



TELETRONICS
INTERNATIONAL INC.

Focusing On Your Needs



Teletronics EZStation5

User Manual

6/18/2009

© 2009 Teletronics International, Inc

Disclaimers

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation or adaptation) without written permission from the copyright owner.

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

We may make improvements or changes in the product described in this documentation at any time. The information regarding the product in this manual is subject to change without notice.

We assume no responsibility for errors contained herein or for direct, indirect, special, incidental or consequential damages with the furnishing, performance or use of this manual or equipment supplied with it, even if the suppliers have been advised about the possibility of such damages.

Electronic Emission Notices

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

FCC INFORMATION

The Federal Communication Commission Radio Frequency Interference Statement includes the following paragraph:

The equipment 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 equipment usage generates radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no grantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

The equipment is for home or office use.

IMPORTANT NOTE

FCC RF Radiation Exposure Statement: This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the antenna and your body and must not be co-located or operating in conjunction with any other antenna or transmitter.

Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Table of Contents

OVERVIEW THE PRODUCT	6
Introduction	6
Features and Benefits.....	7
When to Use Which Mode.....	9
Access Point Mode.....	9
Access Point Client Mode	10
Wireless Routing Client Mode.....	11
Gateway Mode.....	12
Wireless Adapter Mode.....	14
Transparent Client Mode	15
PANEL VIEWS AND DESCRIPTION	17
INSTALL THE HARDWARE.....	19
Antenna Alignment.....	20
Installation Direction.....	21
Setup Requirements	22
Setting Up.....	22
Mount the Unit on a Pole	23
CONFIGURE THE IP ADDRESS.....	25
For Windows 95/98/98SE/ME/NT	25
For Windows XP/2000	27
ACCESS THE WEB INTERFACE.....	29
Access with uConfig	29
Manual access with Internet Explorer	32
PERFORM BASIC CONFIGURATION	34
Setup Management Port.....	34
To Setup DHCP Server.....	40
View Active DHCP Leases	46
Reserve IP Addresses for Predetermined DHCP Clients	47
Delete DHCP Server Reservation	49
Setup WLAN	50
Configure the Basic Setup of the Wireless Mode.....	50
Scan for Site Survey.....	55
View Link Information	58
Scan for Channel Survey	60
Align the Antenna.....	63
Configure the Advanced Setup of the Wireless Mode	65
View the Statistics.....	67

Setup your WAN.....	68
Setup Telnet / SSH	76
Access the TELNET Command Line Interface.....	78
Access the Secure Shell Host Command Line Interface	79
Set the WEB Mode	80
Setup SNMP.....	81
Setup SNMP Trap	82
Setup STP	83
Use MAC Filtering	86
Add a MAC Address to the MAC Address List	87
Delete a MAC Address From All Access Points	90
Delete a MAC address from individual access point	92
Edit MAC Address from the MAC Address List.....	94
PERFORM ADVANCED CONFIGURATION.....	96
Setup Routing	96
Configure Static Routing.....	97
Use Routing Information Protocol.....	98
Use Network Address Translation.....	99
Configure Virtual Servers Based on DMZ Host	100
Configure Virtual Servers Based on Port Forwarding	101
Configure Virtual Servers based on IP Forwarding	105
Control the Bandwidth Available	106
Enable Bandwidth Control	106
Configure WAN Bandwidth Control.....	107
Configure LAN Bandwidth Control.....	108
Perform Remote Management.....	110
Setup Remote Management.....	110
USE PARALLEL BROADBAND	111
Enable Parallel Broadband	112
Setup Email Notification.....	113
Using Static Address Translation.....	115
Use DNS Redirection.....	116
Enable or Disable DNS Redirection	118
Dynamic DNS Setup	119
To enable/disable Dynamic DNS Setup	119
To manage Dynamic DNS List	120
USE THE WIRELESS EXTENDED FEATURES.....	124
Setup WDS2.....	124
Set Virtual AP (Multiple SSID)	128
Set Preferred APs.....	130
Get Long Distance Parameters	131
Set Wireless Multimedia.....	133
Setup Point-to-Point & Point-to-MultiPoint Connection	136

SECURE YOUR WIRELESS LAN	140
Setup WEP	141
Setup WPA-Personal	142
Setup 802.1x/RADIUS	144
Setup WPA Enterprise	146
CONFIGURE THE SECURITY FEATURES	148
Use Packet Filtering	148
Configure Packet Filtering	148
Use URL Filtering	151
Configure URL Filtering	151
Configure the Firewall	152
Configure SPI Firewall	152
Use the Firewall Log	156
View Firewall Logs	156
ADMINISTER THE SYSTEM	157
Use the System Tools	157
Use the Ping Utility	157
Use Syslog	158
Set System Identity	161
Setup System Clock	161
Upgrade the Firmware with UConfig	163
Upgrade the Firmware with Command Line Interface	164
Perform Firmware Recovery	167
Backup or Reset the Settings	169
Reboot the System	172
Change the Password	173
To Logout	174
Use the HELP menu	175
View About System	175
Get Technical Support	176
APPENDIX: USE THE COMMAND LINE INTERFACE	177
APPENDIX: VIRTUAL AP (MULTI-SSID) FAQ	181
APPENDIX: VIEW THE TECHNICAL SPECIFICATIONS	185
TECHNICAL SUPPORT INFORMATION	188

Overview the Product

Introduction

The EZStation5 Outdoor Access Point is a high-performance AP designed for enterprise and outdoor users. The access point is compatible with IEEE 802.11a and supports high-speed data transmission of up to 54Mbps. This equips the access point with network robustness, stability and wider network coverage. Housed in a weatherproof casing, the access point is designed to withstand any outdoor climatic conditions, making it the ideal solution for outdoor applications.

The access point is capable of operating in 7 modes: **Access Point Mode, Client Mode, Wireless Routing Client, Gateway Mode, Wireless Adapter Mode, and Transparent Client Mode** which is specifically developed to be paired with root access point for Point-to-Point and Point-to-MultiPoint connection.

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

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.

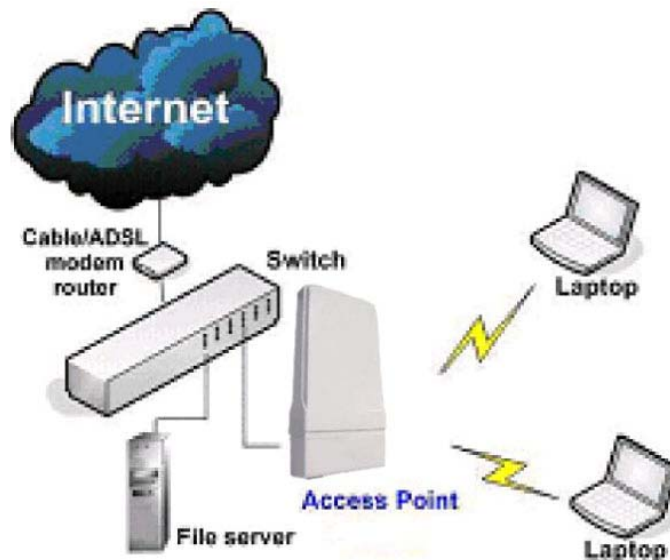
- **WDS2**

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.

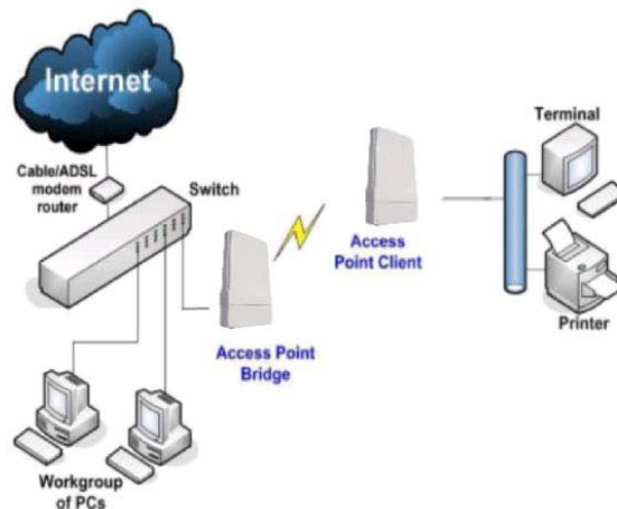
In this mode it can only connect with another access point. Other wireless clients cannot connect to it directly unless they are also connected to the same access point – allowing them to communicate with all devices connected to the Ethernet port of the access point.

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

Optional additional feature:

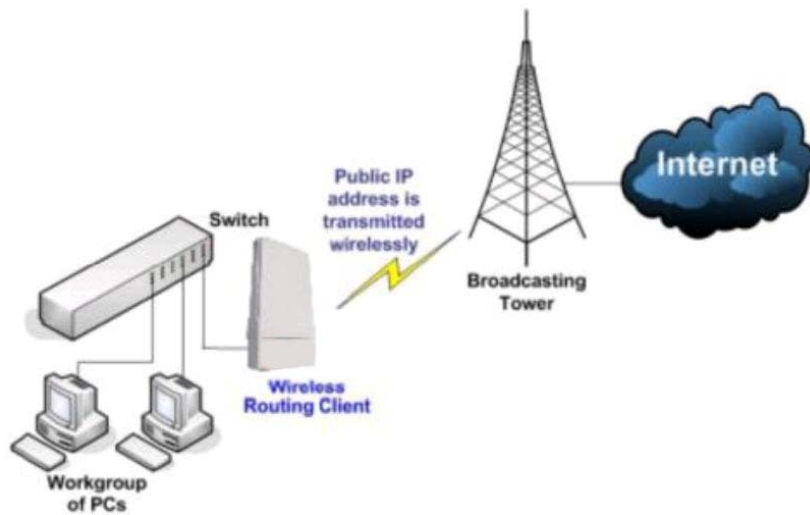
Point-to-Point connection in this operation mode is also supported if you specifically wish to connect with an access point only.

Please refer to the Point-to-Point setup section.



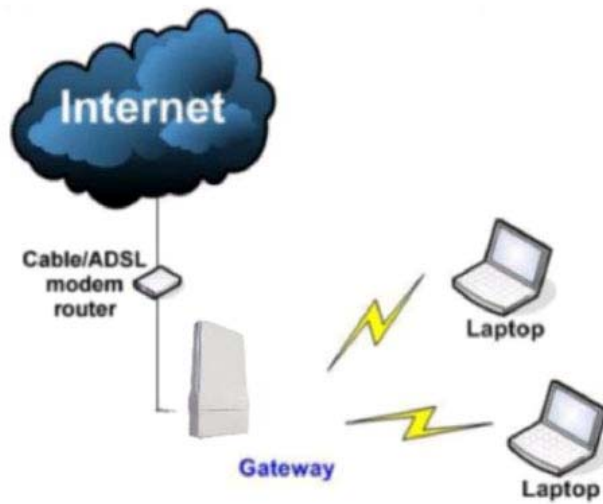
Wireless Routing Client Mode

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)

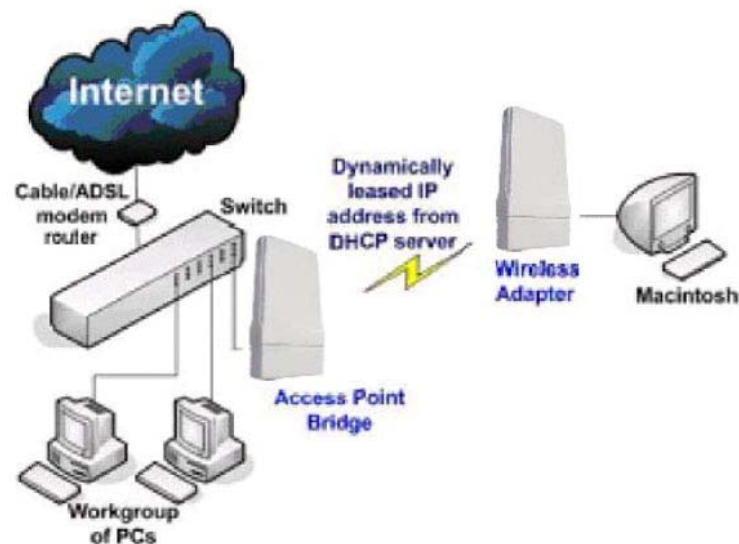
Wireless Adapter Mode

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.

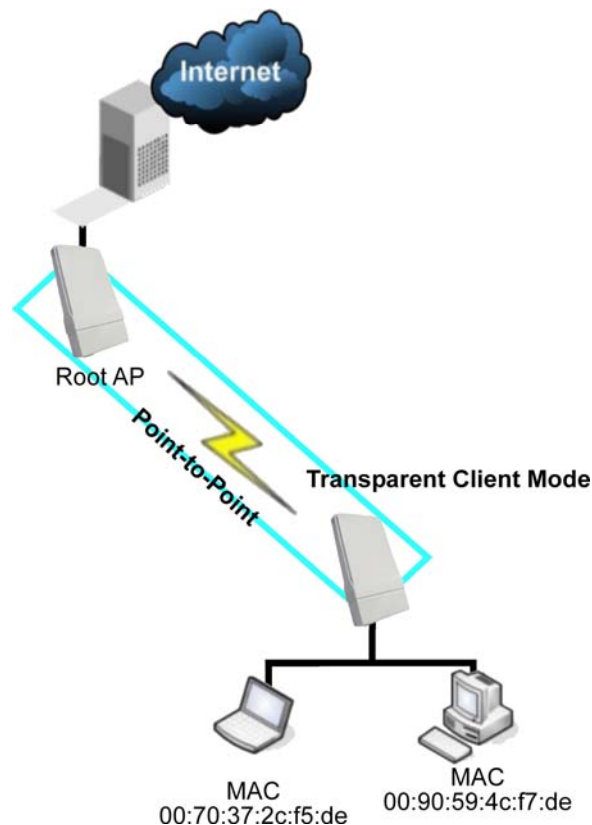


Transparent Client Mode

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

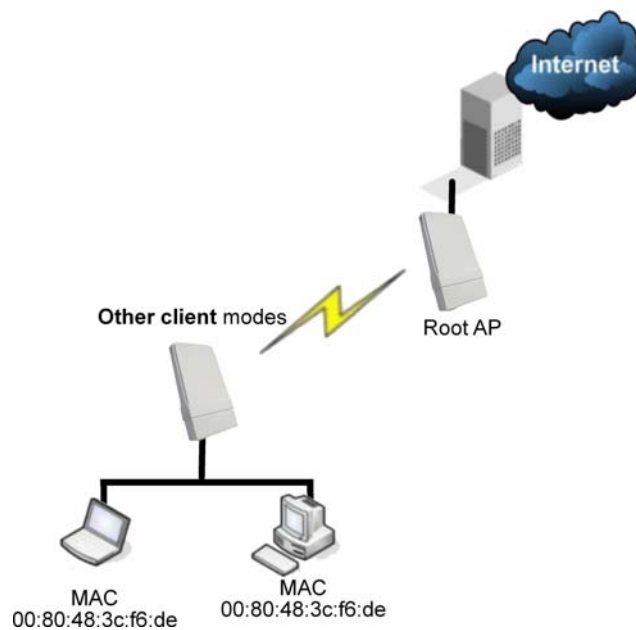
Point-to-Point	Point-to-MultiPoint
An access point acts as Root AP and 1 other access point acts as Transparent Client.	An access point acts as Root AP and several other access point acts as Transparent Clients.

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

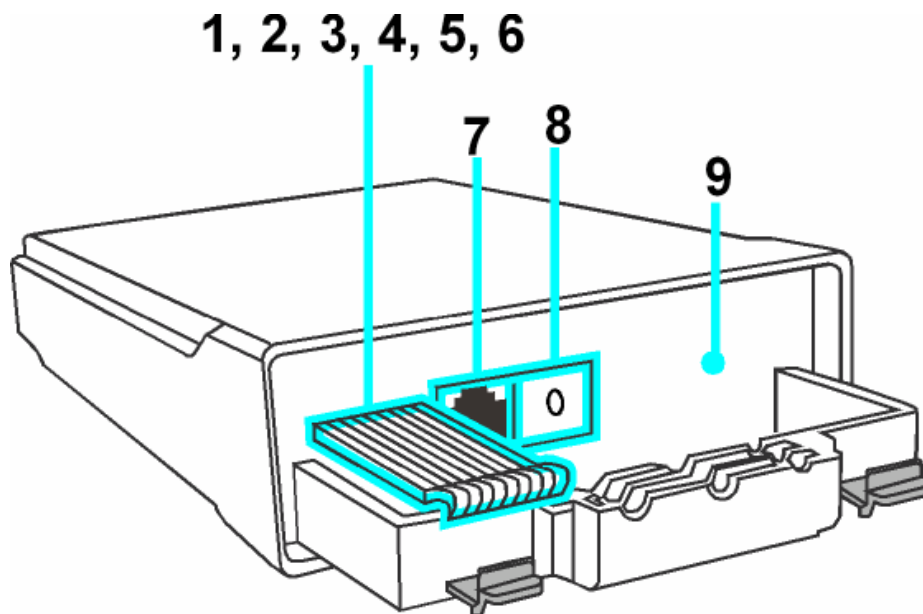


Difference Between other client modes and Transparent Client Mode	
Other client modes	Transparent Client Mode
Connectivity with any standard APs.	Connectivity with RootAP-supported APs.
All devices connected to the Ethernet ports use a common MAC address for communications with the AP.	Devices connected 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.



Panel Views and Description



	Features	Status and Indication	
1	POWER LED	Steady Red	Power is supplied to the device.
		Off	No power is supplied to the device.
2	10 ACT LED	Steady Red	The respective port has successfully connected to the access point.
		Blinking	The respective port is transmitting or receiving data.
		Off	No connection is established.
3	100 ACT LED	Steady Red	The respective port has successfully connected to the access point.
		Blinking Red	The respective port is transmitting or receiving data.
		Off	No connection is established.

4	WLAN LED	Steady Red	Wireless interface up and running. Ready for operation.
		Flashing Red	Activity is detected in the wireless network.
5	WAN Conn LED	Flashing Red	Data transmission at WAN connection.
6	DIAG LED	Flashing Red	It indicates that the firmware is corrupted.
7	LAN	<p>Connection for computer with NIC (Network Interface Card) or Ethernet network card.</p> <p>Device is power up with PoE on this LAN port.</p>	
8	SURGE ARRESTOR	Connect to a ground wire.	
10	RESET BUTTON	<p>To reboot, press once.</p> <p>To reset password, press and hold the button for 5 seconds before releasing it.</p> <p>To restore the factory default settings, press and hold the button for 8 seconds before releasing it.</p>	

Install the Hardware

This section will show you how to install the hardware of the access point.

- **Antenna Alignment**

The antenna alignment of the access point must first be considered to ensure that the signal is strong.

- **Installation Direction**

After considering the antenna alignment, the direction in which the access point is facing must be considered to ensure that the signal is actually being directed to the receiving end.

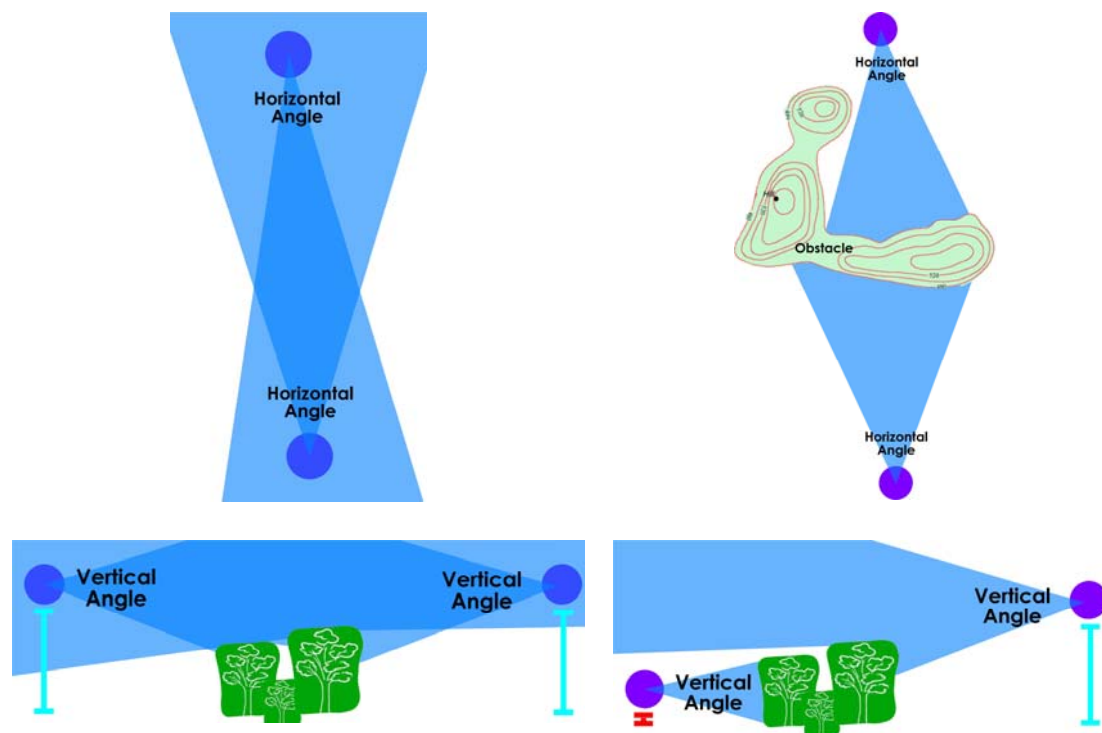
- **Setting Up**

Lastly, after making these considerations and confirming the final position and facing direction of the access point, follow the instructions to physically set up and complete the installation of the access point.

Antenna Alignment

The physical environment of the antenna must be examined when aligning the antenna. Obstructions, available mounting locations, and other factors must be considered. Many objects such as forests, buildings, and hills, can obstruct the antenna, reducing the signal strength. The antenna can be installed at a height above such obstructions, and aligned so that antennas are directed at each other by taking into account the horizontal angle and the vertical angle of the antenna signal.

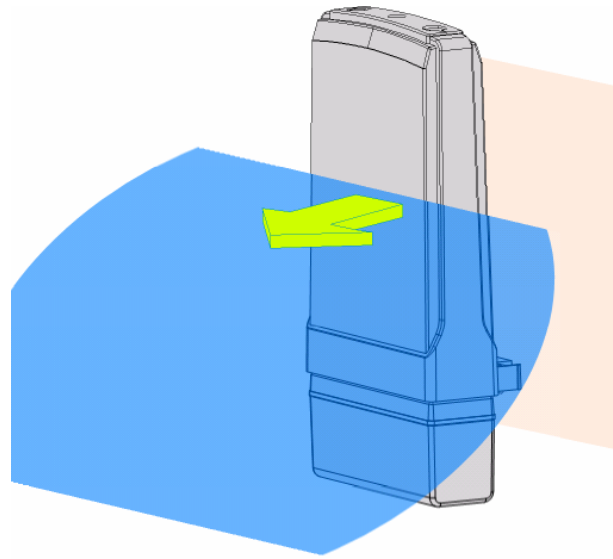
When the antenna is at the optimum alignment, there is less possibility of encountering interference and of causing interference to anyone else, and strong signal strength can be maintained.



NOTE

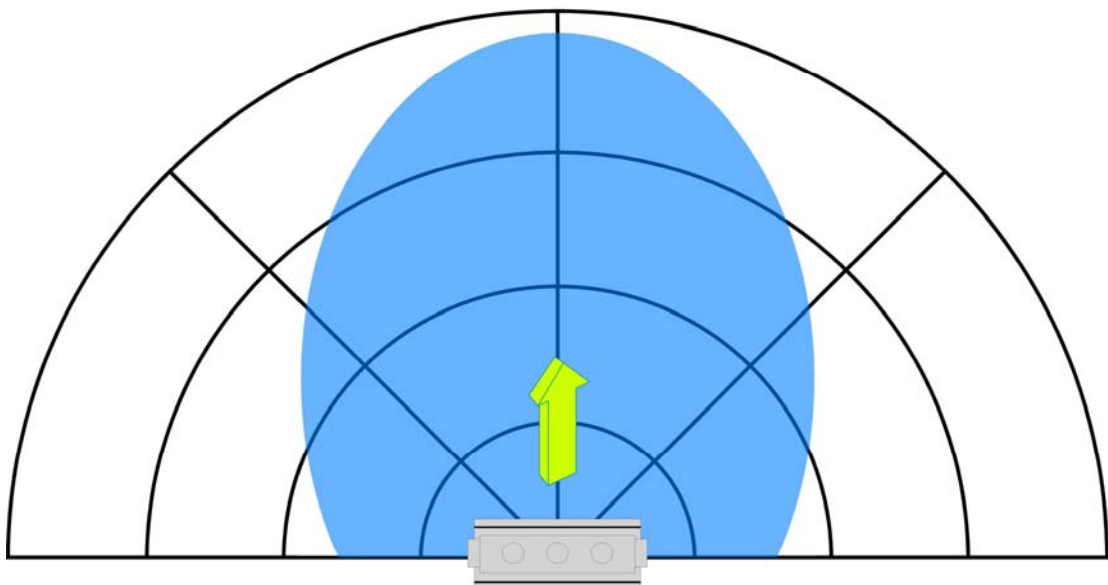
When the antennas are at the same height, it is quite simple to align the antennas. However, when the antennas are at different heights, greater care has to be taken to ensure that the antennas are properly aligned.

Installation Direction



Front Towards Desired Signal Direction

The directional antenna radiates the signal towards the front of the unit. The unit should be installed in a position whereby the front of the unit faces the direction you wish to send the signal to. Therefore the direction you wish to send the signal to has to be considered before going on to the next step of starting to set up the access point.



Front Towards Desired Signal Direction

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.

Setting Up

You can install your access point on a pole. The mounting method will be described as shown below.

Note the following guidelines for choosing the best location for your wireless AP:

- Place the AP as close as possible to the area where users will require access to the WLAN.
- Choose an elevated location where trees, buildings and large steel structures will not obstruct the antenna signals and which offers maximum line-of-sight propagation with the users.
- Select an appropriate antenna to improve range and/or coverage and the access point also lets you fine-tune parameters such as the transmit power to achieve the best results.

Mount the Unit on a Pole

Step 1

Unpack the 2 cable ties from the box.



Step 2

Loop each cable tie through the mounting bracket hole at the top and bottom. Wrap them round the pole and tighten the cable ties to secure the unit to the pole.

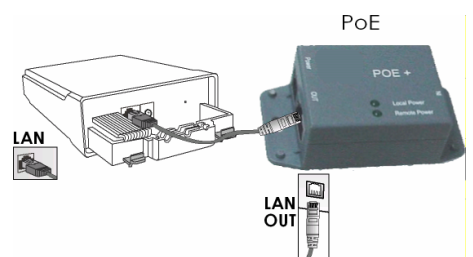


Step 3

Connect one end of an RJ45 Ethernet cable to the LAN OUT port of the Injector and the other end to LAN of the access point.

Maximum length of the RJ45 Category 5 cable is 100 meters*.

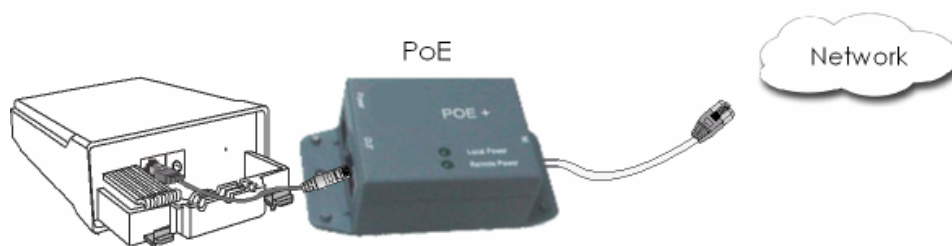
* Up to 200mW radio. For higher power radio need upgrade to higher rating power adapter.



Step 4

Connect the RJ45 Ethernet cable attached to the PoE Injector to a network device, such as to a switch or to the PC you will use to configure the access point.

PoE power input: Passive PoE (range 12V – 24V DC)



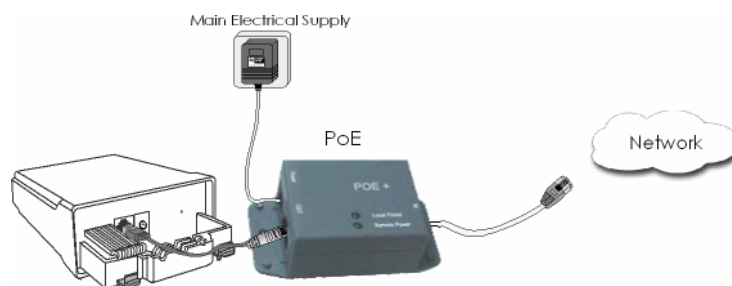
Step 5

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

Now, turn on your power supply. Notice that the **POWER** LED has lighted up. This indicates that the access point is receiving power through the PoE Injector and that connection between the access point and your network has been established.

Note:

Please use the power adapter in the PoE kit. Using a power adapter with a different voltage rating will damage this product.



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:

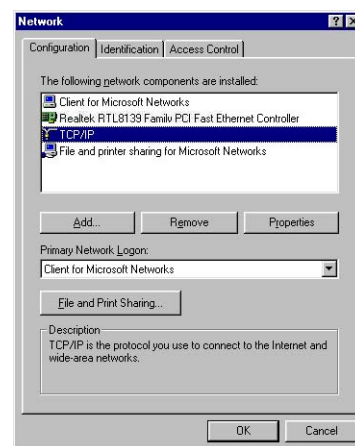
From your desktop, right-click the **Network Neighborhood** icon and select **Properties**.

Step 2:

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

Step 3:

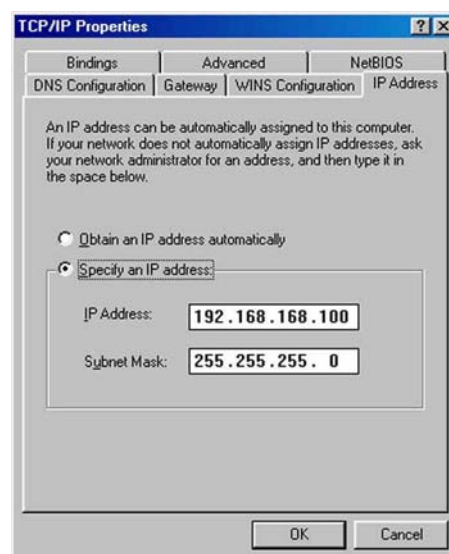
Highlight **TCP/IP** and click on the **Properties** button.



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.

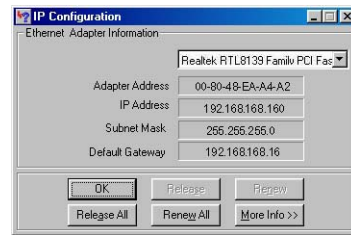


Step 5:

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.



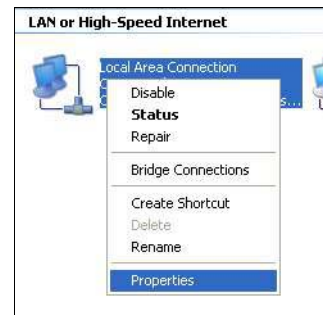
For Windows XP/2000

Step 1:

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

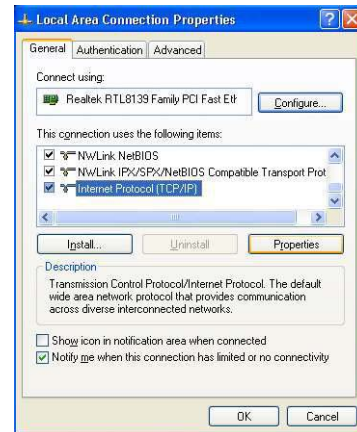
Step 2:

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



Step 3:

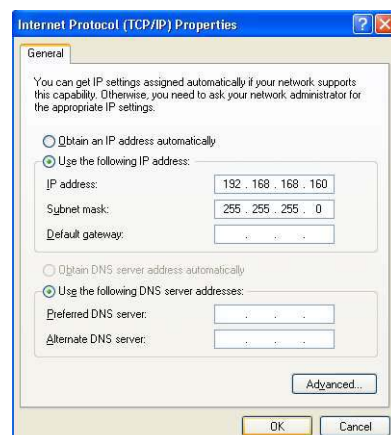
Highlight **Internet Protocol (TCP/IP)** and click on the **Properties** button.



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.

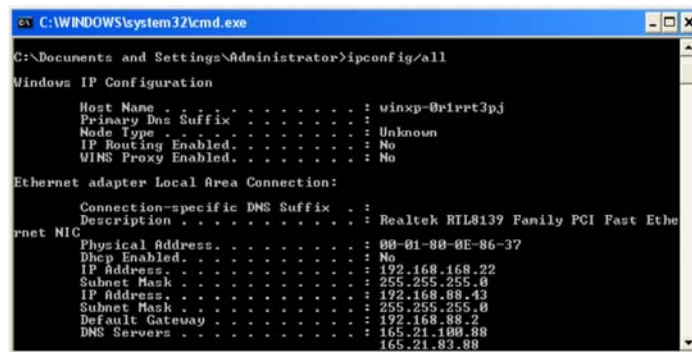


Step 5:

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*



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

Windows IP Configuration

Host Name . . . . . : winxp-01rvrt3pj
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . : Realtek RTL8139 Family PCI Fast Ethernet NIC
   Physical Address. . . . . : 00-01-80-0E-86-37
   Dhcp Enabled. . . . . : No
   IP Address. . . . . : 192.168.168.22
   Subnet Mask . . . . . : 255.255.255.0
   IP Address. . . . . : 192.168.88.43
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 192.168.88.2
   DNS Servers . . . . . : 165.21.188.88
                           165.21.83.88
```

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

Access the Web Interface

Access with uConfig

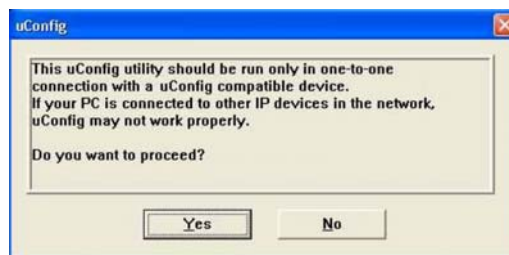
The UConfig utility provides direct access to the web interface.

Step 1:

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

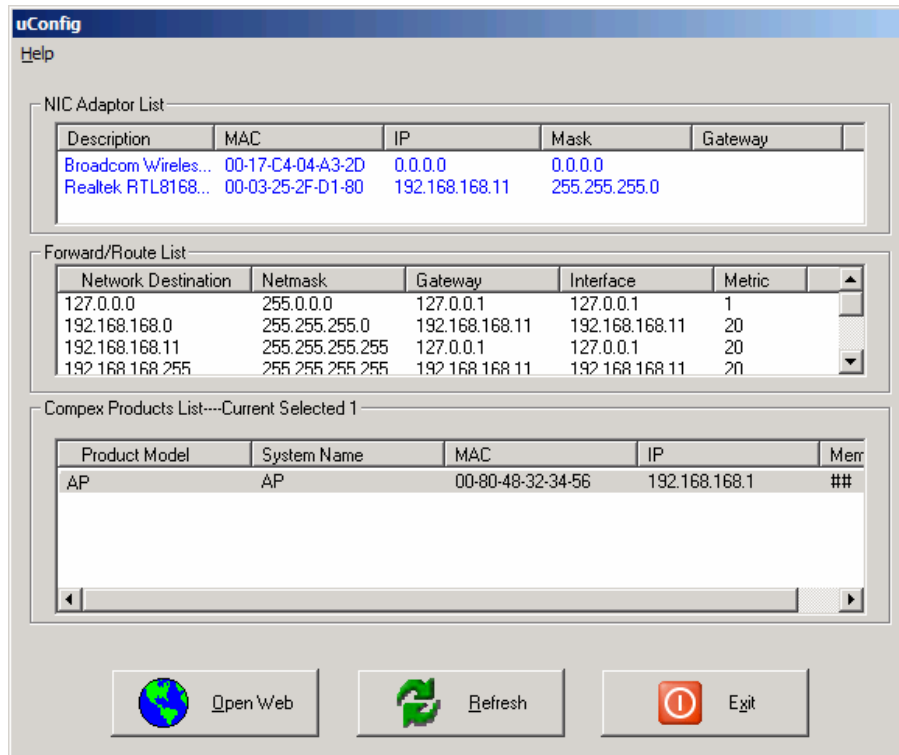
Step 2:

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.



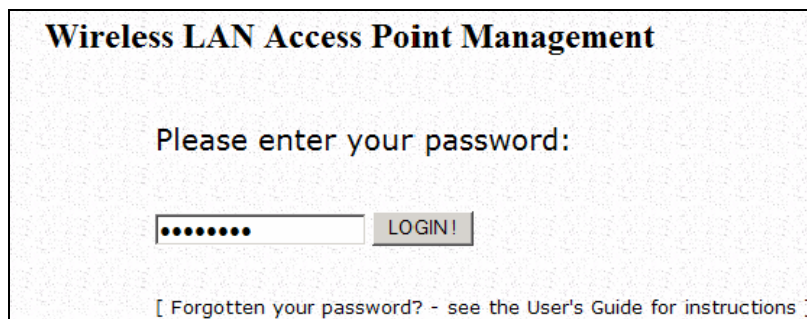
Step 4:

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.



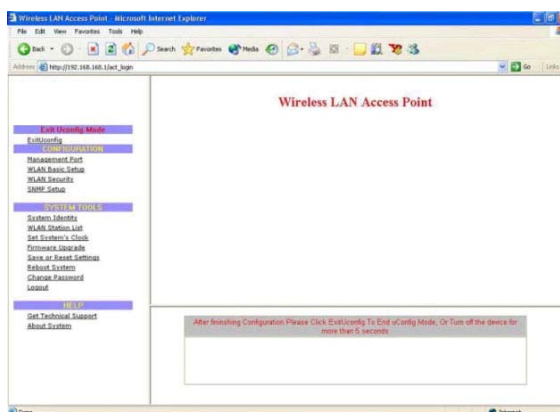
Step 5:

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

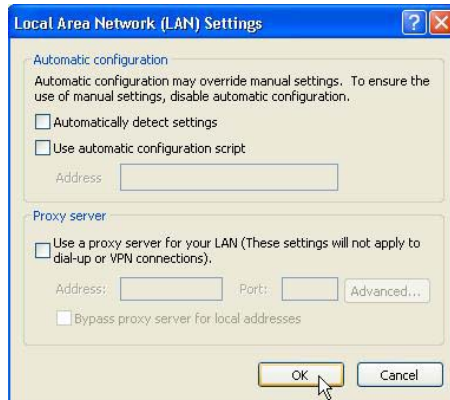
Step 1:

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



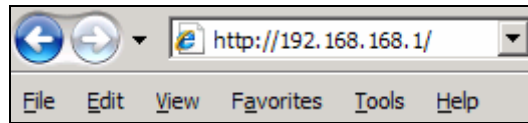
Step 2:

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



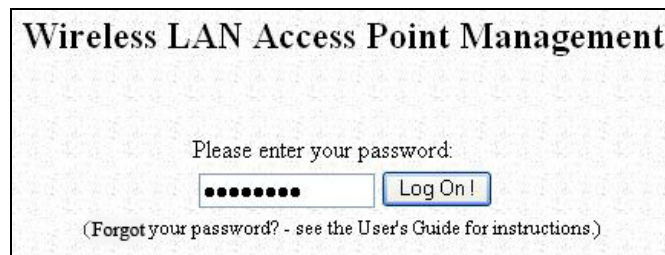
Step 3:

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

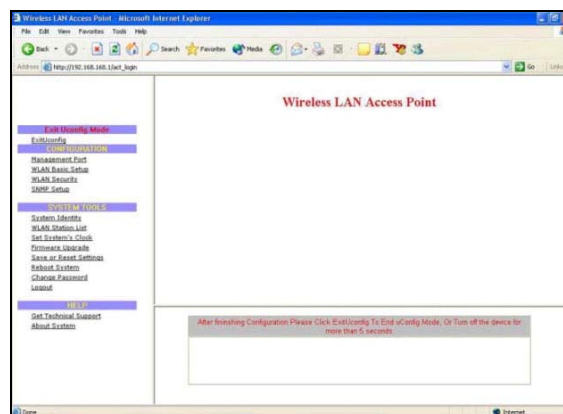


Step 4:

At the login page, click on the **LOG ON !** Button.



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



Perform Basic Configuration

Setup Management Port

At the Management Port Setup page, you may:

- Set Ethernet Link Speed and duplex settings.
- Automatically obtain IP address from DHCP server.
The default IP 192.168.168.1 is used until a new IP is obtained.
Access Point Clients also allows PCs connected to the Ethernet port to obtain IP from the DHCP server at the access point end network.
- Manually define IP address

Follow these steps to set Ethernet Link Speed and duplex settings.

Step 1:

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

Step 2:

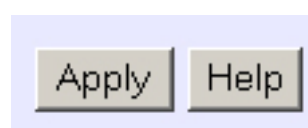
Select the desired **Ethernet Link Speed** and duplex settings.

- Auto: Automatic Detection
- 100 Full: 100BaseT Full-Duplex
- 100 Half: 100BaseT Half-Duplex
- 10 Full: 10BaseT Full-Duplex
- 10 Half: 10BaseT Half-Duplex

Management Port Setup	
Ethernet Link Speed	Auto
IP Address:	4
Network Mask:	0
Default Gateway IP:	

Step 2:

Click the **Apply** button.



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

Step 1:

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

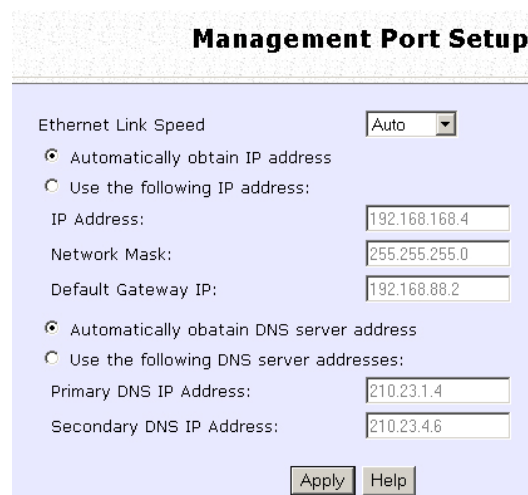
Step 2:

Select to **Automatically obtain IP address**.

Step 3:

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

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



The screenshot shows the 'Management Port Setup' configuration page. It features a title bar with the text 'Management Port Setup'. Below the title bar, there are several configuration options:

- Ethernet Link Speed:** A dropdown menu set to 'Auto'.
- IP Address Configuration:** Two radio buttons are present. The first, 'Automatically obtain IP address', is selected. The second, 'Use the following IP address:', is unselected. Below this, there are three input fields: 'IP Address' (192.168.168.4), 'Network Mask' (255.255.255.0), and 'Default Gateway IP' (192.168.88.2).
- DNS Server Configuration:** Two radio buttons are present. The first, 'Automatically obtain DNS server address', is selected. The second, 'Use the following DNS server addresses:', is unselected. Below this, there are two input fields: 'Primary DNS IP Address' (210.23.1.4) and 'Secondary DNS IP Address' (210.23.4.6).

At the bottom of the form, there are two buttons: 'Apply' and 'Help'.

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

Management Port Setup

Ethernet Link Speed Auto ▾

Automatically obtain IP address
 Use the following IP address:

IP Address:
Network Mask:
Default Gateway IP:

Automatically obtain DNS server address
 Use the following DNS server addresses:

Primary DNS IP Address:
Secondary DNS IP Address:

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

Step 3:

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

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

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

Follow these steps to manually define the IP address.

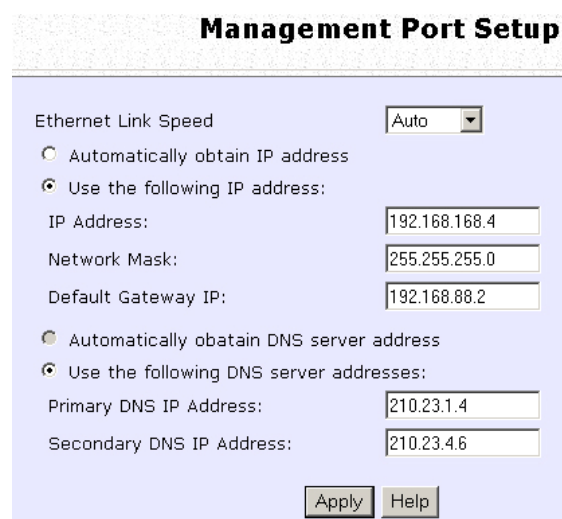
Step 1:

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

Step 2:

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

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



Management Port Setup

Ethernet Link Speed: Auto

Automatically obtain IP address

Use the following IP address:

IP Address: 192.168.168.4

Network Mask: 255.255.255.0

Default Gateway IP: 192.168.88.2

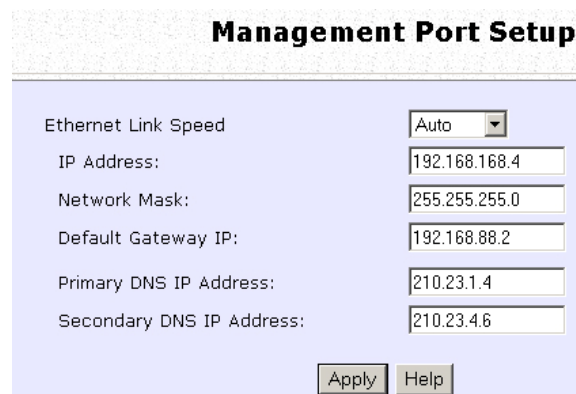
Automatically obtain DNS server address

Use the following DNS server addresses:

Primary DNS IP Address: 210.23.1.4

Secondary DNS IP Address: 210.23.4.6

Apply Help



Management Port Setup

Ethernet Link Speed: Auto

IP Address: 192.168.168.4

Network Mask: 255.255.255.0

Default Gateway IP: 192.168.88.2

Primary DNS IP Address: 210.23.1.4

Secondary DNS IP Address: 210.23.4.6

Apply Help

The parameters are the same in routing mode.

Step 3:

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

This table describes the parameters that can be modified in the **Management Port Setup** page.

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

To Setup DHCP Server

There are 3 DHCP Modes:

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

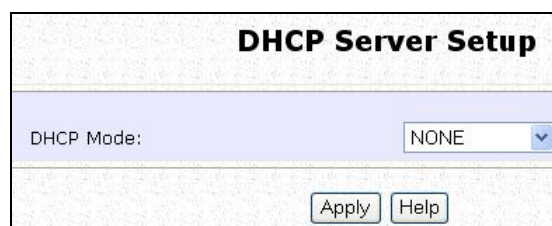
Follow these steps if you do not wish to use DHCP.

Step 1:

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

Step 2:

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



DHCP Server Setup	
DHCP Mode:	NONE
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Step 3:

Click on the **Apply** button.

The following will guide you to setup the DHCP Server.

Step 1:

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

Step 2:

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

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

DHCP Server Setup	
DHCP Mode:	<input type="text" value="DHCP Server"/>
DHCP Start IP Address:	<input type="text" value="192.168.168.100"/>
DHCP End IP Address:	<input type="text" value="192.168.168.254"/>
DHCP Gateway IP Address:	<input type="text" value="192.168.88.2"/>
DHCP Lease Time:	<input type="text" value="3600"/> (seconds)
Primary DNS IP Address:	<input type="text" value="210.23.1.4"/>
Secondary DNS IP Address:	<input type="text" value="210.23.4.6"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Step 3:

Click on the **Apply** button.

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

Parameters	Description
<p>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.</p>	
DHCP Start IP Address	<p>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 <i>192.168.168.100</i>.</p>
DHCP End IP Address	<p>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 <i>192.168.168.254</i>.</p>

<p>DHCP Gateway IP Address</p>	<p>Though the DHCP server usually also acts as the Default Gateway of the DHCP client, the access point allows you to define a different 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.</p> <p>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.</p>
<p>DHCP Lease Time</p>	<p>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.</p>
<p>Primary DNS IP Address</p>	<p>Your ISP usually provides the IP address of the DNS server.</p>
<p>Secondary DNS IP Address</p>	<p>This optional setting is the IP address of a secondary DNS server.</p>

The following will guide you to setup the DHCP Relay.

Step 1:

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

Step 2:

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

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

DHCP Server Setup	
DHCP Mode:	<input type="text" value="DHCP Relay"/>
DHCP server IP:	<input type="text" value="192.168.168.254"/>
DHCP Gateway IP:	<input type="text" value="192.168.1.1"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

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	<p>Though the DHCP server usually also acts as the Default Gateway of the DHCP client, the access point allows you to define a different 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.</p> <p>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.</p>

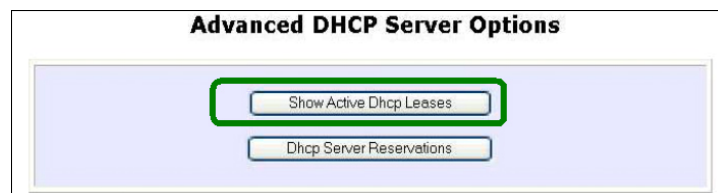
View Active DHCP Leases

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**.



The screenshot shows a table titled "DHCP Active Leases". The table has four columns: "Host Name", "IP Address", "Hardware Address", and "Lease Expired Time". There is one row of data with the following values: "sampleHost", "192.168.168.22", "09-00-7c-01-00-01", and "11". Below the table are three buttons: "Refresh", "Help", and "Back".

Host Name	IP Address	Hardware Address	Lease Expired Time
sampleHost	192.168.168.22	09-00-7c-01-00-01	11



NOTE

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

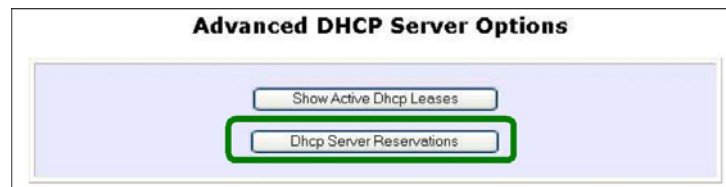
Reserve IP Addresses for Predetermined DHCP Clients

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

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

Step 1:

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



Step 2:

Click on the **Add** button.



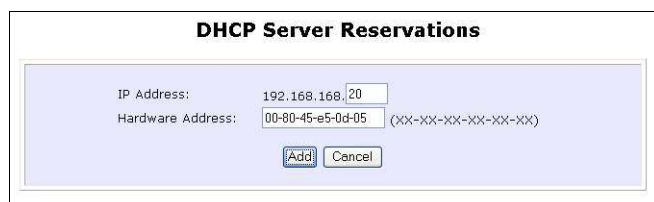
Step 3:

Fill in:

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

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

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



DHCP Server Reservations

IP Address: 192.168.168.20

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

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



DHCP Server Reservations

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

Delete DHCP Server Reservation

Step 1:

Select the reserved IP address to delete.

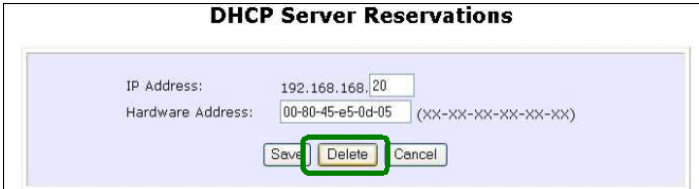


The screenshot shows a table titled "DHCP Server Reservations". The table has two columns: "IP Address" and "Hardware Address". The first row contains the IP address "192.168.168.20" and the hardware address "00-80-45-e5-0d-05". The IP address cell is highlighted with a green border. Below the table are two buttons: "Add" and "Back".

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

Step 2:

Click on the **Delete** button.



The screenshot shows the "DHCP Server Reservations" form. It has two input fields: "IP Address" with the value "192.168.168.20" and "Hardware Address" with the value "00-80-45-e5-0d-05" and a placeholder "(XX-XX-XX-XX-XX-XX)". Below the fields are three buttons: "Save", "Delete", and "Cancel". The "Delete" button is highlighted with a green border.

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.

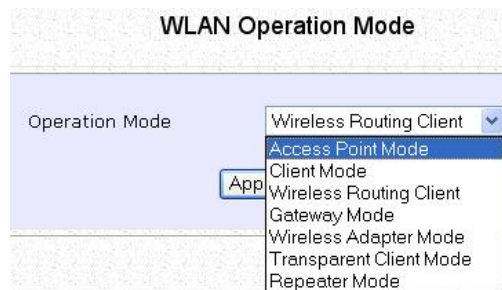


The screenshot shows the 'WLAN Basic Setup' configuration page. It includes the following fields and options:

- Card Status: enable
- The Current Mode: Access Point (with a 'Change' button)
- ESSID: sampleRouter
- Wireless Profile: 802.11a
- Country: NO_COUNTRY_SET-(NA)
- Channel: SmartSelect (with a 'Channel Survey' button)
- Tx Rate: Fully Auto
- Options: Closed System, Act as RootAP, VLANID (with an input field)
- Buttons: 'Apply' and 'Channel Survey'

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.



The screenshot shows the 'WLAN Operation Mode' configuration page. It features a dropdown menu for 'Operation Mode' with the following options:

- Wireless Routing Client
- Access Point Mode (highlighted)
- Client Mode
- Wireless Routing Client
- Gateway Mode
- Wireless Adapter Mode
- Transparent Client Mode
- Repeater Mode

An 'Apply' button is visible next to the dropdown menu.

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**

The screenshot shows the 'WLAN Basic Setup' interface for Client Mode. The title is 'WLAN Basic Setup'. The 'Card Status' is 'enable'. 'The Current Mode' is 'Client' with a 'Change' button. The 'ESSID' is 'sampleRouter' with a 'Site Survey' button. 'Remote AP MAC' is an empty field with a checkbox. 'Wireless Profile' is '802.11a'. 'Country' is 'NO_COUNTRY_SET-(NA)'. 'Tx Rate' is 'Fully Auto'. There is an 'Apply' button at the bottom.

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

The screenshot shows the 'WLAN Basic Setup' interface for Access Point mode. The title is 'WLAN Basic Setup'. The 'Card Status' is 'enable'. 'The Current Mode' is 'Access Point' with a 'Change' button. The 'ESSID' is 'sampleRouter' with a 'Channel Survey' button. 'Wireless Profile' is '802.11a'. 'Country' is 'NO_COUNTRY_SET-(NA)'. 'Channel' is 'SmartSelect'. 'Tx Rate' is 'Fully Auto'. There are checkboxes for 'Closed System', 'Act as RootAP', and 'VLANID' (with an empty input field). There is an 'Apply' button at the bottom.

WLAN Basic Setup page Parameters	Description
<p>The Current Mode</p>	<p>The default operating mode is the Access Point mode. Operating modes:</p> <ul style="list-style-type: none"> • Access Point Mode • Client Mode • Wireless Routing Client • Gateway Mode • Wireless Adapter Mode • Transparent Client Mode • Repeater Mode <p>You can toggle the modes by clicking on the Change button.</p>
<p>ESSID</p>	<p>Enter a preferred name for the wireless network. Your wireless clients must be configured with the same ESSID. This case-sensitive entry can consist of a maximum of 32 characters.</p>
<p>Site Survey</p>	<p>A list of wireless devices in the WLAN that are detected by your access point. Information such as MAC address, channel, SSID, algorithm and signal strength can be found in the listing. This feature is supported by the Access Point Client and Wireless Routing Client modes.</p>

Wireless Profile	<p>A selection of network environment types in which to operate the access point:</p> <ul style="list-style-type: none"> • 802.11a only (Version AG) Supports wireless A clients with data rates of up to 54Mbps in the frequency range of 5GHz. • 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	<p>Choose the Country where you are located.</p>
Channel	<p>This option allows you to select a frequency channel for the wireless communication and is only available in the Access Point, Point to Point and Point to Multiple Point modes. Select SmartSelect to automatically scan and recommend the best channel that the access point can utilize.</p>
Tx Rate	<p>Allows you to choose the rate of data transmission ranging from 1Mbps to Fully Auto.</p>
Closed System	<p>The access point will not broadcast its WLAN name (ESSID) when Closed system is enabled. By default Closed system is disabled.</p>

<p>Act as RootAP</p>	<p>The access point will connect with 1, or multiple clients to create a point-to-point and point-to-multi-point connection network with 2 or more access points.</p> <p>This connection mode is fully compliant with 802.1h standards.</p>
<p>VLAN ID</p>	<p>This is the number that identifies the different virtual network segments to which the network devices are grouped.</p> <p>This can be any number from 1 to 4094.</p>
<p>Channel Survey</p>	<p>A list of channels that are detected by your access point in the WLAN. Information such as frequency, channel, MyQuality, NeighQuality, APCount and Recommendation can be found in the listing.</p> <p>The Access Point and Gateway modes support this feature.</p>

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 screenshot shows the 'WLAN Basic Setup' configuration page. The 'Card Status' is set to 'enable'. The 'Current Mode' is 'Client', with a 'Change' button next to it. The 'ESSID' is 'sampleRouter'. The 'Remote AP MAC' field is empty with a checkbox to its right. The 'Wireless Profile' is '802.11a'. The 'Country' is 'NO_COUNTRY_SET-(NA)'. The 'Tx Rate' is 'Fully Auto'. An 'Apply' button is at the bottom. A 'Site Survey' button is located on the right side of the page, highlighted with a green border.

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.

The screenshot shows the 'Site Survey' results page. It contains a table with the following data:

Bssid	SSID	Chan	Auth	Alg	Signal
<input type="radio"/> 008048003472	Online	6	WPA-PSK	TKIP	8
<input type="radio"/> 00804821f877	tang	10	WPA-EAP	TKIP	2
<input type="radio"/> 00804835891e		10	OPEN	NONE	22
<input type="radio"/> 00804800348d	OMEGA1	8	OPEN	NONE	9
<input type="radio"/> 00804824c675	Any	3	OPEN	NONE	3

Below the table are 'Apply', 'Refresh', and 'Back' buttons.

Step 2:

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

Step 3:

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

Step 4:

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

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



NOTE

Site Survey is used to scan and display all access points based on the current security setting of your access point.

Explanation of the following information supplied by the Site Survey according to the security setting:

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

View Link Information

(Available in Client and Wireless Routing Client modes)

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

The screenshot shows the 'WLAN Basic Setup' configuration page. It includes fields for Card Status (enable), Current Mode (Client), ESSID (sampleRouter), Remote AP MAC, Wireless Profile (802.11a), Country (NO_COUNTRY_SET-(NA)), and Tx Rate (Fully Auto). A 'Show Link Information' button is highlighted with a green box at the bottom of the page.

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

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

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

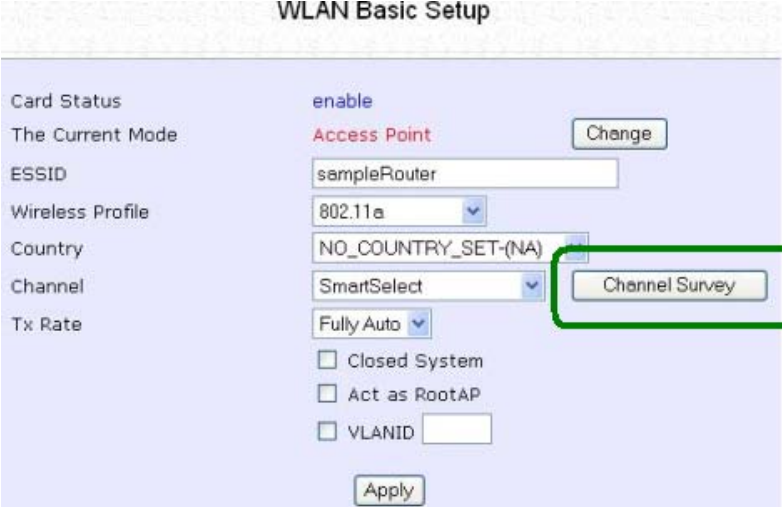
Scan for Channel Survey

(Available in Access Point and Gateway modes)

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

Step 1:

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



The screenshot shows the 'WLAN Basic Setup' configuration page. The page includes several settings: Card Status (enable), The Current Mode (Access Point), ESSID (sampleRouter), Wireless Profile (802.11a), Country (NO_COUNTRY_SET-(NA)), Channel (SmartSelect), and Tx Rate (Fully Auto). There are also checkboxes for 'Closed System', 'Act as RootAP', and 'VLANID'. A 'Channel Survey' button is highlighted with a green box, and an 'Apply' button is at the bottom.

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

Step 2:

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

Step 3:

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

Step 4:

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

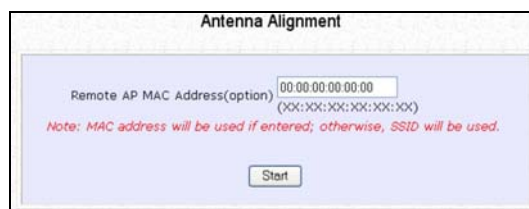
Read-Only Parameters of All Channels Viewable from Channel Survey page	Description
Freq	Frequency of the channel at which your access point is operating.
Channel	Channel of the access point being used for transmission depending on its origin of country.
MyQuality	Interference level of the respective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

Align the Antenna

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

Step 1:

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

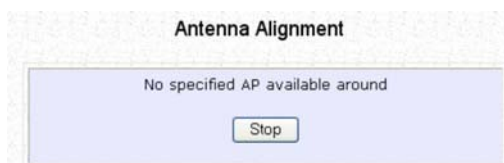


The screenshot shows the 'Antenna Alignment' configuration page. It features a text input field for 'Remote AP MAC Address(option)' with the value '00:00:00:00:00:00' and a placeholder '(XX:XX:XX:XX:XX:XX)'. Below the field is a red note: 'Note: MAC address will be used if entered; otherwise, SSID will be used.' At the bottom of the form is a 'Start' button.

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.



The screenshot shows the 'Antenna Alignment' status screen. It displays the message 'No specified AP available around' in the center. At the bottom of the screen is a '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 points share the same SSID, the access point with the strongest signal will be shown.

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



NOTE

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

NOTE

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

Configure the Advanced Setup of the Wireless Mode

Step 1:

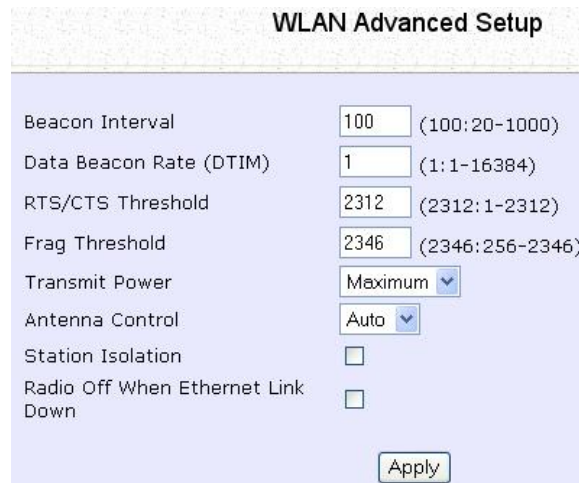
Select **WLAN Setup** from the **CONFIGURATION** menu to expand four sub-menus. From here, select **Advanced**.

Step 2:

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

Step 3:

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



The screenshot shows the 'WLAN Advanced Setup' configuration page. It contains the following settings:

Parameter	Value	Range
Beacon Interval	100	(100:20-1000)
Data Beacon Rate (DTIM)	1	(1:1-16384)
RTS/CTS Threshold	2312	(2312:1-2312)
Frag Threshold	2346	(2346:256-2346)
Transmit Power	Maximum	Dropdown menu
Antenna Control	Auto	Dropdown menu
Station Isolation	<input type="checkbox"/>	Checkbox
Radio Off When Ethernet Link Down	<input type="checkbox"/>	Checkbox

An 'Apply' button is located at the bottom right of the configuration area.

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)	<p>How often the beacon contains a delivery traffic indication message (DTIM). The DTIM identifies which clients have data waiting to be delivered to them.</p> <p>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)</p>
RTS/CTS Threshold	<p>Minimum size of a packet in bytes that will trigger the RTS/CTS mechanism.</p> <p>This value extends from 1 to 2312 bytes.</p>
Frag Threshold	<p>Maximum size that a packet can reach without being fragmented, represented in bytes.</p> <p>This value extends from 256 to 2346 bytes, where a value of 0 indicates that all packets should be transmitted using RTS.</p>
Transmit Power	Drop-down list of a range of transmission power.
Radio Off When Ethernet Link Down	Disables the radio card automatically when the Ethernet link is down.



NOTE

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

View the Statistics

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

Step 1:

Select **WLAN Setup** from the **CONFIGURATION** menu. The sub-menus under **WLAN Setup** expand, select **Statistics**.

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

Step 2:

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

WLAN Station List			
ID	MAC Address	RSSI	TxRate
AP	00:80:48:37:86:dd	1	36Mbps

Step 3:

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

The statistics of the selected wireless client displays.

00:80:48:37:86:dd Statistics						
Authentication Type			Encryption			
Open-System			No			
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	2122	0	0
Transmit	0	0	0	11	0	0

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

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.

The screenshot shows the 'WAN Dynamic Setup' configuration page. It features a list of fields: 'WAN Type' (set to 'Dynamic (DHCP)' with a 'Change' button), 'IP Address' (with a 'Refresh' button), 'Network Mask', 'Gateway IP Address', 'Primary DNS', and 'Secondary DNS'.

Step 3:

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

The screenshot shows the 'Select WAN Type' dialog box with five radio button options: 'Static IP Address', 'Dynamic IP Address' (which is selected), 'PPP over Ethernet', 'PPTP', and 'L2TP'. At the bottom, there are 'Apply', 'Cancel', and 'Help' buttons.

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.

System Identity

System Name :	<input type="text" value="Wireless LAN Access Point"/>
System Contact :	<input type="text" value="unknown"/>
System Location :	<input type="text" value="unknown"/>

Setup your WAN for cable internet whereby fixed WAN IP address is assigned by ISP

WAN Setup Parameters Example:

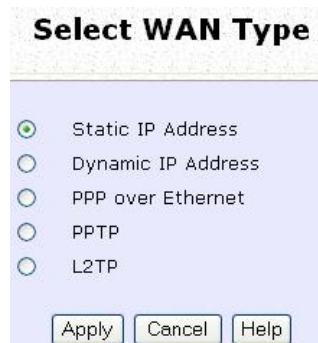
- IP Address: 203.120.12.240
- Network Mask: 255.255.255.0
- Gateway IP Address: 203.120.12.2

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

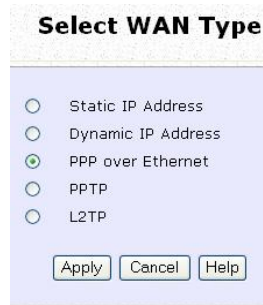
If you subscribe to an ADSL service using PPP over Ethernet (PPPoE) authentication, you can set up your access point's WAN type as follows. For example, you may configure an account whose username is 'guest' as described below:

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.



Select WAN Type

- Static IP Address
- Dynamic IP Address
- PPP over Ethernet
- PPTP
- L2TP

Apply Cancel Help

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.



The screenshot shows the 'WAN PPPoE Setup' configuration page. At the top, it displays 'WAN Type : PPPoE' with a 'Change' button. Below this, there are input fields for 'Username' (containing 'guest') and 'Password'. Two radio button options are present: 'On-Demand' (unselected) and 'Always-On' (selected). The 'On-Demand' option is linked to an 'Idle Timeout (0:disabled)' field set to '30' seconds. The 'Always-On' option is linked to a 'Reconnect Time Factor' field set to '30' seconds. The 'Status' is shown as 'Connecting' with a 'Refresh Status' button. At the bottom, there are fields for 'IP Address', 'Network Mask', 'Default Gateway', 'Primary DNS', and 'Secondary DNS'. At the very bottom of the form are three buttons: 'Apply', 'Email Notification', and 'Help'.

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:

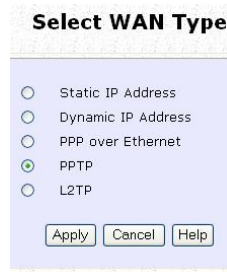
- IP Address: 203.120.12.47
- Network Mask: 255.255.255.0
- VPN Server: 203.120.12.15

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.

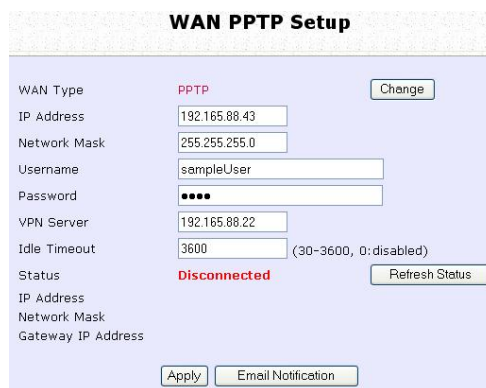


Step 3:

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

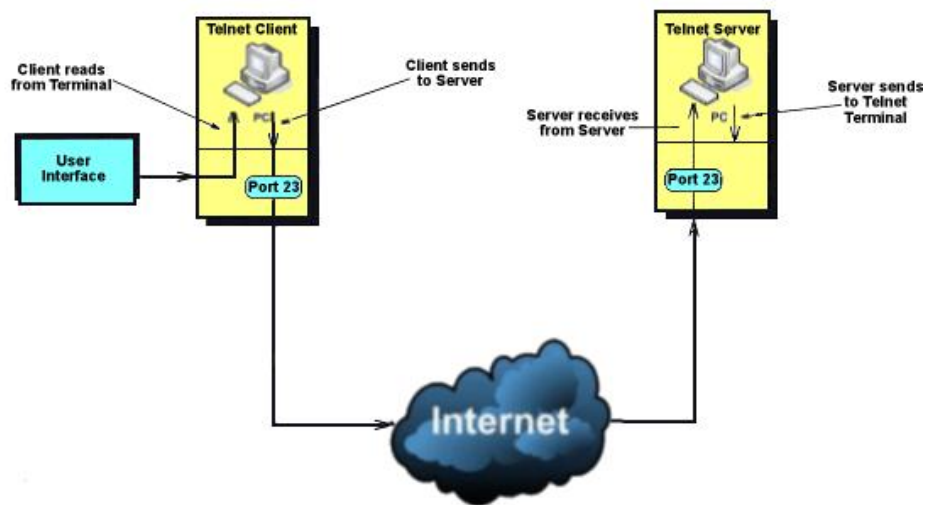
The **Idle Timeout** setting allows you to specify the value in seconds after the last Internet activity by which the access point will disconnect from the ISP. A value of "0" will disable idle timeout.



The screenshot shows the 'WAN PPTP Setup' configuration page. The WAN Type is set to 'PPTP'. The IP Address is 192.165.88.43, Network Mask is 255.255.255.0, Username is sampleUser, Password is masked with dots, and VPN Server is 192.165.88.22. The Idle Timeout is set to 3600 seconds. The Status is 'Disconnected'. There are buttons for 'Change', 'Refresh Status', 'Apply', and 'Email Notification'.

WAN PPTP Setup	
WAN Type	PPTP <input type="button" value="Change"/>
IP Address	<input type="text" value="192.165.88.43"/>
Network Mask	<input type="text" value="255.255.255.0"/>
Username	<input type="text" value="sampleUser"/>
Password	<input type="password" value="••••"/>
VPN Server	<input type="text" value="192.165.88.22"/>
Idle Timeout	<input type="text" value="3600"/> (30-3600, 0:disabled)
Status	Disconnected <input type="button" value="Refresh Status"/>
IP Address	
Network Mask	
Gateway IP Address	
<input type="button" value="Apply"/> <input type="button" value="Email Notification"/>	

Setup Telnet / SSH



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

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

Step 1:

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

Step 2:

1. Select Telnet Server Enable and enter the Port Number to enable.
2. Select SSH Server Enable and enter the Port Number to enable.
3. Enter the **Time out** in seconds for Telnet.

Click the **Apply** button.

Telnet/SSH Setup

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

Step 3:

To add user:

1. Click the **Add** button.



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

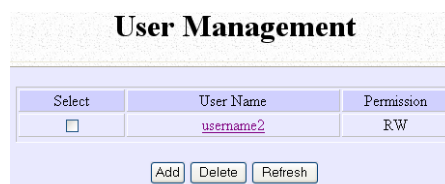


To Delete User:

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



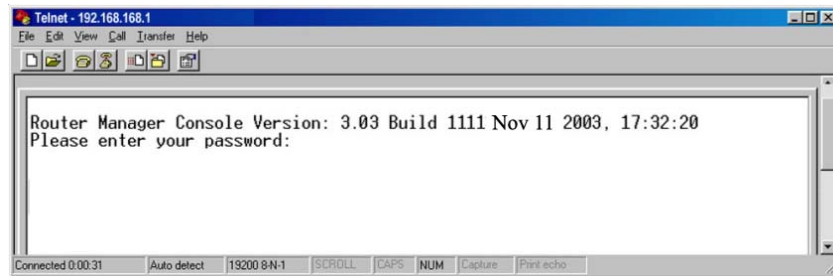
To Refresh User Management list click the **Refresh** button.



Access the TELNET Command Line Interface

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

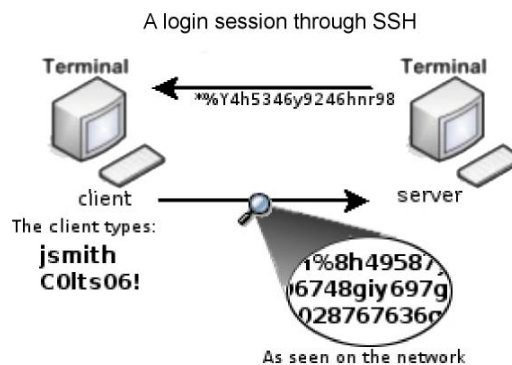
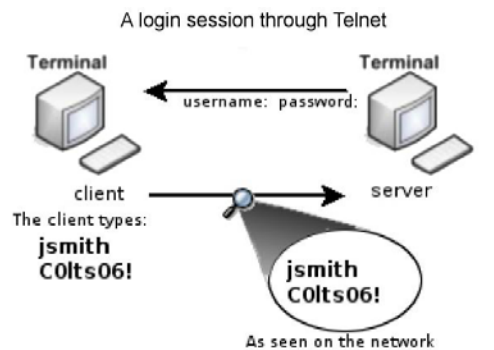
1. Enter **C:\WINDOWS\TELNET 192.168.168.1** at DOS prompt and the TELNET application will launch and connect.
2. At the login prompt, type in the default password "password" and press enter. You will then login to the CLI.



Access the Secure Shell Host Command Line Interface

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

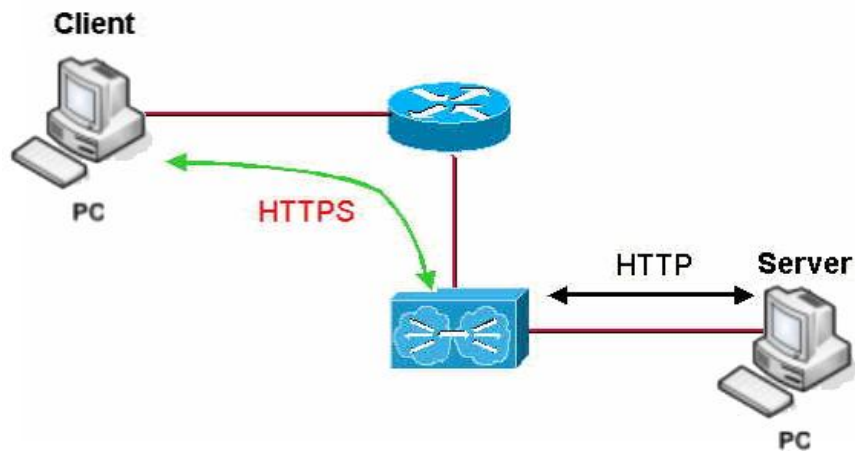
An encrypted connection like SSH is not viewable on the network. The server can still read the information, but only after negotiating the encrypted session with the client.



SSH CLI has a command line interface.

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

Set the WEB Mode



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

Step 1:

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

Step 2:

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

Changes will be effected after reboot.

Web Management Setup

Mode	<input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS (SSL)
<input type="button" value="Apply"/>	

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.



The screenshot shows the 'SNMP Setup' configuration page. It features three input fields: 'SNMP State' with a dropdown menu set to 'Enable', 'Read Password' with a text box containing 'public', and 'Read/Write Password' with a text box containing 'private'. Below these fields is an 'Apply' button.

Setup SNMP Trap

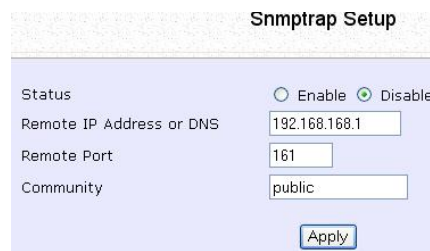
The SNMP Trap saves network resources through eliminating the need for unnecessary SNMP requests by providing notification of significant network events with unsolicited SNMP messages.

Step 1:

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

Step 2:

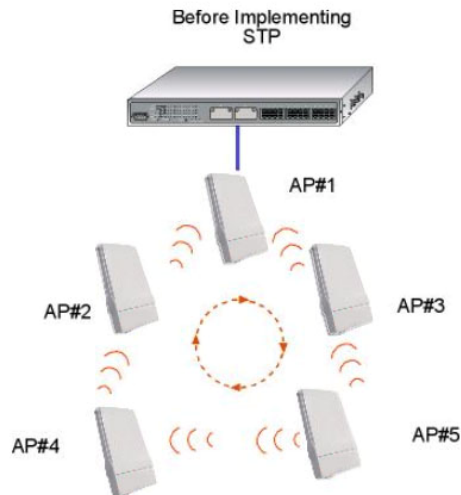
1. Select whether to **Enable** or **Disable** the SNMP Trap.
2. Enter the **Remote IP Address or DNS**.
3. Enter the **Remote Port**.
This is the port number of the SNMP manager.
4. Enter the **Community**.
This is used to authenticate message, and is included in every packet that is transmitted between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



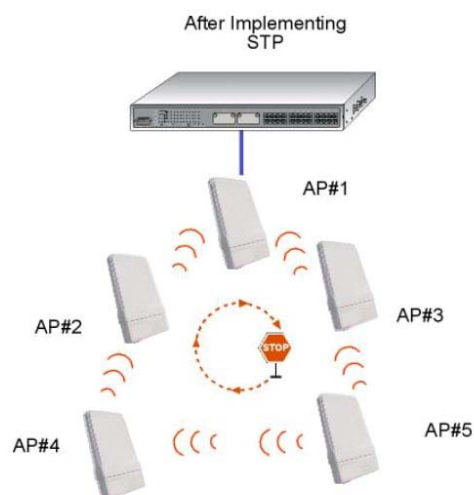
The screenshot shows the 'Snmptrap Setup' configuration page. It features a title bar at the top with the text 'Snmptrap Setup'. Below the title bar, there are four configuration fields: 'Status', 'Remote IP Address or DNS', 'Remote Port', and 'Community'. The 'Status' field has two radio buttons: 'Enable' and 'Disable', with 'Disable' selected. The 'Remote IP Address or DNS' field contains the value '192.168.168.1'. The 'Remote Port' field contains the value '161'. The 'Community' field contains the value 'public'. At the bottom of the form, there is an 'Apply' button.

Setup STP

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

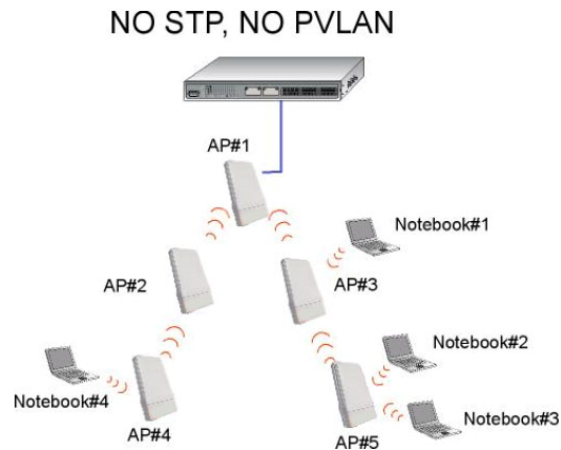


Spanning Tree Protocol (STP) prevents broadcast storms when there are redundant paths in the network. STP creates a tree that spans all devices in an extended network, forcing redundant paths into a standby state, but establishing the redundant links as backup in case the active link should fail. If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



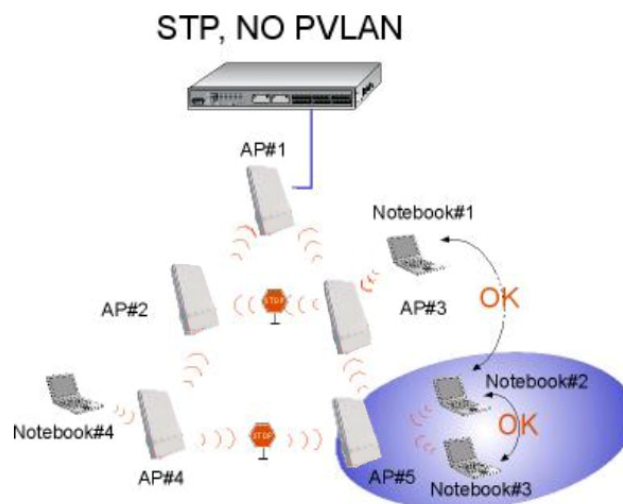
Scenario #1 – (No STP)

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 1:

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

Step 2:

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

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

This is the relative priority.

The lowest priority will be elected as the root.

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

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

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

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

Max Age: (Default: 20, Range: 6 – 40)

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

Spanning Tree Protocol Setup

STP Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
STP Designated Root	32768 00:80:48:3d:0f:80
Priority	<input type="text" value="32768"/> (32768:0-65535)
Hello Time	<input type="text" value="2"/> (2: 1-10)
Forward Delay	<input type="text" value="15"/> (15: 4-30)
Max Age	<input type="text" value="20"/> (20: 6-40)

Use MAC Filtering

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



NOTE

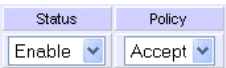



MAC Filtering will not filter any MAC address from the Ethernet port.

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.

	<p>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.</p>
	<p>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.</p>
	<p>MAC Filtering set to Disable. Whether Policy is set to Enable or Deny does not matter.</p>
	<p>MAC Filtering set to Disable. Whether Policy is set to Enable or Deny does not matter.</p>

Click the **Edit** button.



Step 2:

MAC Filter Address List page displays.

Click the **Add** button.

MAC Filter Address List

MAC Address List
ESSID: "sampleRouter"

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

(All changes will take effect after reboot)

Step 3:

The Add MAC Address page displays.

Add MAC Address

MAC Address: (XX-XX-XX-XX-XX-XX)

Comment:

Apply to All:

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

Step 4:

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

Enter the Comment. This describes the MAC Address you have entered.

To apply to all virtual access points, check **Apply to All**.

To apply to specific virtual access point, select the checkbox of the corresponding access point.

Click the **Apply** button.

Add MAC Address

MAC Address: (XX-XX-XX-XX-XX-XX)

Comment:

Apply to All:

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

Step 5:

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



MAC Filter Address List

MAC Address List
ESSID: "sampleRouter"

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

(All changes will take effect after reboot)



NOTE

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

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**.

The screenshot shows the 'MAC Address Filtering' configuration page. It features a table titled 'Radio 1 MAC Filtering Options' with columns for AP Type, ESSID, Security, MACs, Status, and Policy. Below the table are buttons for 'Apply' and 'Back', and a note indicating that changes will take effect after a reboot.

AP Type	ESSID	Security	MACs	Status	Policy
Main AP	sampleRouter	NONE	Edit	Enable	Accept
Virtual AP	VAP1	NONE	Edit	Disable	Deny
Virtual AP	VAP2	NONE	Edit	Enable	Deny

[View Complete MAC List](#)

(All changes will take effect after reboot)

Step 2:

The MAC Filter Address List page displays.

Select the checkbox of the MAC address you wish to delete.

Click the **Delete** button.

The screenshot shows the 'MAC Filter Address List' page. It displays a table with columns for 'Del.', 'MAC Address', 'Comments', and 'Apply to'. The table contains two entries: one with a checkbox and one with a checked checkbox. Below the table are buttons for 'Add', 'Delete', and 'Back', and a note indicating that changes will take effect after a reboot.

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

(All changes will take effect after reboot)

Step 3:

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



The screenshot shows a web interface titled "MAC Filter Address List". Below the title, it says "MAC Address List" and "Radio 1". There is a table with the following data:

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

Below the table are three buttons: "Add", "Delete", and "Back". At the bottom, there is a note: "(All changes will take effect after reboot)".

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.

AP Type	ESSID	Security	MACs	Status	Policy
Main AP	sampleRouter	NONE	Edit	Enable	Accept
Virtual AP	VAP1	NONE	Edit	Disable	Deny
Virtual AP	VAP2	NONE	Edit	Enable	Deny

[View Complete MAC List](#)

(All changes will take effect after reboot)

Step 2:

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

Click the **Delete** button.

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

(All changes will take effect after reboot)

Step 3:

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



The screenshot shows a web interface titled "MAC Filter Address List". Below the title, it indicates "MAC Address List" and "ESSID: 'sampleRouter'". A table contains two entries, each with a delete checkbox, a MAC address, a comment, and an application target. Below the table are "Add", "Delete", and "Back" buttons, and a note that changes take effect after a reboot.

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

(All changes will take effect after reboot)

Edit MAC Address from the MAC Address List

Step 1:

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

Select **Edit**.

The screenshot shows the 'MAC Address Filtering' configuration page. It features a table titled 'Radio 1 MAC Filtering Options' with columns for AP Type, ESSID, Security, MACs, Status, and Policy. The table contains three rows: 'Main AP' with ESSID 'sampleRouter', 'Virtual AP' with ESSID 'VAP1', and 'Virtual AP' with ESSID 'VAP2'. Each row has an 'Edit' link in the MACs column and dropdown menus for Status and Policy. Below the table is a link to 'View Complete MAC List', 'Apply' and 'Back' buttons, and a note: '(All changes will take effect after reboot)'.

AP Type	ESSID	Security	MACs	Status	Policy
Main AP	sampleRouter	NONE	Edit	Enable	Accept
Virtual AP	VAP1	NONE	Edit	Disable	Deny
Virtual AP	VAP2	NONE	Edit	Enable	Deny

[View Complete MAC List](#)

(All changes will take effect after reboot)

Step 2:

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

The screenshot shows the 'MAC Filter Address List' page. It displays the MAC Address List for ESSID: "VAP1". There is a table with columns: Del., MAC Address, Comments, and Apply to. The table contains one row with a checkbox in the Del. column, MAC Address '08-70-f8-70-80-70', Comments 'mac4', and Apply to '1 AP(s)'. Below the table are 'Add', 'Delete', and 'Back' buttons, and a note: '(All changes will take effect after reboot)'.

Del.	MAC Address	Comments	Apply to
<input type="checkbox"/>	08-70-f8-70-80-70	mac4	1 AP(s)

(All changes will take effect after reboot)

Step 3:

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

Click the **Save** button.

MAC Address: (XX-XX-XX-XX-XX-XX)

Comment

Apply to All

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

Step 4:

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

MAC Address List
ESSID: "VAP1"

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

(All changes will take effect after reboot)

Perform Advanced Configuration

Setup Routing

(Available in Wireless Routing Client and Gateway modes)

The access point allows you to add a static routing entry into its routing table to re-route IP packets to another access point. This is useful if your network has more than one access point.



Important:

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

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

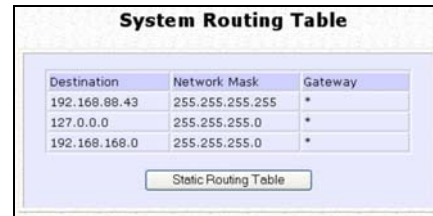
You can add a static routing entry into the access point routing table so that IP packets from the clients in the main office with a destination IP address of 192.168.100.X where X is any number from 2 to 254 will be re-routed to the router, which acts as the gateway to that subnet.



Configure Static Routing

Step 1:

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



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

Static Routing Table



Destination	Network Mask	Gateway
<input type="text"/>	<input type="text"/>	<input type="text"/>

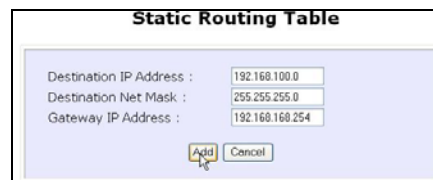
Add Back

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.



Static Routing Table

Destination IP Address :

Destination Net Mask :

Gateway IP Address :

Add Cancel

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



Destination	Network Mask	Gateway
192.168.100.0	255.255.255.0	192.168.168.254

Add Back

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.



Important:

NAT provides for effective broadband Internet sharing, do NOT disable NAT unless it is absolutely necessary.

Configure Virtual Servers Based on DMZ Host

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

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



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

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

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

To disable DMZ, enter **0.0.0.0**

Click the **Apply** button.



NOTE

1. DMZ may not function properly if the DMZ host IP address is changed due to DHCP, therefore, Static IP Address configuration is recommended for the DMZ host.
2. Please note that the DMZ host is susceptible to malicious attacks as ALL of its ports are exposed to the Internet.

Configure Virtual Servers Based on Port Forwarding

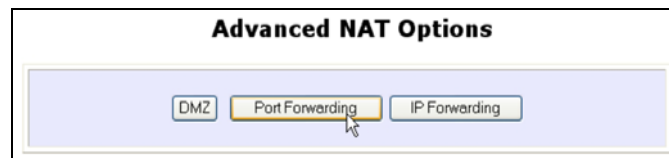
Virtual Server based on Port Forwarding forwards Internet requests arriving at the access point WAN interface to specific PCs in the private network based on their ports.

Step 1:

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**.

Add Port Forward Entry

Known Server

Server Type :

Private IP Address :

Public IP :

From :

To :

Custom Server

Server Type :

Protocol :

Public Port :

From :

To :

Private IP Address :

Private Port From :

Public IP :

From :

To :

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.

Port Forward Entries

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

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.

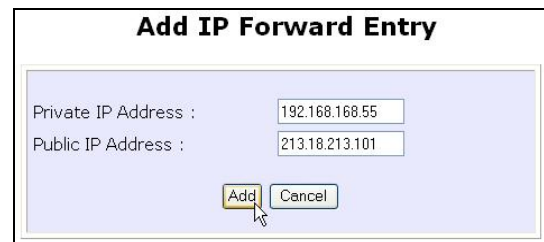


Step 1:
Select **NAT CONFIGURATION** from the command menu.

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**.

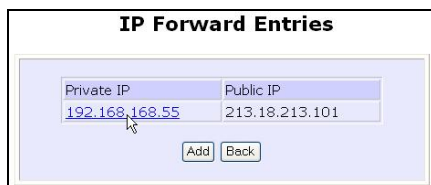
In this example, we would like all requests for 213.18.213.101 to be forwarded to a PC with **Private IP Address** 192.168.168.55.



NOTE

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.

Enable/Disable Bandwidth Control

Bandwidth Control Status : Enable Disable

Apply

WAN Bandwidth Control Setup

Upload/Download Bandwidth Setting

Download Total Rate(kbit):

Upload Total Rate(kbit) :

Apply

LAN Bandwidth Control Setup

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

Step 2:

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

Enable/Disable Bandwidth Control

Bandwidth Control Status : Enable Disable

Apply

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.



The screenshot shows a configuration window titled "WAN Bandwidth Control Setup". Inside the window, there is a section titled "Upload/Download Bandwidth Setting". Below this section, there are two input fields: "Download Total Rate(kbit):" and "Upload Total Rate(kbit) :". Both fields contain the value "0". At the bottom of the window, there is an "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.

LAN Bandwidth Control Setup

Name	Committed Rate(kbit)	Ceil Rate(kbit)	IP/MAC Address	Rule type
sampleRule	10	100	09-00-2B-01-00-00	DownLoad By MAC Address

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

Add Bandwidth Control Entry

Bandwidth Control Rule

Rule Name :

Committed Rate(kbit) :

Ceil Rate(kbit) :

Rule type :

IP/MAC Address :

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.

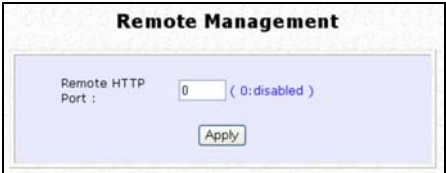
Repeat Steps 1 to Step 3 to add new bandwidth rule.

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 enabled with Port 88 and the Ethernet port becomes a WAN port. To continue using it, open the web manager using the WAN IP with Port 88.
Example: For WAN IP 100.100.100.1 use http://100.100.100.1:88



NOTE

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

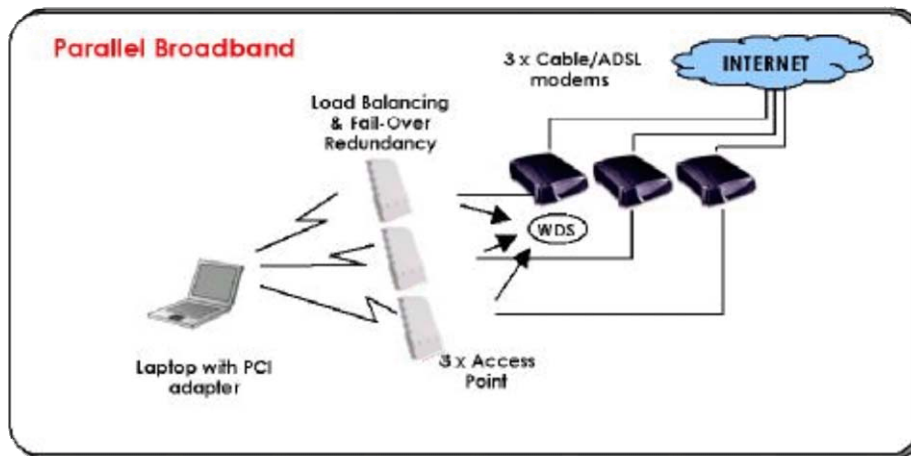
Use Parallel Broadband

(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.

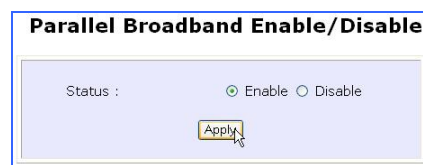
Secondly ensure that either:

- 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 have 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.

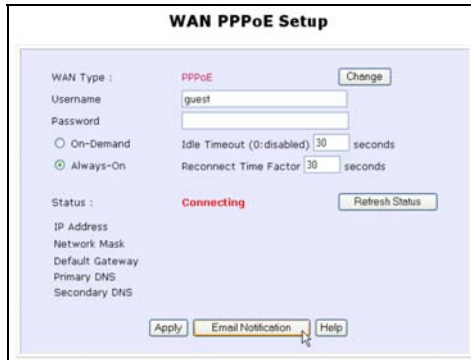


Important:

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

Setup Email Notification

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



The screenshot shows the 'WAN PPPoE Setup' configuration page. The 'WAN Type' is set to 'PPPoE'. The 'Username' is 'guest'. The 'Password' field is empty. The 'On-Demand' radio button is selected, with 'Idle Timeout (0:disabled)' set to 30 seconds and 'Reconnect Time Factor' set to 30 seconds. The 'Status' is 'Connecting'. At the bottom, there are buttons for 'Apply', 'Email Notification', and 'Help'. A mouse cursor is pointing at the 'Email Notification' button.

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

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



The screenshot shows the 'Email Notification' configuration page. The 'Email Notification' checkbox is checked (Enable). The 'Email address of Receiver' is 'mail@yahoo.com'. The 'IP address of Mail Server' is '192.168.88.43' with a checked 'Needs Authentication' box. The 'User Name' is 'sampleUser'. The 'Password' field is masked with dots. The 'Email address of Sender' is 'send@yahoo.com'. At the bottom, there are buttons for 'Apply', 'Back', and 'Refresh'.

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.



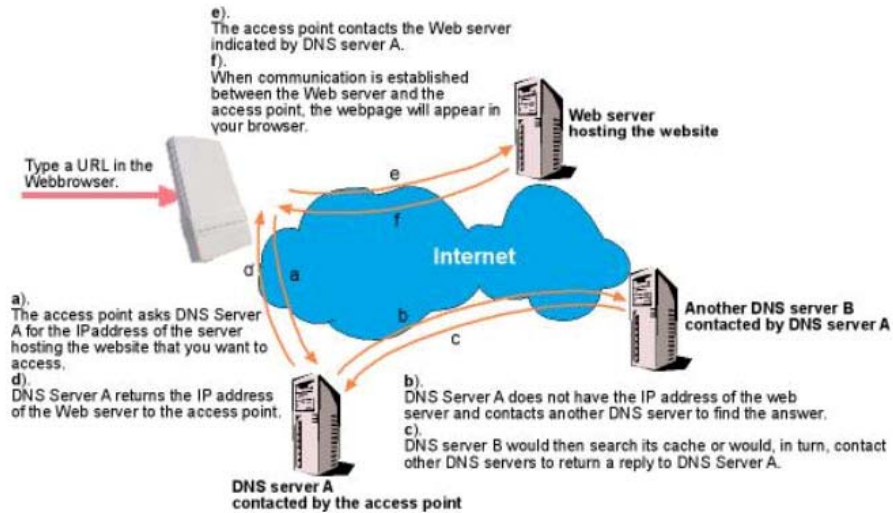
Use DNS Redirection

(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 in the access point LAN Setup and enable DNS Redirection, without having to reconfigure the DNS settings of every LAN client.



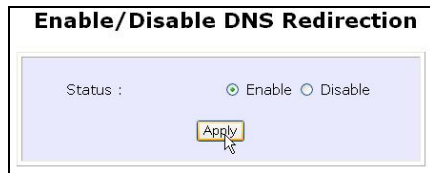
NOTE



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, simply 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.

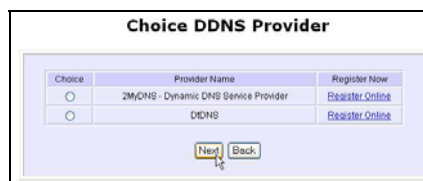
To manage Dynamic DNS List

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.

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

Next Back

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.

Provider: 2MyDNS - Dynamic DNS Service Provider

Domain Name: [] 2mydns.net

WAN IP: [] Auto Detect

Username: []

Password: []

Wildcard: YES NO

Mail Exchanger: []

Backup Mail Exchanger: YES NO

Add Reset Back

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.

The screenshot shows the 'Dynamic DNS Add' form. The provider is set to '2MyDNS - Dynamic DNS Service Provider'. The Domain Name dropdown is open, showing a list of domains including '2mydns.net', '2myip.com', 'anachyonline.net', 'ezgameserver.com', 'mycoding.com', 'my4gb.com', 'onlinepeople.net', and 'tzyplanet.net'. The Mail Exchanger field is currently empty.

The screenshot shows the 'Dynamic DNS List' table. It has two columns: 'Domain Name' and 'Update Status'. The table contains two entries: 'Mx.Cp.dns.mycp.dns.com' and 'people.onlinepeople.net'. Below the table are 'Add' and 'Refresh' buttons.

The screenshot shows the 'Dynamic DNS Edit' form for the domain 'people.onlinepeople.net'. The provider is '2MyDNS - Dynamic DNS Service Provider'. The WAN IP field has an 'Auto Detect' checkbox checked. The Username is 'lester' and the Password is masked with dots. The Wildcard is set to 'NO'. The Mail Exchanger is 'ann_tay@powermatic.com.sg' and the Backup Mail Exchanger is 'NO'. At the bottom are 'Save', 'Reset', 'Delete', and 'Back' buttons.

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.

Choice	Provider Name	Register Now
<input type="radio"/>	2MDNS - Dynamic DNS Service Provider	Register Online
<input checked="" type="radio"/>	DtDNS	Register Online

Next Back

Click on the **Next** button.

Step 2:

Enter your **Domain Name**.

Provider : DtDNS

Domain Name : gamer . 3d-game.com

WAN IP : 192.168.88.44 Auto Detect

Password :

Add Reset Back

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.

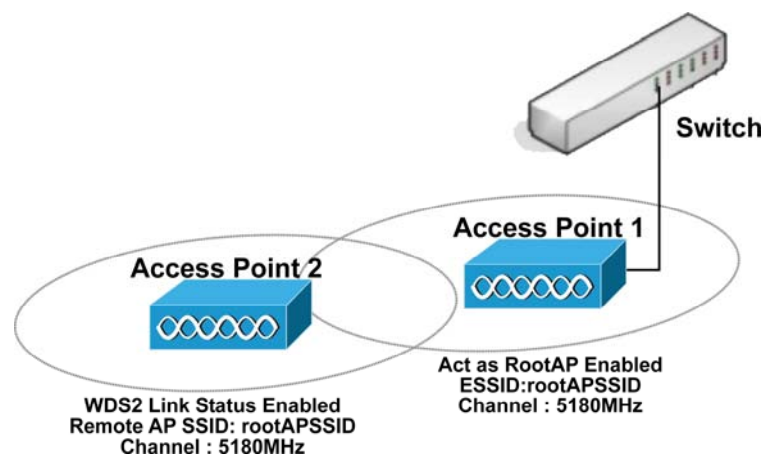
Domain Name	Update Status
people.onlinepeople.net	
cool.3d-game.com	Waiting in queue...

Add Refresh

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.

WLAN Basic Setup	
Card Status	enable
The Current Mode	Access Point <input type="button" value="Change"/>
ESSID	rootAPSSID
Wireless Profile	802.11a
Country	NO_COUNTRY_SET-(NA)
Channel	5180MHz (Channel 36) <input type="button" value="Channel Survey"/>
Tx Rate	Fully Auto
Maximum Associations	32 (32:1-128)
	<input type="checkbox"/> Closed System
	<input checked="" type="checkbox"/> Act as RootAP
	<input type="checkbox"/> VLANID <input type="text"/>
	<input type="button" value="Apply"/>

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.

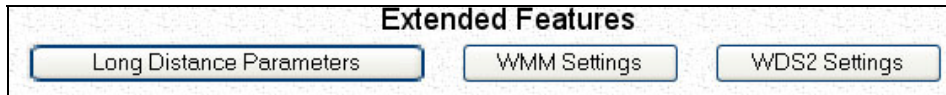
The screenshot shows the 'WLAN Basic Setup' configuration page. The settings are as follows:

Field	Value
Card Status	enable
The Current Mode	Access Point (with a 'Change' button)
ESSID	accesspoint2
Wireless Profile	802.11a
Country	NO_COUNTRY_SET-(NA)
Channel	5180MHz (Channel 36) (with a 'Channel Survey' button)
Tx Rate	Fully Auto
Maximum Associations	32 (32: 1-128)
Closed System	<input type="checkbox"/>
Act as RootAP	<input type="checkbox"/>
VLANID	<input type="checkbox"/> []

An 'Apply' button is located at the bottom of the configuration area.

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**.

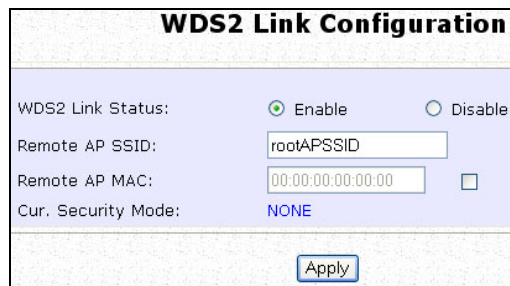
Options for configuring WDS2 link:

- By Remote AP MAC – Enter the Remote AP MAC

A screenshot of the "WDS2 Link Configuration" form. The "WDS2 Link Status" is set to "Enable". The "Remote AP SSID" is "default". The "Remote AP MAC" is "08:00:69:02:01:FC" and the checkbox next to it is checked. The "Cur. Security Mode" is "NONE". An "Apply" button is at the bottom.

OR

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

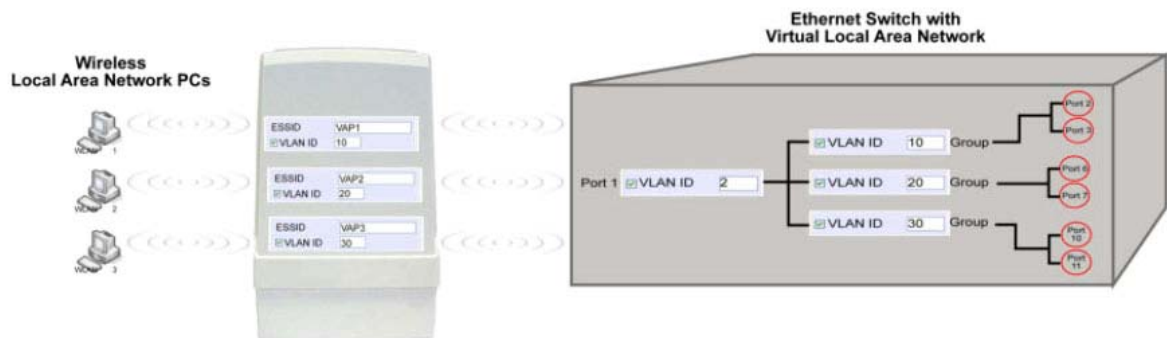
A screenshot of the "WDS2 Link Configuration" form. The "WDS2 Link Status" is set to "Enable". The "Remote AP SSID" is "rootAPSSID". The "Remote AP MAC" is "00:00:00:00:00:00" and the checkbox next to it is unchecked. The "Cur. Security Mode" is "NONE". An "Apply" button is at the bottom.

Click **Apply**.

Set Virtual AP (Multiple SSID)

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

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



How it Works

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

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

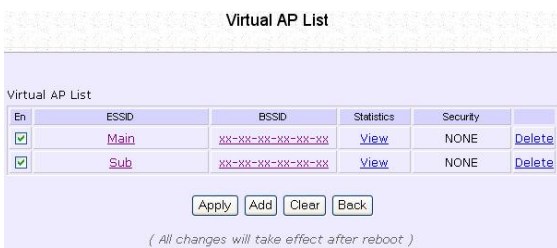
For more information on Virtual AP (Multiple SSID) please refer to Appendix: Virtual AP (Multiple SSID) FAQ.

Follow these steps to setup Virtual AP.

Virtual AP

1

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



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

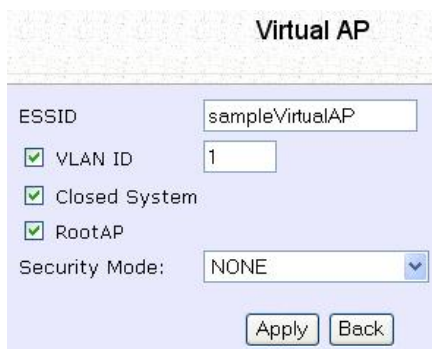
(All changes will take effect after reboot)

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.



Virtual AP

ESSID: sampleVirtualAP

VLAN ID: 1

Closed System

RootAP

Security Mode: NONE

Apply Back

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.

Preferred Access Point MAC Address

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

2

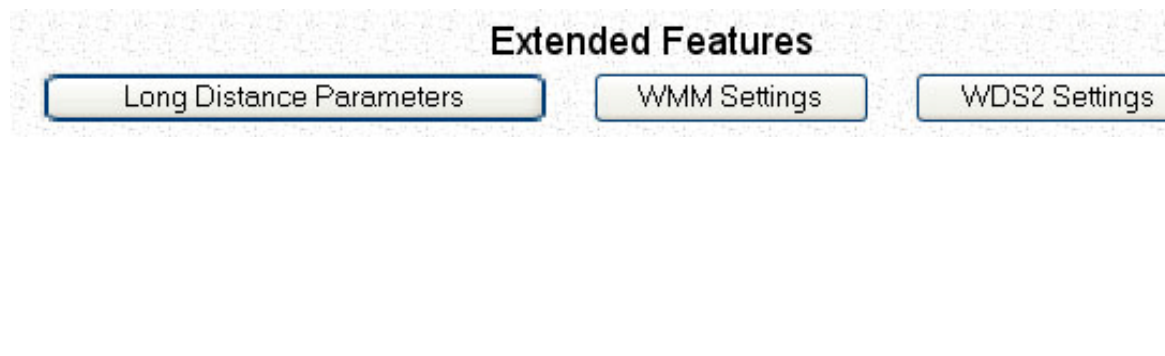
1. Enter the MAC addresses of the preferred APs.
2. Click [Apply](#) to effect the settings.

Get Long Distance Parameters

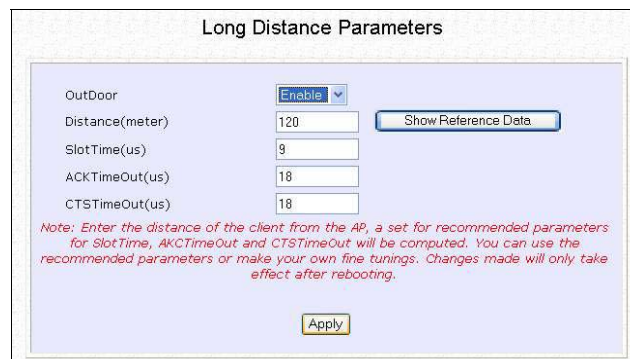
The access point can calculate and display suggested values for certain parameters to use to ensure that efficient wireless communication between physically distant access points.

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

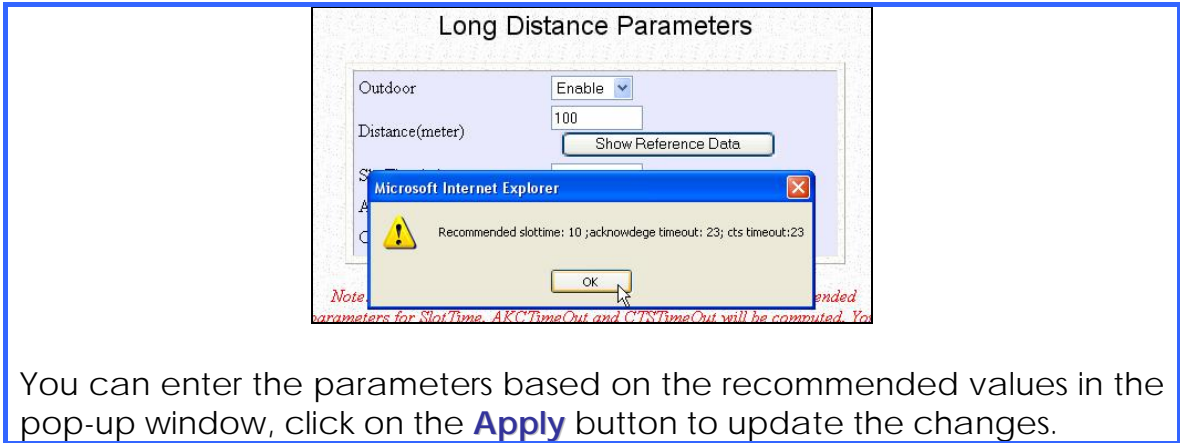
Click on the **Long Distance Parameters** button under the **Extended Features** section.



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



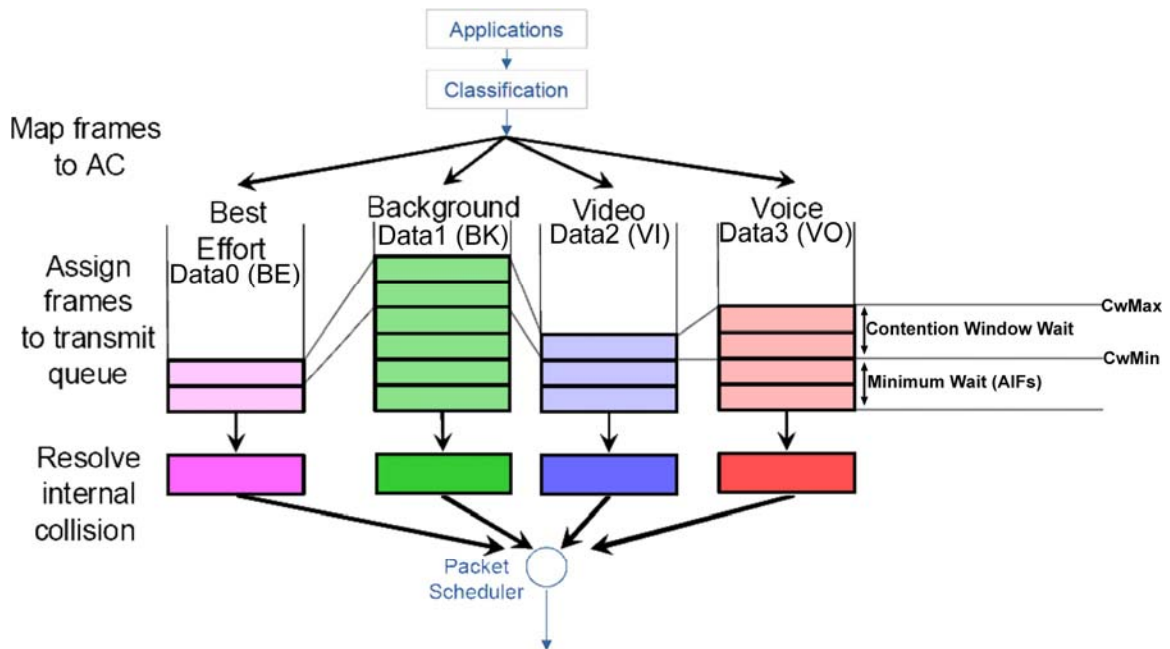
The access point can automatically calculate the values of the parameters to input based on the distance between your access point and the other wireless device. Enter the distance in meters and click on the **Show Reference Data** button.



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

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.



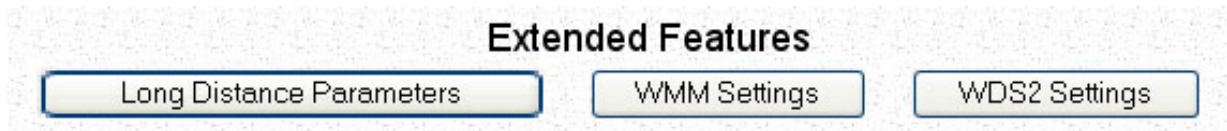
Follow these steps to change the setup Wireless Multimedia on your access point.

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.

Wireless Multimedia (WMM) Enable Disable

AP WMM Parameters:

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

Station WMM Parameters:

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

(All changes will take effect after reboot)

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.

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

RootAP Step 2:

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

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

Follow these steps to setup Transparent Client/s.

Transparent Client Step 1:

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

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

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

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

Transparent Client Step 2:

Select the **Remote AP MAC** checkbox.

Enter the **Remote AP MAC**.

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

Note:

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

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

Secure your Wireless LAN

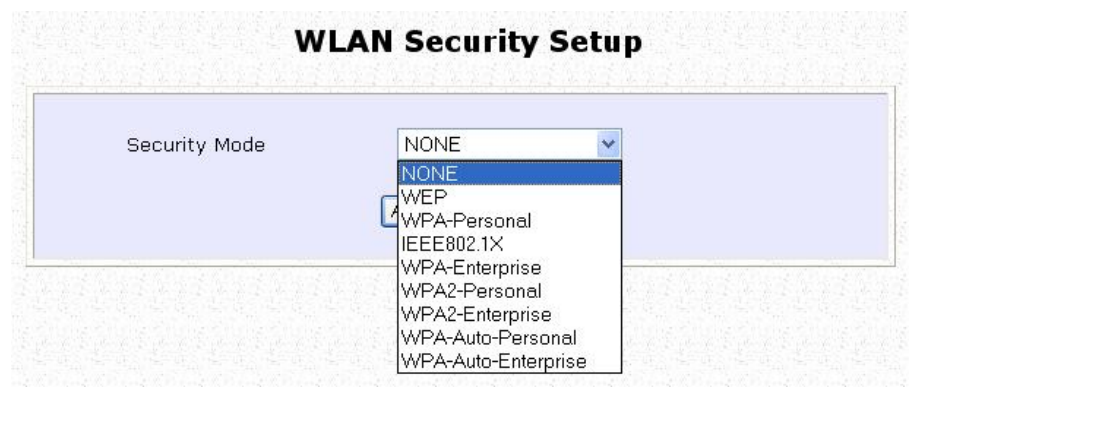
Step 1:

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,

The screenshot shows the 'WEP Setup' configuration page. It includes a 'Key String Type' section with two radio button options: 'Hex (0~9, a~f, A~F) Length 10 or 26' (which is selected) and 'Ascii (0~9, a~z, A~Z) Length 5 or 13'. Below this is a 'Transmission key:' dropdown menu currently set to 'Key 1'. There are four key configuration sections, each with a radio button for '64Bit' (selected) and '128Bit', a text input field, and a 'Reset' button. An 'Apply' button is positioned at the bottom right of the configuration area.

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.

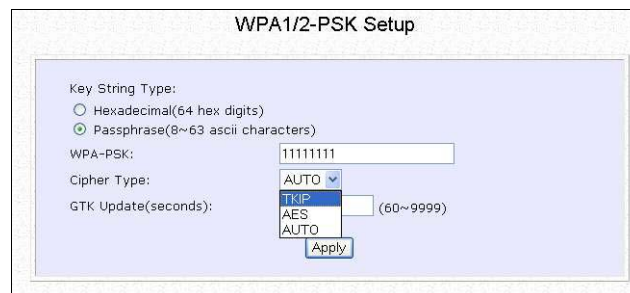
Click on the **Apply** button and reboot your access point.

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,



WPA1/2-PSK Setup

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

WPA-PSK: 11111111

Cipher Type:

GTK Update(seconds): (60~9999)

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

For WPA-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,

IEEE 802.1X Setup	
Primary RADIUS Server IP	0.0.0.0
Secondary RADIUS Server IP	0.0.0.0
Authentication Port	1812
Accounting Port	1813
Shared Secret Key	*****
Broadcast Key Rotation(seconds)	600 (60~9999)
Key Length	128 bits

Step 1:

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

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

Step 2:

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

Step 3:

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

Step 4:

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

Step 5:

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

Step 6:

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

- **64-bit**

10 hexadecimal or 5 ASCII Text

- **128-bit**

26 hexadecimal or 13 ASCII Text

Step 7:

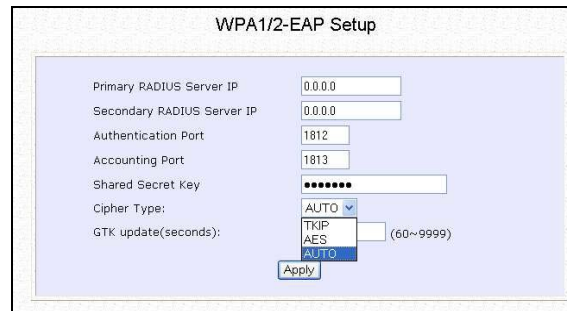
Click the **Apply** button and reboot your system, after which your settings will become effective.

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,



WPA1/2-EAP Setup	
Primary RADIUS Server IP	0.0.0.0
Secondary RADIUS Server IP	0.0.0.0
Authentication Port	1812
Accounting Port	1813
Shared Secret Key	*****
Cipher Type:	AUTO
GTK update(seconds):	(60~9999)
Apply	

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

For WPA- 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.

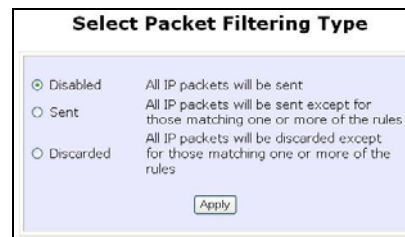


Packet Filter Configuration

Packet Filter Type : Disabled

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.

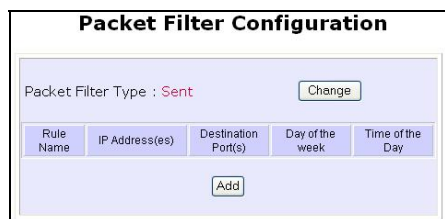


Select Packet Filtering Type

Disabled All IP packets will be sent

Sent All IP packets will be sent except for those matching one or more of the rules

Discarded All IP packets will be discarded except for those matching one or more of the rules



Packet Filter Configuration

Packet Filter Type : Sent

Rule Name	IP Address(es)	Destination Port(s)	Day of the week	Time of the Day



Add a new Packet Filter rule

Rule Name :

IP Address : Any

From : 192.168.168.

To : 192.168.168.

Destination Port : Any

From :

To :

Day of the Week : Any

From : Mon

To : Fri

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

From : (hh:mm)

To : (hh:mm)

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



Rule Name :

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.

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

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

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

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

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

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

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

Destination Port : Range
From : 21
To : 81

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

Destination Port : Single
From : 25
To :

- **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.

Destination Port : Any
From :
To :

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

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

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

- **Any** day

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

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.

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

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

Step 5:

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

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

Add a new Packet Filter rule

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

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.

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.

Firewall Configuration

Warning: Incorrect configuration may cause undesirable behavior.

Firewall Status: Enable Disable

Allow user visit LAN from WAN port

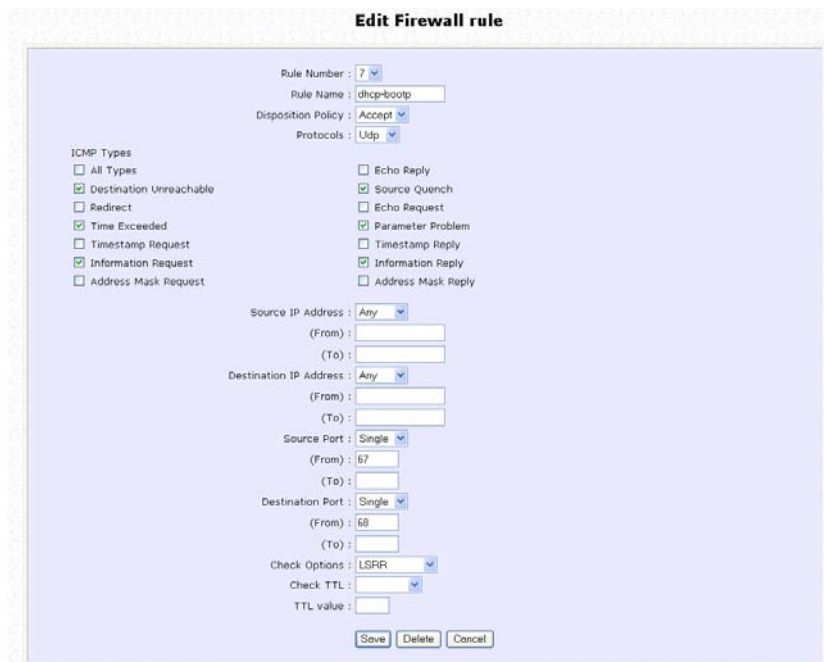
Log Information

Accepted: TCP Packets UDP Packets
 ICMP Packets IGMP Packets

Denied: TCP Packets UDP Packets
 ICMP Packets IGMP Packets

No.	Active	Name	Disposition Policy	Protocol	Source Address(es)	Destination Address(es)	Source Ports	Destination Ports
0	<input type="checkbox"/>	ICMP-DENY	Deny	ICMP	Any	Any	Any	Any
1	<input type="checkbox"/>	TCP-DENY	Deny	TCP	Any	Any	Any	Any
2	<input checked="" type="checkbox"/>	IGMP	Accept	IGMP	Any	Any	Any	Any
3	<input checked="" type="checkbox"/>	UDP	Accept	UDP	Any	Any	53	Any
4	<input checked="" type="checkbox"/>	[192.168.0.0]	Accept	TCP	Any	Any	Any	80-85
5	<input checked="" type="checkbox"/>	[192.168.0.0]	Accept	TCP	Any	Any	Any	8080
6	<input checked="" type="checkbox"/>	UDP	Accept	UDP	Any	Any	1645	Any
7	<input checked="" type="checkbox"/>	[192.168.0.0]	Accept	UDP	Any	Any	87	88

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

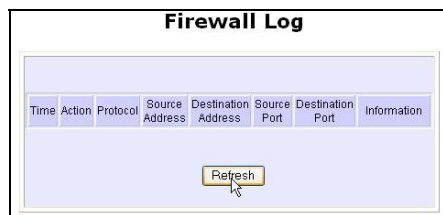
Use the Firewall Log

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

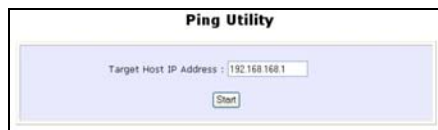
Use the Ping Utility

(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:

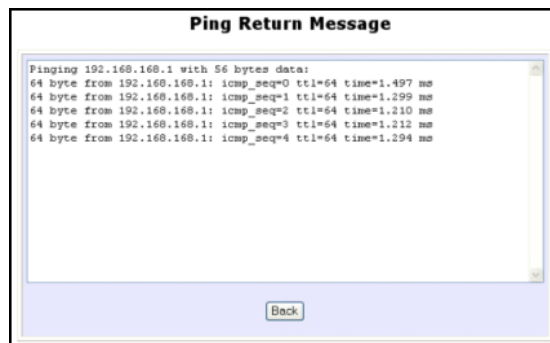
Select [Ping Utility](#) under the [SYSTEM TOOLS](#) command menu.



Step 2:

Enter the IP address of the target host to ping.

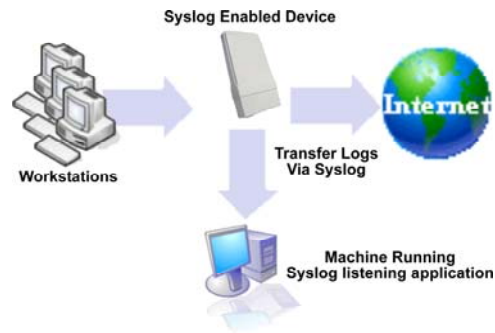
Click the [Start](#) button.



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:

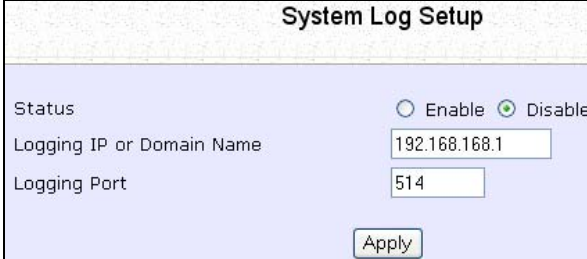
- **Enable** or **Disable** system logging.
- Set the **Remote IP Address or Domain Name** and **Remote Port** for the router to send the system log messages to.

Follow these steps to setup Syslog:

Step 1:

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

Step 2:



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

Select to **Enable** Syslog.

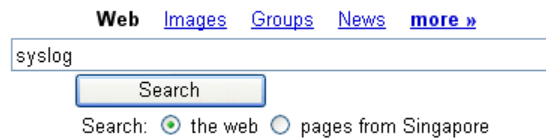
Enter the **Logging IP or Domain Name**

Enter the **Logging Port**

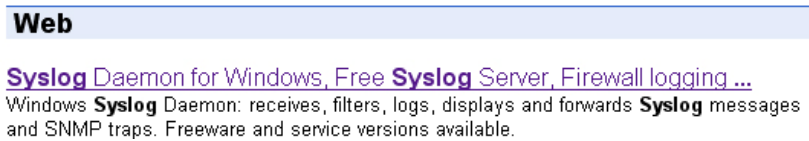
Click **Apply** to make the changes.

Follow these sample steps to view logged information:

Step 1:
Search for a Syslog listening application.



Step 2:
Select a Syslog listening application.



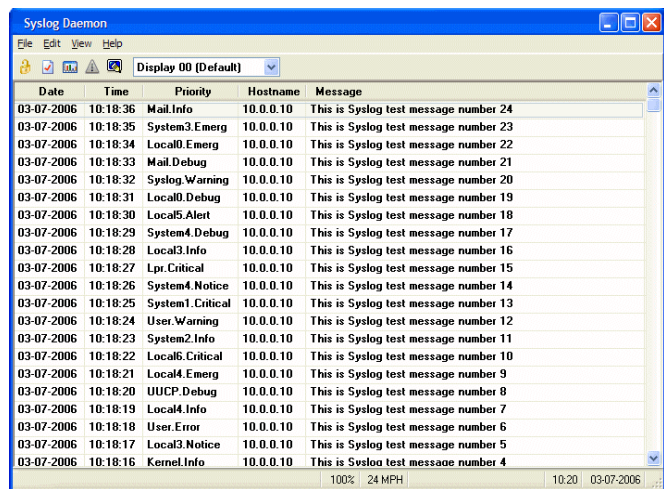
Step 3:
Download Syslog listening application.



Step 4:
Install Syslog listening application.



Step 5:
View logged information on Syslog listening application.



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.



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

Step 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**.

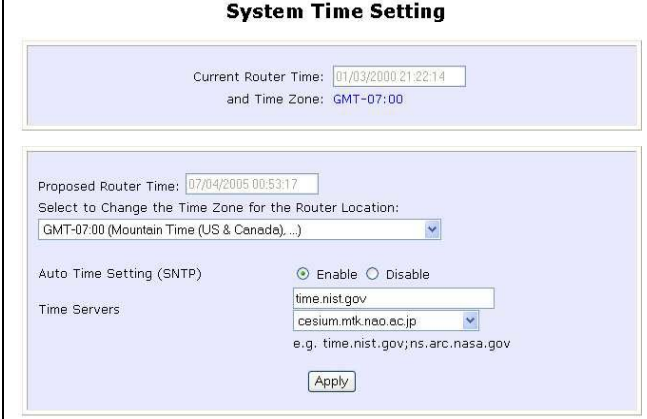
This entry identifies the device location, especially when there are multiple devices.

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.



The screenshot shows a window titled "System Time Setting". It contains the following fields and controls:

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

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.



Step 4:

You need to reboot the system after the firmware upgrade.



NOTE

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

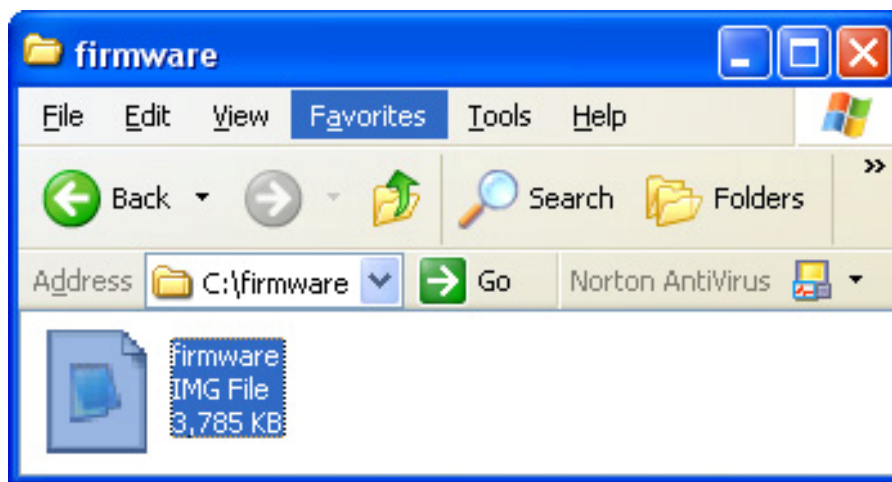
Upgrade the Firmware with Command Line Interface

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

Follow these steps to upgrade firmware from Command Line Interface (CLI).

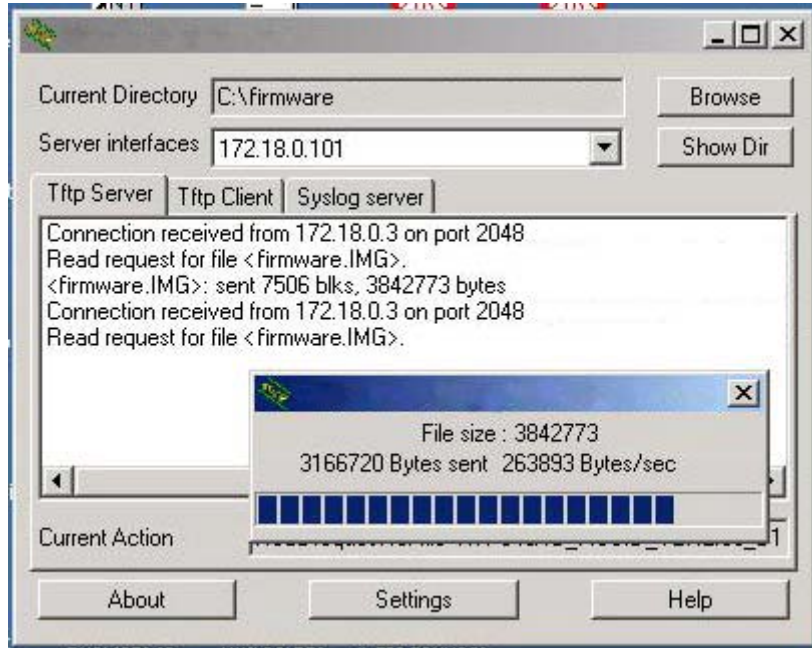
Step 1:

Ensure that you have the updated firmware available.



Step 2:

On the PC connected to the AP, run a TFTP server and setup to point to the same firmware image filename.

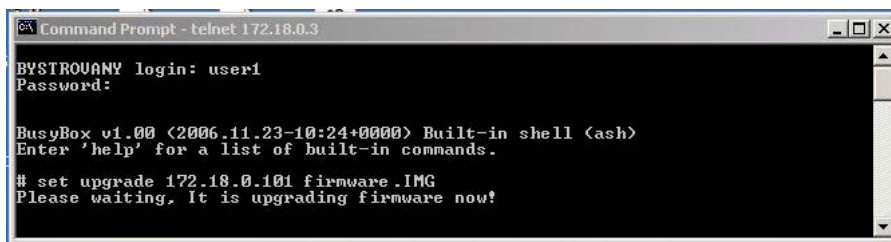


Sample Screenshot

Step 3:

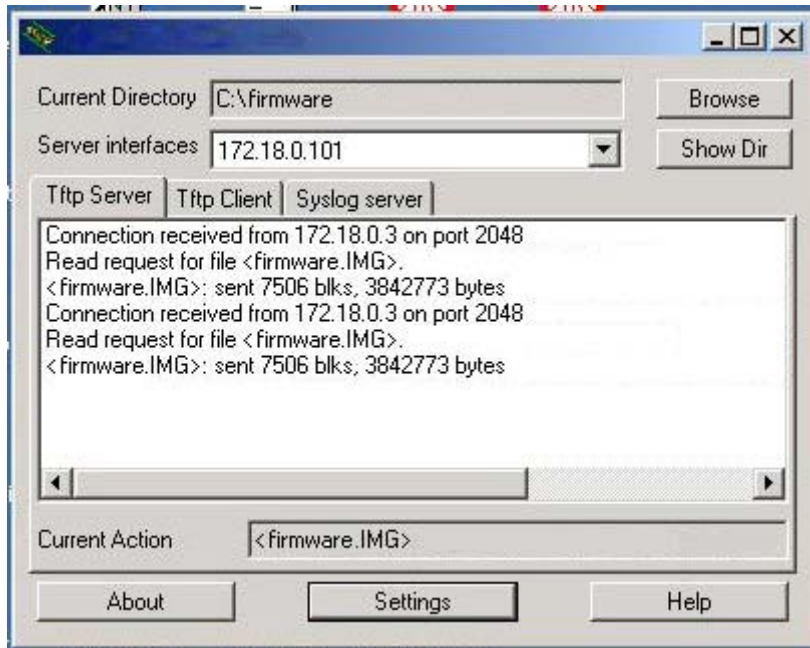
In the Command Line Interface, enter the command with the IP address of the AP and the filename of the firmware image as the parameters:

Set upgrade <IP address of AP> <firmware image filename>

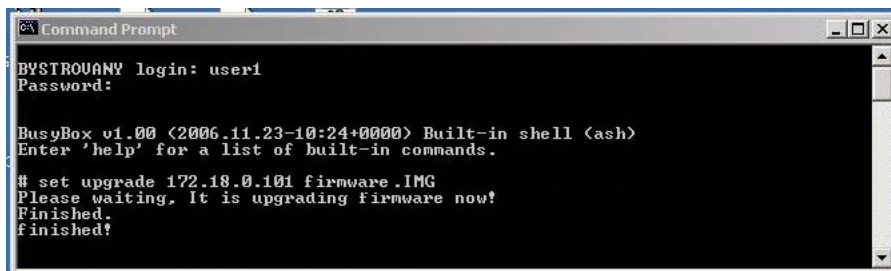


Step 4:

These screens display when upgrade is done.



Sample Screenshot



NOTE



The firmware upgrade process must NOT 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 (M) 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:\accesspoint\accesspointxxx.IMG**, then replace the command with this new path and firmware name. For example:

C:\accesspoint\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.

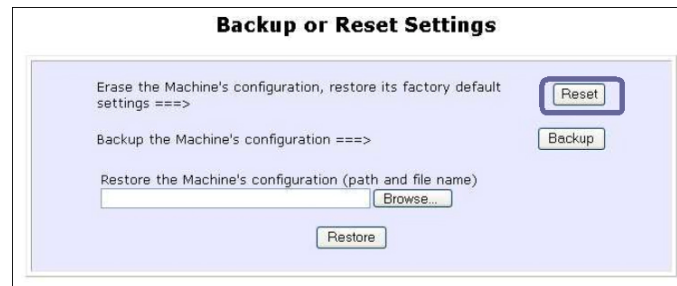
Reset your settings

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.



The screenshot shows a web interface titled "Backup or Reset Settings". It contains three main sections:

- The first section is "Erase the Machine's configuration, restore its factory default settings ==>" with a "Reset" button to its right.
- The second section is "Backup the Machine's configuration ==>" with a "Backup" button to its right.
- The third section is "Restore the Machine's configuration (path and file name)" which includes a text input field, a "Browse..." button, and a "Restore" button below it.

Step 3:

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

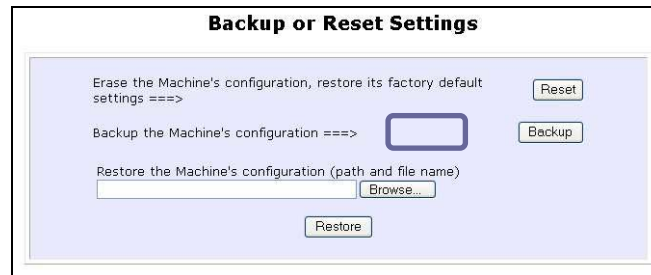
Backup your Settings

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.



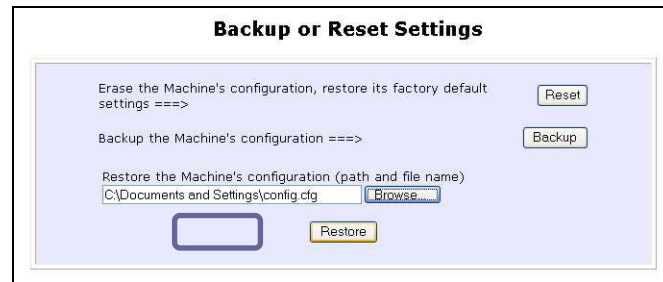
Restore your Settings

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.



The screenshot shows a web form titled "Change Password". It contains three input fields: "Current Password:" with 7 dots, "New Password:" with 5 dots, and "Confirm Password:" with 5 dots. Below the fields is an "Apply" button.

To Logout

Step 1:

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

Step 2:

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



Wireless LAN Access Point Management

Please enter your password:

(Forgot your password? - see the User's Guide for instructions.)

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 06:45:50
BIOS/Loader Version :	2.31 (build 0310)
Firmware Version :	2.06 (build 1229)
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 :	

Get Technical Support

This page displays the contact information of technical support centres around the world.

If further information unavailable in the manual or data sheet is required, please contact a Technical Support Centre by mail, email, fax or telephone.

Click on **Get Technical Support** from the **HELP** menu.

Support Information

For technical support email to: support@compex.com.sg

For updates connect to the following Web Sites:

<http://www.cpx.com>

<http://www.compex.com.sg>

Regional Technical Support Centers

U.S.A., Canada, Latin America and South America :

Compex Inc.

840 Columbia Street, Suite B, Brea, CA92821,USA

Tel : (714) 482-0333

Fax : (714) 482-0332

800 Line: (800) 279-8891

Support email: support@cpx.com

Asia, Australia, New Zealand, Middle East and the rest of the world :

Compex Systems Pte. Ltd.

135, Joo Seng Road, #08-01,

PM Industrial Building

Singapore 368363

HotLine : (65) 6-286-1805

Fax : (65) 6-283-8337

Appendix: Use the Command Line Interface

Get Operation List

SYNTAX	DESCRIPTION
Get tasks	Display all active process/tasks.
Get sysinfo	Display system information.
Get aplist	Display list of access points discovered.
Get athstats	Display wireless driver information.
Get brinfo	Display bridge and interfaces information.
Get brmacshow	Display bridge learned MAC address list.
Get bssinfo.	Display current radio information.
Get channel	Display current wireless channel number.
Get chanlist	Display current domain wireless channels.
Get ieee80211stats	Display ieee80211 protocol statistics.
Get routeshow	Display the routing table information.
Get stalist	Display a list of currently associated stations.
Get linkinfo	Display client link information (Client mode only)
Get macstats	Display a list of currently learnt wireless device MAC addresses.
Get opmode	Display current wireless operation mode.
Get wmode	Display wireless mode

Set Operation List

SYNTAX	DESCRIPTION
Set factorydefault	Set factorydefault – restore configuration to factory default.
Restart	Do a warm reboot.

Save Configuration

SYNTAX	DESCRIPTION
Commit	Save current configuration to flash. Most commands require rebooting to take effect after saving.

Long Range

Check for recommended values from long distance option setup page.

SYNTAX	DESCRIPTION
Set outdoor <enable/disable>	Enable outdoor for long-range connection.
Set distance <value>	Set the connection distant (value in decimal)
Set acktimeout <value>	Set the ACK timeout (value in decimal)
Set ctstimeout <value>	Set the CTS timeout (value in decimal)
Set slottimeout <value>	Set the Slot timeout (value in decimal)

TX Power

SYNTAX	DESCRIPTION
Set txpower <string>	(Default full) auto, 1, 2, 3, 4, ..., 17, full, min

TX Rate

SYNTAX	DESCRIPTION
Set txrate <string>	Values are: (default auto) (802.11a)-- 6, 9, 12, 18, 24, 36, 48, 54, auto (Version AG) (802.11b/g mixed)-- 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54, auto (802.11b-only)-- 1, 2, 5.5, 11, auto

Wireless Mode

SYNTAX	DESCRIPTION
Set wirelessmode <string>	Supported strings are: auto, 11a, 11b, 11g, pureg, superg, supera
Set autochannelselect enable/disable	Enable or disable smart channel select during power up.
Set radio_off_eth_down enable/disable	Enable or disable auto turn off radio when Ethernet port connection link is lost.

WEP Key

Must first set a key entry type, then proceed to set the key index, size, and value.

SYNTAX	DESCRIPTION
Set key <keyindex> <keysize> <keyvalue>	Set keyentrymethod hex/ascii
Set key <keyindex> default	Set default key.

Add or Delete User

SYNTAX	DESCRIPTION
Set user < [-r -w] > <password> username	To add a user.
Set user -d username	To delete user.

Country Code

SYNTAX	DESCRIPTION
Set countrycode <iso.name>	List of countries:
Set countrycode <2 letter string>	<pre> {0, "NA"}, {CTRY_ALBANIA, "AL"}, {CTRY_ALGERIA, "DZ"}, {CTRY_ARGENTINA, "AR"}, {CTRY_ARMENIA, "AM"}, {CTRY_AUSTRALIA, "AU"}, {CTRY_AUSTRIA, "AT"}, {CTRY_AZERBAIJAN, "AZ"}, {CTRY_BAHRAIN, "BH"}, {CTRY_BELARUS, "BY"}, {CTRY_BELGIUM, "BE"}, {CTRY_BELIZE, "BZ"}, {CTRY_BOLIVIA, "BO"}, {CTRY_BRAZIL, "BR"}, {CTRY_BRUNEI_DARUSSALAM, "BN"}, {CTRY_BULGARIA, "BG"}, {CTRY_CANADA, "CA"}, {CTRY_CHILE, "CL"}, {CTRY_CHINA, "CN"}, {CTRY_COLOMBIA, "CO"}, {CTRY_COSTA_RICA, "CR"}, {CTRY_CROATIA, "HR"}, {CTRY_CYPRUS, "CY"}, {CTRY_CZECH, "CZ"}, {CTRY_DENMARK, "DK"}, {CTRY_DOMINICAN_REPUBLIC, "DO"}, {CTRY_ECUADOR, "EC"}, {CTRY_EGYPT, "EG"}, {CTRY_EL_SALVADOR, "SV"}, {CTRY_ESTONIA, "EE"}, {CTRY_FINLAND, "FI"}, {CTRY_FRANCE, "FR"}, {CTRY_FRANCE2, "F2"}, {CTRY_GEORGIA, "GE"}, {CTRY_GERMANY, "DE"}, {CTRY_GREECE, "GR"}, {CTRY_GUATEMALA, "GT"}, {CTRY_HONDURAS, "HN"}, {CTRY_HONG_KONG, "HK"}, {CTRY_HUNGARY, "HU"}, {CTRY_ICELAND, "IS"}, {CTRY_INDIA, "IN"}, {CTRY_INDONESIA, "ID"}, </pre>

	{CTRY_IRAN, "IR" }, {CTRY_IRELAND, "IE" }, {CTRY_ISRAEL, "IL" }, {CTRY_ITALY, "IT" }, {CTRY_JAPAN, "JP" }, {CTRY_JAPAN1, "J1" }, {CTRY_JAPAN2, "J2" }, {CTRY_JAPAN3, "J3" }, {CTRY_JAPAN4, "J4" }, {CTRY_JAPAN5, "J5" }, {CTRY_JAPAN6, "J6" }, {CTRY_JORDAN, "JO" }, {CTRY_KAZAKHSTAN, "KZ" }, {CTRY_KOREA_NORTH, "KP" }, {CTRY_KOREA_ROC, "KR" }, {CTRY_KOREA_ROC2, "K2" }, {CTRY_KOREA_ROC3, "K3" }, {CTRY_KUWAIT, "KW" }, {CTRY_LATVIA, "LV" }, {CTRY_LEBANON, "LB" }, {CTRY_LIECHTENSTEIN, "LI" }, {CTRY_LITHUANIA, "LT" }, {CTRY_LUXEMBOURG, "LU" }, {CTRY_MACAU, "MO" }, {CTRY_MACEDONIA, "MK" }, {CTRY_MALAYSIA, "MY" }, {CTRY_MALTA, "MT" }, {CTRY_MEXICO, "MX" }, {CTRY_MONACO, "MC" }, {CTRY_MOROCCO, "MA" }, {CTRY_NETHERLANDS, "NL" }, {CTRY_NEW_ZEALAND, "NZ" }, {CTRY_NORWAY, "NO" }, {CTRY_OMAN, "OM" }, {CTRY_PAKISTAN, "PK" }, {CTRY_PANAMA, "PA" }, {CTRY_PERU, "PE" }, {CTRY_PHILIPPINES, "PH" }, {CTRY_POLAND, "PL" }, {CTRY_PORTUGAL, "PT" }, {CTRY_PUERTO_RICO, "PR" }, {CTRY_QATAR, "QA" }, {CTRY_ROMANIA, "RO" }, {CTRY_RUSSIA, "RU" }, {CTRY_SAUDI_ARABIA, "SA" }, {CTRY_SINGAPORE, "SG" }, {CTRY_SLOVAKIA, "SK" }, {CTRY_SLOVENIA, "SI" }, {CTRY_SOUTH_AFRICA, "ZA" }, {CTRY_SPAIN, "ES" }, {CTRY_SWEDEN, "SE" }, {CTRY_SWITZERLAND, "CH" }, {CTRY_SYRIA, "SY" }, {CTRY_TAIWAN, "TW" }, {CTRY_THAILAND, "TH" }, {CTRY_TRINIDAD_Y_TOBAGO, "TT" }, {CTRY_TUNISIA, "TN" }, {CTRY_TURKEY, "TR" }, {CTRY_UKRAINE, "UA" }, {CTRY_UAE, "AE" }, {CTRY_UNITED_KINGDOM, "GB" }, {CTRY_UNITED_STATES, "US" }, {CTRY_URUGUAY, "UY" }, {CTRY_UZBEKISTAN, "UZ" }, {CTRY_VENEZUELA, "VE" }, {CTRY_VIET_NAM, "VN" }, {CTRY_YEMEN, "YE" }, {CTRY_ZIMBABWE, "ZW" },
--	--

Channel

SYNTAX	DESCRIPTION
Set channel <value>	(Value in decimal)

SSID

SYNTAX	DESCRIPTION
Set ssid <string>	(Not More than 32 characters)

Closed System

SYNTAX	DESCRIPTION
Set hidessid enable/disable	Enable or disable broadcasting of SSID.

Per Node

SYNTAX	DESCRIPTION
Set apbridge enable/disable	Enable or disable isolation of wireless client.

RTS, Fragment, and Beacon Interval

SYNTAX	DESCRIPTION
Set rts <value>	(Value in decimal, default 2312, range 1 to 2312)
Set fragment <value>	(Value in decimal, default 2346, range, 256 to 2346)
Set beaconintval <value>	(Value in decimal, default 1, range 1 to 1000)
Set dtim <value>	Data Beacon Rate (value in decimal, default 1, range 1 to 16384)

WLAN State

SYNTAX	DESCRIPTION
Get wlanstate	Display whether status of current wireless operation is Enabled or Disabled.
Set wlanstate enable/disable	Set to Disable to turn off wireless operation. Set to Enable to turn back on wireless operation. Note: When executing this command, please ensure that you are not connected on wireless with device or you will be disconnected from the device and network. The wireless operation can only be Enabled from the Ethernet port or UTP cable connection to device.

Reset Button

SYNTAX	DESCRIPTION
Get buttonpassreset	Display the status of Reset Button operation. If status is (Enabled), resetting of password by pressing Reset Button is allowed. If status is (Disabled), resetting of password by pressing Reset Button is not allowed.
Set buttonpassreset enable/disable	Set to Disable to prevent resetting of password by pressing Reset button. Set to Enable to allow resetting of password by pressing Reset button.

Upgrade Firmware

SYNTAX	DESCRIPTION
Set upgrade <IP address of AP> <firmware image filename>	To upgrade firmware in CLI enter this command with the IP address of AP and the firmware image filename.

Appendix: Virtual AP (Multi-SSID) FAQ

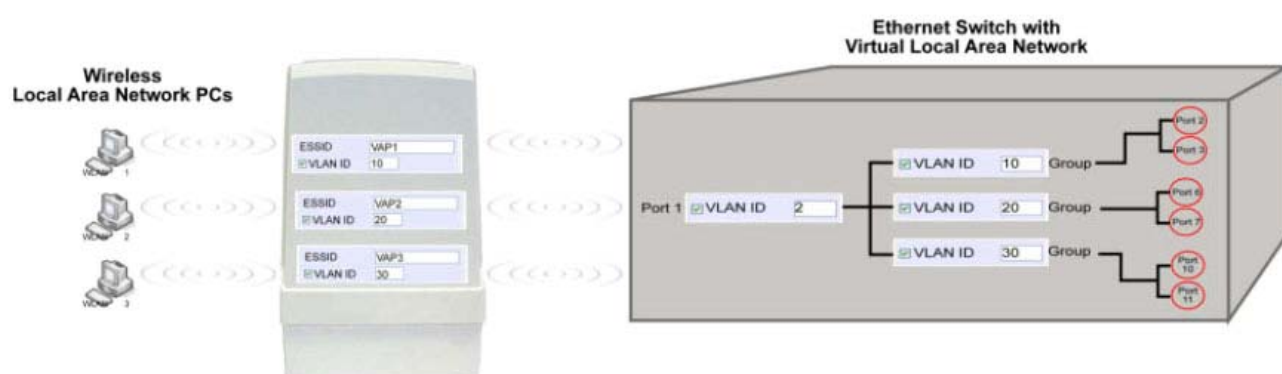
Q1) What is mSSID?

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.

Q3) Can I update my access point to this mSSID firmware?

Yes. You can retain your access point configuration when you update to the mSSID firmware if the current firmware running is v1.3x and above.

If AP is running the following configuration setup, updating to the mSSID firmware will affect the configuration.

If AP is running as PtP (Point-To-Point) or PtMP (Point-To-MultiPoint) mode.

The reason it cannot retain the configuration is because mSSID uses a new PtP and PtMP connection setup method called: RootAP and Transparent Client. This method is compliant with IEEE 802.11h standard.

AP is running very old firmware v1.2x and below.

Q4) Can I update to mSSID firmware but setup only one SSID connection?

Yes, mSSID firmware operation is similar to previous single SSID firmware when setup with one SSID.

If the existing AP is running v1.3x firmware, after updating to mSSID it will retain and continue to run the previous configuration. No reconfiguration is needed.

Q5) I have a MAC Filtering table set from a previous firmware. Will updating to mSSID cause the MAC table to be lost?

No, if your firmware is v1.3x and higher, updating to mSSID firmware will retain all entries in the MAC table.

However, if you switch back from mSSID to the previous sSSID firmware, the MAC table will be lost.

Q6) I have Pseudo VLAN for Per Group enabled. Will updating to mSSID firmware still support wireless clients with MAC addresses listed in Per Group?

The mSSID firmware replaces Pseudo VLAN and integrates it into VAP (Virtual AP) and MAC Filtering.

Thus, Pseudo VLAN with its VLAN ID and MAC listing will be lost after updating to mSSID firmware.

Refer to the user manual on how to create new VAP with VLAN ID and MAC Filtering.

Similarly, Per Node (control to isolate wireless station in AP) being part of Pseudo VLAN will also be lost.

This option can be enabled again with the option "Station Isolation" in VAP setup page.

Q7) I have WDS setup in my network. Will mSSID still support this?

WDS has the limitation that it can only support WEP security key.

To support higher wireless security it is replaced with Repeater mode in mSSID firmware.

Thus, updating to mSSID will disconnect the WDS links and connections with the rest of the APs.

It is recommended to connect directly to each AP to update the firmware, then set to Repeater mode and configure it before updating the next AP. This way you can build back the connections.

Refer to the user manual for more details instructions on the setup.

Updating to the mSSID firmware is not necessary if you do not need the higher wireless security support.

Q8) I have 2 of the access point units installed at a site about 2km from each other running PtP modes.

Should I update to mSSID firmware? Can I do it from one location to update the firmware like I do with the current single SSID firmware?

The setup for PtP and PtMP for mSSID firmware is different the current sSSID firmware.

After mSSID firmware starts up, the link between the 2 APs will be lost.

The recommended method is to setup 2 similar model units in the office. Load the mSSID firmware and create the new PtP / PtMP configuration using the actual parameters of the 2 units on site that you will update.

After testing the connection to be working in the office, backup the configuration file for each unit.

Go to the first site to update the mSSID firmware and restore the configuration for the site, then go to the next site and do the same.

When both APs are up again, the network at both sides should be connected with the new PtP setup.

** Note: If existing PtP connection is running well, it is not necessary to update to the mSSID firmware.

Unless you have the following concerns:

Current firmware PtP is not compliant with IEEE 802.11h standard and the respective country authority requires it to be changed.

Current firmware PtP wireless security only supports WEP key and you are very concerned about the vulnerability to being hacked.

Appendix: View the Technical Specifications

Safety and Electromagnetic Conformance	<ul style="list-style-type: none"> • FCC Part 15 SubPart B and SubPart C (for wireless module) • EN 300 328-2 • EMC CE EN 301 489 (EN300 826) • EN 55022 (CISPR 22)/EN 55024 Class B • EN 61000-3-2 • EN 61000-3-3 • CE EN 60950 • EN 301 893
Industrial Standards	<ul style="list-style-type: none"> • IEEE 802.11a (Version AG) • IEEE 802.11b • IEEE 802.11g
Data Rates	<ul style="list-style-type: none"> • Network speeds dynamically shift between 1,2, 5.5, 11, 12, 18, 24, 36, 48, 54 Mbps
Frequency Range	
IEEE 802.11a (Version AG):	5.180 ~ 5.825 GHz
IEEE 802.11b:	2.4 ~ 2.4835 GHz
IEEE 802.11g:	2.4 ~ 2.497 GHz
Wireless Operation Modes	<ul style="list-style-type: none"> • Access Point Mode • Client Mode • Wireless Routing Client • Gateway Mode • Wireless Adapter Mode • Transparent Client Mode • Repeater Mode
Security	<ul style="list-style-type: none"> • 64 - bit / 128 - bit WEP • WPA-Enterprise, WPA-Personal, WPA2-Enterprise, WPA2-Personal, WPA-Auto-Enterprise, WPA-Auto-Personal • Tagged VLAN • IEEE 802.1x – TLS, TTLS, PEAP, EAP-SIM

Network Interface	1x RJ45 10/100 Mbps auto-negotiating Ethernet port
Modulation	<ul style="list-style-type: none"> • BPSK (Binary Phase Shift Keying) • QPSK (Quadrature Phase Shift Keying) • CCK (Complementary Code Keying) • 16 QAM, 64 QAM (Quadrature Amplitude Modulation)
Radio Technology	<ul style="list-style-type: none"> • DSSS (Direct Sequence Spread Spectrum) • OFDM (Orthogonal Frequency Division Multiplexing)
Output Power IEEE 802.11a (Version AG):	20 - 26 dBm (depend on configuration)
IEEE 802.11b:	20 - 26 dBm (depend on configuration)
IEEE 802.11g:	20 - 26 dBm (depend on configuration)
SNMP	<ul style="list-style-type: none"> • SNMP (RFC 1157) • MIB II (RFC 1213)
LED Indicators	<ul style="list-style-type: none"> • Power • Diagnostic • LAN Link/Activity • WLAN Link/Activity

IP Addressing	All classful/classless subnets
Management	<ul style="list-style-type: none"> • Telnet Command Console • HTTP Web Management • SSH • Syslog
Built-in DHCP Server	Yes
DHCP Reservation	By MAC address
Operating Channels	<ul style="list-style-type: none"> • 11 Channels: US and Canada • 13 Channels: Europe • 14 Channels: Japan
Load Balancing	Parallel Broadband (in Gateway mode)
Fail-Over Redundancy	Parallel Broadband (in Gateway mode)
Virtual Server	IP and Port Forwarding, De-Militarised Zone
IP Packet Filtering	<ul style="list-style-type: none"> • Time-based • By TCP Port • By Source IP
IP Routing	Static & Dynamic Entry
VPN Client Pass-Through	PPTP, IPsec
Configuration Interface	Web-based Configuration Menu
Profile Backup & Restore	Yes
Firmware Upgrade	Yes
Power Requirements	Passive PoE (range 12V – 24V DC)