and **(To)** fields blank.



Step 5:
Click on the **Apply** button to make the new rule effective.

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



Step 6:
In this example, we would 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.

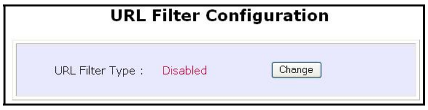
Therefore, for a rule we name BlockCS, and add the entries depicted on the left. Clicking on the **Add** button will effect your packet filter rule.

Use URL Filtering

URL Filtering allows you to block objectionable websites from your LAN users.

Configure URL Filtering

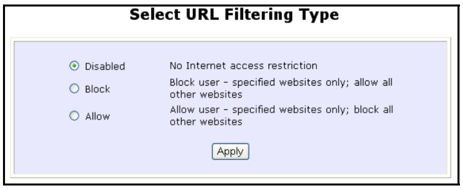
Step 1:
Select **URL Filtering** from the **Security Configuration** command menu.

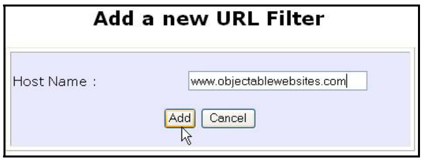


Step 2:
To select the **URL Filter Type**, click the **Change** button.

Step 3:
Select to **Block** or **Allow**, and then click on the **Apply** button. The default is **Disabled**, which allows all websites to be accessed.

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.

Use Multicast Filtering

This feature lets you allow or disallow streaming over the Internet, if you have registered to ISP services providing videos and TV channel streaming.

1

Click **Multicast** from the **Security Configuration** menu.

2

Enabling the filter disallows video streaming over the Internet whereas disabling the filter would allow it.
Click **Apply** to complete setup.

Note: This feature is enabled by default.
If such services have been subscribed to, set this feature to **Disable**.

Configure the Firewall

Configure SPI Firewall

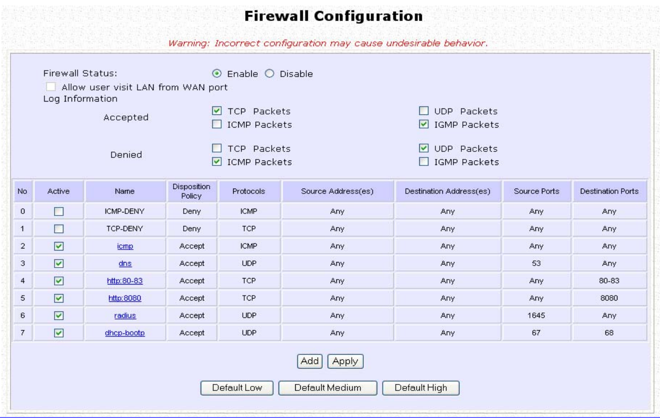
Stateful Packet Inspection (SPI) thwarts common hacker attacks like IP Spoofing, Port Scanning, Ping of Death, and SynFlood by comparing certain key parts of the packet to a database of trusted information before allowing it through.

NOTE
Firewall security rules should be planned carefully as incorrect configuration may cause improper network function.

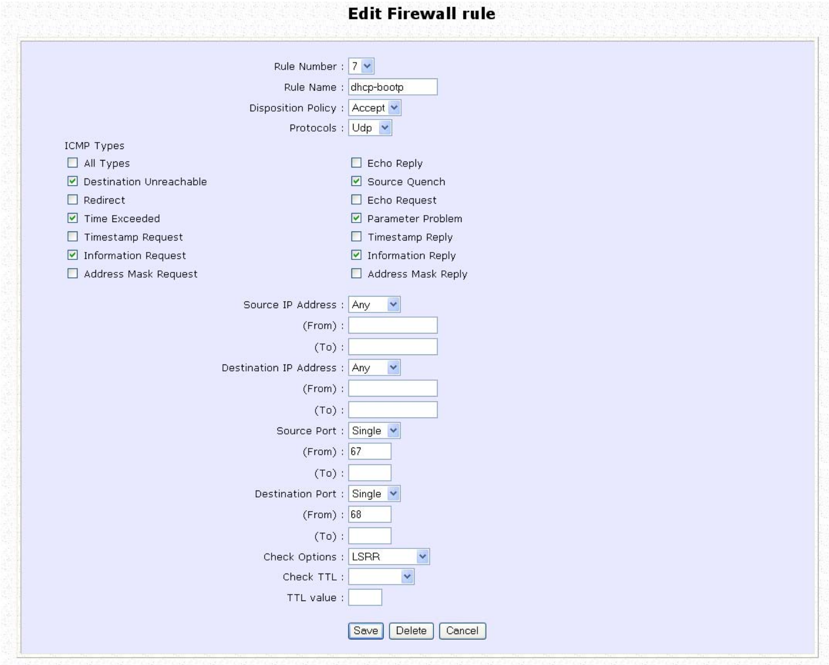
Select **Firewall Configuration** from the **Security Configuration** command menu.

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

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.



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.



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 and 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.

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 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.

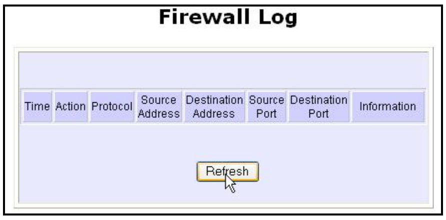
Destination Port	:	This parameter determines the application from the specified destination port. Users can either set a single port number or a range of port numbers.
Check Options	:	This parameter refers to the options in the packet header. The available selection options are abbreviated as follows: 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

Use the Firewall Log

The Firewall Log captures and stores network traffic information such as the type of data traffic, the time, the source and destination address / port, as well as the action taken by the firewall.

View Firewall Logs

Step 1:
Select **Firewall Log** from the **SECURITY CONFIGURATION** command menu.



Step 2:
Click on the **Refresh** button to see the information captured in the log:

- **Time** at which the packet was detected by the firewall.
- **Action**, which states whether the packet was accepted or denied.
- **Protocol** type of the packet.
- **Source Address** from which the packet originated
- **Destination Address** to which the packet was intended.
- **Source Port** from which the packet was initiated.
- **Destination Port** to which the packet was meant for.
- Any **Information**.

Administer the System

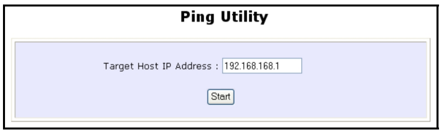
Use the System Tools

Use the Ping Utility

(Available in Wireless Routing Client and Gateway modes.)

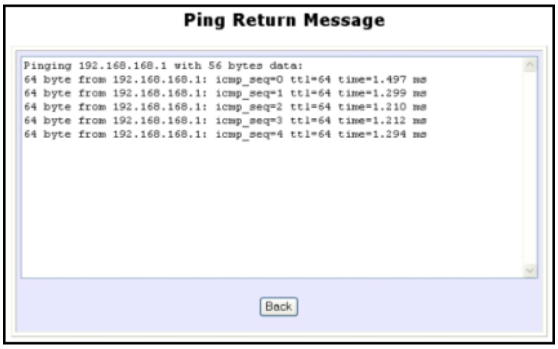
You can check whether the access point can communicate (ping) with another network host with the Ping Utility.

Step 1:
Select Ping Utility under the SYSTEM TOOLS command menu.



Step 2:
Enter the IP address of the target host to ping.

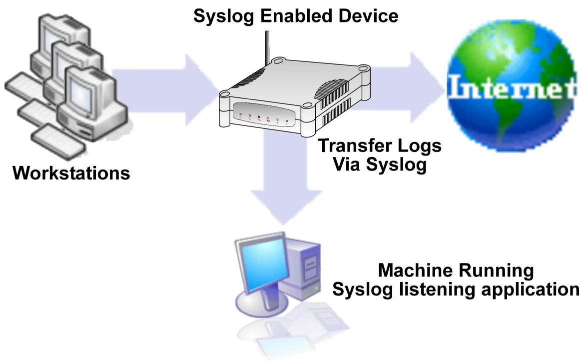
Click the Start button.



The Ping messages are 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.

Follow these steps to setup Syslog:

Step 1:
Click on **Syslog** from the **SYSTEM TOOLS** menu.

Step 2:

Select to **Enable** Syslog.

Enter the **Logging IP or Domain Name**

Enter the **Logging Port**

Click **Apply** to make the changes.

Follow these sample steps to view logged information:

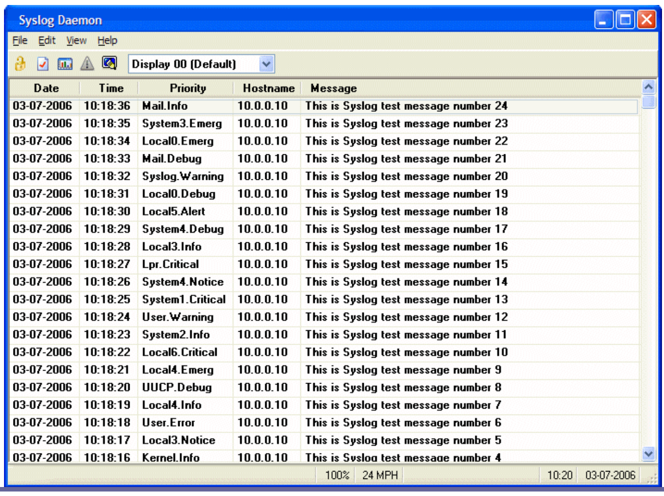
Step 1:
Search for a Syslog listening application.

Step 2:
Select a Syslog listening application.

Step 3:
Download Syslog listening application.

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	UUCP.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

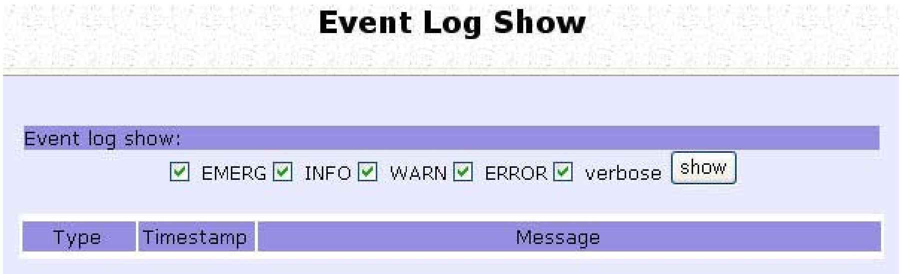
Show Event Log

An entry is added to the Event log when there is a significant occurrence in the network. Emergency, informational, warning, error, and messages for troubleshooting are recorded in the Event Log. With the event logs you can obtain information about your network. The event logs help you identify and diagnose possible network problems.

Follow these steps to show the Event Log:

Step 1:

Click on **Event Log** from the **SYSTEM TOOLS** menu.



Step 2:

Select which type of event log to show.

Event Log Types	
EMERG	Indicates that the network is unusable.
INFO	Indicates an informational message only.
WARN	Indicates a warning condition.
ERROR	Indicates an error condition.
verbose	Used for troubleshooting.

Step 3:

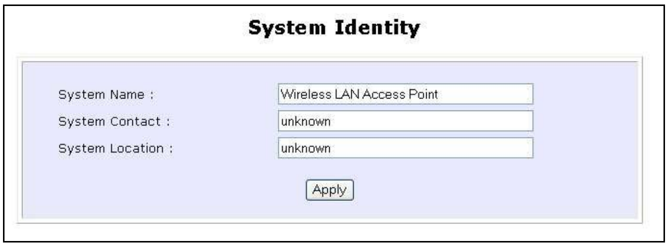
Click the **Show** button, the event log messages will be shown along with the time they were generated.

Set System Identity

You can set the **System Identity** of the access point to be uniquely identifiable.

Step 1:

Select **System Identity** from the **SYSTEM TOOLS** menu.



Step 2:

Enter a unique **System Name**.

Step 3:

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

Step 4:

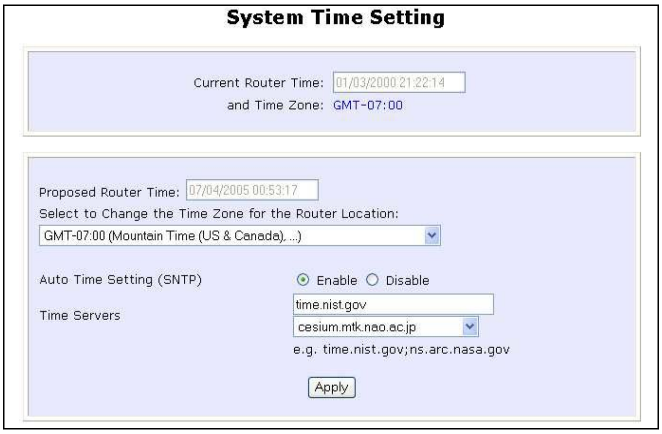
Enter the **System Location**.
This entry identifies the device location, especially when there are multiple devices.

Step 5:

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

Setup System Clock

Step 1:
Select **System Clock Setup** from the **SYSTEM TOOLS** menu.



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.

Upgrade the Firmware with uConfig

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 the updated firmware available.

Step 1:

Select **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.

You need to reboot the system after the firmware upgrade.

NOTE

The firmware upgrade process must <u>NOT</u> be interrupted; otherwise the device might become unusable.

Perform Firmware Recovery

If the system fails to launch properly, the access point will automatically switch to loader mode and the diagnostic LED will remain lighted. The firmware should then be reloaded.

Access Point State	Diagnostic LED () 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 to confirm if firmware failure has occurred.

Step 1:

Stop power supply and disconnect the access point from the network.

Step 2:

Connect the LAN port of the access point to the LAN port of your computer with an MDI cable.

Step 3:

Power on the access point, and 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.

It is recommended that your computer IP address is set to 192.168.168.100 and the network mask is set to 255.255.255.0

Step 4:

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

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** refers 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:\AP\accesspointxxx.IMG, then replace the command with this new path and firmware name. For example:
C:\AP\TFTP –i 192.168.168.1 PUT accesspointxxx.img

The recovery process takes place.
You can monitor the progress of the recovery process with the diagnostic LED.

When firmware restoration is complete, reboot the access point and it will be ready to operate.

Backup or Reset the Settings

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

Reset your settings

Step 1:

Select **Backup or Reset Settings** from the **SYSTEM TOOLS** menu.

Step 2:

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

Step 3:

The system will prompt you to reboot your device, click on the **Reboot** button.

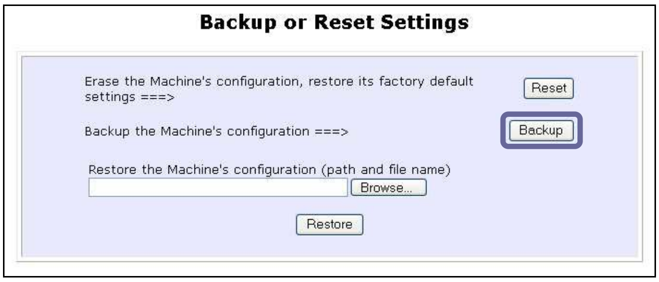
Backup your Settings

Step 1:

Select **Backup or Reset Settings** from the **SYSTEM TOOLS** menu.

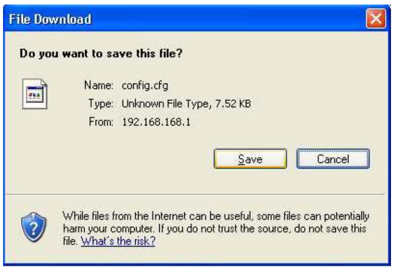
Step 2:

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



Step 3:

Save your configuration file to your local disk.



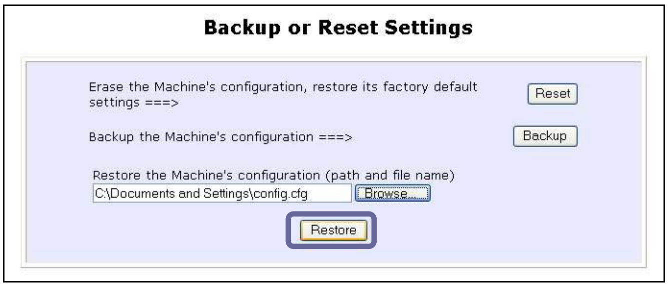
Restore your Settings

Step 1:

Select **Backup or Reset Settings** from the **SYSTEM TOOLS** menu.

Step 2:

To restore previously saved settings, click on the **Browse...** button and select the folder where you saved your configuration file.



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

Reboot the System

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

Step 1:

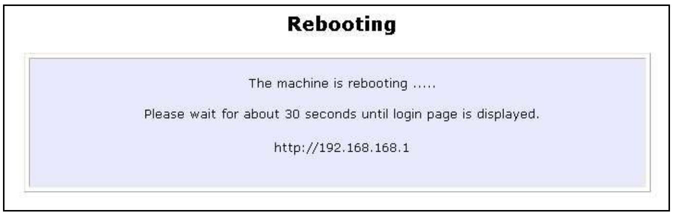
Select **Reboot System** from the **SYSTEM TOOLS** menu.

Step 2:

Click on the **Reboot** button.

Step 3:

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



Change the Password

It is recommended that the login password is changed from the factory default password.

Step 1:

Select **Change Password** from the **SYSTEM TOOLS** menu.

Step 2:

Key in the **Current Password**. The password is case-sensitive and defaulted to ***password***

Enter the **New Password** field and then **Confirm Password**.

Step 3:

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

To Logout

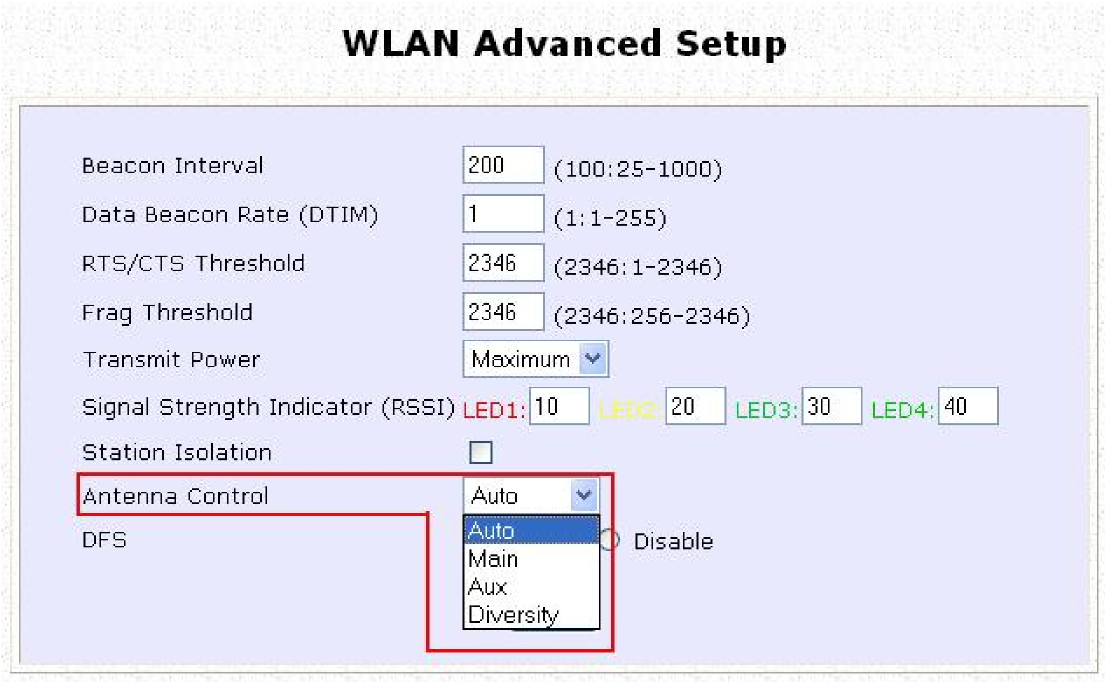
Step 1:

Select **Logout** from the **SYSTEM TOOLS** menu.

Step 2:

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

Antenna Control and Signal Strength Indicators



Antenna control default is **Auto**

In **Auto** mode, during power up, it detects the port(s) have connected an antenna. Then switch to either Main , Aux or Diversity mode. It will not save the selection. So each time it will do auto-detect when power up or when device reboot.

Select **MAIN:** will run transmit/receive signal only at antenna connected to **Main** port of radio card.

Select **AUX**: will run transmit/receive signal only at antenna connected to the **Aux** port of radio card

Select **DIVERSITY:** will run transmit/receive signal at both antennas connected to **Main** and **Aux** ports of radio card

Signal Strength Indicator settings.

LED1 (Red color) indicates low signal level
LED2 (Yellow color) indicates higher low signal level
LED3 (Green) indicates lower high signal level
LED4 (Green) indicates high signal level

The values can be adjusted to the show signal strength over any signal range. e.g. if the location max signal RSSI is 30, the 4 LEDs values can be programmed into 4 group levels,LED1=5, LED2=10, LED3=20, LED4=30 When signal exceed RSSI 5,LED1 wil light up. When RSSI exceed 10, LED1 and LED2 light up. When RSSI exceed 30, all 4 LEDs will light up.

Use the HELP menu

View About System

System Information displays system configuration information that may be required by support technicians for troubleshooting.

Select **About System** from the **HELP** menu.

The **System Information** page displays information about the access point configuration settings.

System Information

Device:	
System Up Time :	0 Days 06:45:58
BIOS/Loader Version :	2.43 (build 0310)
Firmware Version :	1.16 (build 0529)
Network Address Translation :	Enabled
Wireless:	
Hardware Address :	00-80-48-37-95-8b
WLAN name (ESSID):	Access Point
Operating frequency :	0MHz
Operating Channel :	0
Security mode :	None
RSSI:	0
LAN Port:	
Hardware Address :	00-80-48-37-95-8a
IP Address :	192.168.168.1
Network Mask :	255.255.255.0
DHCP Server :	Enabled
WAN Port:	
Hardware Address :	00-80-48-37-95-8b
WAN Type :	Dynamic (DHCP)
IP Address :	
Network Mask :	
Default Gateway :	

Additional System Information Tools

Click **Show ARP** to display the current connected list of devices.

Show ARP Table

IP address	MAC address	Interface
192.168.168.215	00:80:48:15:BF:5A	br0

Refresh

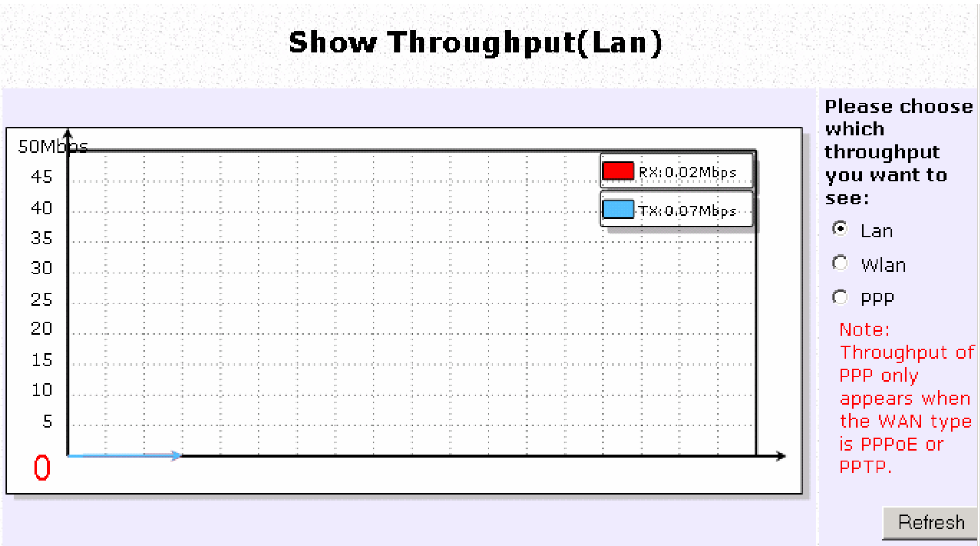
Click **Show Bridge Table** to display the active list of MAC addresses in current bridge table

Show Bridge Table

MAC Address	Interfaces	Ageing Timer
00:80:48:15:bf:5a	no	0.06
00:80:48:48:00:10	yes	0.00
00:80:48:48:00:11	yes	0.00

Refresh

Click **Show Throughput** to display the plot of receive and transmit traffic for the following interfaces, LAN , WLAN and WAN PPP. Click on one to view.



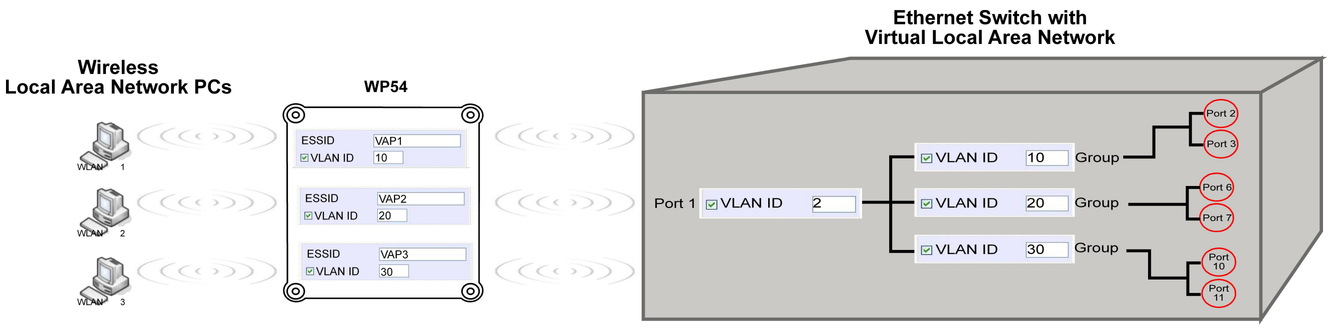
Appendix: Virtual AP (Multi-SSID) FAQ

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 internet-sharing 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.

Technical Support Information

The warranty information and registration form are found in the Quick Install Guide.

For technical support, you may contact Compex or its subsidiaries. For your convenience, you may also seek technical assistance from the local distributor, or from the authorized dealer/reseller that you have purchased this product from. For technical support by email, write to support@compex.com.sg.

Refer to the table below for the nearest Technical Support Centres:

Technical Support Centres	
Contact the technical support centre that services your location.	
U.S.A., Canada, Latin America and South America	
Asia, Australia, New Zealand, Middle East and the rest of the World	
✉ Write	Compex Systems Pte Ltd 135, Joo Seng Road #08-01, PM Industrial Building Singapore 368363
☎ Call	Tel: (65) 6286-1805 (8 a.m.-5 p.m. local time) Tel: (65) 6286-2086 (Ext.199 Technical Support)
Internet access	E-mail: support@compex.com.sg
Website:	http://www.compex.com.sg

We value your feedback. If you have any suggestions on improving, we would like to hear from you.

Please contact us at:
Fax: (65) 62809947
Email: feedback@compex.com.sg

We hope this manual was helpful to you. For more Compex information, please visit us at www.compex.com.sg