



networks@work

# USER'S MANUAL



COMPEX

**WPE53G**  
WPE53G  
WPE53G  
WPE53G  
WPE53G

RoHS-compliant

**© Copyright 2007 Compex Systems Pte Ltd**

All Rights Reserved

This document contains information, which is protected by copyright. Reproduction, adaptation or translation without prior permission is prohibited, except as allowed under the copyright laws.

**Trademark Information**

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

Notice: Copyrights © 2007 by Compex, Inc. All rights reserved. Reproduction, adaptation, or translation without prior permission of Compex, Inc. is prohibited, except as allowed under the copyright laws.

Manual Revision by Jojo

Manual Number: U-0587-V1.12C Version 1.12 July 2008

**Disclaimer**

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

**FCC NOTICE**

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

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

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

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

This device may not cause harmful interference, and

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

**RF Exposure warning**

The equipment complies with FCC RF exposure limits set forth for an uncontrolled environment.

The equipment must not be co-located or operating in conjunction with any other antenna or transmitter.

ICES 003 Statement

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

**Declaration of Conformity**

Compex, Inc. declares the following:

Product Name: Wireless Network Access Point

Model No.: WPE53G conforms to the following Product Standards:

This device complies with the Electromagnetic Compatibility Directive (89/336/EEC) issued by the Commission of the European Community. Compliance with this directive implies conformity to the following European Norms (in brackets are the equivalent international standards.)

**Electromagnetic Interference (Conduction and Radiation):** EN 55022 (CISPR 22)

**Electromagnetic Immunity:** EN 55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11)

**Low Voltage Directive:** EN 60 950: 1992+A1: 1993+A2: 1993+A3: 1995+A4: 1996+A11: 1997.

*Therefore, this product is in conformity with the following regional standards: FCC Class B:* following the provisions of FCC Part 15 directive, **CE Mark:** following the provisions of the EC directive.

Compex, Inc. also declares that:

The wireless card in this product complies with the R&TTE Directive (1999/5/EC) issued by the Commission of the European Community. Compliance with this directive implies conformity to the following:

**EMC Standards:** FCC: 47 CFR Part 15, Subpart B, 47 CFR Part 15, Subpart C (Section 15.247); CE: EN 300 328-2, EN 300 826 (EN 301 489-17)

*Therefore, this product is in conformity with the following regional standards: FCC Class B:* following the provisions of FCC Part 15 directive, **CE Mark:** following the provisions of the EC directive.

**Firmware**

This manual is written based on Firmware version 2

# Table of Contents

OVERVIEW THE PRODUCT .....	1
Introduction .....	1
Features and Benefits.....	2
When to Use Which Mode.....	4
Access Point Mode.....	4
Access Point Client Mode .....	5
Wireless Routing Client Mode.....	6
Gateway Mode.....	7
Wireless Adapter Mode.....	9
Transparent Client Mode .....	10
Repeater Mode.....	12
PANEL VIEWS AND DESCRIPTION .....	13
INSTALL THE HARDWARE.....	14
Setup Requirements .....	14
Using power adapter to supply power to the unit.....	14
Using PoE to supply power to the unit .....	16
Setup for Windows XP/2000.....	18
ACCESS THE WEB INTERFACE.....	20
Access with uConfig .....	20
Manual access with Internet Explorer .....	23
PERFORM BASIC CONFIGURATION .....	25
Setup Management Port.....	25
Setup DHCP Server.....	30
View Active DHCP Leases .....	36
Reserve IP Addresses for Predetermined DHCP Clients .....	37
Delete DHCP Server Reservation .....	39
Setup WLAN .....	40
Configure the Basic Setup of the Wireless Mode.....	40
Scan for Site Survey.....	45
View Link Information .....	47
Scan for Channel Survey .....	49
Align the Antenna.....	52
Configure the Advanced Setup of the Wireless Mode .....	54
View the Statistics.....	56
Setup Your WAN.....	57
Setup Telnet / SSH .....	64
Access the TELNET Command Line Interface.....	66

Access the Secure Shell Host Command Line Interface .....	67
Set the WEB Mode .....	68
Use MAC Filtering .....	69
Add a MAC Address to the MAC Address List .....	70
Delete a MAC Address from All Access Points.....	73
Delete a MAC Address from Individual Access Point .....	75
Edit MAC Address from the MAC Address List.....	77
PERFORM ADVANCED CONFIGURATION.....	79
Setup Routing .....	79
Configure Static Routing.....	80
Use Routing Information Protocol.....	81
Use Network Address Translation.....	82
Configure Virtual Servers Based on DMZ Host .....	83
Configure Virtual Servers Based on Port Forwarding .....	84
Configure Virtual Servers based on IP Forwarding .....	88
Control the Bandwidth Available .....	89
Enable Bandwidth Control .....	89
Configure WAN Bandwidth Control.....	90
Configure LAN Bandwidth Control.....	91
Perform Remote Management.....	93
Setup Remote Management.....	93
USE PARALLEL BROADBAND .....	94
Enable Parallel Broadband .....	95
Setup Email Notification.....	96
Using Static Address Translation.....	97
Use DNS Redirection.....	98
Enable or Disable DNS Redirection .....	100
Dynamic DNS Setup .....	101
To enable/disable Dynamic DNS Setup .....	101
To manage Dynamic DNS List .....	102
USE THE WIRELESS EXTENDED FEATURES.....	106
Setup WDS2.....	106
Set Virtual AP (Multiple SSID) .....	110
Set Preferred APs.....	112
Get Long Distance Parameters .....	113
Set Wireless Multimedia.....	115
Setup Point-to-Point & Point-to-MultiPoint Connection .....	118
Setup Repeater.....	122
SECURE YOUR WIRELESS LAN .....	127
Setup WEP .....	128
Setup WPA-Personal .....	129

Setup 802.1x/RADIUS for Access Point.....	131
Setup 802.1x/RADIUS for Client .....	133
Setup WPA Enterprise for Access Point .....	135
Setup WPA Enterprise for Client.....	136
CONFIGURE THE SECURITY FEATURES .....	139
Use Packet Filtering.....	139
Configure Packet Filtering .....	139
Use URL Filtering.....	142
Configure URL Filtering .....	142
Configure the Firewall.....	143
Configure SPI Firewall .....	143
Use the Firewall Log .....	147
View Firewall Logs .....	147
ADMINISTER THE SYSTEM.....	148
Use the System Tools.....	148
Use the Ping Utility .....	148
Use Syslog .....	149
Setup System Clock .....	152
Upgrade the Firmware with uConfig .....	153
Upgrade the Firmware with Command Line Interface .....	155
Perform Firmware Recovery .....	157
Backup or Reset the Settings.....	159
Reboot the System.....	162
Change the Password.....	163
To Logout.....	164
Use the HELP menu .....	165
View About System.....	165
Get Technical Support .....	166
APPENDIX: USE THE COMMAND LINE INTERFACE .....	167
APPENDIX: VIRTUAL AP (MULTI-SSID) FAQ.....	172
APPENDIX: VIEW THE TECHNICAL SPECIFICATIONS .....	176

# Overview the Product

## Introduction

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

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

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

# Features and Benefits

- **Compact Form Factor**

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

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

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

- **Long Range Support**

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

- **Bandwidth Control**

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

- **Wireless Distribution System (WDS2)**

WDS2 connects access points using MAC address / ESSID to create a wider network so mobile users can roam while remaining connected to network resources.



- **Parallel Broadband**

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

- **Antenna Control and Alignment**

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

- **DHCP Relay**

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

- **Remote Firmware Upgrade**

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

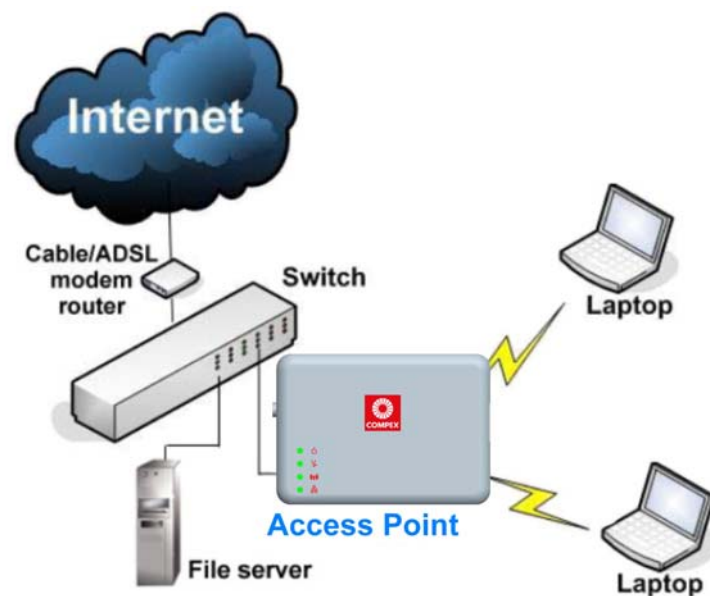
- **RIP 1 / 2**

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

# When to Use Which Mode

## Access Point Mode

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



# Access Point Client Mode

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

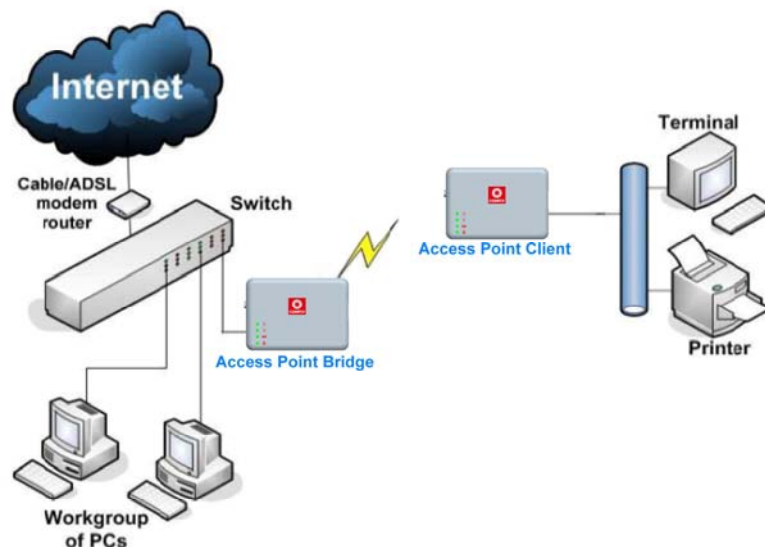
In this mode it can only connect with another access point. Other wireless clients cannot connect to it directly unless they are also connected to the same access point – allowing them to communicate with all devices connected to the Ethernet port of the access point.

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

Optional additional feature:

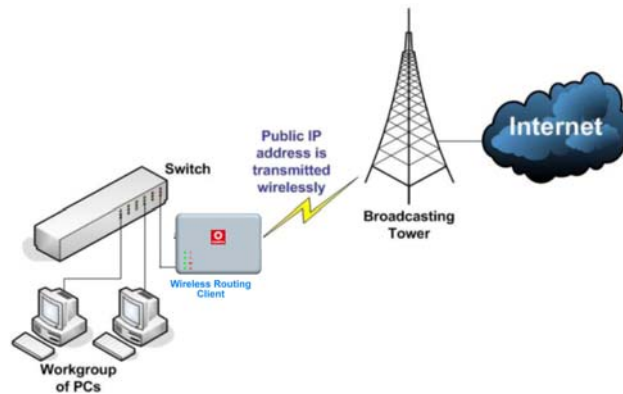
Point-to-Point connection in this operation mode is also supported if you specifically wish to connect with an access point only.

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



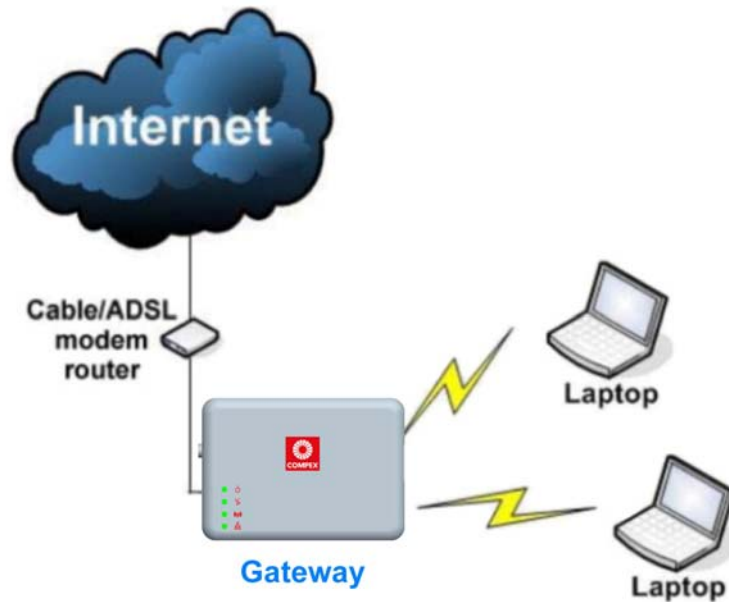
# Wireless Routing Client Mode

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



# Gateway Mode

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



Broadband Internet Access Type:

**Static IP Address**

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

**Dynamic IP Address**

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

- Singapore Cable Vision
- @HOME Cable Services

**PPP over Ethernet (PPPoE)**

Use PPPoE if you are using ADSL services in a country utilizing standard PPPoE authentication, for instance:

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

**PPTP**

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

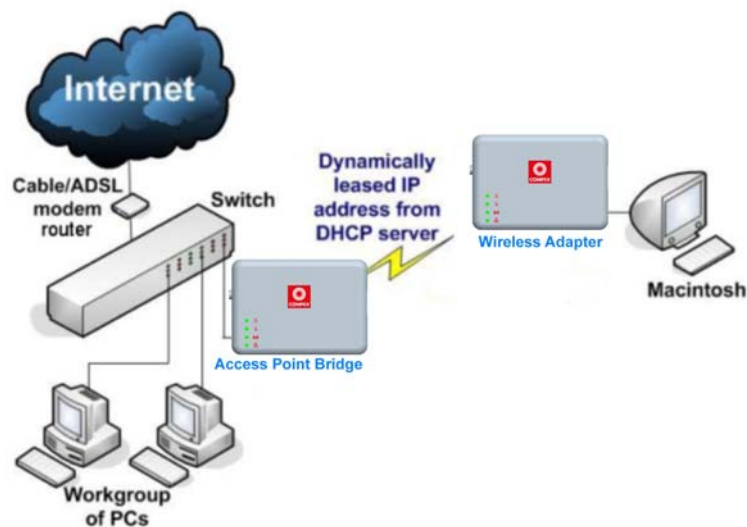
# Wireless Adapter Mode

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

Optional additional feature:

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

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

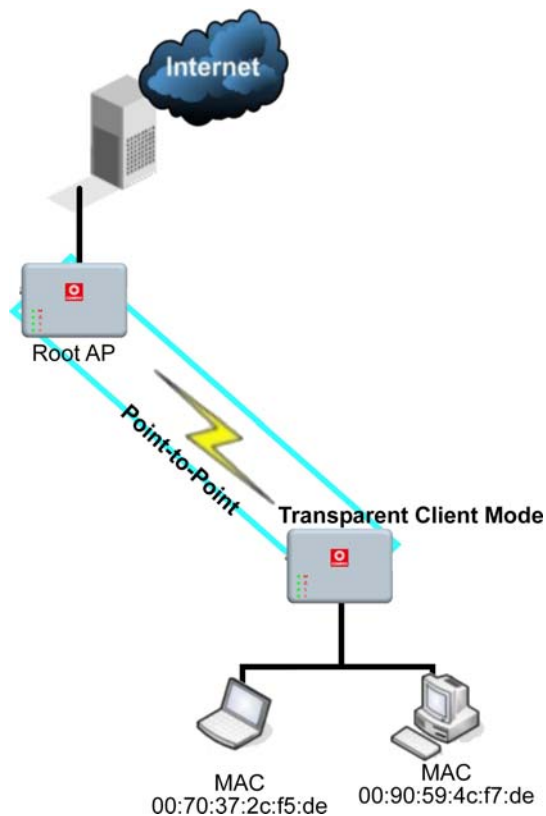


# Transparent Client Mode

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

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

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

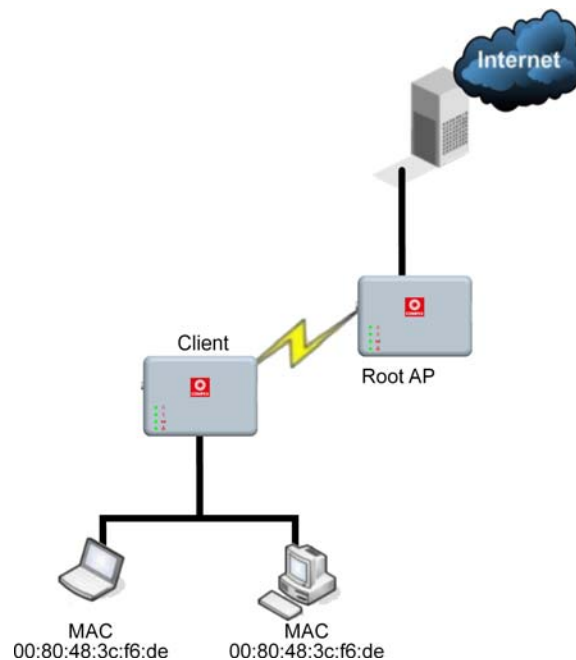


- Current Comtex model that provide RootAP support are: WP54x series; WPP54x series; WP18; and NP18A. For newer models, please contact your Comtex supplier or visit the Comtex web site.



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

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

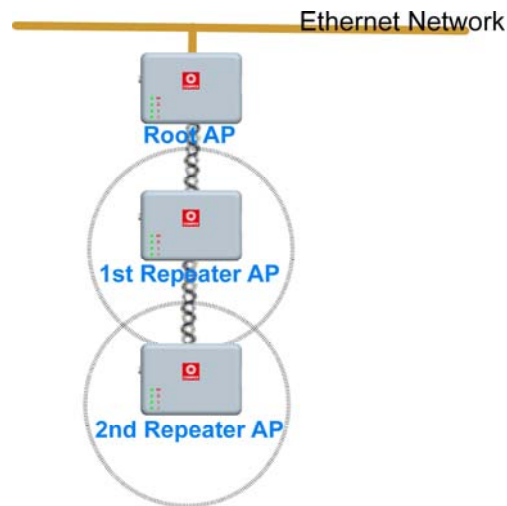


# Repeater Mode

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

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

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



# Panel Views and Description



# Install the Hardware

## Setup Requirements

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

## Using power adapter to supply power to the unit

**\* Caution: LV model DC Jack input voltage range is 9-15VDC  
HV model DC Jack input voltage range is 15-24VDC**

**\*\*\* DO NOT use power adapter from HV model on LV model**

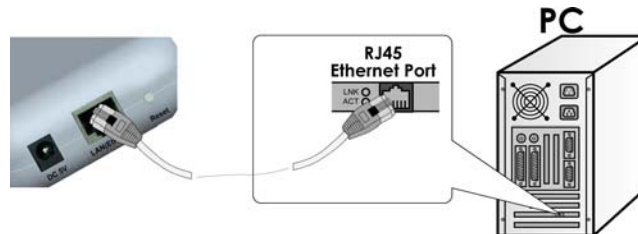
Step 1:

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



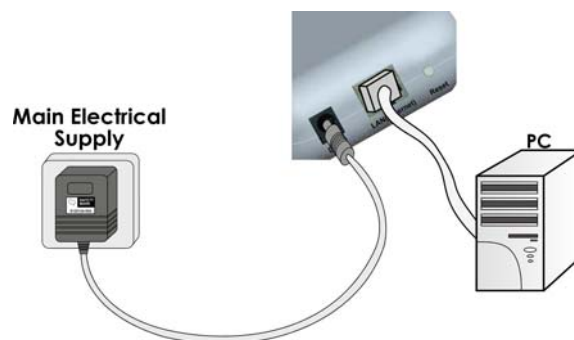
Step 2:

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



Step 3:

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



Step 4:

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

## Using PoE to supply power to the unit (supported on HV model only)

PoE is supported in the HV model. Power input range from 15-48VDC  
PoE supplies power to startup access point via the Ethernet cable connection.

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

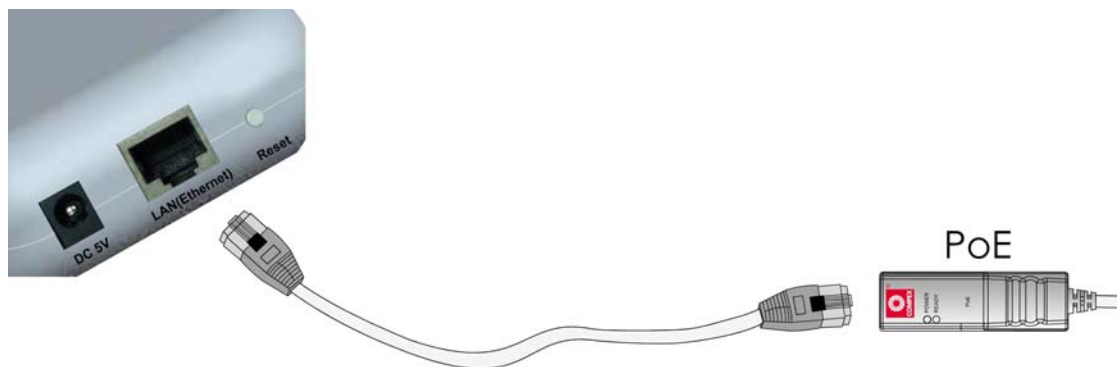
Step 1:

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



Step 2:

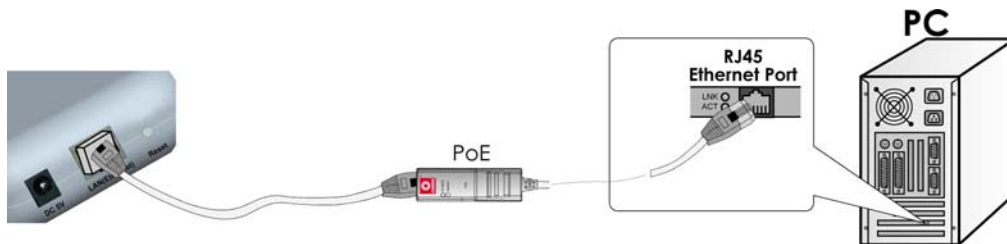
Use an RJ45 Ethernet cable to connect one end of the cable to the Ethernet socket of PoE and the other end to one of the Ethernet ports of the access point.



**Step 3:**

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

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

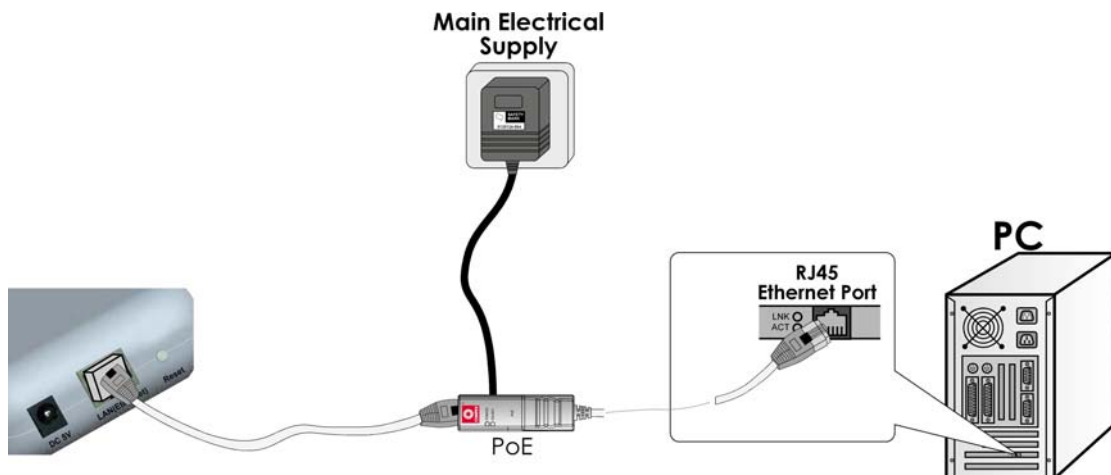


**Step 4:**

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

**Note:**

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



**Step 5:**

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

# Setup for Windows XP/2000

Step 1:

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

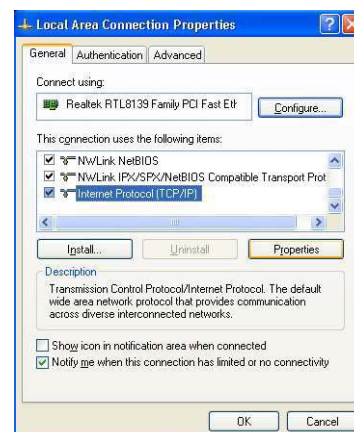
Step 2:

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



Step 3:

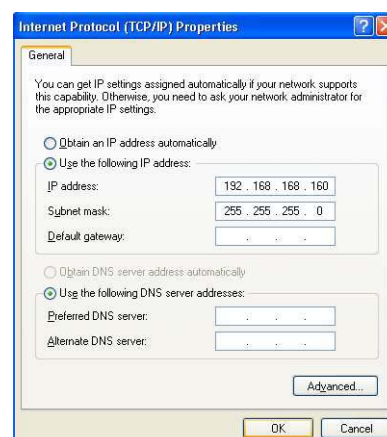
Highlight **Internet Protocol (TCP/IP)** and click on the **Properties** button.



Step 4:

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

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



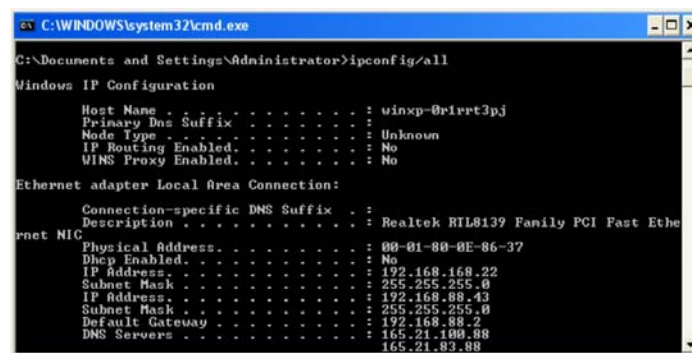


Step 5:

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

Step 6:

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



```
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 . . . . . : 165.21.189.88
                           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:

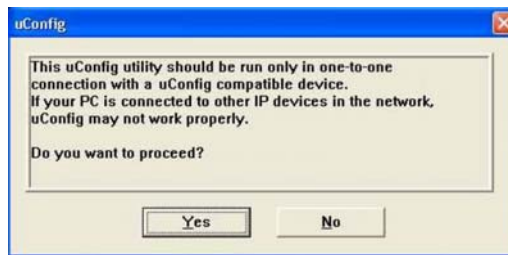
Insert the Product CD into your CD-ROM drive, the CD will autorun.

Step 2:

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

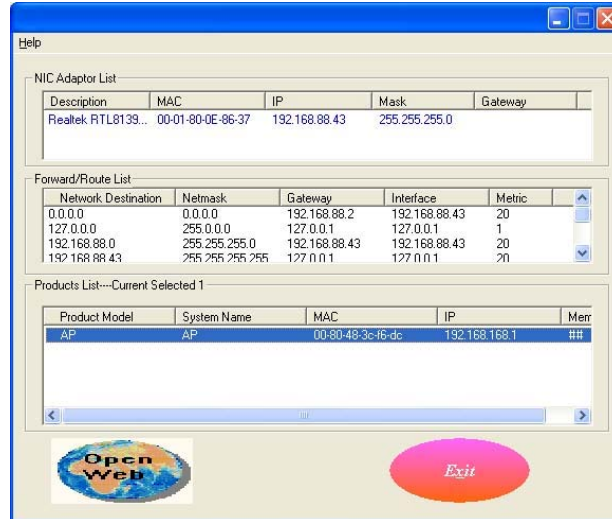
Step 3:

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



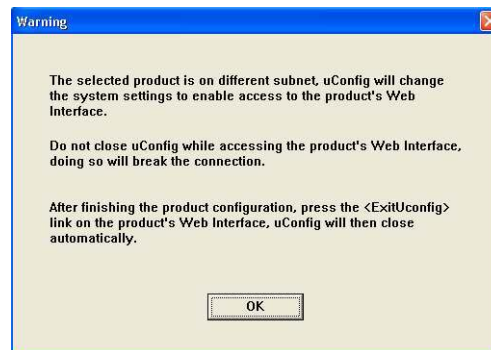
#### Step 6:

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



#### Step 7:

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



Step 8:

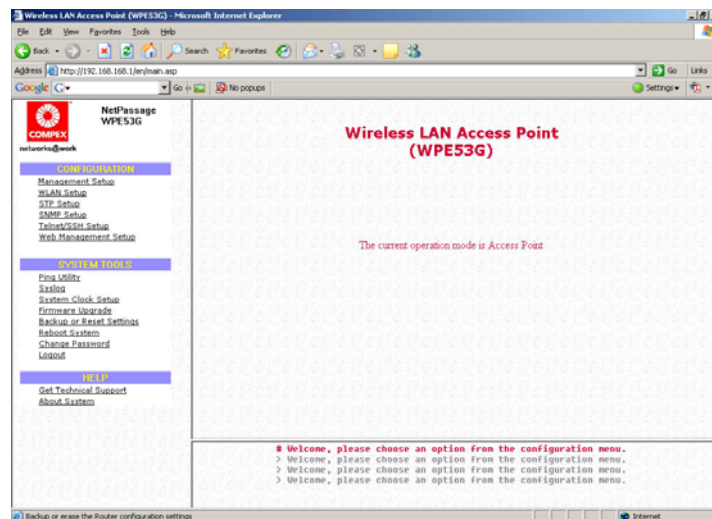
At the login page, press the **LOGIN** button to enter the configuration page. The default password is: password



The image shows a web page titled "Wireless LAN Access Point Management". It contains a text prompt "Please enter your password:" followed by a password input field with a masked password "\*\*\*\*\*" and a "LOGIN!" button. Below the login area, there is a link that says "[ Forgot your password? - see the User's Guide for instructions ]".

Step 9:

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



# Manual access with Internet Explorer

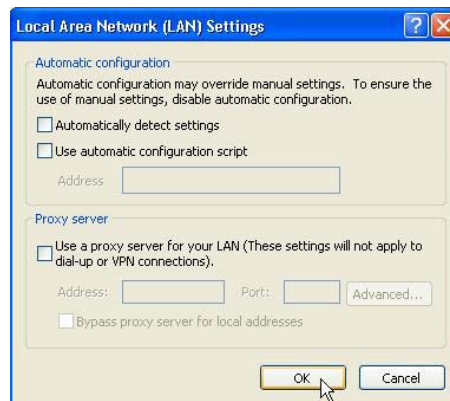
Step 1:

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



Step 2:

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



Step 3:

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

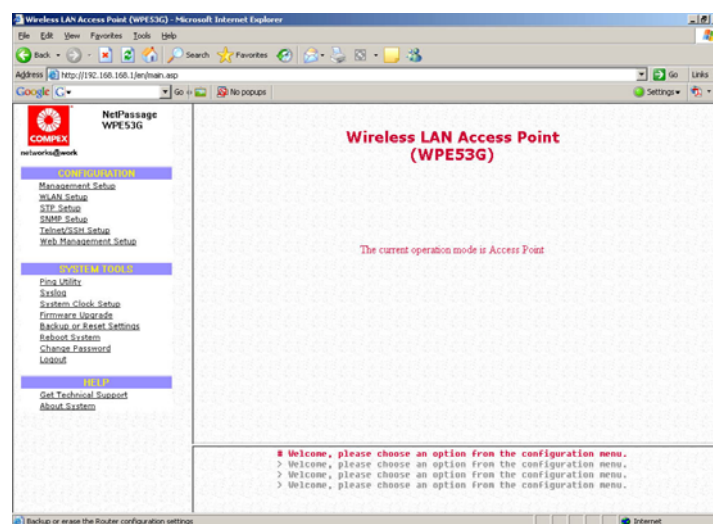
Step 4:

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



The image shows a web page titled "Wireless LAN Access Point Management". It contains a text prompt "Please enter your password:" followed by a password input field with masked characters (dots) and a "LOGIN" button. Below the login area, there is a link that says "[ Forgot your password? - see the User's Guide for instructions ]".

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



# Perform Basic Configuration

## Setup Management Port

At the Management Port Setup page, you may:

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

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

Step 1:

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

Step 2:

Select to **Automatically obtain IP address**.

Step 3:

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

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

**Management Port Setup**

☒ 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 **Automatically obtain DNS server address**.

**Management Port Setup**

☒ Automatically obtain IP address  
☐ Use the following IP address:

IP Address:   
Network Mask:   
Default Gateway IP:

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

Primary DNS IP Address:   
Secondary DNS IP Address:

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

Step 4:

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



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

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

Follow these steps to manually define the IP address.

Step 1:

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

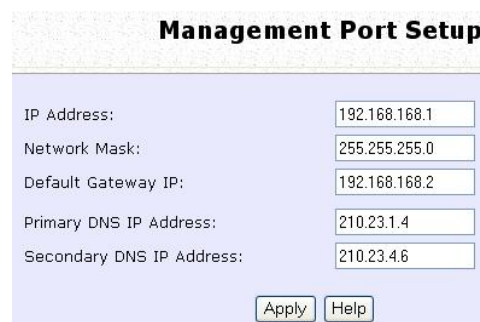
Step 2:

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

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



The screenshot shows the 'Management Port Setup' web interface. It has a title bar 'Management Port Setup'. Below it, there are two radio button options: 'Automatically obtain IP address' (unselected) and 'Use the following IP address:' (selected). Under the selected option, there are three input fields: 'IP Address:' with value '192.168.168.1', 'Network Mask:' with value '255.255.255.0', and 'Default Gateway IP:' with value '192.168.88.2'. Below these, there are two more radio button options: 'Automatically obtain DNS server address' (unselected) and 'Use the following DNS server addresses:' (selected). Under the selected option, there are two input fields: 'Primary DNS IP Address:' with value '210.23.1.4' and 'Secondary DNS IP Address:' with value '210.23.4.6'. At the bottom right, there are two buttons: 'Apply' and 'Help'.



The screenshot shows the 'Management Port Setup' web interface. It has a title bar 'Management Port Setup'. Below it, there are two radio button options: 'Automatically obtain IP address' (unselected) and 'Use the following IP address:' (selected). Under the selected option, there are three input fields: 'IP Address:' with value '192.168.168.1', 'Network Mask:' with value '255.255.255.0', and 'Default Gateway IP:' with value '192.168.168.2'. Below these, there are two more radio button options: 'Automatically obtain DNS server address' (unselected) and 'Use the following DNS server addresses:' (selected). Under the selected option, there are two input fields: 'Primary DNS IP Address:' with value '210.23.1.4' and 'Secondary DNS IP Address:' with value '210.23.4.6'. At the bottom right, there are two buttons: 'Apply' and '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>

# 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.

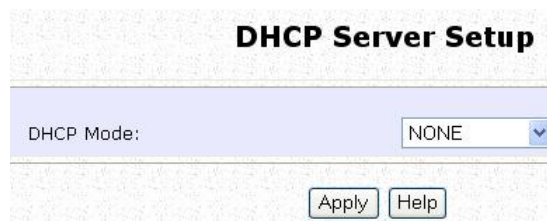
Follow these steps if you do not wish to use DHCP.

Step 1:

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

Step 2:

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



The screenshot shows a web interface for 'DHCP Server Setup'. It features a light blue header with the title. Below the header, there is a section with a light blue background containing the label 'DHCP Mode:' and a dropdown menu currently set to 'NONE'. At the bottom of this section, there are two buttons: 'Apply' and '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)
<input checked="" type="checkbox"/> Always use these DNS servers	
Primary DNS IP Address:	<input type="text" value="210.23.1.4"/>
Secondary DNS IP Address:	<input type="text" value="210.23.4.6"/>
<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>

DHCP Gateway IP Address	<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>
DHCP Lease Time	This is the length of time that the client may use the assigned address before having to check with the DHCP server to see if the Address is still valid.
Always use these DNS servers	Select this option to always use the DNS servers specified.
Primary DNS IP Address	Your ISP usually provides the IP address of the DNS server.
Secondary DNS IP Address	This optional setting is the IP address of a secondary DNS server.

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

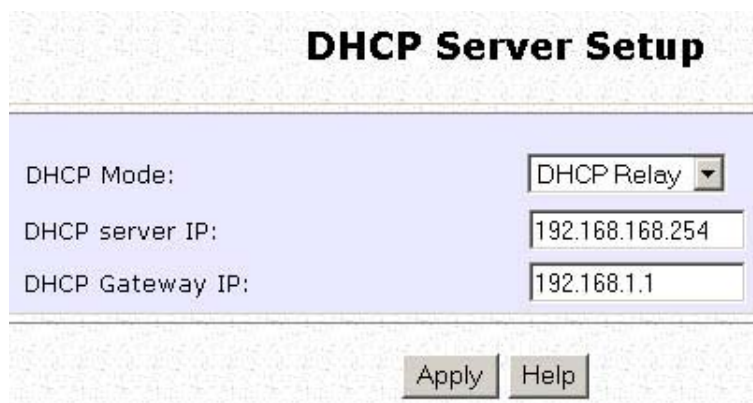
Step 1:

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

Step 2:

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

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



The screenshot shows a web-based configuration window titled "DHCP Server Setup". It contains three input fields: "DHCP Mode:" with a dropdown menu set to "DHCP Relay", "DHCP server IP:" with the value "192.168.168.254", and "DHCP Gateway IP:" with the value "192.168.1.1". At the bottom right, there are two buttons: "Apply" and "Help".

DHCP Server Setup	
DHCP Mode:	DHCP Relay
DHCP server IP:	192.168.168.254
DHCP Gateway IP:	192.168.1.1

Apply 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>

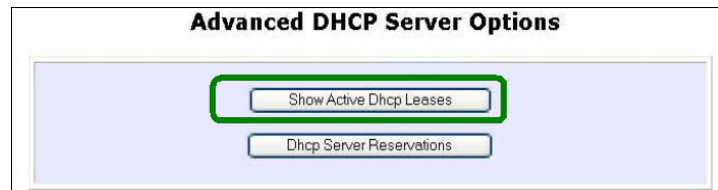
# View Active DHCP Leases

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**.

DHCP Active Leases			
Host Name	IP Address	Hardware Address	Lease Expired Time
sampleHost	192.168.168.22	09-00-7c-01-00-01	11
<div>Refresh Help Back</div>			



## 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.

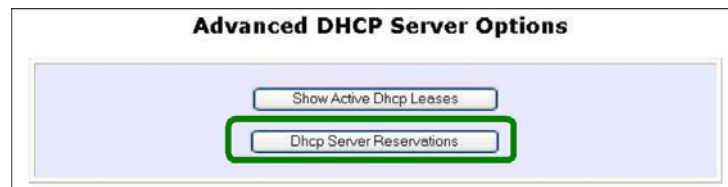
# Reserve IP Addresses for Predetermined DHCP Clients

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.



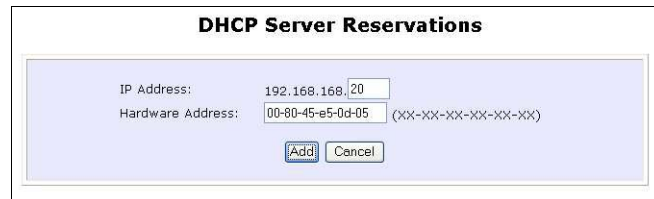
Step 3:

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.



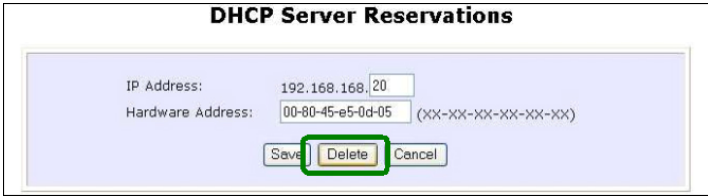
The screenshot shows a window titled "DHCP Server Reservations". Inside, there is a table with two columns: "IP Address" and "Hardware Address". The first row contains the values "192.168.168.20" and "00-80-45-e5-0d-05". The IP address cell is highlighted with a green border. Below the table are two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

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

Add Back

Step 2:

Click on the **Delete** button.



The screenshot shows a form titled "DHCP Server Reservations". 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.

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

Save Delete Cancel

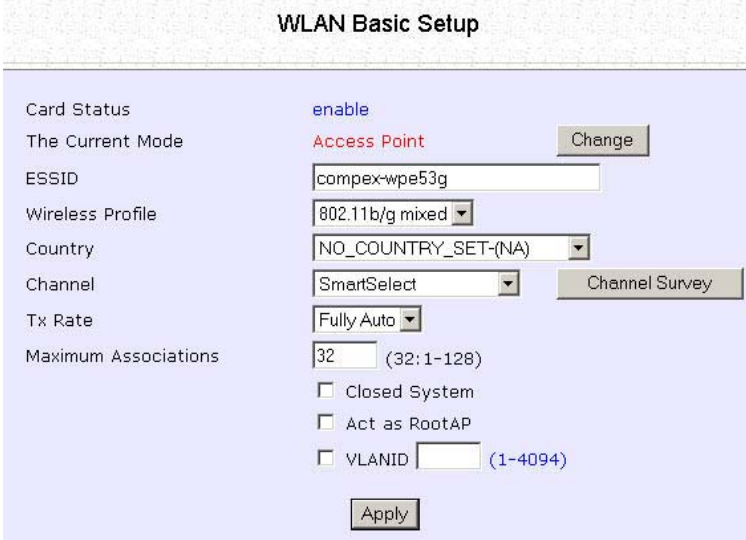
The **DHCP Server Reservations** table refreshes to display your changes.

# Setup WLAN

## Configure the Basic Setup of the Wireless Mode

Step 1:

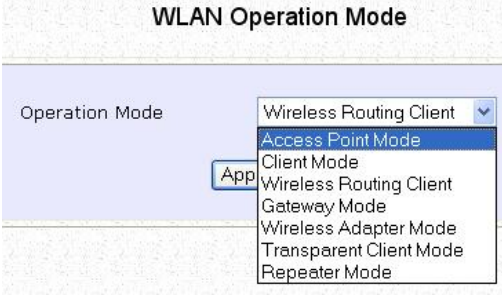
Select **WLAN Setup** from the **CONFIGURATION** menu and you will see the sub menus expanded under **WLAN Setup**, select **Basic**. The default operating mode of the access point is the **Access Point** mode.



The screenshot shows the 'WLAN Basic Setup' page. It contains several configuration fields: 'Card Status' is set to 'enable'; 'The Current Mode' is 'Access Point' with a 'Change' button; 'ESSID' is 'compex-wpe53g'; 'Wireless Profile' is '802.11b/g mixed'; 'Country' is 'NO\_COUNTRY\_SET-(NA)'; 'Channel' is 'SmartSelect' with a 'Channel Survey' button; 'Tx Rate' is 'Fully Auto'; 'Maximum Associations' is '32' (range 1-128). There are also checkboxes for 'Closed System', 'Act as RootAP', and 'VLANID' (range 1-4094). An 'Apply' button is at the bottom.

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' page. The 'Operation Mode' dropdown menu is open, showing options: 'Wireless Routing Client', 'Access Point Mode' (highlighted), 'Client Mode', 'Wireless Routing Client', 'Gateway Mode', 'Wireless Adapter Mode', 'Transparent Client Mode', and 'Repeater Mode'. An 'Apply' button is visible next to the dropdown.

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' page for 'Client Mode'. The page has a light blue background. At the top, the title 'WLAN Basic Setup' is centered. Below the title, there are several configuration fields: 'Card Status' is set to 'enable'; 'The Current Mode' is 'Client' with a 'Change' button next to it; 'ESSID' is 'compex-wpe53g' with a 'Site Survey' button to its right; 'Remote AP MAC' is '00:00:00:00:00:00' with an unchecked checkbox; 'Wireless Profile' is '802.11b/g mixed'; 'Country' is 'NO\_COUNTRY\_SET-(NA)'; and 'Tx Rate' is 'Fully Auto'. An 'Apply' button is at the bottom center.

Card Status	enable
The Current Mode	Client <input type="button" value="Change"/>
ESSID	compex-wpe53g <input type="button" value="Site Survey"/>
Remote AP MAC	00:00:00:00:00:00 <input type="checkbox"/>
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Tx Rate	Fully Auto
<input type="button" value="Apply"/>	

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

The screenshot shows the 'WLAN Basic Setup' page for 'Access Point Mode'. The page has a light blue background. At the top, the title 'WLAN Basic Setup' is centered. Below the title, there are several configuration fields: 'Card Status' is set to 'enable'; 'The Current Mode' is 'Access Point' with a 'Change' button next to it; 'ESSID' is 'compex-wpe53g'; 'Wireless Profile' is '802.11b/g mixed'; 'Country' is 'NO\_COUNTRY\_SET-(NA)'; 'Channel' is 'SmartSelect' with a 'Channel Survey' button to its right; 'Tx Rate' is 'Fully Auto'; 'Maximum Associations' is '32' with '(32: 1-128)' in parentheses; and there are three unchecked checkboxes: 'Closed System', 'Act as RootAP', and 'VLANID' (with '(1-4094)' in parentheses). An 'Apply' button is at the bottom center.

Card Status	enable
The Current Mode	Access Point <input type="button" value="Change"/>
ESSID	compex-wpe53g
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect <input type="button" value="Channel Survey"/>
Tx Rate	Fully Auto
Maximum Associations	32 (32: 1-128)
<input type="checkbox"/> Closed System	
<input type="checkbox"/> Act as RootAP	
<input type="checkbox"/> VLANID (1-4094)	
<input type="button" value="Apply"/>	

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



<b>Wireless Profile</b>	<p>A selection of network environment types in which to operate the access point:</p> <ul style="list-style-type: none"> <li>• <b>802.11b only</b> Supports wireless B clients with data rates of up to 11Mbps in the frequency range of 2.4GHz.</li> <li>• <b>802.11b/g mixed</b> Supports both wireless B and G clients.</li> <li>• <b>802.11g only</b> Supports wireless-G clients that offer transmission rates of up to 54Mbps in the 2.4GHz frequency band.</li> <li>• <b>superG</b> Supports wireless superG clients that offer transmission rates of up to 108Mbps in the 5GHz frequency band.</li> </ul>
<b>Country</b>	Choose the <b>Country</b> where you are located.
<b>Channel</b>	<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.</p> <p>Select SmartSelect to automatically scan and recommend the best channel that the access point can utilize.</p>
<b>Tx Rate</b>	Allows you to choose the rate of data transmission ranging from <b>1Mbps</b> to <b>Fully Auto</b> .
<b>Closed System</b>	The access point will not broadcast its <b>WLAN name (ESSID)</b> when <b>Closed system</b> is enabled. By default <b>Closed system</b> is disabled.


<b>Act as RootAP</b>	<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>
<b>VLAN ID</b>	<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>
<b>Channel Survey</b>	<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 image shows the 'WLAN Basic Setup' configuration page. It includes fields for Card Status (enable), The Current Mode (Client), ESSID (compex-wpe53g), Remote AP MAC (00:00:00:00:00:00), Wireless Profile (802.11b/g mixed), Country (NO\_COUNTRY\_SET-(NA)), and Tx Rate (Fully Auto). A 'Site Survey' button is located on the right side of the form.

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 image shows the 'Site Survey' results page with a table of detected access points. The table has columns for Bssid, SSID, Chan, Auth, Alg, and Signal. There are 8 rows of data, each with a radio button in the first column. An 'Apply' button is at the bottom of the table.

	Bssid	SSID	Chan	Auth	Alg	Signal
<input type="radio"/>	0080482cd08b	Powermatic Hotspot (802.11g)	5	WPA-PSK	AES	8
<input type="radio"/>	008048ff0029	compex-np25g	2	WPA-PSK	AES	7
<input type="radio"/>	0080483bd71b	54g-after-import	3	OPEN	WEP	12
<input type="radio"/>	0080483d83e1	np28g-test-eng	1	OPEN	NONE	36
<input type="radio"/>	068048ff0029	compex-np25g	2	OPEN	NONE	8
<input type="radio"/>	0080483cfbdf	compex-wp18-card1	4	OPEN	NONE	7
<input type="radio"/>	0080483f30b3	zapova_2	5	WPA-PSK	TKIP	34

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
<b>Bssid</b>	Wireless MAC address of the access point in a wireless network infrastructure.
<b>SSID</b>	Network name that uniquely identifies the network to which the access point is connected.
<b>Chan</b>	Channel being used for transmission.
<b>Auth</b>	Types of authentication, such as WPA, WPA-Personal, etc being used by the access point.
<b>Alg</b>	Types of algorithm, such as WEP, TKIP, etc being used by the access point.
<b>Signal</b>	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 **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
<b>State</b>	Displays whether the <b>State</b> is <b>Scanning</b> or <b>Associated</b> , and MAC address of the access point to which the client is connected.
<b>Current Channel</b>	Channel presently being used for transmission.
<b>Tx Rate</b>	Rate of data transmission in Mbps.
<b>Signal Strength</b>	Intensity of the signal received, in percentage.

# 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. It includes fields for Card Status (enable), The Current Mode (Access Point), ESSID (compex-wpe53g), Wireless Profile (802.11b/g mixed), Country (NO\_COUNTRY\_SET-(NA)), Channel (SmartSelect), Tx Rate (Fully Auto), and Maximum Associations (32). A 'Channel Survey' button is located next to the Channel field. Other options like 'Closed System', 'Act as RootAP', and 'VLANID' are also visible at the bottom.

WLAN Basic Setup	
Card Status	enable
The Current Mode	Access Point <span>Change</span>
ESSID	compex-wpe53g
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect <span>Channel Survey</span>
Tx Rate	Fully Auto
Maximum Associations	32 (32:1-128)
<input type="checkbox"/> Closed System	
<input type="checkbox"/> Act as RootAP	
<input type="checkbox"/> VLANID <span>(1-4094)</span>	
<span>Apply</span>	

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

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.



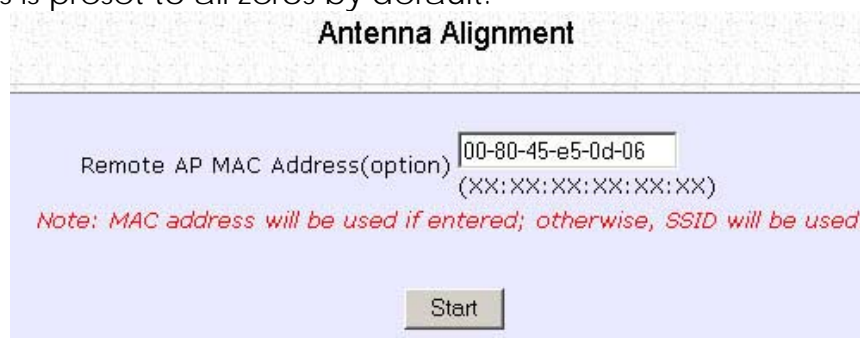
Read-Only Parameters of All Channels Viewable from Channel Survey page	Description
<b>Freq</b>	Frequency of the channel at which your access point is operating.
<b>Channel</b>	Channel of the access point being used for transmission depending on its origin of country.
<b>MyQuality</b>	Interference level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

# 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.

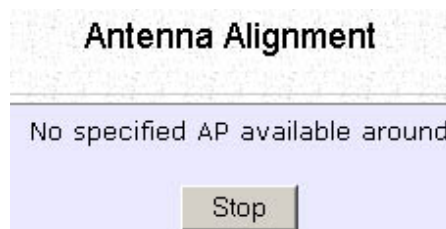


The screenshot shows the 'Antenna Alignment' web interface. It has a title bar 'Antenna Alignment' and a light blue background. A label 'Remote AP MAC Address(option)' is next to a text input field containing '00-80-45-e5-0d-06'. Below the input field is a placeholder '(XX:XX:XX:XX:XX:XX)'. A red note below the input field reads: 'Note: MAC address will be used if entered; otherwise, SSID will be used.' At the bottom center 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' web interface in a status state. It has a title bar 'Antenna Alignment' and a light blue background. The main text in the center reads 'No specified AP available around'. At the bottom center 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 point share the same SSID, the access point with the strongest signal will be shown.

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

**NOTE**

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

**NOTE**

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

# Configure the Advanced Setup of the Wireless Mode

Step 1:

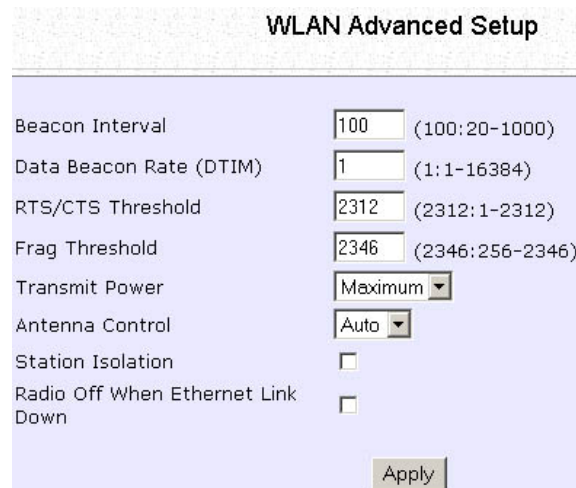
Select **WLAN Setup** from the **CONFIGURATION** menu to expand four sub-menus. From here, select **Advanced**.

Step 2:

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

Step 3:

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



The screenshot shows the 'WLAN Advanced Setup' configuration page. It contains several settings with input fields and checkboxes. The settings are: Beacon Interval (100), Data Beacon Rate (DTIM) (1), RTS/CTS Threshold (2312), Frag Threshold (2346), Transmit Power (Maximum), Antenna Control (Auto), Station Isolation (unchecked), and Radio Off When Ethernet Link Down (unchecked). An 'Apply' button is located at the bottom right of the form.

WLAN Advanced Setup	
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
Antenna Control	Auto
Station Isolation	<input type="checkbox"/>
Radio Off When Ethernet Link Down	<input type="checkbox"/>
<input type="button" value="Apply"/>	

Advanced Setup Parameters	Description
<b>Beacon Interval (Only in Access Point mode)</b>	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.
<b>Data Beacon Rate (DTIM) (Only in Access Point mode)</b>	<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>
<b>RTS/CTS Threshold</b>	<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>
<b>Frag Threshold</b>	<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>
<b>Transmit Power</b>	Drop-down list of a range of transmission power.
<b>Radio Off When Ethernet Link Down</b>	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 Connection List			
ID	MAC Address	RSSI	TxRate
AP	<a href="#">00:80:48:ff:00:2c</a>	0	0Mbps
<div>RefreshBack</div>			

Step 3:

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

The statistics of the selected wireless client displays.

00:80:48:ff:00:2c Statistics						
Authentication Type				Encryption		
Open				No		
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	14794	0	0
Transmit	0	0	0	10998	0	0
<div>Back</div>						

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.

Step 3:

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

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

WAN Setup Parameters Example:

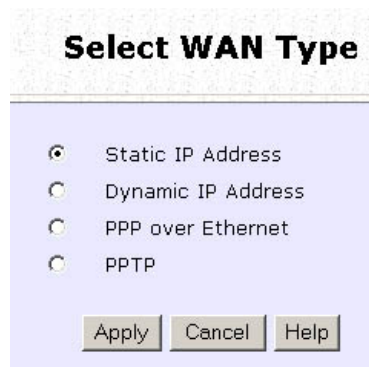
- IP Address: 203.120.12.240
- Network Mask: 255.255.255.0
- Gateway IP Address: 203.120.12.2

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.



**Select WAN Type**

☒ Static IP Address

☐ Dynamic IP Address

☐ PPP over Ethernet

☐ PPTP

Apply Cancel Help

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.



**WAN Static Setup**

WAN Type: Static Change

IP Address: 203.120.12.240

Network Mask: 255.255.255.0

Gateway IP Address: 203.120.12.2

Apply Help



### Setup your WAN for ADSL Internet using PPP over Ethernet

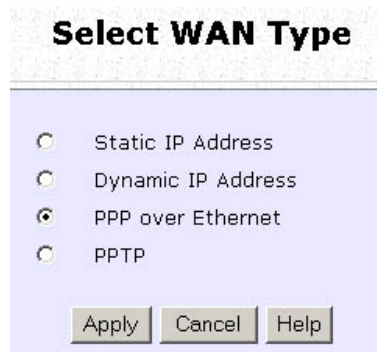
If you subscribe to an ADSL service using PPP over Ethernet (PPPoE) authentication, you can set up your access point's WAN type as follows. For example, you may configure an account whose username is 'guest' as described below:

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.



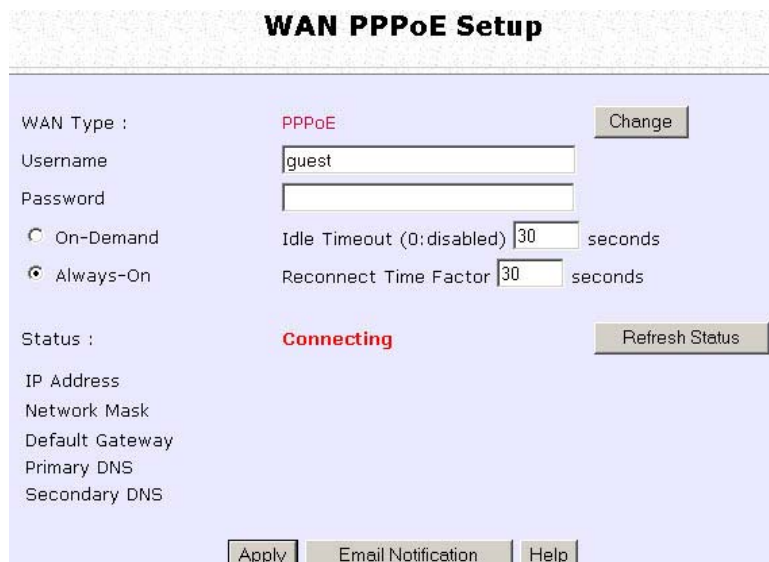
The screenshot shows a window titled "Select WAN Type". It contains four radio button options: "Static IP Address", "Dynamic IP Address", "PPP over Ethernet" (which is selected), and "PPTP". At the bottom of the window are three buttons: "Apply", "Cancel", and "Help".

### 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.



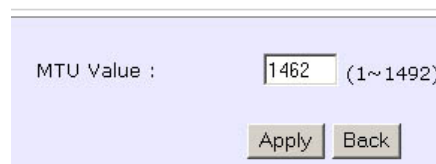
The image shows a web-based configuration page titled "WAN PPPoE Setup". The page has a light blue background. At the top, the title "WAN PPPoE Setup" is centered in bold black text. Below the title, the "WAN Type" is set to "PPPoE" in red text, with a "Change" button to its right. The "Username" field contains the text "guest". The "Password" field is empty. There are two radio buttons for connection mode: "On-Demand" (unselected) and "Always-On" (selected). To the right of the "Always-On" radio button, there are two input fields: "Idle Timeout (0:disabled)" with the value "30" and "seconds", and "Reconnect Time Factor" with the value "30" and "seconds". Below these, the "Status" is "Connecting" in red text, with a "Refresh Status" button to its right. At the bottom, there are several fields for network configuration: "IP Address", "Network Mask", "Default Gateway", "Primary DNS", and "Secondary DNS", all of which are currently empty. At the very bottom, there 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**.

#### **MTU Setup**

A screenshot of a web form titled "MTU Setup". The form has a light blue background. It contains a label "MTU Value :" followed by a text input field containing the number "1462". To the right of the input field is the text "(1~1492)". Below the input field are two buttons: "Apply" and "Back", both in grey boxes.

## Setup your WAN for ADSL Internet using Point-to-Point Tunneling Protocol (PPTP)

WAN Setup Parameters Example:

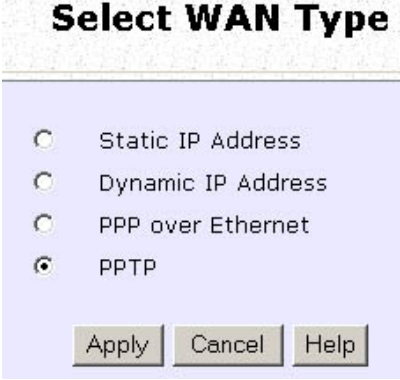
- IP Address: 203.120.12.47
- Network Mask: 255.255.255.0
- VPN Server: 203.120.12.15

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.



**Select WAN Type**

☐ Static IP Address

☐ Dynamic IP Address

☐ PPP over Ethernet

☒ PPTP

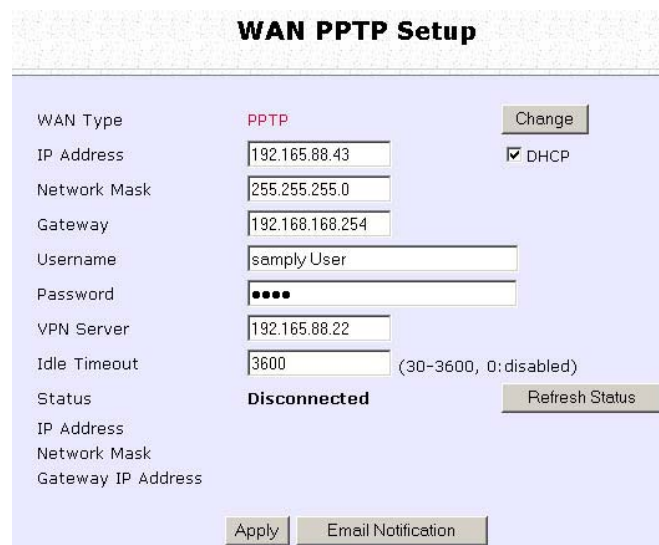
Apply Cancel Help

Step 3:

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

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

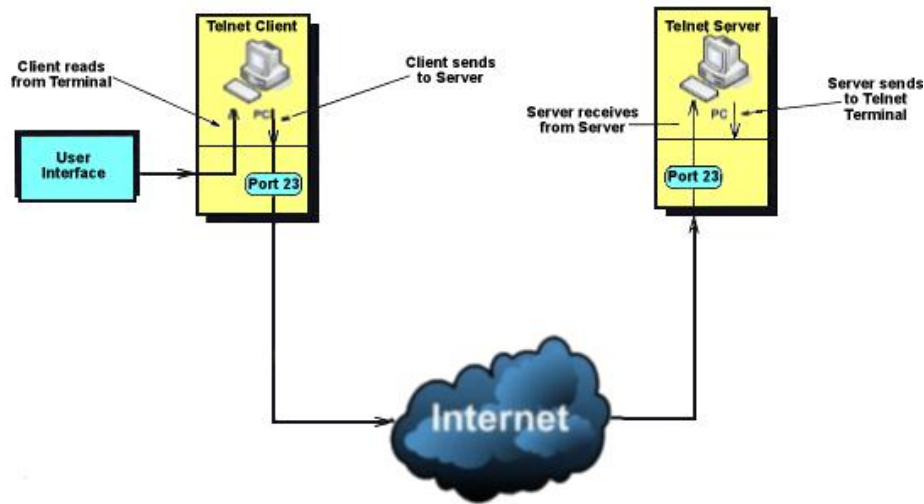
The **Idle Timeout** setting allows you to specify the value in seconds after the last Internet activity by which the access point will disconnect from the ISP. A value of "0" will disable idle timeout.



The image shows a web-based configuration page titled "WAN PPTP Setup". The page has a light blue background and contains several input fields and buttons. The "WAN Type" is set to "PPTP" with a "Change" button next to it. The "IP Address" field contains "192.165.88.43" and the "DHCP" checkbox is checked. The "Network Mask" field contains "255.255.255.0". The "Gateway" field contains "192.168.168.254". The "Username" field contains "sample User". The "Password" field is masked with four dots. The "VPN Server" field contains "192.165.88.22". The "Idle Timeout" field contains "3600" with a note "(30-3600, 0: disabled)". The "Status" is "Disconnected" with a "Refresh Status" button. At the bottom, there are "Apply" and "Email Notification" buttons.

WAN PPTP Setup	
WAN Type	PPTP <span>Change</span>
IP Address	192.165.88.43 <span><input checked="" type="checkbox"/> DHCP</span>
Network Mask	255.255.255.0
Gateway	192.168.168.254
Username	sample User
Password	••••
VPN Server	192.165.88.22
Idle Timeout	3600 (30-3600, 0: disabled)
Status	Disconnected <span>Refresh Status</span>
IP Address	
Network Mask	
Gateway IP Address	
<span>Apply</span> <span>Email Notification</span>	

# Setup Telnet / SSH



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

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

Step 1:

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

Step 2:

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

Click the **Apply** button.

Telnet/SSH Setup	
<input type="checkbox"/> Telnet Server Enable	Port Number <input type="text" value="23"/>
<input type="checkbox"/> SSH Server Enable	Port Number <input type="text" value="22"/>
<input type="button" value="Apply"/>	

Step 3:

To add user:

1. Click the **Add** button.



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

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



User Name:   
Password:   
Permission:


To Delete User:

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



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

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

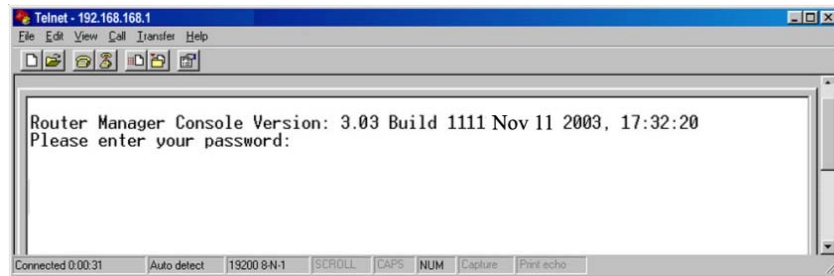


Select	User Name	Permission
<input type="checkbox"/>	username2	RW

# Access the TELNET Command Line Interface

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

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

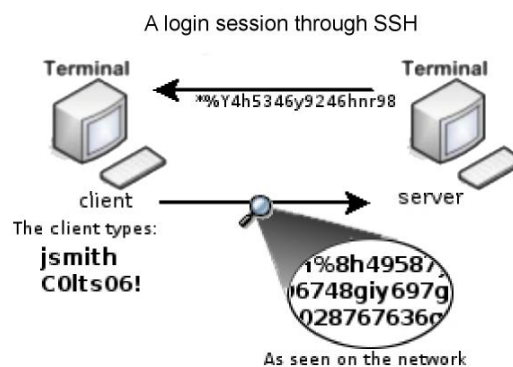
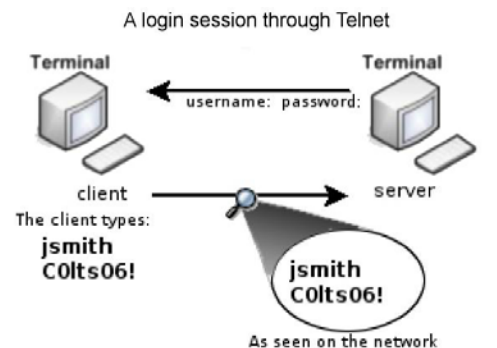




# Access the Secure Shell Host Command Line Interface

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

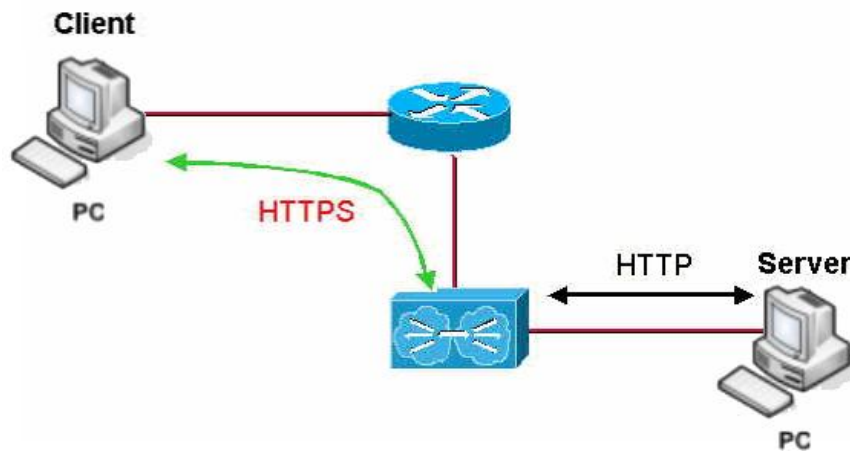
An encrypted connection like SSH is not viewable on the network. The server can still read the information, but only after negotiating the encrypted session with the client.



SSH CLI has a command line interface.

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

# Set the WEB Mode



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

Step 1:

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

Step 2:

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

Changes will be effected after reboot.

**Web Server Setup**

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

# 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.

<table><tr><td>Status</td><td>Policy</td></tr><tr><td>Enable</td><td>Accept</td></tr></table>	Status	Policy	Enable	Accept	MAC Filtering set to <b>Enable</b> with Policy to <b>Accept</b> only the MAC addresses in the MAC Filter Address List and deny all other MAC addresses.
Status	Policy				
Enable	Accept				
<table><tr><td>Status</td><td>Policy</td></tr><tr><td>Enable</td><td>Deny</td></tr></table>	Status	Policy	Enable	Deny	MAC Filtering set to <b>Enable</b> with Policy to <b>Deny</b> all the MAC addresses in the MAC Filter Address List and accept all other MAC addresses.
Status	Policy				
Enable	Deny				
<table><tr><td>Status</td><td>Policy</td></tr><tr><td>Disable</td><td>Accept</td></tr></table>	Status	Policy	Disable	Accept	MAC Filtering set to <b>Disable</b> . Whether Policy is set to <b>Enable</b> or <b>Deny</b> does not matter.
Status	Policy				
Disable	Accept				
<table><tr><td>Status</td><td>Policy</td></tr><tr><td>Disable</td><td>Deny</td></tr></table>	Status	Policy	Disable	Deny	MAC Filtering set to <b>Disable</b> . Whether Policy is set to <b>Enable</b> or <b>Deny</b> does not matter.
Status	Policy				
Disable	Deny				

Click the **Edit** button.

**MAC Address Filtering**

Radio 1 MAC Filtering Options :

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

[View Complete MAC List](#)

( All changes will take effect after reboot )

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
------	-------------	----------

( 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 for 'Radio 1 MAC Filtering Options' with columns for AP Type, ESSID, Security, MACs, Status, and Policy. The table lists three entries: 'Main AP' (sampleRouter, NONE, Edit, Enable, Accept), 'Virtual AP' (VAP1, NONE, Edit, Disable, Deny), and 'Virtual AP' (VAP2, NONE, Edit, Enable, Deny). Below the table is a link for '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	<a href="#">Edit</a>	Enable	Accept
Virtual AP	VAP1	NONE	<a href="#">Edit</a>	Disable	Deny
Virtual AP	VAP2	NONE	<a href="#">Edit</a>	Enable	Deny

[View Complete MAC List](#)

[Apply](#) [Back](#)

( 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 for 'Radio 1' with columns for Del., MAC Address, Comments, and Apply to. The table lists two entries: '08-70-f8-70-80-70' (mac1, all) and '00-b0-d0-86-bb-f7' (mac3, 1 AP(s)). The checkbox for the second entry is checked. 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	mac1	all
<input checked="" type="checkbox"/>	00-b0-d0-86-bb-f7	mac3	1 AP(s)

[Add](#) [Delete](#) [Back](#)

( 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 four columns: "Del.", "MAC Address", "Comments", and "Apply to". The table contains one row with a checkbox in the "Del." column, the MAC address "08-70-f8-70-80-70" in the "MAC Address" column, the comment "mac1" in the "Comments" column, and the value "all" in the "Apply to" column. Below the table are three buttons: "Add", "Delete", and "Back". At the bottom, there is a note: "( All changes will take effect after reboot )".

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

Add Delete Back

( 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.

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. There are three rows: 'Main AP' (sampleRouter, NONE, Edit, Enable, Accept), 'Virtual AP' (VAP1, NONE, Edit, Disable, Deny), and 'Virtual AP' (VAP2, NONE, Edit, Enable, Deny). Below the table is a link 'View Complete MAC List' and buttons 'Apply' and 'Back'. A note at the bottom states '( All changes will take effect after reboot )'.

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

[View Complete MAC List](#)

[Apply](#) [Back](#)

( 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: Del., MAC Address, Comments, and Apply to. There are three rows: '08-70-f8-70-80-70' (checkbox unchecked, comment 'mac1', apply to 'all'), '09-70-f8-70-80-70' (checkbox checked, comment 'mac2', apply to 'all'), and '00-b0-d0-86-bb-f7' (checkbox unchecked, comment 'mac3', apply to '1 AP(s)'). Below the table are buttons 'Add', 'Delete', and 'Back'. A note at the bottom states '( All changes will take effect after reboot )'.

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

[Add](#) [Delete](#) [Back](#)

( 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 "ESSID: \*sampleRouter\*". There is a table with four columns: "Del.", "MAC Address", "Comments", and "Apply to". The table contains two rows of data. Below the table are three buttons: "Add", "Delete", and "Back". At the bottom, a note states "( All changes will take effect after reboot )".

Del.	MAC Address	Comments	Apply to
<input type="checkbox"/>	08-70-f9-70-60-70	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 lists three entries: Main AP (sampleRouter, NONE, Edit, Enable, Accept), Virtual AP (VAP1, NONE, Edit, Disable, Deny), and Virtual AP (VAP2, NONE, Edit, Enable, Deny). Below the table is a link to 'View Complete MAC List' and 'Apply' and 'Back' buttons. A note at the bottom states '( All changes will take effect after reboot )'.

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

[View Complete MAC List](#)

( All changes will take effect after reboot )

Step 2:

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'. A table lists the MAC address '08-70-f8-70-80-70' with a checkbox in the 'Del.' column, comments 'mac4', and 'Apply to' '1 AP(s)'. Below the table are 'Add', 'Delete', and 'Back' buttons. A note at the bottom states '( All changes will take effect after reboot )'.

Del.	MAC Address	Comments	Apply to
<input type="checkbox"/>	<a href="#">08-70-f8-70-80-70</a>	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: 08-70-f8-70-80-70 (XX-XX-XX-XX-XX-XX)

Comment: mac4

Apply to All: ☐

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

Save Cancel

### 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

Add Delete Back

( 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.

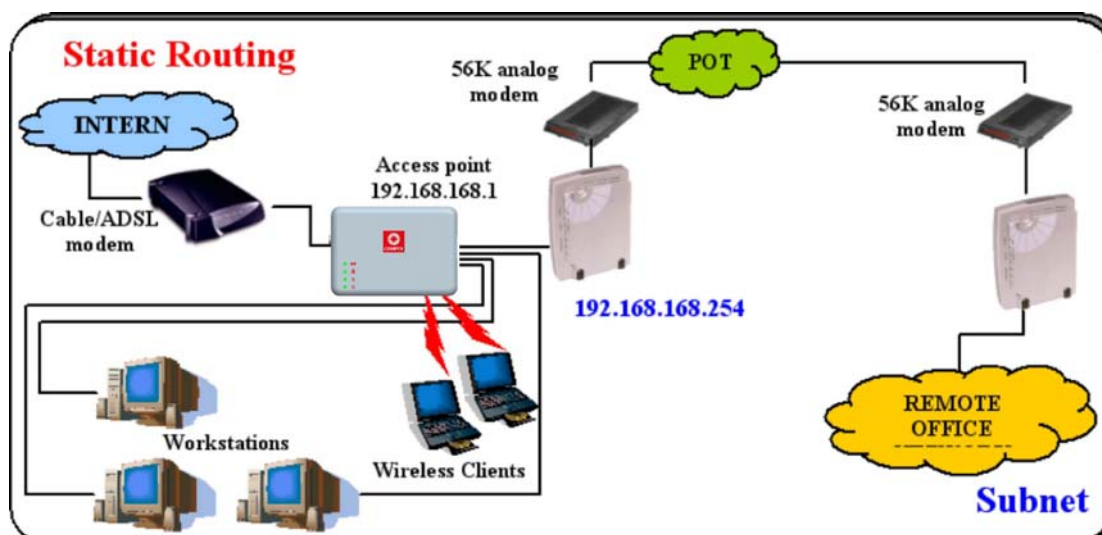


### Important:

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	*
192.168.168.0	255.255.255.0	*

Static Routing Table

Step 2:

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

Destination	Network Mask	Gateway

Add Back

Step 3:

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

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

Destination IP Address :	<input type="text" value="192.168.100.0"/>
Destination Net Mask :	<input type="text" value="255.255.255.0"/>
Gateway IP Address :	<input type="text" value="192.168.168.254"/>
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	

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 : HTTP

Private IP Address :

Public IP : All

From :

To :

Add Help Cancel

**Custom Server**

Server Type : LAN Game

Protocol : UDP

Public Port : Range

From : 15

To : 89

Private IP Address : 192.168.168.55

Private Port From : 30

Public IP : All

From :

To :

Add Cancel

## 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.

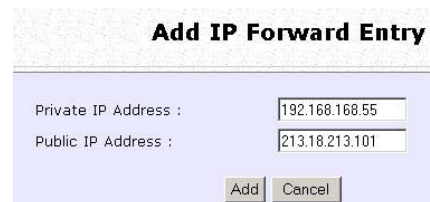


Step 1:  
Select **NAT** from the **CONFIGURATION** command menu.

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

Step 3:  
In the **Add IP Forward Entry** page, enter the **Private IP Address** and **Public IP Address**.

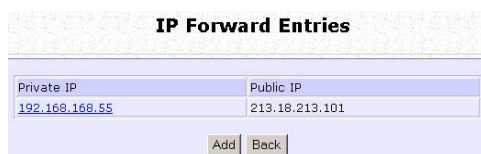
In this example, we would like all requests for 213.18.213.101 to be forwarded to a PC with **Private IP Address** 192.168.168.55.

A screenshot of the 'Add IP Forward Entry' form. It has a title bar 'Add IP Forward Entry'. Below the title bar, there are two input fields: 'Private IP Address : 192.168.168.55' and 'Public IP Address : 213.18.213.101'. At the bottom, there are two buttons: 'Add' and 'Cancel'.

## NOTE

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

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

A screenshot of the 'IP Forward Entries' window. It has a title bar 'IP Forward Entries'. Below the title bar, there is a table with two columns: 'Private IP' and 'Public IP'. The 'Private IP' column contains the value '192.168.168.55' and the 'Public IP' column contains the value '213.18.213.101'. At the bottom, there are two buttons: 'Add' and 'Back'.

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

# Control the Bandwidth Available

(Available in Wireless Routing Client and Gateway modes)

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

## Enable Bandwidth Control

Step 1:

Select **Bandwidth Control** from the **CONFIGURATION** command menu.

**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)	Ceil Rate(kbit)	IP/MAC Address	Rule type
------	----------------------	-----------------	----------------	-----------

Add

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:

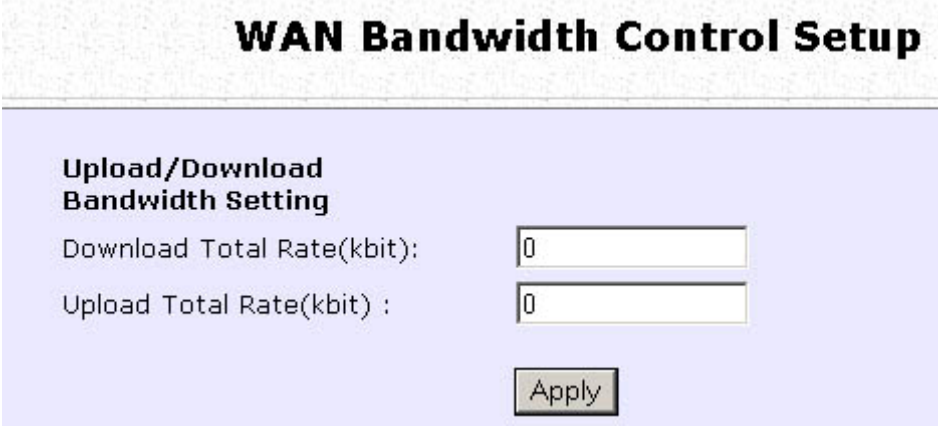
Select **WAN Bandwidth Control Setup** from the **Bandwidth Control** sub-menu from the **CONFIGURATION** command menu.

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 web interface titled "WAN Bandwidth Control Setup". Below the title is a section labeled "Upload/Download Bandwidth Setting". This section contains two input fields: "Download Total Rate(kbit):" and "Upload Total Rate(kbit) :". Both fields have a value of "0" entered. Below these fields is an "Apply" button.

WAN Bandwidth Control Setup	
<b>Upload/Download Bandwidth Setting</b>	
Download Total Rate(kbit):	<input type="text" value="0"/>
Upload Total Rate(kbit) :	<input type="text" value="0"/>
<input type="button" value="Apply"/>	



# 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:

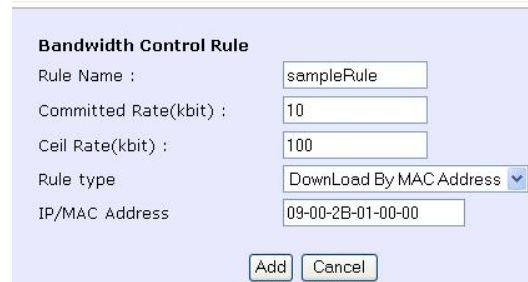
Click the **Add** button to create the bandwidth rule for LAN user.

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
<input type="button" value="Add"/>				

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

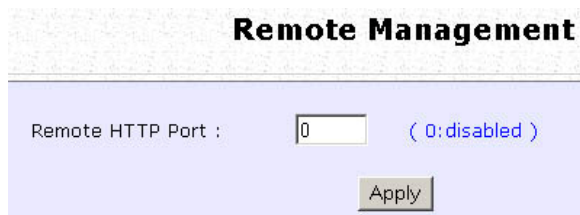
Repeat Steps 1 to Step 3 to add new bandwidth rule.

# 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.

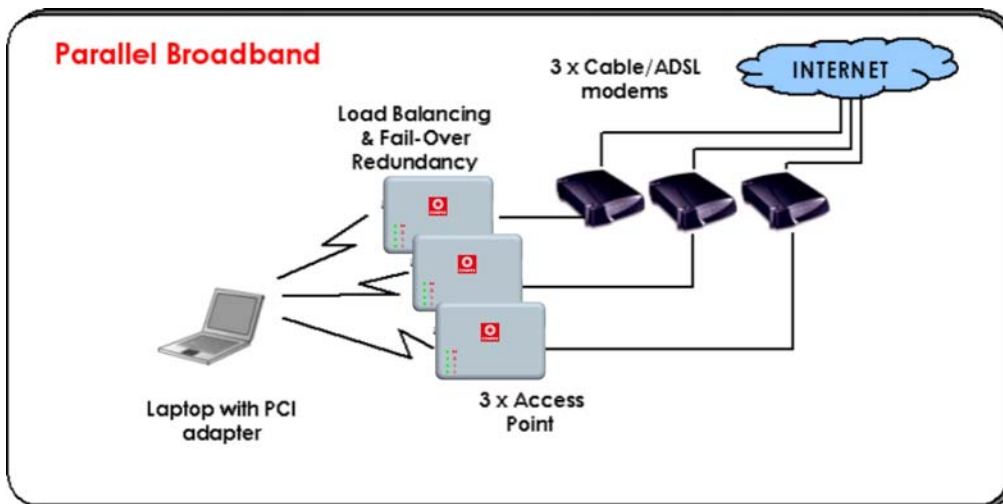
# Use Parallel Broadband

(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.

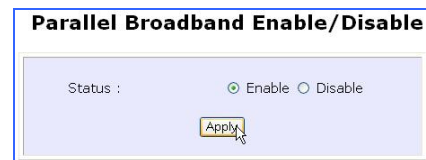
Then all the access points has to have the DHCP server, followed by the Parallel Broadband feature, enabled through the web-based configuration. Please note that all the access points need to be interconnected.

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

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

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

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

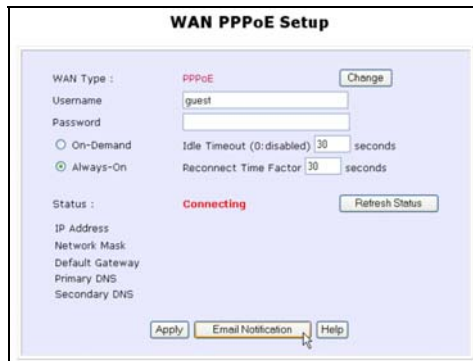


## Important:

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.

A screenshot of the 'WAN PPPoE Setup' window. It shows fields for WAN Type (set to PPPoE), Username (guest), Password, and radio buttons for On-Demand and Always-On (selected). There are also fields for Idle Timeout and Reconnect Time Factor, both set to 30 seconds. The Status is 'Connecting'. At the bottom, there are buttons for Apply, Email Notification (highlighted with a mouse cursor), and Help.

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

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

A screenshot of the 'Email Notification' window. It has a title bar 'Email Notification'. Inside, there's a section 'Email Notification:' with 'Enable' selected and 'Disable' unselected. Below are fields for 'Email address of Receiver:' (mail@yahoo.com), 'IP address of Mail Server:' (192.168.88.43) with a checked 'Needs Authentication' checkbox, 'User Name:' (sampleUser), 'Password:' (masked with dots), and 'Email address of Sender:' (send@yahoo.com). There's a 'Status:' label. At the bottom are 'Apply', 'Back', and 'Refresh' buttons.

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.

**Enable/Disable Static Address Translation**

Status : ☒ Enable ☐ Disable

Apply

# Use DNS Redirection

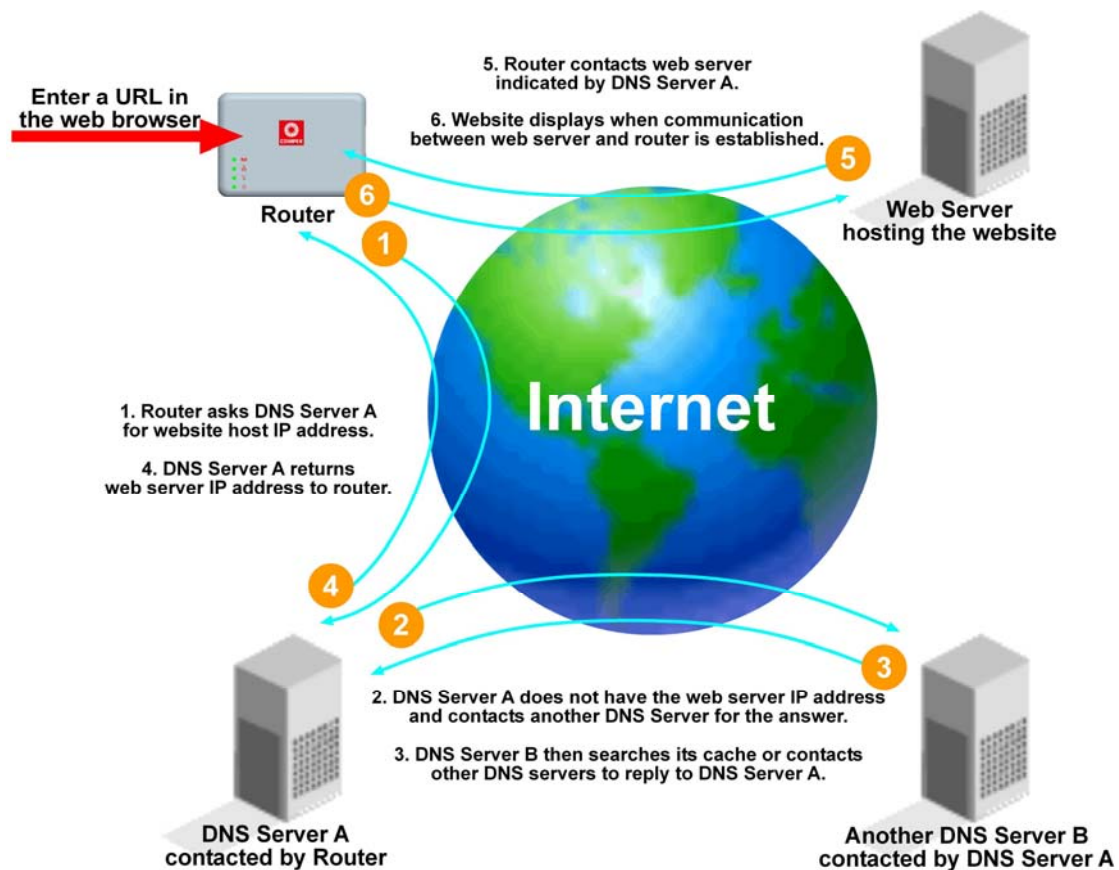
(Available in Wireless Routing Client and Gateway modes)

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.



The screenshot shows a configuration window titled "Enable/Disable DNS Redirection". Below the title bar, there is a section labeled "Status :". To the right of this label are two radio buttons: "Enable" (which is selected) and "Disable". Below these options is an "Apply" button.

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.



The screenshot shows a configuration window titled "Enable/Disable Dynamic DNS". Inside the window, there is a section labeled "Dynamic DNS Status :". To the right of this label are two radio buttons: "Enable" (which is selected) and "Disable". Below these options is an "Apply" button.

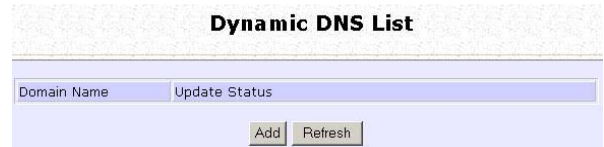
# To manage Dynamic DNS List

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.



The screenshot shows a web interface titled "Dynamic DNS List". It features a table with two columns: "Domain Name" and "Update Status". Below the table, there are two buttons: "Add" and "Refresh".

Step 3:

To add a new Dynamic DNS, click on the Add button.

The **Choice DDNS Provider** page appears.

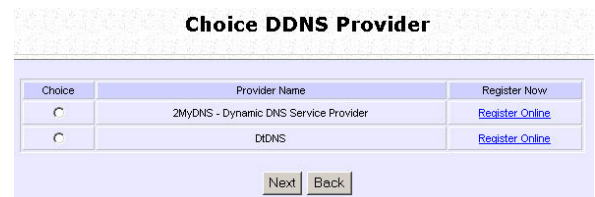
There are two default providers that you can use.

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.



The screenshot shows a web interface titled "Choice DDNS Provider". It contains a table with three columns: "Choice", "Provider Name", and "Register Now". There are two rows of providers listed. Below the table, there are "Next" and "Back" buttons.

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

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

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](http://www.mydomain.2mydns.net) or [ftp.mydomain.2mydns.net](http://ftp.mydomain.2mydns.net) can still reach your hostname.

**Dynamic DNS Add**

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

Domain Name :

WAN IP :

Username :

Password :

Wildcard : ☒ YES ☐ NO

Mail Exchanger : ☒ YES ☐ NO

Backup Mail Exchanger : ☒ YES ☐ NO

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.

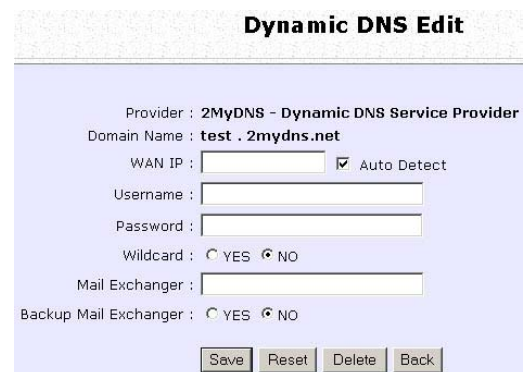
Step 6:  
Click on the Add button.

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 List' interface. It features a table with two columns: 'Domain Name' and 'Update Status'. The 'Domain Name' column contains a single entry, 'test.2mydns.net', which is a hyperlink. Below the table, there are two buttons: 'Add' and 'Refresh'.



The screenshot shows the 'Dynamic DNS Edit' interface. It contains the following fields and options:

- Provider : 2MyDNS - Dynamic DNS Service Provider
- Domain Name : test . 2mydns.net
- WAN IP : [text input] ☒ Auto Detect
- Username : [text input]
- Password : [text input]
- Wildcard : ☐ YES ☒ NO
- Mail Exchanger : [text input]
- Backup Mail Exchanger : ☐ YES ☒ NO

At the bottom, there are four buttons: 'Save', 'Reset', 'Delete', and 'Back'.

Select **DtDNS** as DDNS Service Provider:

Step 1:

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

Click on the **Next** button.

Step 2:

Enter your **Domain Name**.

Step 3:

The **Auto Detect** checkbox is selected by default.

The **WAN IP** field is empty by default.

These default settings should be used if dynamic WAN IP connection is used.

If your ISP connection uses dynamic WAN IP:

Select the **Auto Detect** checkbox to let the DtDNS server learn your current WAN IP address.

Enter your DtDNS account **Username** and **Password**.

If your ISP connection uses a fixed WAN IP:

Enter the IP address in the **WAN IP** field.

Deselect the **Auto Detect** checkbox.

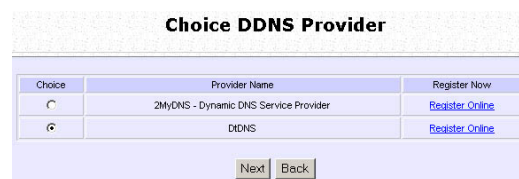
The access point will update the DtDNS server with the specified WAN IP.

Step 4:

Then click on the **Add** button.

Step 5:

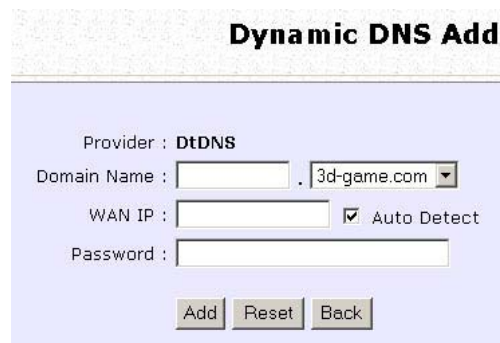
While the new domain name is being added to the list, the message 'Waiting in queue...' will be displayed under the **Update Status** column of the **Dynamic DNS List** table.



The screenshot shows the 'Choice DDNS Provider' interface. It features a table with three columns: 'Choice', 'Provider Name', and 'Register Now'. The first row shows a radio button, '2MyDNS - Dynamic DNS Service Provider', and a 'Register Online' link. The second row shows a selected radio button, 'DtDNS', and another 'Register Online' link. Below the table are 'Next' and 'Back' buttons.

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

Next Back



The screenshot shows the 'Dynamic DNS Add' form. It includes fields for 'Provider' (set to DtDNS), 'Domain Name' (with a dropdown showing '3d-game.com'), 'WAN IP' (empty), and 'Password' (empty). The 'Auto Detect' checkbox is checked. At the bottom are 'Add', 'Reset', and 'Back' buttons.

Provider : DtDNS

Domain Name :  . 3d-game.com

WAN IP :  ☒ Auto Detect

Password :

Add Reset Back



The screenshot shows the 'Dynamic DNS List' table. It has two columns: 'Domain Name' and 'Update Status'. The first row shows 'people.onlinepeople.net'. The second row shows 'cool-3d-game.com' and 'Waiting in queue...'. At the bottom are 'Add' and 'Refresh' buttons.

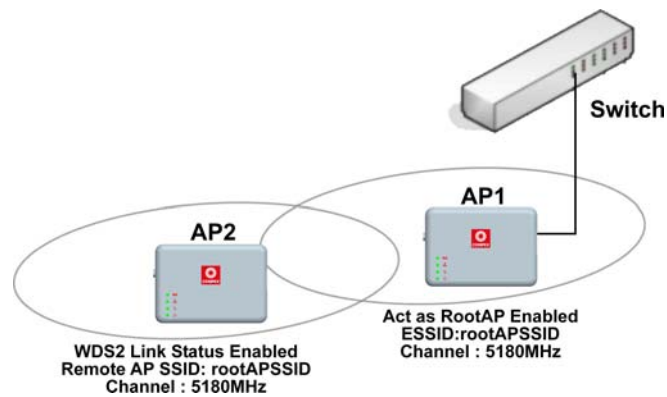
Domain Name	Update Status
<a href="#">people.onlinepeople.net</a>	
<a href="#">cool-3d-game.com</a>	Waiting in queue...

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**

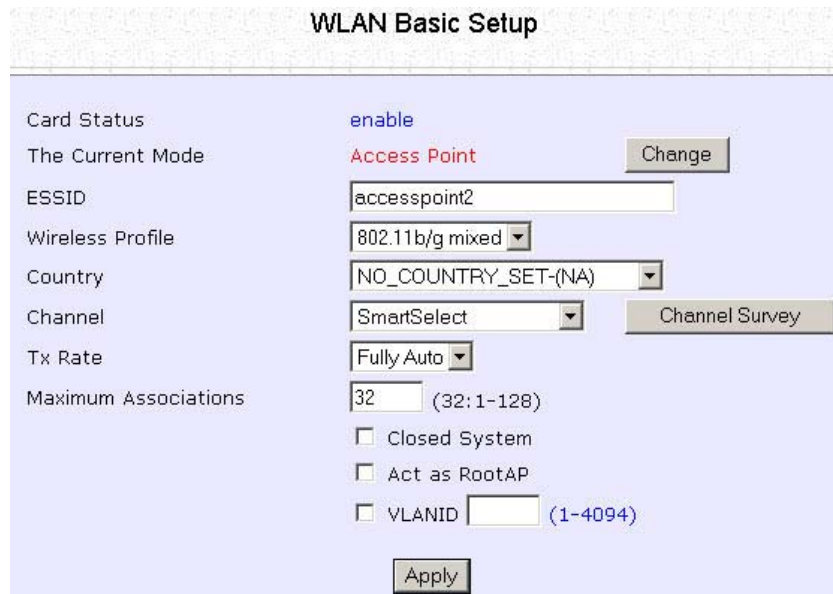
Card Status	enable
The Current Mode	Access Point <span>Change</span>
ESSID	rootAP
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect <span>Channel Survey</span>
Tx Rate	Fully Auto
Maximum Associations	32 (32: 1-128)
	<input type="checkbox"/> Closed System
	<input checked="" type="checkbox"/> Act as RootAP
	<input type="checkbox"/> VLANID (1-4094)
	<span>Apply</span>

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:

Setting	Value
Card Status	enable
The Current Mode	Access Point
ESSID	accesspoint2
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect
Tx Rate	Fully Auto
Maximum Associations	32 (32: 1-128)
Closed System	<input type="checkbox"/>
Act as RootAP	<input type="checkbox"/>
VLANID	<input type="text"/> (1-4094)

Buttons: Change, Channel Survey, Apply

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' with a checked checkbox. The 'Cur. Security Mode' is 'NONE'. There is an 'Apply' button at the bottom.

OR

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

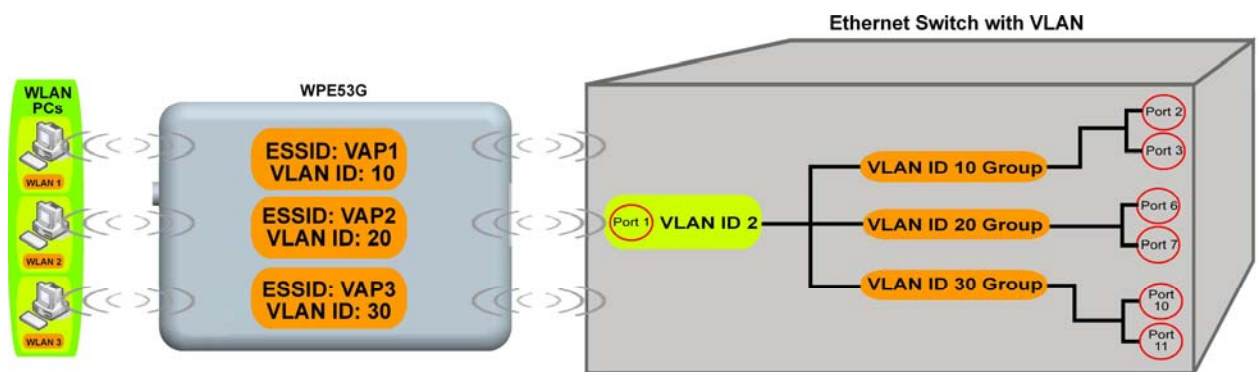
A screenshot of the 'WDS2 Link Configuration' form. The 'WDS2 Link Status' is set to 'Enable'. The 'Remote AP SSID' is 'default'. The 'Remote AP MAC' is '08:00:69:02:01:FC' with a checked checkbox. The 'Cur. Security Mode' is 'NONE'. There is an 'Apply' button at the bottom.

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**.

2

Virtual AP List

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

[Apply](#) [Add](#) [Clear](#) [Back](#)

( All changes will take effect after reboot )

Virtual AP List page displays.

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

Click Add to goto add Virtual AP page.

3

Virtual AP

ESSID:

☒ VLAN ID:

☒ Closed System

☒ RootAP

Security Mode:

[Apply](#) [Back](#)

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.

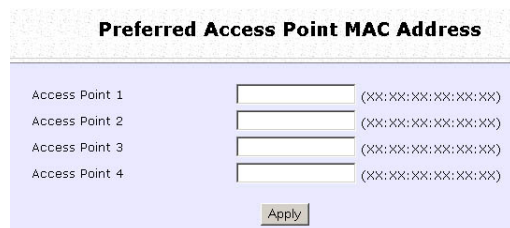
Follow these steps to specify your preferred APs.

## Preferred APs

1

1. Click on **WLAN Setup** from the **CONFIGURATION** menu.

2. Select Preferred APs.



The screenshot shows a configuration page titled "Preferred Access Point MAC Address". It contains four rows, each labeled "Access Point 1" through "Access Point 4". Each row has a text input field followed by a placeholder MAC address in the format (XX:XX:XX:XX:XX:XX). Below the input fields is an "Apply" button.

2

1. Enter the MAC addresses of the preferred APs.

2. Click **Apply** to effect the settings.

# Get Long Distance Parameters

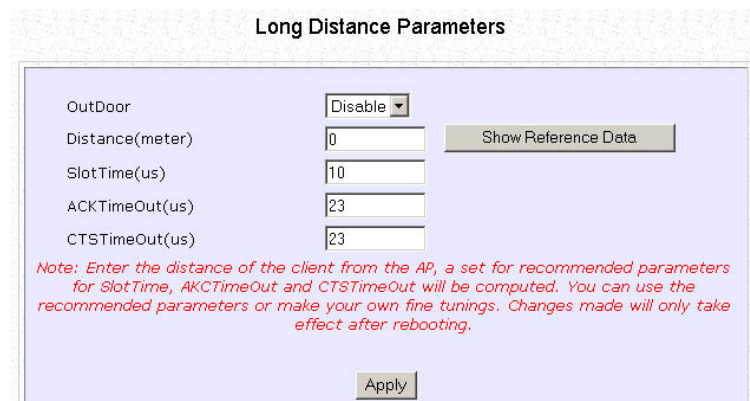
The access point can calculate and display suggested values for certain parameters to use to ensure that efficient wireless communication between physically distant access points.

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

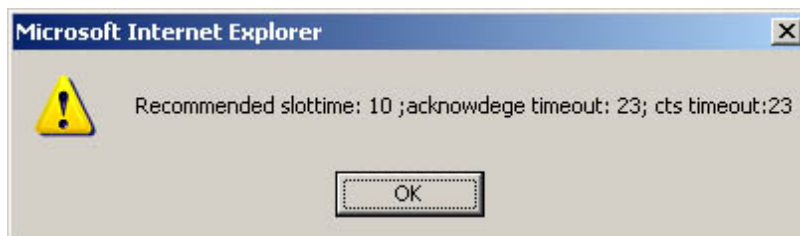
Click on the **Long Distance Parameters** button under the **Extended Features** section.



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

A screenshot of the "Long Distance Parameters" configuration page. It features a form with the following fields: "OutDoor" (a dropdown menu set to "Disable"), "Distance(meter)" (a text input field with "0"), "SlotTime(us)" (a text input field with "10"), "ACKTimeOut(us)" (a text input field with "23"), and "CTSTimeOut(us)" (a text input field with "23"). To the right of the "Distance(meter)" field is a button labeled "Show Reference Data". Below the input fields is a red note: "Note: Enter the distance of the client from the AP, a set for recommended parameters for SlotTime, ACKTimeOut and CTSTimeOut will be computed. You can use the recommended parameters or make your own fine tunings. Changes made will only take effect after rebooting." At the bottom center is an "Apply" button.

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



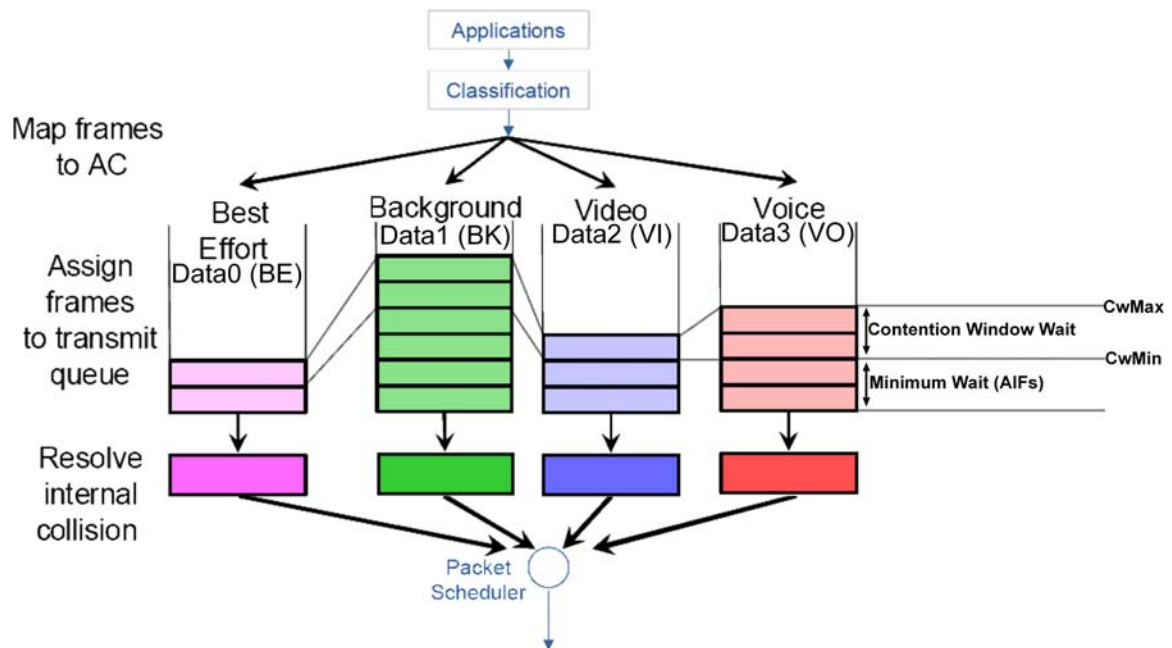
You can enter the parameters based on the recommended values in the pop-up window, click on the **Apply** button to update the changes.

Long Distance Parameters	Description
<b>Outdoor</b>	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.
<b>Distance</b>	Determines the distance between your access point and the remote access point in meters.
<b>Slot Time</b>	The amount of time is divided and each unit of time is called one slot time.
<b>ACK Timeout</b>	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.
<b>CTS Timeout</b>	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.

The image shows the "WMM Setup" page. At the top, there's a title "WMM Setup". Below it, there's a section "Wireless Multimedia (WMM)" with two radio buttons: "Enable" (selected) and "Disable". Below this, there's a section "AP WMM Parameters:" with a table. The table has columns: "Data", "AIFs", "cwMin", "cwMax", "TxOp limit", and "NoAck". The rows are "Data0 (BE)", "Data1 (BK)", "Data2 (VI)", and "Data3 (VO)". Below this, there's a section "Station WMM Parameters:" with a similar table. The columns are "Data", "AIFs", "cwMin", "cwMax", "TxOp limit", and "ACM". The rows are "Data0 (BE)", "Data1 (BK)", "Data2 (VI)", and "Data3 (VO)". At the bottom, there are three buttons: "Apply", "Default", and "Back". Below the buttons, there's a note: "( All changes will take effect after reboot )".

Data	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"/>

Data	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"/>

Apply Default Back

( 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**.

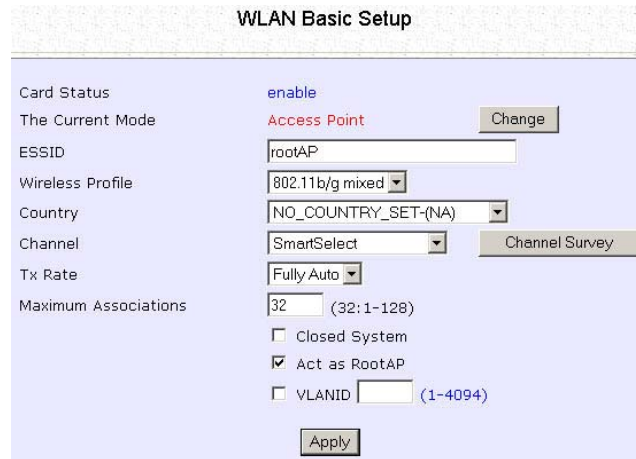
Ensure that **The Current Mode** is set to **Access Point**.

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 <span>Change</span>
ESSID	rootAP
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect <span>Channel Survey</span>
Tx Rate	Fully Auto
Maximum Associations	32 (32;1-128)
<input type="checkbox"/> Closed System	
<input type="checkbox"/> Act as RootAP	
<input type="checkbox"/> VLANID (1-4094)	
<span>Apply</span>	

## RootAP Step 2:

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



The image shows a web-based configuration page titled "WLAN Basic Setup". It contains several settings for a wireless network. The "Card Status" is set to "enable". The "The Current Mode" is set to "Access Point" with a "Change" button next to it. The "ESSID" is set to "rootAP". The "Wireless Profile" is set to "802.11b/g mixed". The "Country" is set to "NO\_COUNTRY\_SET-(NA)". The "Channel" is set to "SmartSelect" with a "Channel Survey" button next to it. The "Tx Rate" is set to "Fully Auto". The "Maximum Associations" is set to "32" with a range of "(32: 1-128)". There are three checkboxes: "Closed System" (unchecked), "Act as RootAP" (checked), and "VLANID" (unchecked) with a range of "(1-4094)". An "Apply" button is at the bottom.

WLAN Basic Setup	
Card Status	enable
The Current Mode	Access Point <span>Change</span>
ESSID	rootAP
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect <span>Channel Survey</span>
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 (1-4094)	
<span>Apply</span>	

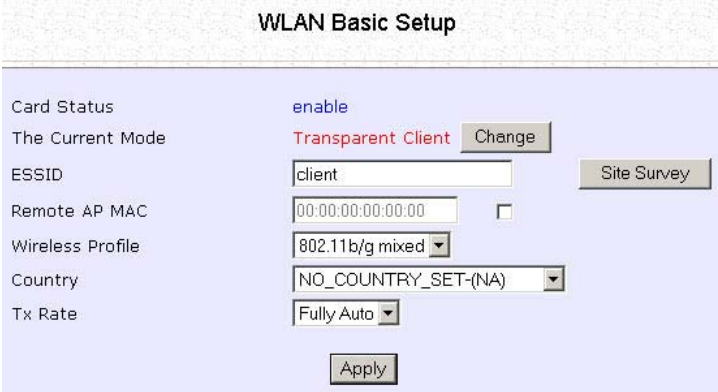
Follow these steps to setup Transparent Client/s.

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.



The screenshot shows the 'WLAN Basic Setup' configuration page. It features a table-like layout with configuration parameters on the left and their values on the right. The parameters include Card Status, The Current Mode, ESSID, Remote AP MAC, Wireless Profile, Country, and Tx Rate. The 'The Current Mode' is set to 'Transparent Client' with a 'Change' button next to it. The 'ESSID' is set to 'client' with a 'Site Survey' button. The 'Remote AP MAC' is set to '00:00:00:00:00:00' with a checkbox. The 'Wireless Profile' is set to '802.11b/g mixed' and the 'Country' is set to 'NO\_COUNTRY\_SET-(NA)'. The 'Tx Rate' is set to 'Fully Auto'. An 'Apply' button is at the bottom.

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

Transparent Client Step 2:

Select the **Remote AP MAC** checkbox.

Enter the **Remote AP MAC**.



The image shows a screenshot of a web-based configuration page titled "WLAN Basic Setup". The page has a light blue background. On the left side, there is a list of configuration items: "Card Status", "The Current Mode", "ESSID", "Remote AP MAC", "Wireless Profile", "Country", and "Tx Rate". To the right of these labels are the corresponding configuration fields. "Card Status" is set to "enable". "The Current Mode" is set to "Transparent Client" with a "Change" button next to it. "ESSID" is set to "client" with a "Site Survey" button to its right. "Remote AP MAC" is set to "09:00:2B:23:00:00" with a checked checkbox to its right. "Wireless Profile" is set to "802.11b/g mixed" with a dropdown arrow. "Country" is set to "NO\_COUNTRY\_SET-(NA)" with a dropdown arrow. "Tx Rate" is set to "Fully Auto" with a dropdown arrow. At the bottom center of the form is an "Apply" button.

Configuration Item	Value
Card Status	enable
The Current Mode	Transparent Client
ESSID	client
Remote AP MAC	09:00:2B:23:00:00
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Tx Rate	Fully Auto

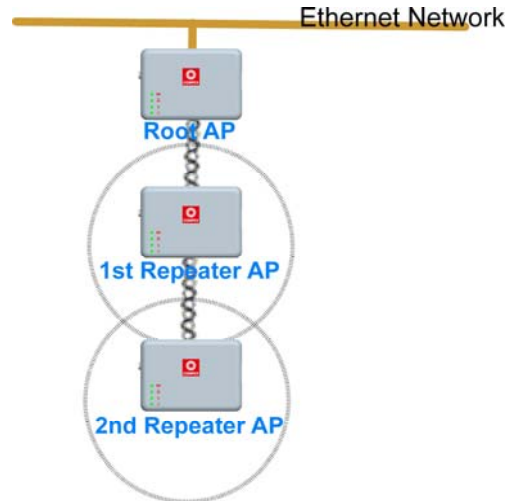
Note:

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

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

# Setup Repeater

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



Example: Network diagram with 2 repeater hops.



## NOTE

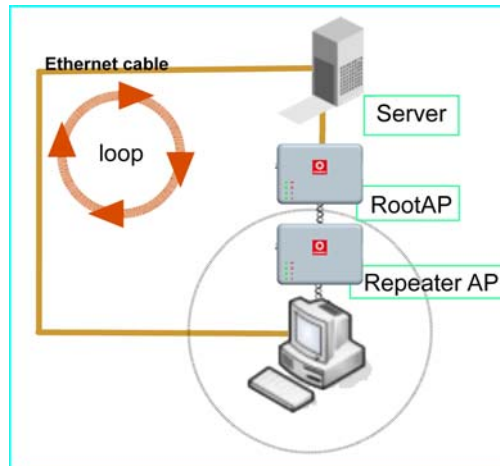
As bandwidth degrades with every repeater hop it is recommended that a limit of **4 hops** is not exceeded.





### NOTE

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



Follow these settings to setup the root AP.

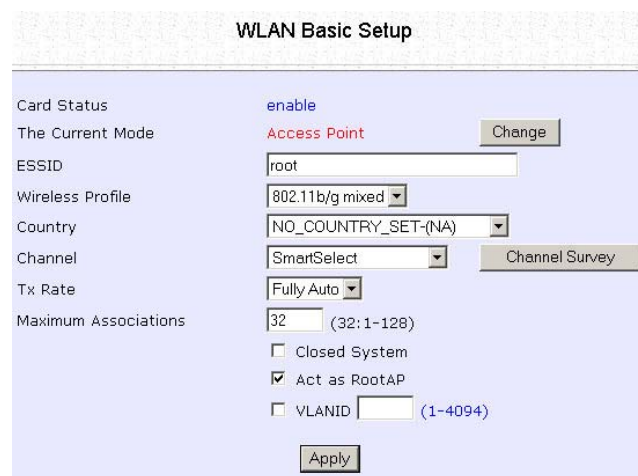
Root AP Settings:

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

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

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

Select **Act as RootAP**.



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

Setting	Value
Card Status	enable
The Current Mode	Access Point (with a 'Change' button)
ESSID	root
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect (with a 'Channel Survey' button)
Tx Rate	Fully Auto
Maximum Associations	32 (32: 1-128)
Closed System	<input type="checkbox"/>
Act as RootAP	<input checked="" type="checkbox"/>
VLANID	<input type="text"/> (1-4094)

An 'Apply' button is located at the bottom of the form.

Click **Apply**.

Follow these settings to setup the repeater.

#### Repeater Settings:

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

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

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



The screenshot shows the 'Repeater Basic Setup' configuration page. It features a light blue background with a white header bar containing the title 'Repeater Basic Setup'. Below the header, there is a table-like structure with configuration options on the left and their values on the right. The options include 'Card Status' (enable), 'The Current Mode' (Repeater), 'ESSID' (repeater), 'Remote ESSID' (default), 'Remote BSSID' (00:00:00:00:00:00), 'Wireless Profile' (802.11b/g mixed), 'Country' (NO\_COUNTRY\_SET-(NA)), and 'Tx Rate' (Fully Auto). There are also checkboxes for 'Closed System' and buttons for 'Change', 'Site Survey', and 'Apply'.

Configuration Option	Value
Card Status	enable
The Current Mode	Repeater
ESSID	repeater
Remote ESSID	default
Remote BSSID	00:00:00:00:00:00
Wireless Profile	802.11b/g mixed
Country	NO_COUNTRY_SET-(NA)
Tx Rate	Fully Auto

Buttons: Change, Site Survey, Apply, Closed System (checkbox)

Options for defining the root AP:

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

ESSID	<input type="text" value="repeater"/>
Remote ESSID	<input type="text" value="default"/>

OR

- Enter the **Remote ESSID**.

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

OR

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

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

Click **Apply**.

# Secure your Wireless LAN

Step 1:

Select **Security** from **WLAN Setup** under the **CONFIGURATION** menu.

Step 2:

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

Click on the **Apply** button.

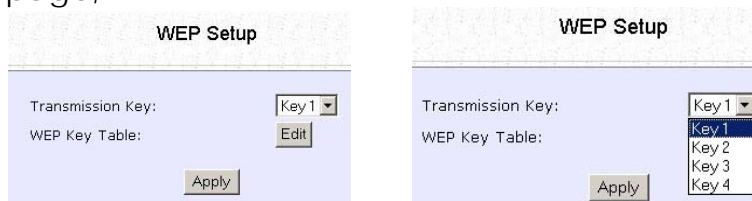


## NOTE

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

# Setup WEP

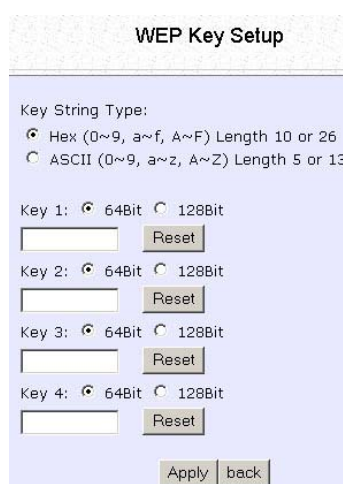
At the **WEP Setup** page,



Step 1:

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

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



Step 2:

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

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

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

Step 3:

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

- **64-bit WEP**

10 hexadecimal or 5 ASCII Text

- **128-bit WEP**

26 hexadecimal or 13 ASCII Text

To clear the values that you 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, Repeater and Gateway Modes)

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:

Cipher Type:

GTK Update(seconds):  (60~9999)

Apply

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:

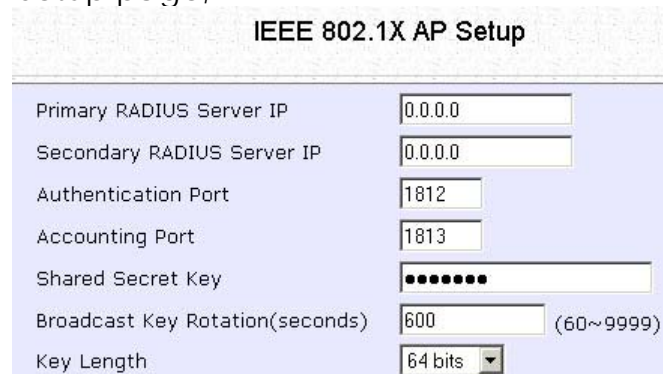
Click the **Apply** button and reboot your system, after which your settings will become effective.



# Setup 802.1x/RADIUS for Access Point

(Available in Access Point, Repeater and Gateway Modes)

At the IEEE 802.1x AP Setup page,



The screenshot shows the 'IEEE 802.1X AP Setup' page with the following fields and values:

Field	Value
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	64 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

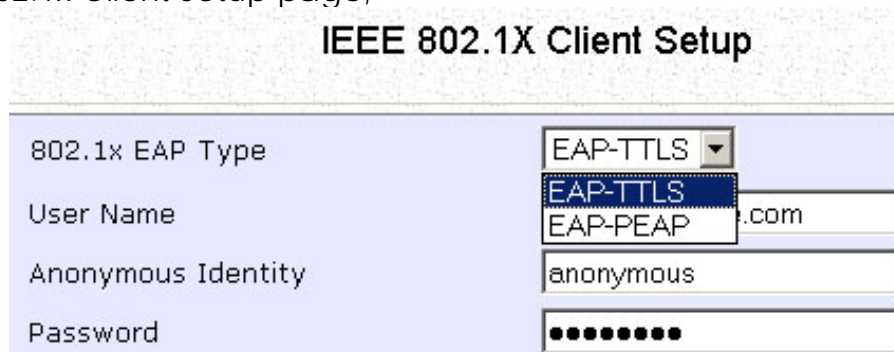
Step 7:

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

# Setup 802.1x/RADIUS for Client

(Available in Client, Transparent Client, Wireless Routing Client and Wireless Adapter Modes)

At the IEEE 802.1x Client Setup page,



The screenshot shows the 'IEEE 802.1X Client Setup' window. It contains four fields: '802.1x EAP Type' with a dropdown menu showing 'EAP-TTLS' selected, 'User Name' with a text box containing 'user@example.com', 'Anonymous Identity' with a text box containing 'anonymous', and 'Password' with a text box containing ten dots. The 'EAP-TTLS' option is highlighted in blue in the dropdown menu.

Step 1:

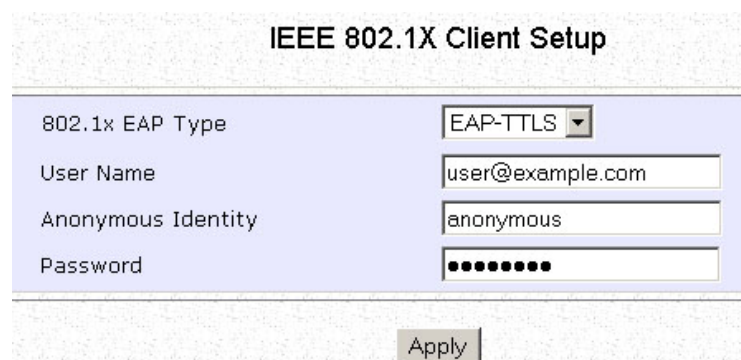
Select whether to use **EAP-TTLS** or **EAP-PEAP** 802.1x EAP Type.

Step 2:

Both **EAP-TTLS** (Extensible Authentication Protocol - Tunneled Transport Layer Security) and **EAP-PEAP** (Protected Extensible Authentication Protocol) support identity hiding. In the WLAN, the access point generates an identity request. To preserve anonymity, the client responds with only enough information to allow the RADIUS server to process the request.

If using **EAP-TTLS** 802.1x EAP Type:

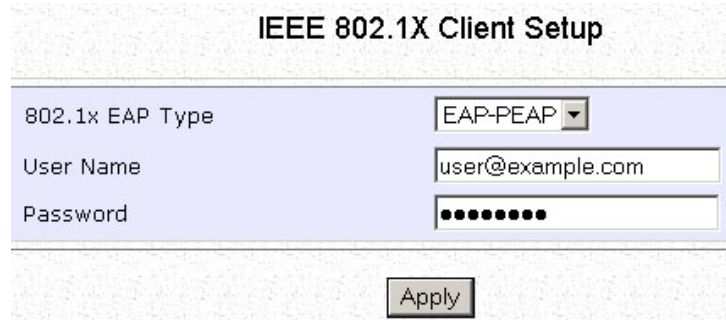
- Enter the **User Name**.
- Enter the **Anonymous Identity** attribute for EAP-TTLS.
- Enter the **Password**.



The screenshot shows the 'IEEE 802.1X Client Setup' window with the same fields as before, but now filled out. The '802.1x EAP Type' dropdown still shows 'EAP-TTLS'. The 'User Name' text box contains 'user@example.com', the 'Anonymous Identity' text box contains 'anonymous', and the 'Password' text box contains ten dots. An 'Apply' button is visible at the bottom right of the window.

If using **EAP-PEAP 802.1x EAP Type**:

- Enter the **User Name**.
- Enter the **Password**.



IEEE 802.1X Client Setup	
802.1x EAP Type	EAP-PEAP
User Name	user@example.com
Password	••••••••
<input type="button" value="Apply"/>	

Step 3:

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

# Setup WPA Enterprise for Access Point

(Available in Access Point, Repeater and Gateway Modes)

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

At the **WPA1/2-Enterprise AP Setup** page,

The screenshot shows the 'WPA1/2-Enterprise AP Setup' page with the following fields:

WPA1/2-Enterprise AP Setup	
Primary RADIUS Server IP	<input type="text" value="0.0.0.0"/>
Secondary RADIUS Server IP	<input type="text" value="0.0.0.0"/>
Authentication Port	<input type="text" value="1812"/>
Accounting Port	<input type="text" value="1813"/>
Shared Secret Key	<input type="password" value="••••••"/>
GTK update(seconds):	<input type="text" value="600"/> (60~9999)

## Step 1:

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

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

## Step 2:

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

## Step 3:

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

## Step 4:

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

## Step 5:

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 6:

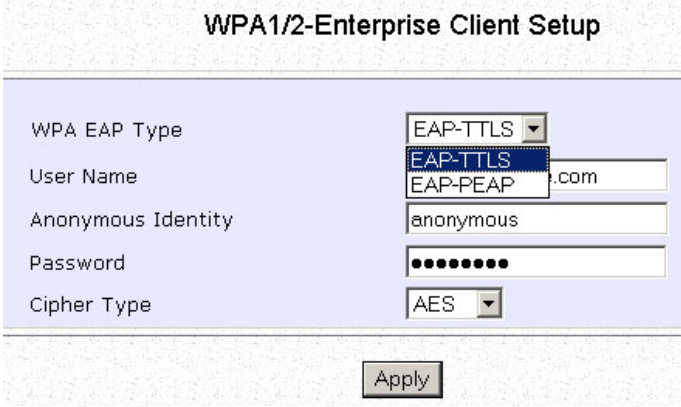
Click the **Apply** button and reboot your system, after which your settings will become effective.

# Setup WPA Enterprise for Client

(Available in Client, Transparent Client, Wireless Routing Client and Wireless Adapter Modes)

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

At the **WPA1/2-Enterprise Client Setup** page,



The screenshot shows a web-based configuration interface titled "WPA1/2-Enterprise Client Setup". The interface has a light blue background with a white border. It contains several input fields and dropdown menus for configuring WPA Enterprise security. The fields are labeled "WPA EAP Type", "User Name", "Anonymous Identity", "Password", and "Cipher Type". The "WPA EAP Type" dropdown is set to "EAP-TTLS". The "User Name" field contains "EAP-TTLS" and the "Anonymous Identity" field contains "anonymous". The "Password" field is masked with dots. The "Cipher Type" dropdown is set to "AES". An "Apply" button is located at the bottom right of the form.

WPA1/2-Enterprise Client Setup	
WPA EAP Type	EAP-TTLS
User Name	EAP-TTLS .com
Anonymous Identity	anonymous
Password	.....
Cipher Type	AES
<input type="button" value="Apply"/>	

### Step 1:

Select whether to use **EAP-TTLS** or **EAP-PEAP** WPA EAP Type.

### Step 2:

Both **EAP-TTLS** (Extensible Authentication Protocol - Tunneled Transport Layer Security) and **EAP-PEAP** (Protected Extensible Authentication Protocol) support identity hiding. In the WLAN, the access point generates an identity request. To preserve anonymity, the client responds with only enough information to allow the RADIUS server to process the request.

If using **EAP-TTLS** WPA EAP Type:

- Enter the **User Name**.
- Enter the **Anonymous Identity** attribute for EAP-TTLS.
- Enter the **Password**.
- Enter the **Cipher Type**.

### 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).

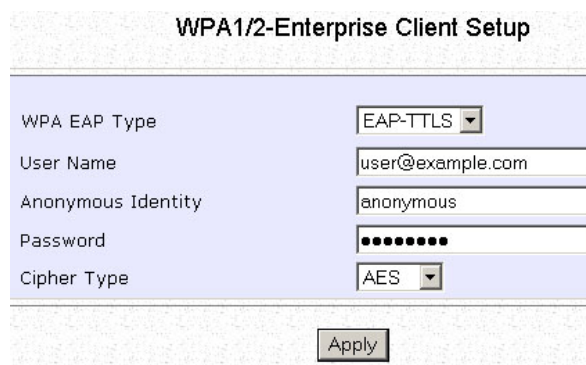
### For WPA2- Enterprise

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.



The screenshot shows a dialog box titled "WPA1/2-Enterprise Client Setup". It contains the following fields and controls:

Field	Value
WPA EAP Type	EAP-TTLS (dropdown menu)
User Name	user@example.com
Anonymous Identity	anonymous
Password	••••••••
Cipher Type	AES (dropdown menu)

At the bottom right of the dialog is an "Apply" button.

If using **EAP-PEAP** WPA EAP Type:

- Enter the **User Name**.
- Enter the **Anonymous Identity** attribute for EAP-TTLS.
- Enter the **Password**.
- Enter the **Cipher Type**.

#### 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).

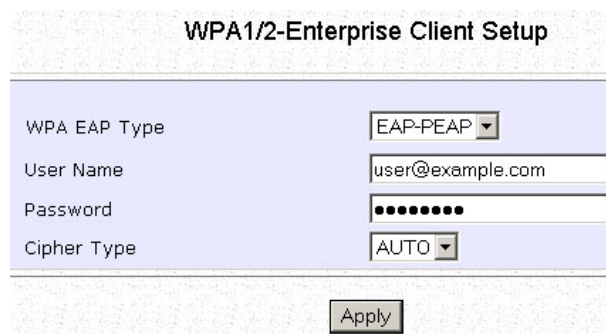
#### For WPA2- Enterprise

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.



The screenshot shows a dialog box titled "WPA1/2-Enterprise Client Setup". It contains four fields: "WPA EAP Type" with a dropdown menu set to "EAP-PEAP", "User Name" with a text box containing "user@example.com", "Password" with a text box filled with dots, and "Cipher Type" with a dropdown menu set to "AUTO". An "Apply" button is located at the bottom right of the dialog box.

Step 3:

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

(Available in Wireless Routing Client and Gateway modes)

Step 1:

Select **Packet Filtering** from the **Security Configuration** command menu.



**Packet Filter Configuration**

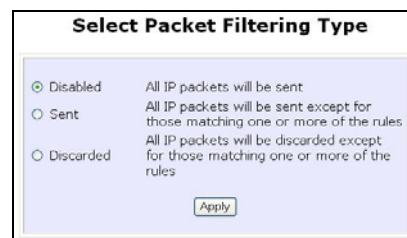
Packet Filter Type : Disabled Change

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.



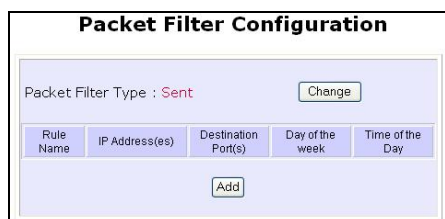
**Select Packet Filtering Type**

☒ 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

Apply



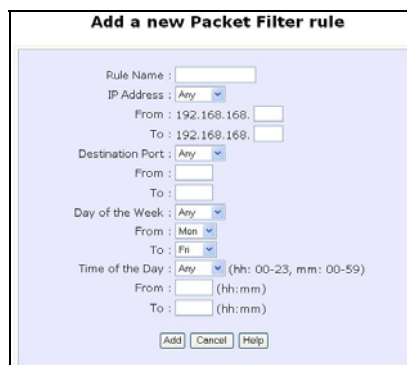
**Packet Filter Configuration**

Packet Filter Type : Sent Change

Rule Name	IP Address(es)	Destination Port(s)	Day of the week	Time of the Day
<span>Add</span>				

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.



**Add a new Packet Filter rule**

Rule Name :

IP Address :

From : 192.168.168.

To : 192.168.168.

Destination Port :

From :

To :

Day of the Week :

From :

To :

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

From :  (hh:mm)

To :  (hh:mm)

Add Cancel Help



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

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

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

- A **Range** of time

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

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

- **Any** time

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

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

(Available in Wireless Routing Client and Gateway modes)

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

(Available in Wireless Routing Client and Gateway modes)

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.

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"/>	ICMP	Accept		ICMP	Any	Any	Any	Any
3	<input checked="" type="checkbox"/>	SSH	Accept		UDP	Any	Any	22	Any
4	<input checked="" type="checkbox"/>	ftp (0-65)	Accept		TCP	Any	Any	Any	20-65
5	<input checked="" type="checkbox"/>	ftp (800)	Accept		TCP	Any	Any	Any	8000
6	<input checked="" type="checkbox"/>	radius	Accept		UDP	Any	Any	1645	Any
7	<input checked="" type="checkbox"/>	dhcp-boots	Accept		UDP	Any	Any	67	68

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 value 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 of the ICMP parameters.
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

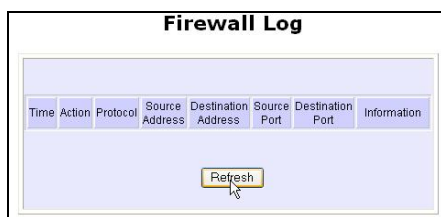
The Firewall Log captures and stores network traffic information such as the type of data traffic, the time, the source and destination address / port, as well as the action taken by the firewall.

## View Firewall Logs

(Available in Wireless Routing Client and Gateway modes)

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:

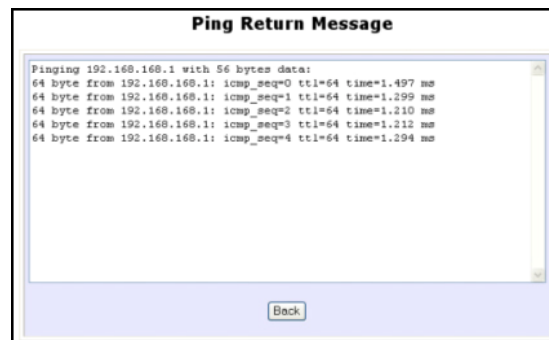
Select **Ping Utility** under the **SYSTEM TOOLS** command menu.



Step 2:

Enter the IP address of the target host to ping.

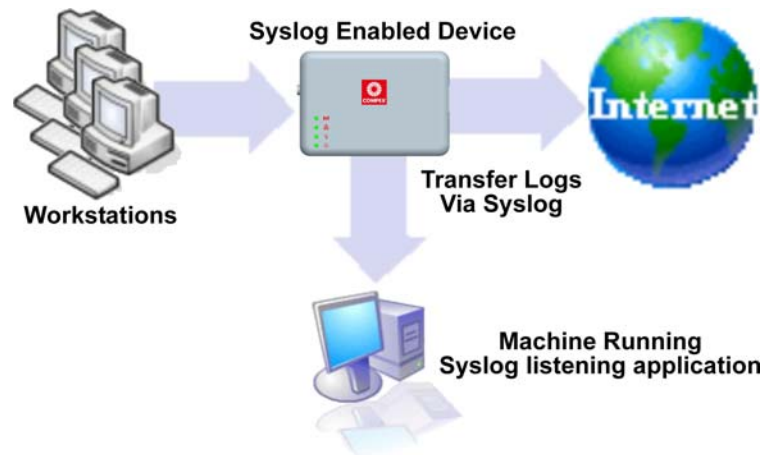
Click the **Start** button.



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:

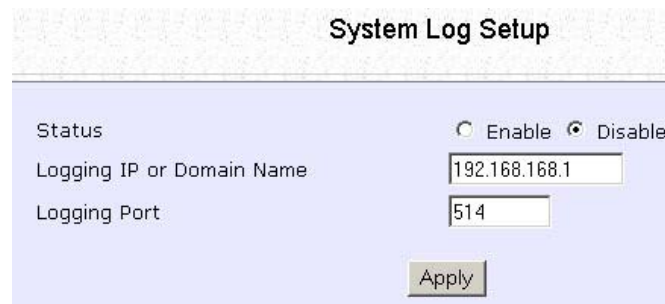
- **Enable** or **Disable** system logging.
- Set the **Remote IP Address or Domain Name** and **Remote Port** for the router to send the system log messages to.

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 configuration area.

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.

Web Images Groups News more »

syslog

Search

Search: ☒ the web ☐ pages from Singapore

Step 2:

Select a Syslog listening application.

Web

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

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

Step 3:

Download Syslog listening application.

Download Now

Step 4:

Install Syslog listening application.



Step 5:

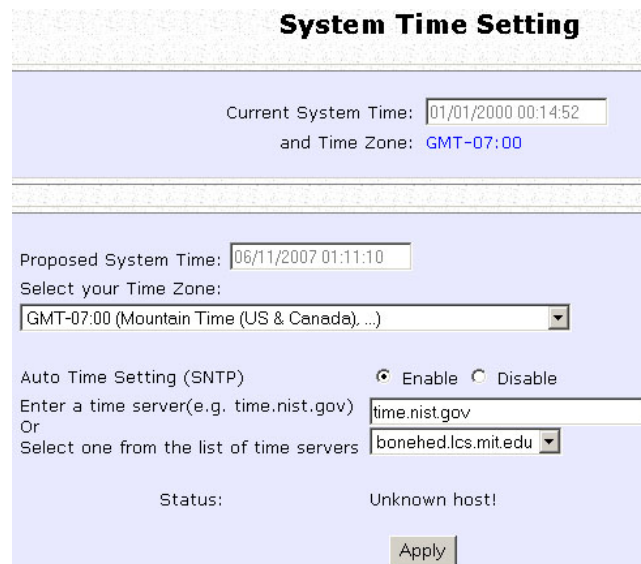
View logged information on Syslog listening application.

Syslog Daemon				
File Edit View Help				
Display 00 (Default)				
Date	Time	Priority	Hostname	Message
03-07-2006	10:18:36	Mail.Info	10.0.0.10	This is Syslog test message number 24
03-07-2006	10:18:35	System3.Emerg	10.0.0.10	This is Syslog test message number 23
03-07-2006	10:18:34	Local0.Emerg	10.0.0.10	This is Syslog test message number 22
03-07-2006	10:18:33	Mail.Debug	10.0.0.10	This is Syslog test message number 21
03-07-2006	10:18:32	Syslog.Warning	10.0.0.10	This is Syslog test message number 20
03-07-2006	10:18:31	Local0.Debug	10.0.0.10	This is Syslog test message number 19
03-07-2006	10:18:30	Local5.Alert	10.0.0.10	This is Syslog test message number 18
03-07-2006	10:18:29	System4.Debug	10.0.0.10	This is Syslog test message number 17
03-07-2006	10:18:28	Local3.Info	10.0.0.10	This is Syslog test message number 16
03-07-2006	10:18:27	Lpr.Critical	10.0.0.10	This is Syslog test message number 15
03-07-2006	10:18:26	System4.Notice	10.0.0.10	This is Syslog test message number 14
03-07-2006	10:18:25	System1.Critical	10.0.0.10	This is Syslog test message number 13
03-07-2006	10:18:24	User.Warning	10.0.0.10	This is Syslog test message number 12
03-07-2006	10:18:23	System2.Info	10.0.0.10	This is Syslog test message number 11
03-07-2006	10:18:22	Local6.Critical	10.0.0.10	This is Syslog test message number 10
03-07-2006	10:18:21	Local4.Emerg	10.0.0.10	This is Syslog test message number 9
03-07-2006	10:18:20	UUCP.Debug	10.0.0.10	This is Syslog test message number 8
03-07-2006	10:18:19	Local4.Info	10.0.0.10	This is Syslog test message number 7
03-07-2006	10:18:18	User.Error	10.0.0.10	This is Syslog test message number 6
03-07-2006	10:18:17	Local3.Notice	10.0.0.10	This is Syslog test message number 5
03-07-2006	10:18:16	Kernel.Info	10.0.0.10	This is Syslog test message number 4

# Setup System Clock

Step 1:

Select **System Clock Setup** from the **SYSTEM TOOLS** menu.



The screenshot shows a web interface titled "System Time Setting". It displays the "Current System Time" as 01/01/2000 00:14:52 and the "Time Zone" as GMT-07:00. Below this, it shows the "Proposed System Time" as 06/11/2007 01:11:10. A dropdown menu for "Select your Time Zone:" is set to "GMT-07:00 (Mountain Time (US & Canada), ...)". Under "Auto Time Setting (SNTP)", the "Enable" radio button is selected. There are two input fields for time servers: "time.nist.gov" and "bonehed.lcs.mit.edu". The status is "Unknown host!". An "Apply" button is at the bottom.

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.



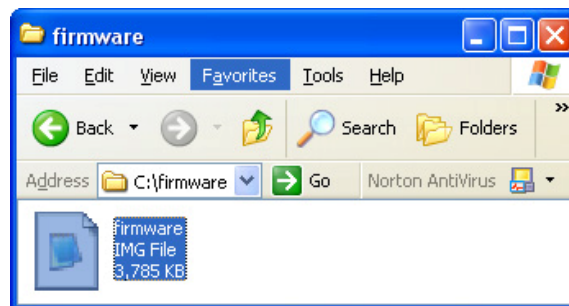
# Upgrade the Firmware with Command Line Interface

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).

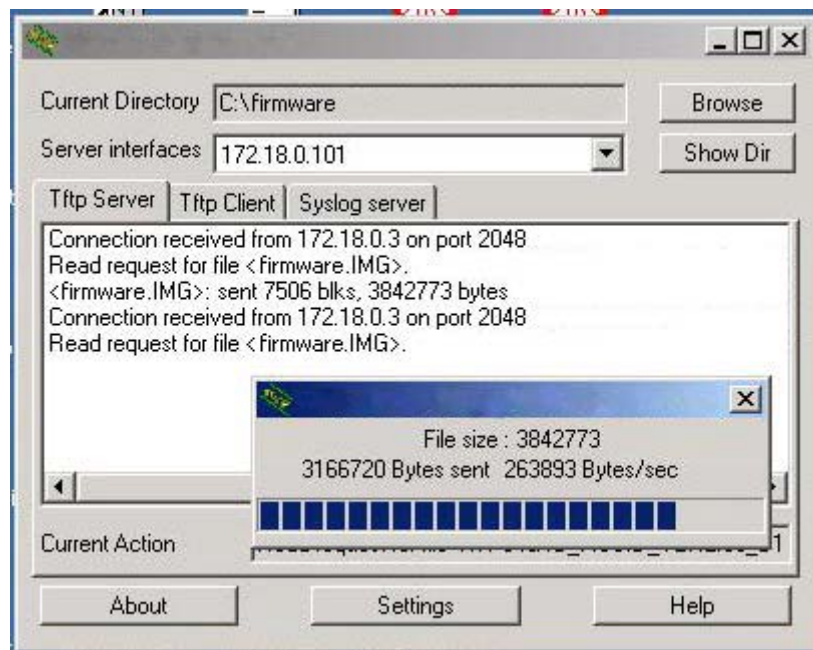
## Step 1:

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.

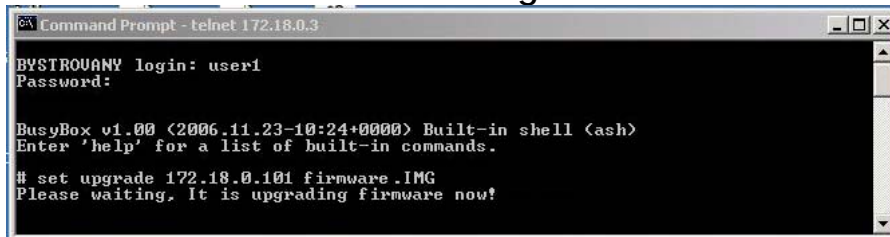


Sample Screenshot

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>**



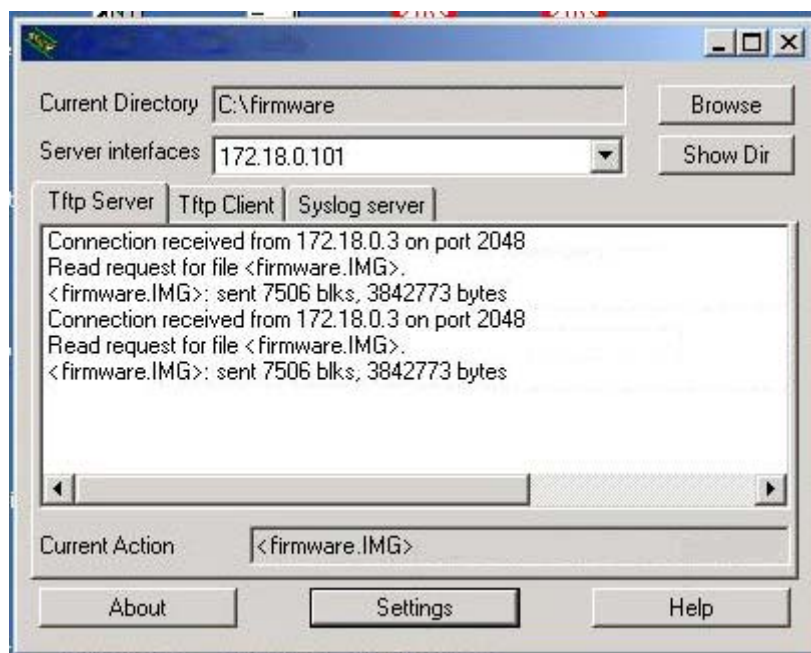
```
Command Prompt - telnet 172.18.0.3
BYSTROUANY login: user1
Password:

BusyBox v1.00 (2006.11.23-10:24+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

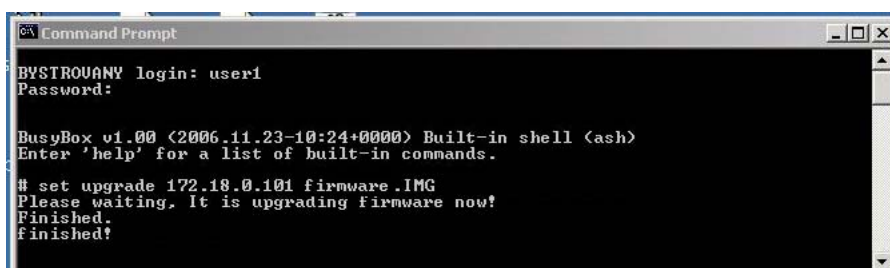
# set upgrade 172.18.0.101 firmware.IMG
Please waiting, It is upgrading firmware now!
```

Step 4:

These screens display when upgrade is done.



Sample Screenshot



```
Command Prompt
BYSTROUANY login: user1
Password:

BusyBox v1.00 (2006.11.23-10:24+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

# set upgrade 172.18.0.101 firmware.IMG
Please waiting, It is upgrading firmware now!
Finished.
finished!
```



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

Before starting, check the status of the diagnostic LED 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.

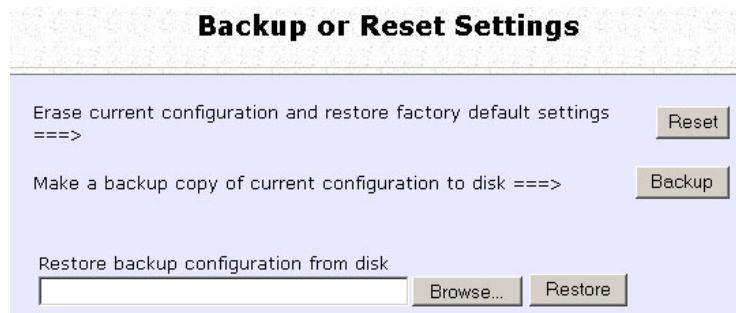
## Reset your settings

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: 1. "Erase current configuration and restore factory default settings ==>" with a "Reset" button. 2. "Make a backup copy of current configuration to disk ==>" with a "Backup" button. 3. "Restore backup configuration from disk" with a text input field, a "Browse..." button, and a "Restore" button.

Step 3:

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

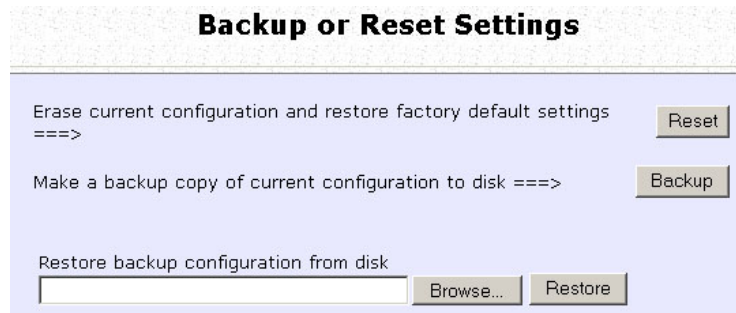
## Backup your Settings

Step 1:

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

Step 2:

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



Step 3:

Save your configuration file to your local disk.



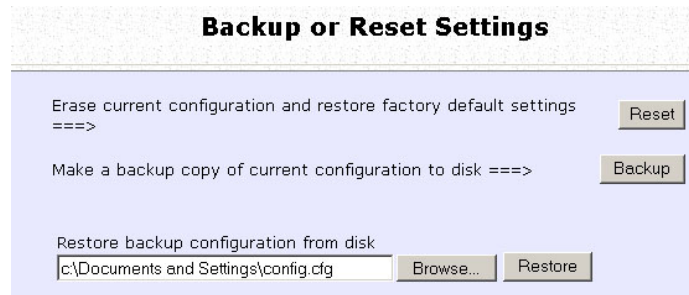
## Restore your Settings

Step 1:

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

Step 2:

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



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

Step 2:

# Reboot the System

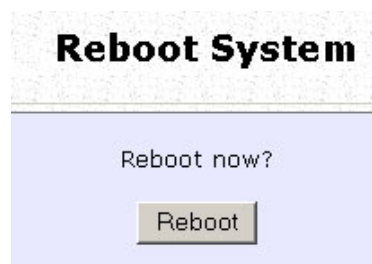
Most of the changes you make to the system settings require a system reboot before the new parameters can take effect.

Step 1:

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

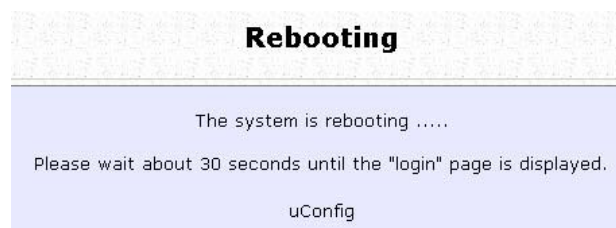
Step 2:

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.

A screenshot of a web-based 'Change Password' form. The form has a title bar at the top that says 'Change Password'. Below the title bar, there are three input fields. The first is labeled 'Current Password:' and contains four dots. The second is labeled 'New Password:' and also contains four dots. The third is labeled 'Confirm Password:' and contains four dots. At the bottom of the form, there is a button labeled 'Apply'.

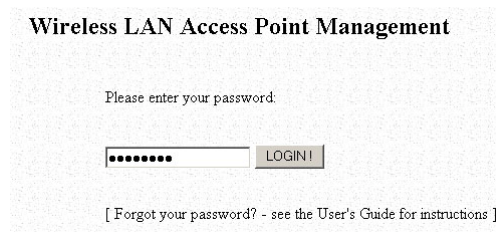
# To Logout

Step 1:

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

Step 2:

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



The image shows a login screen titled "Wireless LAN Access Point Management". It has a light gray background with a subtle pattern. The text "Please enter your password:" is centered above a password input field. The input field contains seven dots. To the right of the input field is a button labeled "LOGIN!". Below the input field and button, there is a link that says "[ 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	
<b>Device:</b>	
System Up Time :	0 Days 00:01:32
BIOS/Loader Version :	2.41 (build 0516)
Firmware Version :	2.01 (build 20-April-2007)
NetWork Mode :	Inherent Bridge
<b>Wireless:</b>	
Hardware Address :	00-80-48-ff-00-2c
WLAN name (ESSID):	compex-wpe53g
Operating frequency :	2427MHz
Operating Channel :	4
Security Mode :	None
<b>Management Port:</b>	
Hardware Address :	00-80-48-ff-00-2b
IP Address :	192.168.168.1
Network Mask :	255.255.255.0
DHCP Server :	Disabled

# 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.

A screenshot of a 'Support Information' box with a light blue background and a thin border. The box contains text about product registration and regional technical support centers.

**Support Information**

To register your product, obtain product information, documentation and updates, go to:  
<http://www.cpx.com>  
<http://www.complex.com.sg>

**Regional Technical Support Centers**

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

Complex Inc.  
840 Columbia Street, Suite B, Brea, CA92821,USA  
Tel : (714) 482-0333  
Fax : (714) 482-0332  
800 Line: (800) 279-8891  
Email: [support@cpx.com](mailto:support@cpx.com)

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

Complex 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 ctsttimeout <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, and 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:  {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" }, {CTRY_IRAN, "IR" }, {CTRY_IRELAND, "IE" }, {CTRY_ISRAEL, "IL" },
Set countrycode <2 letter string>	

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



## Custom Configuration Update

Custom Configuration Update

SYNTAX	Cfgfile <operation type> <IP of PC running TFTP server> <filename>										
DESCRIPTION	<p>The cfgfile command is used for managing simple configuration changes to multiple access points. It is useful for when the user has many access points to configure and the configuration is mostly the same.</p> <p><b>For example if user needs to configure ten access points, and just change the IP address configuration:</b></p> <ol style="list-style-type: none"><li>1. Configure the first access point with the common configuration for all the access points using web manager</li><li>2. Export the access point configuration file with cfgfile in Telnet.</li><li>3. Edit the IP addresses in the access point configuration files to customise them for the individual access points.</li><li>4. Import the edited access point configuration files to the respective access points with cfgfile in Telnet.</li></ol> <p><b>Requirement and Explanation:</b></p> <p>The cfgfile command uses the TFTP (Trivial File Transfer Protocol). This command transfers the access point configuration file to and from the access point. It has 4 operation types for these transfers – Backup, Restore, Export, and Import.</p> <p>Before executing the cfgfile command, there are some requirements that have to be met in order for the command to execute successfully. The TFTP server has to be running on the PC with the Telnet connection to the access point.</p> <p>Make a note of the directory where the access point configuration file is located in. This directory can be a folder on the hard drive of the PC with the Telnet connection. It can also be any storage device that is connected o this PC. The TFTP server has to be set up to point to this directory.</p> <p>This table explains the different Operation Types.</p> <table><tr><th colspan="2">Operation Type</th></tr><tr><td>Backup</td><td><p>The Backup operation saves the configuration from the access point to the configuration file defined in &lt;filename&gt; and stored on the PC.</p><p>This is a binary file (*.bin) which must not be edited as doing so will corrupt it.</p><p>(Access Point → PC)</p></td></tr><tr><td>Restore</td><td><p>The Restore operation returns the access point back to the previous configuration according to the configuration file defined in &lt;filename&gt; on the PC.</p><p>This is a binary file (*.bin) which must not be edited as doing so will corrupt it.</p><p>(PC → Access Point)</p></td></tr><tr><td>Export</td><td><p>The Export operation extracts a portion of the access point configuration to a text file on the PC which can be edited to further customise it for each access point.</p><p>This text file can then be imported into other access points with the Import cfgfile operation.</p><p>(Access Point → PC)</p></td></tr><tr><td>Import</td><td><p>The Import Operation uploads the configuration to the access point.</p><p>This configuration is the access point configuration which has been exported previously with the Export cfgfile operation and then further edited to customise for each access point.</p><p>(PC → Access Point)</p></td></tr></table>	Operation Type		Backup	<p>The Backup operation saves the configuration from the access point to the configuration file defined in &lt;filename&gt; and stored on the PC.</p> <p>This is a binary file (*.bin) which must not be edited as doing so will corrupt it.</p> <p>(Access Point → PC)</p>	Restore	<p>The Restore operation returns the access point back to the previous configuration according to the configuration file defined in &lt;filename&gt; on the PC.</p> <p>This is a binary file (*.bin) which must not be edited as doing so will corrupt it.</p> <p>(PC → Access Point)</p>	Export	<p>The Export operation extracts a portion of the access point configuration to a text file on the PC which can be edited to further customise it for each access point.</p> <p>This text file can then be imported into other access points with the Import cfgfile operation.</p> <p>(Access Point → PC)</p>	Import	<p>The Import Operation uploads the configuration to the access point.</p> <p>This configuration is the access point configuration which has been exported previously with the Export cfgfile operation and then further edited to customise for each access point.</p> <p>(PC → Access Point)</p>
Operation Type											
Backup	<p>The Backup operation saves the configuration from the access point to the configuration file defined in &lt;filename&gt; and stored on the PC.</p> <p>This is a binary file (*.bin) which must not be edited as doing so will corrupt it.</p> <p>(Access Point → PC)</p>										
Restore	<p>The Restore operation returns the access point back to the previous configuration according to the configuration file defined in &lt;filename&gt; on the PC.</p> <p>This is a binary file (*.bin) which must not be edited as doing so will corrupt it.</p> <p>(PC → Access Point)</p>										
Export	<p>The Export operation extracts a portion of the access point configuration to a text file on the PC which can be edited to further customise it for each access point.</p> <p>This text file can then be imported into other access points with the Import cfgfile operation.</p> <p>(Access Point → PC)</p>										
Import	<p>The Import Operation uploads the configuration to the access point.</p> <p>This configuration is the access point configuration which has been exported previously with the Export cfgfile operation and then further edited to customise for each access point.</p> <p>(PC → Access Point)</p>										

# Appendix: Virtual AP (Multi-SSID) FAQ

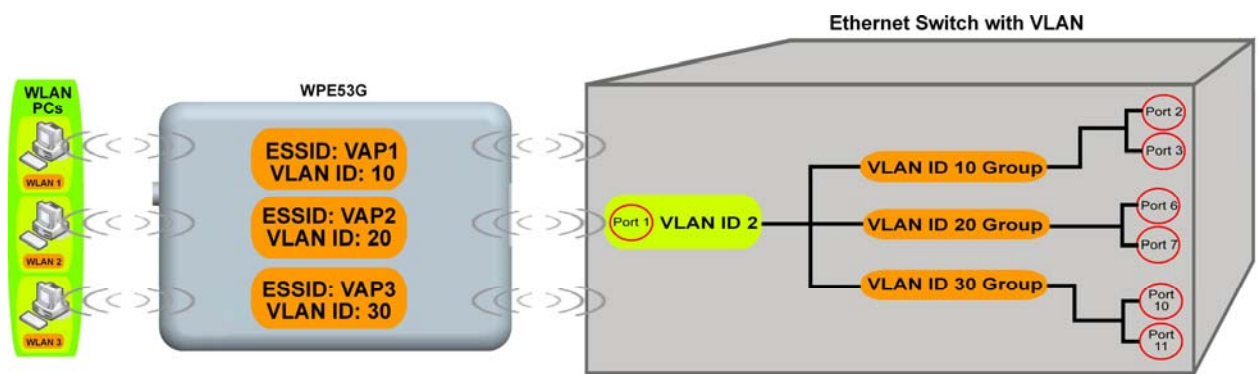
Q1) What is mSSID?

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

<b>Safety and Electromagnetic Conformance</b>	<ul style="list-style-type: none"> <li>FCC Part 15 SubPart B and SubPart C (for wireless module)</li> <li>EN 300 328-2</li> <li>EMC CE EN 301 489 (EN300 826)</li> <li>EN 55022 (CISPR 22)/EN 55024 Class B</li> <li>EN 61000-3-2</li> <li>EN61000-3-3</li> <li>CE EN 60950</li> </ul>
<b>Standards</b> IEEE802.11b:  IEEE802.11g:  Super-G model:	<ul style="list-style-type: none"> <li>11Mbps, 5.5Mbps, 2Mbps, 1Mbps</li> <li>54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps, 6Mbps, automatically fallback to 5.5Mbps, 2Mbps, 1Mbps</li> <li>108Mbps, 96Mbps, 72Mbps, 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 6Mbps</li> </ul>
<b>Frequency Range IEEE 802.11b/g:</b>	2.412GHz ~ 2.462GHz (US & Canada) 2.412GHz ~ 2.472GHz (Europe) 2.412GHz ~ 2.484GHz (Japan)
<b>Max Tx Power:</b>	17dBm
<b>Security</b>	<ul style="list-style-type: none"> <li>64 - bit / 128 - bit WEP</li> <li>WPA-EAP, WPA-PSK, WPA2</li> <li>Tagged VLAN</li> <li>IEEE 802.1x – TLS, TTLS, PEAP, EAP-SIM</li> </ul>
<b>Network Interface</b>	<ul style="list-style-type: none"> <li>10/100 Mbps auto-negotiating Ethernet port (RJ45)</li> </ul>
<b>Modulation Techniques</b>	OFDM (BPSK, QPSK, 16-QAM, 64-QAM), DSSS (BPSK, QPSK, CCK)
<b>Operating Channels</b>	<ul style="list-style-type: none"> <li>11 Channels (US and Canada)</li> <li>13 Channels (Europe)</li> <li>14 Channels (Japan)</li> </ul>
<b>Advanced Wireless Feature</b>	<ul style="list-style-type: none"> <li>Virtual AP</li> <li>Long Distance Parameters Setup</li> <li>Smart Select</li> <li>HTTPS</li> </ul>
<b>Antenna</b>	Detachable 2dBi antenna with SMA connector
<b>Management</b>	<ul style="list-style-type: none"> <li>HTTP Web Management</li> <li>Telnet</li> <li>SSH</li> </ul>
<b>Built-in DHCP Server</b>	Yes
<b>DHCP Reservation</b>	By MAC address
<b>Configuration Backup &amp; Restore</b>	Yes

<b>Firmware Upgrade</b>	Yes
<b>Power Requirements</b> DC Jack: LV model HV model  PoE (HV model):	9-15VDC 15-24VDC  15-48VDC [pair +ve(4,5) and –ve(7,8)]
<b>Operating Temp:</b>	-20°C to +70°C
<b>Storage Temp:</b>	-30°C to +80°C
<b>Operating Humidity:</b>	10% to 80% RH Humidity (RH – Relative Humidity)
<b>Physical Dimensions</b>	91.8mm x 66mm x 25mm (H x W x D)

# Technical Support Information

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

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

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

Technical Support Centres	
Contact the technical support centre that services your location.	
U.S.A., Canada, Latin America and South America	
✉ Write	Compex, Inc. 840 Columbia Street, Suite B Brea, CA 92821, USA
☎ Call	Tel: +1 (714) 482-0333 (8 a.m.-5 p.m. Pacific time)
	Tel: +1 (800) 279-8891 (Ext.122 Technical Support)
☎ Fax	Fax: +1 (714) 482-0332
Asia, Australia, New Zealand, Middle East and the rest of the World	
✉ Write	Compex Systems Pte Ltd 135, Joo Seng Road #08-01, PM Industrial Building Singapore 368363
☎ Call	Tel: (65) 6286-1805 (8 a.m.-5 p.m. local time)
☎ Fax	Tel: (65) 6286-2086 (Ext.199 Technical Support)
	Fax: (65) 6283-8337
Internet access	E-mail: <a href="mailto:support@compex.com.sg">support@compex.com.sg</a> FTPsite: <a href="ftp.compex.com.sg">ftp.compex.com.sg</a>
Website:	<a href="http://www.cpx.com">http://www.cpx.com</a> or <a href="http://www.compex.com.sg">http://www.compex.com.sg</a>

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

Please contact us at:

Fax: (65) 62809947

Email: [feedback@compex.com.sg](mailto:feedback@compex.com.sg)

We hope this manual was helpful to you. For more Compex information, please visit us at [www.compex.com.sg](http://www.compex.com.sg)