



networks@work

USER'S MANUAL



COMPEX NETPASSAGE SERIES

WP54G 1D & 6D

WP54G 1D & 6D

WP54G 1D & 6D

WP54G 1D & 6D

WP54G 1D & 6D

Manual Number: U-0478-V1.3C

© Copyright 2006 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®, ReadyLINK® and MicroHub® are registered trademarks of Compex, Inc. Microsoft Windows and the Windows logo are the trademarks of Microsoft Corp. NetWare is the registered trademark of Novell Inc. All other brand and product names are trademarks or registered trademarks of their respective owners.

Notice: Copyrights © 2006 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 Daniel

Manual Number: U-0478-V1.3C Version 1.3 September 2006

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.

Your Feedback

We value your feedback. If you find any errors in this user's manual, or if you have suggestions on improving, we would like to hear from you. Please contact us at:

Fax: (65) 62809947

Email: feedback@compex.com.sg

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.

Products that contain a radio transmitter are labelled with FCC ID and may also carry the FCC logo.

Caution: Exposure to Radio Frequency Radiation.

To comply with the FCC RF exposure compliance requirements, the following antenna installation and device operating configurations must be satisfied:

- a. For configurations using the integral antenna, the separation distance between the antenna(s) and any person's body (including hands, wrists, feet and ankles) must be at least 2.5cm (1 inch).
- b. For configurations using an approved external antenna, the separation distance between the antenna and any person's body (including hands, wrists, feet and ankles) must be at least 20cm (8 inch).

The transmitter shall not be collocated with other transmitters or antennas.

ICES 003 Statement

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

Declaration of Conformity

Compex, Inc. declares the following:

Product Name: Wireless Access Point with PoE

Model No.: WP54G 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.

Technical Support Information

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

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

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

Technical Support Centres	
Contact the technical support centre that services your location.	
U.S.A., Canada, Latin America and South America	
 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: support@compex.com.sg FTPsite: ftp.compex.com.sg
Website:	http://www.cpx.com or http://www.compex.com.sg

About This Document

The product described in this document, Complex Wireless-G 54Mbps XR™ Managed Access Point, WP54G is a licensed product of Complex Systems Pte Ltd. This document contains instructions for installing, configuring and using Access point. It also gives an overview of the key applications and the networking concepts with respect to the product.

This documentation is for both Network Administrators and the end user who possesses some basic knowledge in the networking structure and protocols.

It makes a few assumptions that the host computer has already been installed with TCP/IP and already up & running and accessing the Internet. Procedures for Windows 98SE/ME/2000/XP operating systems are included in this document. However, for other operating system, you may need to refer to your operating system's documentation for networking.

How to Use this Document

This document may become superseded, in which case you may find its latest version at: <http://www.complex.com.sg>

The document is written in such a way that you as a user will find it convenient to find specific information pertaining to the product. It comprises of chapters that explain in details on the installation and configuration of WP54G.

Firmware

This manual is written based on Firmware version 2.02

Conventions

In this document, special conventions are used to help and present the information clearly. The Wireless Access Point with PoE is often referred to as *WP54G* or *access point* or *AP* in this document. Below is a list of conventions used throughout.



NOTE

This section will consist of important features or instructions



CAUTION

This section concerns risk of injury, system damage or loss of data



WARNING

This section concerns risk of severe injury

References on Menu Command, Push Button, Radio Button, LED and Label appear in **Bold**. For example, "Click on **Ok**."

Copyrights © 2006 Complex Systems Pte Ltd	i
Trademark Information	i
Disclaimer.....	i
Your Feedback.....	i
FCC NOTICE	ii
Declaration of Conformity	ii
Technical Support Information	iii
About This Document.....	iv
How to Use this Document	iv
Firmware	iv
Conventions.....	iv

CHAPTER 1: PRODUCT OVERVIEW..... 7

Introduction.....	7
Features and Benefits.....	8
When to use which mode	10
Access Point Mode.....	10
Access Point Client Mode	11
Wireless Routing Client Mode	12
Gateway Mode.....	13
Wireless Adapter Mode	15
Transparent Client Mode.....	16
Repeater Mode.....	18

CHAPTER 2: HARDWARE INSTALLATION 19

Setup Requirements	19
Hardware Installation	19
OPTION One: Using power adapter to supply power to the unit.....	19
OPTION Two: Using PoE to supply power to the unit.....	21
Optional: Mounting on the Wall	24

CHAPTER 3: ACCESS TO WEB-BASED INTERFACE 25

Access to the Web interface with uConfig.....	25
Manual access to web-based interface via Internet Explorer	29

CHAPTER 4: COMMON CONFIGURATION	34
Management Port Setup	34
Setting up your LAN	35
To view the active DHCP leases	38
To reserve specific IP addresses for predetermined DHCP clients	39
WLAN Setup	42
To configure the Basic setup of the wireless mode	43
To configure the Security setup of the wireless mode	59
To configure the Advanced setup of the wireless mode	59
Statistics	62
WAN Setup	67
Telnet/SSH Setup	74
TELNET Command Line Interface	77
Secure Shell Host Command Line Interface	78
Web Management Setup	80
SNMP Setup	81
STP Setup	82
MAC Filtering	87
<i>Add a MAC address to the MAC Address List.</i>	88
<i>Delete a MAC address from all access points.</i>	91
<i>Delete a MAC address from individual access point.</i>	93
<i>Edit MAC address from the MAC Address List.</i>	95
 CHAPTER 5: WLAN SECURITY	 97
How to set up WEP	98
How to set up WPA-Personal	100
How to set up 802.1x/RADIUS	102
How to set up WPA Enterprise	104
 CHAPTER 6: WIRELESS EXTENDED FEATURES	 107
Virtual AP (Multiple SSID)	107
Preferred APs (Only available in Client Mode)	109
Long Distance Parameters	110
Point-to-Point & Point-to-MultiPoint Setup	113
Repeater Setup	116

CHAPTER 7: ADVANCED CONFIGURATION	121
Routing	121
To configure Static Routing of WP54G	122
NAT.....	123
To configure Virtual Servers based on De-Militarized Zone Host	124
To configure Virtual Servers based on Port Forwarding	126
To configure Virtual Servers based on IP Forwarding	129
Bandwidth Control.....	130
To enable or disable Bandwidth Control.....	130
To configure WAN Bandwidth Control Setting	131
To configure LAN Bandwidth Control Setting	132
Remote Management	134
To set up Remote Management	134
Parallel Broadband.....	135
To enable Parallel Broadband on WP54G	136
Email Notification	137
Static Address Translation.....	139
DNS Redirection	141
To enable/disable DNS Redirection.....	143
Dynamic DNS Setup	143
To enable/disable Dynamic DNS Setup.....	144
To manage Dynamic DNS List.....	145
 CHAPTER 8: SECURITY CONFIGURATION	 150
Packet Filtering	150
To configure Packet Filtering.....	150
URL Filtering	154
To configure URL Filtering.....	154
Firewall Configuration	155
To configure SPI Firewall.....	155
Firewall Logs	159
To view Firewall Logs.....	159
 CHAPTER 9: SYSTEM UTILITIES	 160
Using the SYSTEM TOOLS Menu.....	160
Ping Utility.....	160
System Identity.....	161
System Clock Setup	162

Firmware Upgrade	163
Backup or Reset Settings	165
Reboot System.....	168
Change Password.....	169
Logout	170
Using the HELP menu	171
Get Technical Support	171
About System.....	172
 APPENDIX I: FIRMWARE RECOVERY	 173
 APPENDIX II: TCP/IP CONFIGURATION	 175
For Windows 95/98/98SE/ME/NT	175
For Windows XP/2000.....	178
 APPENDIX III: PANEL VIEWS & DESCRIPTIONS	 181
 APPENDIX IV: COMMAND LINE INTERFACE COMMANDS...	184
 APPENDIX V: VIRTUAL AP (MULTI-SSID) FAQ	 189
 APPENDIX VI: TECHNICAL SPECIFICATIONS.....	 193

Chapter 1: Product Overview

INTRODUCTION

The Wireless Access Point with PoE is a high-performance access point (AP) that is designed for enterprise and public access applications. Embedded with the Atheros chipset, it boasts network robustness, stability and wider network coverage. Based on 802.11g, the access point supports high-speed data transmission of up to 54Mbps in the 2.4GHz frequency band.

The access point is capable of operating in 7 modes: **Access Point Mode**, **Client Mode**, **Wireless Routing Client**, **Gateway Mode**, **Wireless Adapter Mode**, **Transparent Client Mode** which is specifically developed to be paired with root access point for Point-to-Point and Point-to-MultiPoint connection, and **Repeater Mode**. Which makes it suitable for a wide variety of wireless applications, including long-distance deployments.

Equipped with an SMA connector for external antenna support, the access point provides a wider coverage for your network. Moreover, its integrated Power over Ethernet (PoE) allows the access point to be used in areas where power outlets are not readily available.

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

The access point also incorporates a unique set of advanced features such as: Virtual AP to deliver multiple services; Long-Range parameter fine-tuning which provide the access point with the ability to auto-calculate parameters such as slot time; ACK time-out and CTS time-out to achieve a longer range; Spanning Tree Protocol (STP) which provides extra redundancy and the ability to auto-reconfigure when there are changes in the network topology; HTTPS which feature additional authentication and encryption; and Telnet which allows remote connection; and SSH which provides a secure host connection.

FEATURES AND BENEFITS

The access point has been designed for high performance and offers a rich suite of features, with which you should acquaint yourself to be able to exploit your access point's full potential.

- **Point-to-Point & Point-to-MultiPoint Support**
Point-to-Point and Point-to-MultiPoint communication between different buildings enables you to bridge wireless clients that are kilometres apart while unifying the networks.
- **Virtual AP (Multiple SSID)**
Virtual AP implements mSSID (Multi-SSID)
This allows a single wireless card to be set up with multiple virtual AP connections with different SSIDs or BSSID (Basic Service Set Identifier) and security modes.
- **Highly Secured Wireless Network**
The access point supports the highest available wireless security standard: Wi-Fi Protected Access 2. WPA2 has two different modes: WPA2-Personal for SOHO users and WPA2-Enterprise for Enterprise users. The access point also supports IEEE 802.1x for secure and centralized user-based authentication. Wireless clients are thus required to authenticate through highly secure methods like EAP-TLS, EAP-TTLS, and EAP-PEAP, in order to obtain access to the network.
- **Smart Select**
This feature will automatically scan and recommend the best channel that the access point can utilize.
- **uConfig Utility**
Compex's exclusive **uConfig** utility allows users to access the user-friendly Web configuration interface of the access point without having to change the TCP/IP setup of the workstation.

- **STP**
Spanning-Tree Protocol provides path redundancy while preventing undesirable loops in the network. It forces certain redundant data paths into a standby (blocked) state. If one network segment in the Spanning-Tree Protocol becomes unreachable, or if Spanning-Tree Protocol costs change, the spanning-tree algorithm reconfigures the spanning-tree topology and re-establishes the link by activating the standby path.
- **HTTPS**
WP54G supports HTTPS (SSL) in addition to the standard HTTP. HTTP (SSL) features additional authentication and encryption for secure communication.
- **Telnet**
Telnet allows a computer to remotely connect to the WP54G CLI (Command Line Interface) for control and monitoring.
- **SSH**
SSH (Secure Shell Host) establishes a secure host connection to the WP54G CLI for control and monitoring.

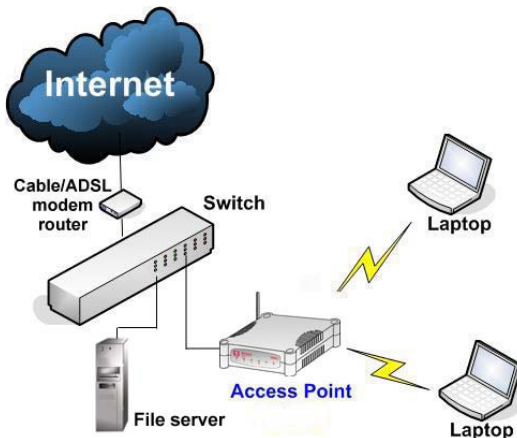
WHEN TO USE WHICH MODE

The access point is versatile in the sense that it may operate in six different types of modes: **Access Point Mode**, **Client Mode**, **Wireless Routing Client**, **Gateway Mode**, **Wireless Adapter Mode**, **Transparent Client Mode** and **Repeater Mode**.

This section presents a brief outline of the different network applications that can be accommodated through the different modes of the access point.

ACCESS POINT MODE

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



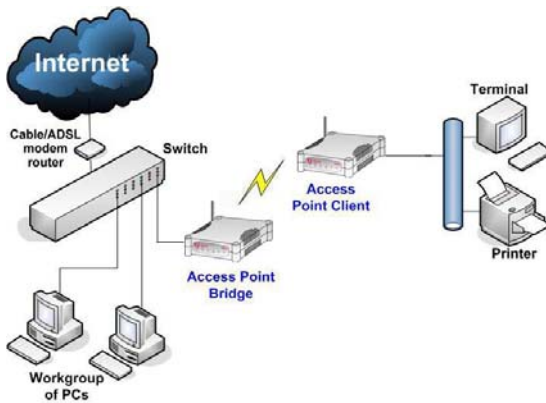
In the example above, the wireless users will be able to access the file server connected to the switch through the access point in **Access Point** mode.

ACCESS POINT CLIENT MODE

In **Access Point Client** mode, the device acts as a wireless client.

When connected to an access point, it will create a network link between the Ethernet network connected at this client device, and the wireless and Ethernet network connected at the access point.

In this mode it can only connect with an access point. Other wireless clients cannot connect with it directly unless connected to the same access point - allowing them to communicate with all devices connected at the Ethernet port of the WP54G.



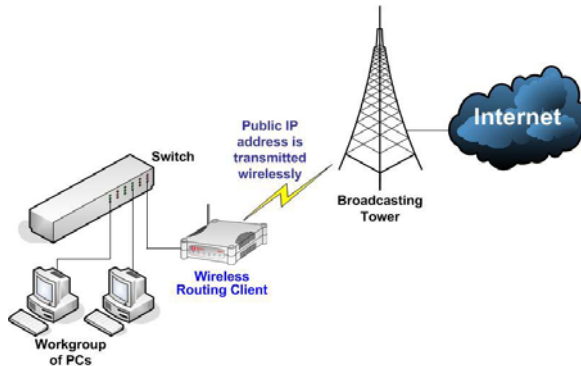
In the example above, the workgroup PCs will be able to access the printer connected to the access point in **Access Point Client** mode.

Optional additional feature:

Point-to-Point connection in this operation mode is also supported if you specifically wish to connect with an AP only. Please refer to Point-to-Point setup section.

WIRELESS ROUTING CLIENT MODE

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



The above illustration describes how this mode operates.

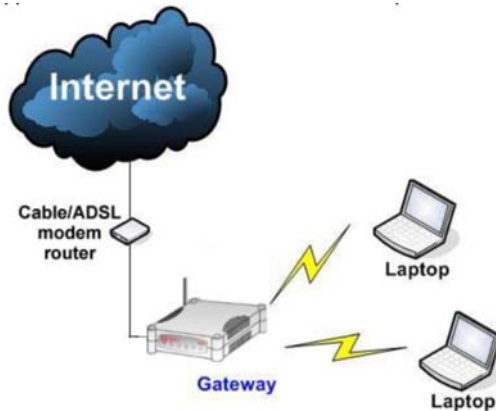
Optional additional feature:

Point-to-Point connection in this operation mode is also supported if you specifically wish to connect with an AP only. Please refer to Point-to-Point setup section.

GATEWAY MODE

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

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



Static IP address

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

Dynamic IP address

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

This type of connection applies for instance to:

- Singapore Cable Vision subscribers
- @HOME Cable Service users

PPP over Ethernet (PPPoE)

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

For instance if you are using:

T-1 connection in Germany or

SingNet Broadband or Pacific Internet Broadband in Singapore.

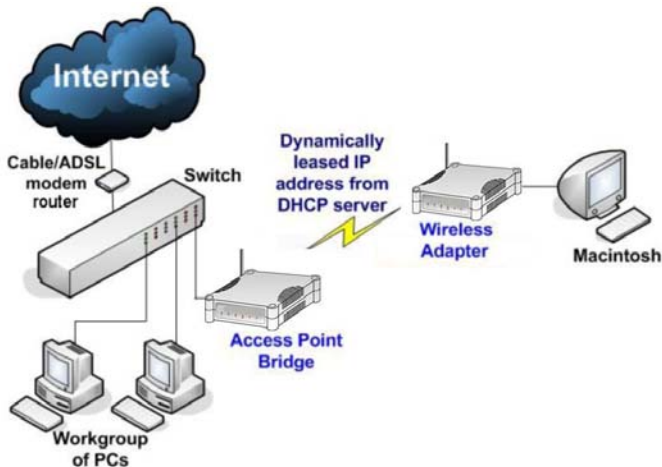
PPTP

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

WIRELESS ADAPTER MODE

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

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



Optional additional feature:

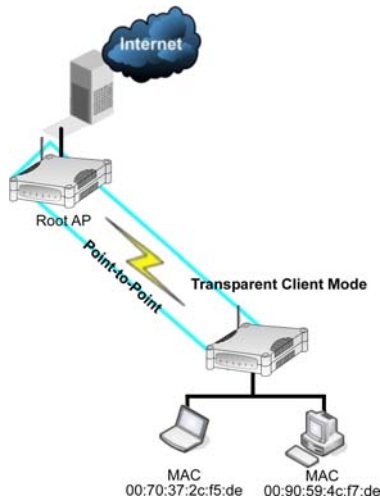
Point-to-Point connection in this operation mode is also supported if you specifically wish to connect with an AP only. Please refer to Point-to-Point setup section.

TRANSPARENT CLIENT MODE

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

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

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

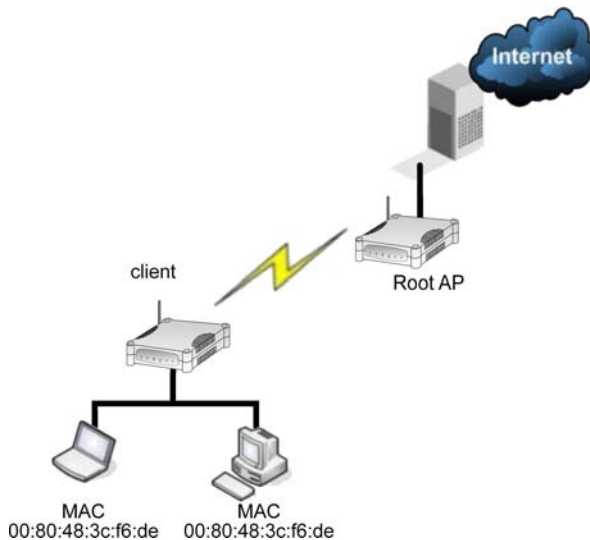


- Current CompeX model that provide RootAP support are: WP54x series; WPP54x series; WP18; and NP18A.
For newer models, please contact your CompeX supplier or visit the CompeX web site.

Difference Between other client modes and Transparent Client Mode

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

Transparent Client Mode is more transparent, making it more suitable for linking two networks as point-to-point, or point-to-multi-point network connection.

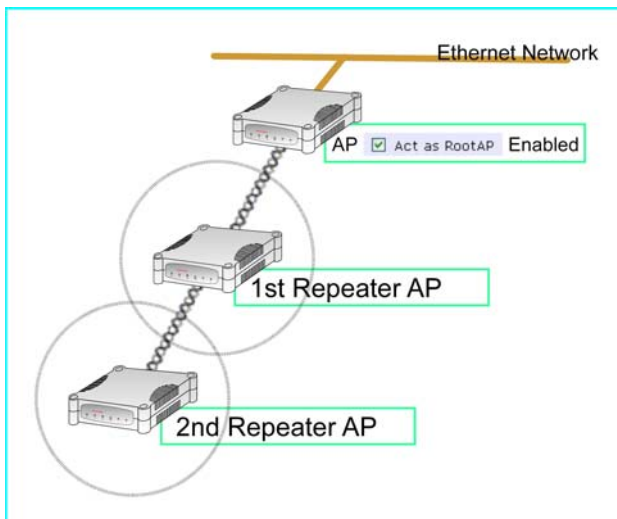


REPEATER MODE

The access point has a built-in **Repeater Mode** to extend the range and greatly enhance the performance of the wireless network by allowing communications over much greater distances.

In **Repeater Mode**, the access point regenerates network signals to extend the range of the existing network infrastructure. It receives and retransmits signals. This allows it to act as a relay for signals on the network.

For more information on the Repeater Mode operation mode, please refer to the Repeater Setup section.



Chapter 2: Hardware Installation

SETUP REQUIREMENTS

Before starting, please verify that the following is available:

- CAT5/5e networking cable
- At least one computer is installed with a Web browser and a wired or wireless network interface adapter
- TCP/IP protocol is installed and IP address parameters are properly configured on all your network's nodes

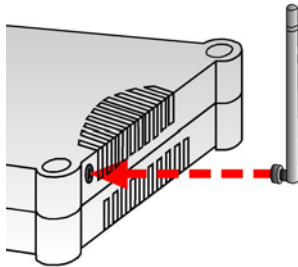
HARDWARE INSTALLATION

The access point can be powered using either the power adapter provided or a PoE Injector. The installation process for both options is described below.

OPTION ONE: USING POWER ADAPTER TO SUPPLY POWER TO THE UNIT

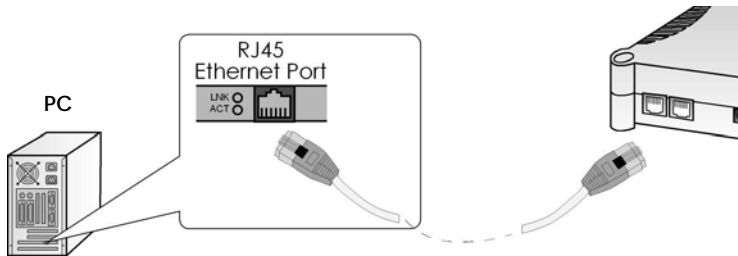
Step 1:

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



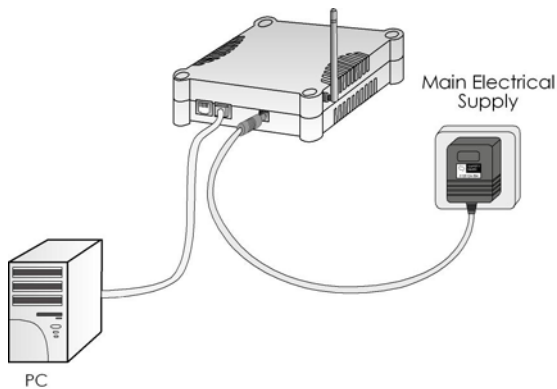
Step 2:

Insert one end of the Ethernet cable to any of the Ethernet ports 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.

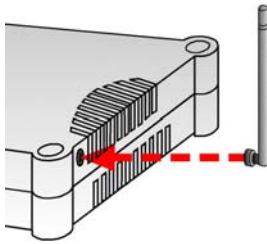
OPTION TWO: USING PoE TO SUPPLY POWER TO THE UNIT

The access point is fully compatible with a Power-Over-Ethernet (PoE) kit. A PoE accessory supplies operational power to the wireless AP via the Ethernet cable connection.

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

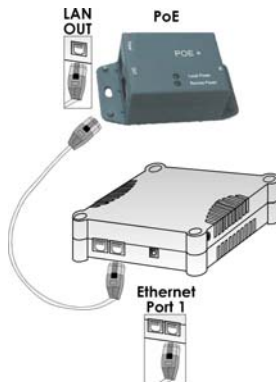
Step 1:

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



Step 2:

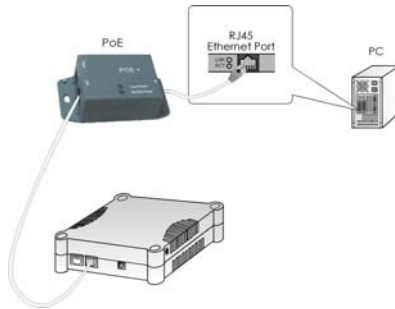
Use an RJ45 Ethernet cable to connect one end of the cable to the LAN OUT port of the Injector and the other end to Ethernet port 1 of the access point.



Step 3:

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

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

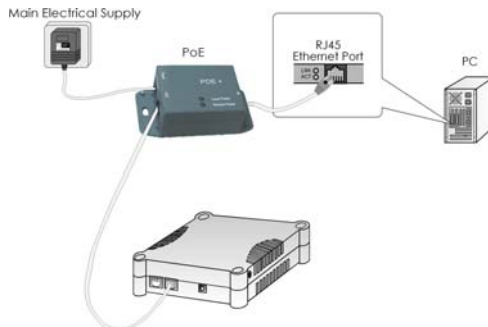


Step 4:

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

Note:

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



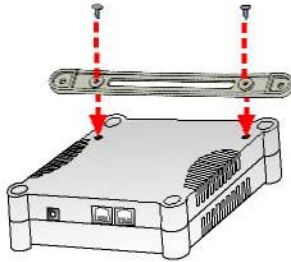
Step 5:

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

OPTIONAL: MOUNTING ON THE WALL

Step 1:

Screw the mount onto the unit.



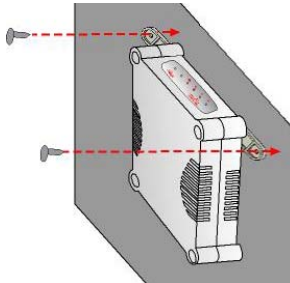
Step 2:

Align the unit and mount to the wall.

Use the mount as a guide, make 2 marks and drill 2 holes into the wall.

Step 3:

Next, secure the unit and mount to the wall.



Chapter 3: Access to Web-based Interface

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

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

ACCESS TO THE WEB INTERFACE WITH UCONFIG

Complex has developed a powerful uConfig utility that has been designed to give you direct access to the Web interface.

Step 1:

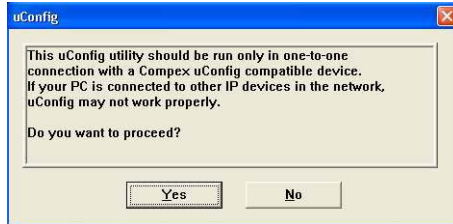
Insert the Product CD into your CD-ROM drive. The CD will run automatically.

Step 2:

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

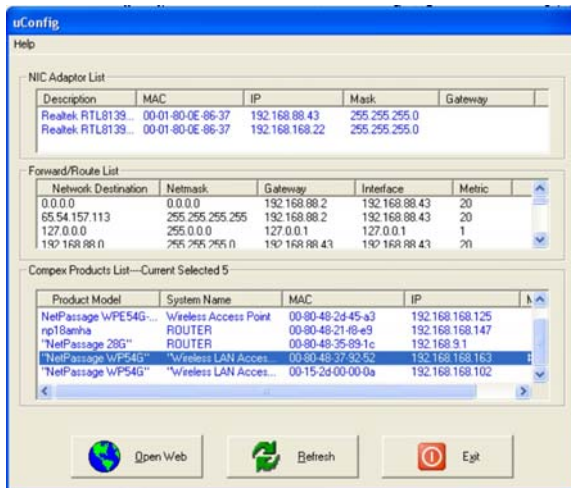
Step 3:

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



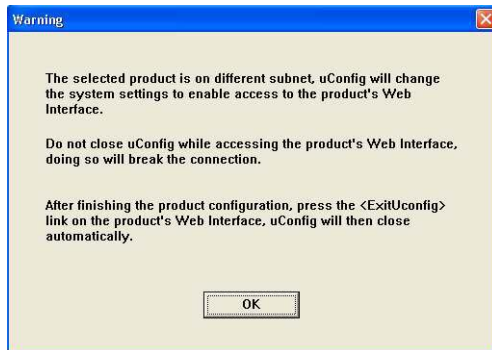
Step 4:

Select **WP54G** in the **Complex Products List** section and click on the **Open Web** button. To retrieve and display the latest device(s) in the list, click on the **Refresh** button.



Step 5:

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



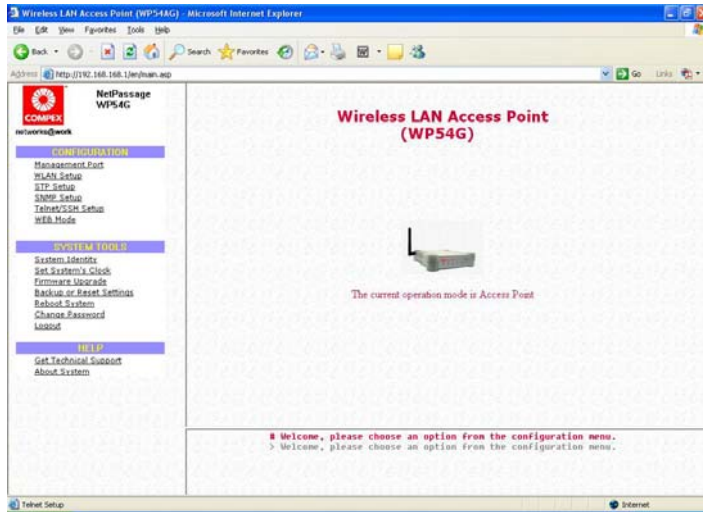
Step 6:

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



Step 7:

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



MANUAL ACCESS TO WEB-BASED INTERFACE VIA INTERNET EXPLORER

EXPLORER

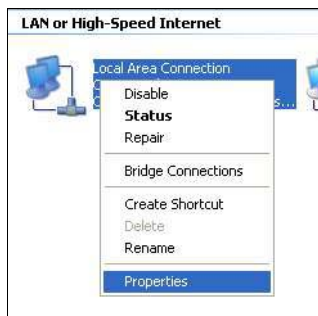
For this method, you need to assign an IP address to your PC so that it belongs to the same subnet as your access point. In this example, we are using Windows XP for illustration. For Windows 98/98SE/2000/NT/ME, kindly refer to **Appendix II "TCP/IP Configuration"**.

Step 1:

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

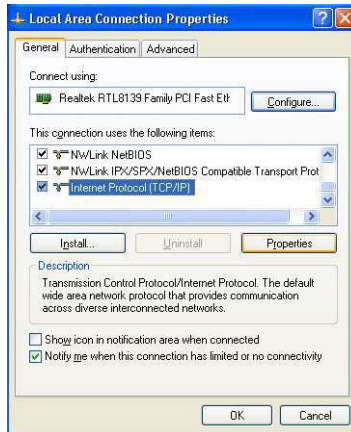
Step 2:

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



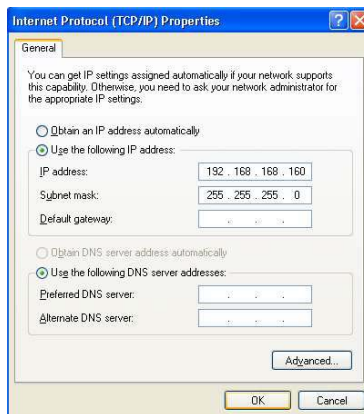
Step 3:

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



Step 4:

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

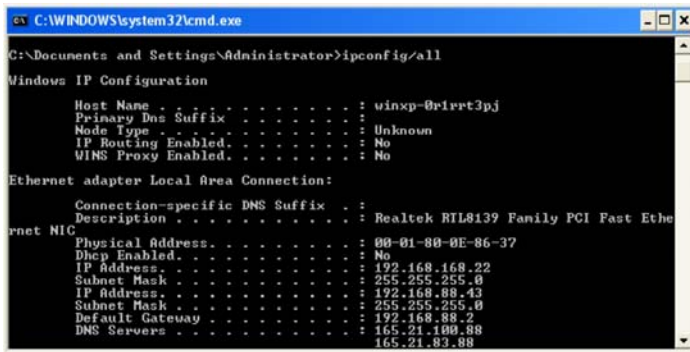


Step 5:

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

Step 6:

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



Your PC is now ready to configure your access point.

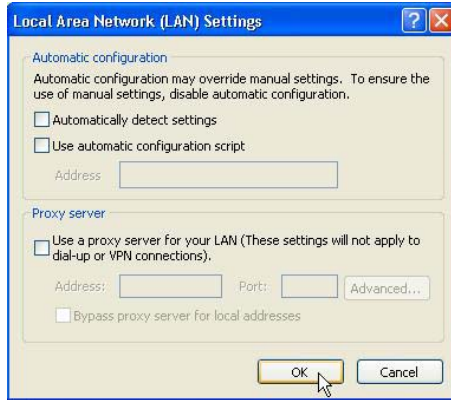
Step 7:

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



Step 8:

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



Step 9:

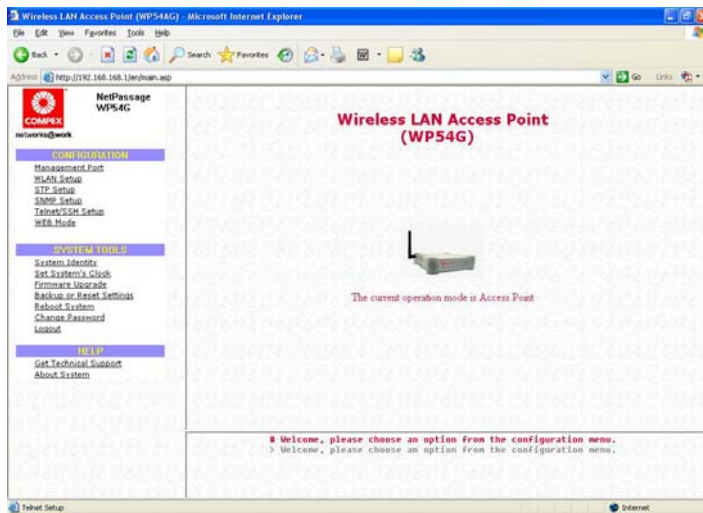
At the **Address** bar, enter `http://192.168.168.1` and press **Enter** on your keyboard.

Step 10:

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



You will then reach the home page of your access point's Web interface.



Chapter 4: Common Configuration

This chapter illustrates the following features, which are available in ALL the operating modes of your access point, unless stated otherwise.

- [Management Port](#)
- [WLAN Basic Setup](#)
- [WLAN Security](#)
- [STP Setup](#)
- [SNMP](#)
- [MAC Filtering](#)
- [Antenna Alignment](#)

MANAGEMENT PORT SETUP

This section shows you how to customize the parameters of your access point to suit the needs of your network. It also explains how to make use of the built-in DHCP server of your access point.

SETTING UP YOUR LAN

You can opt to adjust the default values of your access point and customize them to your network settings.

Step 1:

Click on **Management Port** from the **CONFIGURATION** menu.

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

IP Address:	<input type="text" value="192.168.168.1"/>
Network Mask:	<input type="text" value="255.255.255.0"/>
Management Gateway IP:	<input type="text"/>
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="192.168.168."/>
DHCP Lease Time:	<input type="text" value="3600"/> (seconds)
<input type="checkbox"/> Always use these DNS servers	
Primary DNS IP Address:	<input type="text"/>
Secondary DNS IP Address:	<input type="text"/>
DHCP Server:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Advanced DHCP Server Options

Step 2:

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 192.168.168.1.</p>
Network Mask	<p>The Network Mask serves to identify the subnet in which your Access point resides. The default network mask is 255.255.255.0.</p>
Management Gateway IP	<p>(Optional) As a bridge Access Point, the access point does not usually communicate with devices on other IP subnets. However, the Management Gateway here acts as the equivalent of the Default Gateway of a PC, to allow the access point to communicate with devices on different subnets. For instance, if you want to access the access point from the Internet or from a router on the LAN, enter the router IP address in the Management Gateway IP field.</p> <p>The Management Gateway IP address of your access point is set to nil by default.</p>
<p>The next two fields (DHCP Start IP Address and DHCP End IP Address) 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. The value that you input here should belong to the same subnet as your access point. For example, if the IP address and network mask of your access point are 192.168.168.1 and 255.255.255.0 respectively, the DHCP Start IP Address should be 192.168.168.X, where X can take any value from 2 to 254. It is pre-set to 192.168.168.100.</p>
DHCP End IP Address	<p>This is the last IP address that the DHCP server can assign. It should also belong to the same subnet as your access point. For instance, if the IP address and network mask of your access point are 192.168.168.1 and 255.255.255.0 respectively, the DHCP End IP Address should be 192.168.168.X, where X can take any value from 2 to 254. It is pre-set as 192.168.168.254.</p>

Parameters	Description
DHCP Gateway IP Address	<p>Though usually, the DHCP server also acts as the Default Gateway of the DHCP client, the access point gives you the option 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 to the other LAN through the Default Gateway defined by the DHCP Gateway IP Address.</p> <p>For instance, if the access point is used in Access Point Client mode and 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 can enable the DHCP server of the access point and set the IP address of X as the DHCP Gateway IP Address, the PC will then obtain its IP address from the access point and access the Internet through X.</p>
Always use these DNS servers	Enable this checkbox if you want the access point to only use the DNS server(s) you have specified below.
Primary DNS IP Address	Your ISP usually provides the IP address of the DNS server.
Secondary DNS IP Address	This optional field is reserved for the IP address of a secondary DNS server.
DHCP Server	If you disable the DHCP server, you will need to manually configure the TCP/IP parameters of each computer in your network.

TO VIEW THE ACTIVE DHCP LEASES

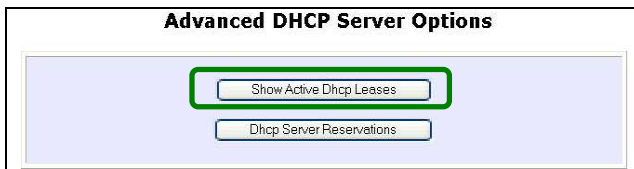
The following will guide you to a page display of the active IP address leases that have been allocated by the built-in DHCP server of Access point.

Step 1:

Click on **Management Port** from the **CONFIGURATION** menu.

Step 2:

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



The **DHCP Active Leases** table displays:

- The **Host Name** of the DHCP client
- The **IP Address** that has been allocated to the DHCP client
- Its **Hardware (MAC) Address**
- 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



NOTE

Invalid date and time displayed in the **Lease Expired Time** column indicates that the clock of your access point has not been properly set. Please refer to the **SYSTEM TOOLS** section for more details on how to set the system clock.

TO RESERVE SPECIFIC IP ADDRESSES FOR PREDETERMINED DHCP CLIENTS

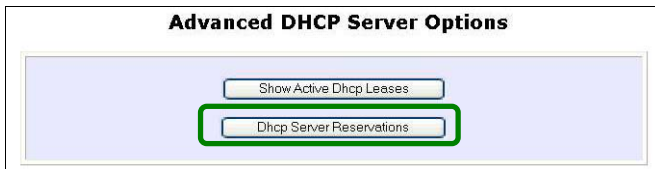
Making an IP address reservation lets you inform the DHCP server to exclude that specific address from the pool of free IP addresses it draws on for dynamic IP address allocation.

For instance, if you set up a publicly accessible FTP/HTTP server within your private LAN, while that server would require 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.

The following shows you how to reserve a particular IP address.

Step 1:

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



Step 2:

Click on **Add** button.



Step 3:

Fill in:

The host portion of the **IP Address** to reserve.

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

Press the **Apply** button to make your new entry effective.

DHCP Server Reservations

IP Address:

Hardware Address: (XX-XX-XX-XX-XX-XX)

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

DHCP Server Reservations

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

DELETE DHCP SERVER RESERVATION

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

Step 1:

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

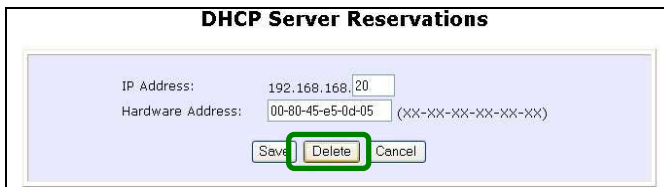


The screenshot shows a window titled "DHCP Server Reservations" containing a table with two columns: "IP Address" and "Hardware Address". The first row contains the values "192.168.168.20" and "00-80-45-e5-0d-05". The IP address cell is highlighted with a green box. Below the table are "Add" and "Back"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

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

Step 2:

Click on the **Delete** button.



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

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

WLAN SETUP

This section shows how to perform the following functions:

Basic:

This function performs a basic setup of operation modes.

Security:

This function performs data encryption and protection for the access point.

Kindly refer to Chapter 5 on **WLAN Security** for details.

Advanced:

This function furthers the basic configuration of the access point by setting the system's additional parameters: **Virtual AP** and **Long Distance Parameters**.

Kindly refer to Chapter 6 on **Wireless Extended Features** for details.

Statistics:

This function uses the **Scan Feature** to monitor and interpret the statistics data collected.

MAC Filtering (only applicable to Access Point and Repeater modes):

MAC Filtering acts as a security measure by restricting the users accessing to the network through their MAC address.

Antenna Alignment:

It is a tool for aligning outdoor antenna between 2 access points over long distances. The signal level can be checked from the web page and also from the DIAG LED indicator.

TO CONFIGURE THE BASIC SETUP OF THE WIRELESS MODE

The following will guide you to configure the basic setup of the wireless mode you have selected.

Step 1:

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

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

WLAN Basic Setup

Card Status	enable
The Current Mode	Access Point <input type="button" value="Change"/>
ESSID	<input type="text" value="sampleRouter"/>
Wireless Profile	802.11a
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect <input type="button" value="Channel Survey"/>
Tx Rate	Fully Auto

Closed System
 Act as RootAP
 VLANID

Step 2: (Optional: Change Current mode)

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

WLAN Operation Mode

Operation Mode

APP

- Wireless Routing Client
- Access Point Mode
- Client Mode
- Wireless Routing Client
- Gateway Mode
- Wireless Adapter Mode
- Transparent Client Mode
- Repeater Mode

Step 3:

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

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

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

WLAN Basic Setup

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

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


WLAN Basic Setup

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

This table describes the parameters that can be modified in the **WLAN Basic Setup** page.

Parameters	Description
The Current Mode	<p>The default operating mode of the access point is the Access Point mode. The access point can operate in 6 modes:</p> <ul style="list-style-type: none">• Access Point Mode• Client Mode• Wireless Routing Client• Gateway Mode• Wireless Adapter Mode• Transparent Client Mode• Repeater Mode <p>You can toggle the mode by clicking on the Change button.</p>
ESSID	<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>
Site Survey	<p>A list of wireless devices that are detected by your access point in the WLAN. Information such as MAC address, channel, SSID, algorithm and signal strength can be found in the listing.</p>

Wireless Profile	<p>A selection of network environment types in which to operate the access point:</p> <ul style="list-style-type: none"> • 802.11b only This mode supports wireless B clients with data rates of up to 11Mbps in the frequency range of 2.4GHz. • 802.11b/g mixed This mode supports both wireless B and G clients. • 802.11g only This mode supports wireless-G clients that offer transmission rates of up to 54Mbps in the 2.4GHz frequency band.
Country	<p>Choose the Country where you are located.</p>
Channel	<p>This option allows you to select a frequency channel for the wireless communication. This parameter is only available in the Access Point, Transparent Client, and Repeater modes.</p> <p>Select SmartSelect to automatically scan and recommend the best channel that the access point can utilize.</p>
Tx Rate	<p>Allow you to choose the rate of data transmission from 1Mbps to Fully Auto.</p>
Closed System	<p>The access point will not broadcast its WLAN name (ESSID) when Closed system is enabled. By default Closed system is disabled.</p>

<p>Act as RootAP</p>	<p>The access point will connect with one or multiple clients to create a point-to-point and point-to-multi-point connections network with 2 or more APs.</p> <p>This connection method is fully compliant with 802.1h standards.</p> <hr/> <p> NOTE A Repeater AP can connect to an AP only if the option <input checked="" type="checkbox"/> Act as RootAP is set or checked in the AP setup.</p> <p>Similarly, if a second Repeater AP is to be connected to this first Repeater AP to extend the distance and coverage further, the option <input checked="" type="checkbox"/> Act as RootAP on the first Repeater AP must be set or checked before this second Repeater AP can connect to it.</p>
<p>VLANID</p>	<p>Select and specify the VLANID. This is a number to identify the different virtual network segments to which the network devices are grouped. This can be any number from 1 to 4094.</p>
<p>Channel Survey</p>	<p>A list of channels that are detected by your access point in the WLAN. Information such as frequency, channel, MyQuality, NeighQuality, APCount and Recommendation can be found in the listing.</p> <p>The Access Point and Gateway modes support this feature.</p>

SCAN FOR SITE SURVEY

(Only For Client Mode and Wireless Routing Client Mode)

Step 1:

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

The screenshot shows the 'WLAN Basic Setup' page with the following configuration:

- Card Status: enable
- The Current Mode: Client (with a 'Change' button)
- ESSID: sampleRouter (with a 'Site Survey' button highlighted in green)
- Remote AP MAC: [Empty field] (with a checkbox)
- Wireless Profile: 802.11a
- Country: NO_COUNTRY_SET-(NA)
- Tx Rate: Fully Auto

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

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 'Site Survey' results page displays the following table:

Bssid	SSID	Chan	Auth	Alg	Signal
<input type="radio"/> 008048003472	PMD-28G-Online	6	WPA-PSK	TKIP	8
<input type="radio"/> 008048015403	wp54-1C	1	RSN-PSK	AES	3
<input type="radio"/> 00804830b5bd	wpe-A	6	WPA-PSK	TKIP	3
<input type="radio"/> 00804821f877	np18a-tang	10	WPA-EAP	TKIP	2
<input type="radio"/> 00804835891e		10	OPEN	NONE	22
<input type="radio"/> 00804800348d	OMEGA1	8	OPEN	NONE	9
<input type="radio"/> 00804800345d	complex-np28g-with-superg-supergg	7	OPEN	NONE	5
<input type="radio"/> 00804824c675	Any	3	OPEN	NONE	3
<input type="radio"/> 008048358861	complex-np28g	6	OPEN	NONE	7

Buttons: Apply, Refresh, Back

Step 2:

To connect the WP54G-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 this screen.

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

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



NOTE

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

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

SHOW LINK INFORMATION

(Only For Client Mode and Wireless Routing Client mode)

Step 1:

To view the connection status when WP54G-client is linked to another access point, click on the **Show Link Information** button.

WLAN Basic Setup

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

Link Information

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

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

This table describes the parameters that can be viewed from the [Link Information](#) page.

Parameters	Description
State	Refers to the MAC address of the BSS (AP to which the WP54G-client is connected).
Current Channel	The channel that is being presently used for transmission.
Tx Rate	The rate of data transmission in Mbps.
Signal Strength	Given in percentage, showing the intensity of the signal received.

SCAN FOR CHANNEL SURVEY

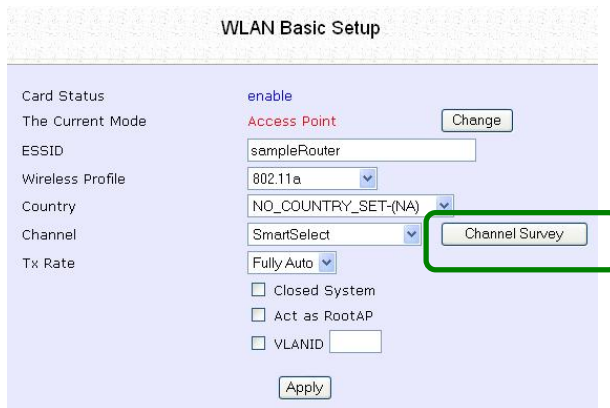
(available For Access Point Mode and Gateway Mode)

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

When the users want to scan for and find the best channel, they can use **Channel Survey**.

Step 1:

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



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

Field	Value
Card Status	enable
The Current Mode	Access Point (with a 'Change' button)
ESSID	sampleRouter
Wireless Profile	802.11a
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect
Tx Rate	Fully Auto

Below the Channel field, there are three checkboxes: 'Closed System', 'Act as RootAP', and 'VLANID' (with an empty input field). An 'Apply' button is at the bottom. A 'Channel Survey' button is highlighted with a green box.

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

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

The values indicate the level of interference.
 The higher the value, the higher the interference.
 If the value is zero, there is no interference.

Step 5:

To connect the WP54G-client to one of the channels detected, select the radio button corresponding to the channel you want to connect to.

Step 6:

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

Step 7:

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

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

Parameters	Description
Freq	Refers to the frequency of the channel at which your access point is operating.
Channel	Refers to the channel of the access point being used for transmission depending on its origin of country.
MyQuality	Indicates the interference level of the respective channel with this AP. The lower the value, the less interference.
APCount	Refers to the total number of access points operating at the current channel.
NeighQuality	Indicates the interference level with those discovered APs at those respective channels. The lower the value, the less interference.
Recommendation	Indicates the best channel for the AP device to use in its current environment.

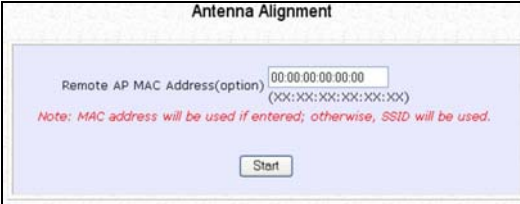
ANTENNA ALIGNMENT

(available For All Modes)

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

Step 1:

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

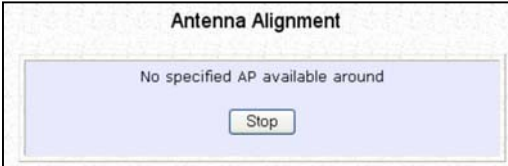


The screenshot shows the 'Antenna Alignment' configuration page. At the top, the title 'Antenna Alignment' is centered. Below it, there is a text input field labeled 'Remote AP MAC Address(option)' with the value '00:00:00:00:00:00' entered. Below the input field, the format '(XX:XX:XX:XX:XX:XX)' is shown in smaller text. 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 of the page, there is a 'Start' button.

Step 2:

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

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



The screenshot shows the 'Antenna Alignment' status screen. At the top, the title 'Antenna Alignment' is centered. Below it, the text 'No specified AP available around' is displayed. At the bottom center of the page, there 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 make sure that the correct SSID is entered. If more than one access point (AP) share the same SSID, the **Antenna Alignment** tool will show the strongest signal AP.

The DIAG LED indicates the signal strength as described below:

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



NOTE

The signal strength of below RSSI of 10 is not recommended for outdoor long distance connection.



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

TO CONFIGURE THE SECURITY SETUP OF THE WIRELESS MODE

Kindly refer to Chapter 5 on **WLAN Security** for details on setting the different security modes of the access point.

TO CONFIGURE THE ADVANCED SETUP OF THE WIRELESS MODE

The following will guide you to configure the advanced setup of the wireless mode you have selected.

Step 1:

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

Step 2:

In the **WLAN Advanced Setup** page, enter the parameters.

Step 3:

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

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	
Radio Off When Ethernet Link Down	<input type="checkbox"/>	
Antenna Control	Auto	

Apply

Extended Features

Wireless Pseudo VLAN WDS Configuration

Long Distance Parameters

This table describes the parameters that can be modified in the **WLAN Advanced Setup** page.

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

Radio Off When Ethernet Link Down	The Radio Off When Ethernet Link Down function detects when the Ethernet link is down and disables the radio card automatically.
Antenna Control	The Antenna Control function allows you to control whether to use the: <ul style="list-style-type: none">• Main antenna• Aux (auxiliary) antenna• Auto (Default), to monitor the signal from each antenna and automatically switch to the one with better signal



NOTE

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

STATISTICS

The following shows you the information on the wireless device that is connected to the WLAN.

IN ACCESS POINT MODE

Step 1:

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

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

Step 2:

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

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

Step 3:

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

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

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

IN CLIENT MODE

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

00:80:48:37:86:dd Statistics						
Authentication Type			Encryption			
Open-System			No			
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	2122	0	0
Transmit	0	0	0	11	0	0
<input type="button" value="Back"/>						

In **Client** mode, you are not allowed to view other wireless clients' statistics. To view other wireless clients information, you need to change to Access Point mode.

IN WIRELESS ROUTING CLIENT, WIRELESS ADAPTER, AND TRANSPARENT CLIENT MODES

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

00:80:48:37:91:9d Statistics						
Authentication Type				Encryption		
Open-System				No		
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	1056	0	0
Transmit	0	0	0	12	0	0
<input type="button" value="Back"/>						

IN GATEWAY MODE

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

00:80:48:37:91:9d Statistics						
Authentication Type			Encryption			
Open-System			No			
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	1056	0	0
Transmit	0	0	0	12	0	0
<input type="button" value="Back"/>						

To view the statistics information if a wireless client connected to the AP, click on the MAC address of that client.

IN REPEATER MODE

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

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

Repeater WLAN Statistics

Local Connection List

ID	MAC Address	RSSI	TxRate
AP	00:80:48:3d:0f:81	-	-

Remote Connection Status

Freq.(No.)	MAC Address	RSSI	TxRate	State
0M (0)	06:80:48:3d:0f:81	0		Scanning

To check the details on individual wireless client, click on the MAC Address in the lists.

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

06:80:48:3d:0f:81 Statistics

Authentication Type		Encryption				
Open-System		No				
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	3601	0	0
Transmit	0	0	0	6116	0	0

WAN SETUP

(only supported by Wireless Routing Client and Gateway)

A correct **WAN Setup** allows you to successfully share your Internet connection among the wired and wireless clients of the access point. To do so, you need to identify the type of broadband Internet access you are subscribed to. If you are using:

- **Cable Internet where the ISP dynamically assigns a WAN IP address** to you, refer to WAN Setup - Cable Internet with Dynamic IP Assignment.
- **Cable Internet where your ISP provides you with a fixed WAN IP address** (or a range of fixed IP addresses), refer to WAN Setup - Cable Internet with Static IP Assignment.
- **ADSL Internet that requires standard PPP over Ethernet (PPPoE)** for authentication, refer to WAN Setup - ADSL Internet using PPP over Ethernet (PPPoE).
- **ADSL Internet that requires standard Point-to-Point Tunneling Protocol (PPTP)** for authentication, refer to WAN Setup - ADSL Internet using Point to Point Tunneling Protocol (PPTP).

WAN Setup - Cable Internet with Dynamic IP Assignment

The access point is pre-configured to support a WAN type that dynamically obtains an IP address from the ISP. However, you may verify the WAN settings with the following steps:

Step 1:

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

Step 2:

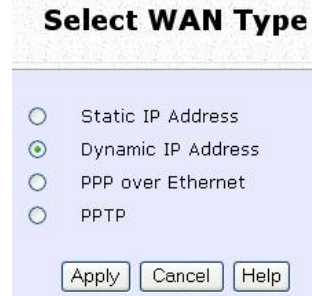
On the **WAN Dynamic Setup** screen that follows, verify that the **WAN Type** reads **Dynamic (DHCP)** in red colour. Otherwise, click on the **Change** button.

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

Step 3:

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

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



Note:

Additional configuration might be required before your ISP will allocate an IP address to the access point.

Certain ISPs require authentication through a DHCP Client ID before releasing a public IP address to you. The access point uses the System Name in the System Identity as the DHCP Client ID.

Therefore, if this is the case, refer to your ISP for the correct DHCP Client ID to be set and follow **steps 4 - 5** to accomplish the setup.

Step 4:

Steps 4 - 5 are for those who need to set up the **System Name** in **System Identity** so that your ISP can authenticate it as a valid DHCP Client ID.

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

Step 5:

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

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



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

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

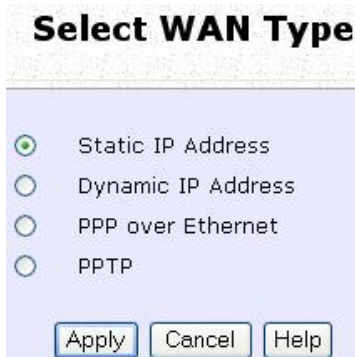
WAN Setup - Cable Internet with Static IP Assignment

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

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

Step 1:

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



Select WAN Type

Static IP Address
 Dynamic IP Address
 PPP over Ethernet
 PPTP

Apply Cancel Help

Step 2:

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

Step 3:

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

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



WAN Static Setup

WAN Type: Static Change

IP Address: 203.120.12.240

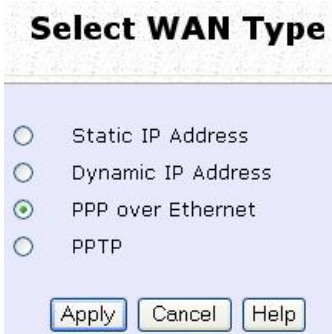
Network Mask: 255.255.255.0

Gateway IP Address: 203.120.12.2

Apply Help

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

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



Select WAN Type

Static IP Address

Dynamic IP Address

PPP over Ethernet

PPTP

Step 3:

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

Step 4:

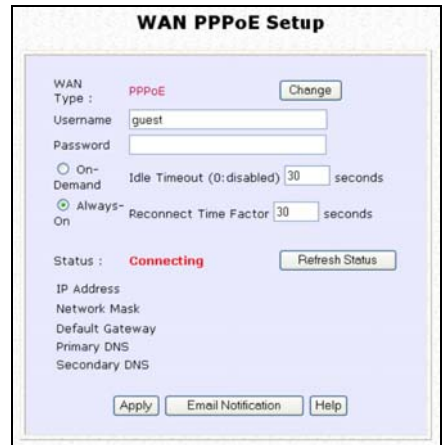
Select **Always-On** if you want your access point to always maintain a connection with the ISP. Otherwise, you may select **On-Demand**. The access point will then connect to the ISP automatically when it receives Internet requests from the PCs in your network.

Step 1:

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

Step 2:

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



WAN PPPoE Setup

WAN Type : **PPPoE**

Username

Password

On-Demand Idle Timeout (0:disabled) seconds

Always-On Reconnect Time Factor seconds

Status : **Connecting**

IP Address
Network Mask
Default Gateway
Primary DNS
Secondary DNS

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

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**.

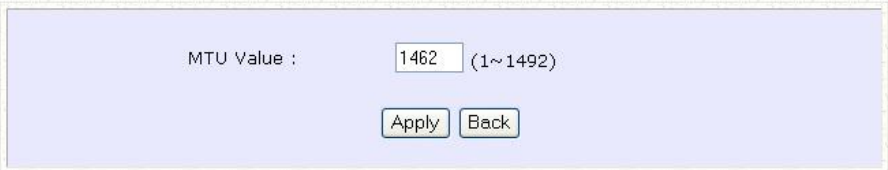
Advanced WAN Options



The **MTU Value** has a range of 1 to 1492.

Enter the **MTU Value** and click **Apply**.

MTU Setup

A screenshot of a web interface titled "MTU Setup". It shows a light blue rectangular area containing the text "MTU Value :". To the right of this text is 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".

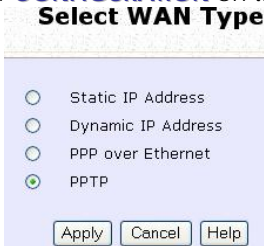
WAN Setup – ADSL Internet using PPTP

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

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

Step 1:

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



Select WAN Type

Static IP Address
 Dynamic IP Address
 PPP over Ethernet
 PPTP

Apply Cancel Help

Step 2:

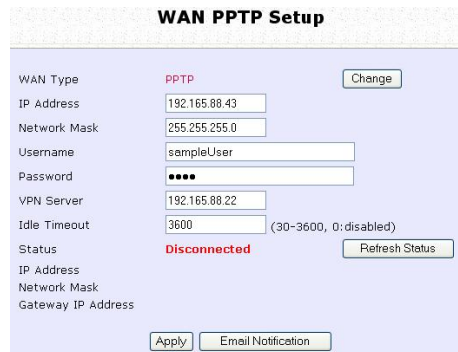
Access the **Select WAN Type** page and choose **PPTP** before clicking the **Apply** button. You will then be brought to the following page requiring your inputs.

Step 3:

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

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

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



WAN PPTP Setup

WAN Type: PPTP (Change)

IP Address: 192.165.88.43

Network Mask: 255.255.255.0

Username: sampleUser

Password: ****

VPN Server: 192.165.88.22

Idle Timeout: 3600 (30-3600, 0: disabled)

Status: Disconnected (Refresh Status)

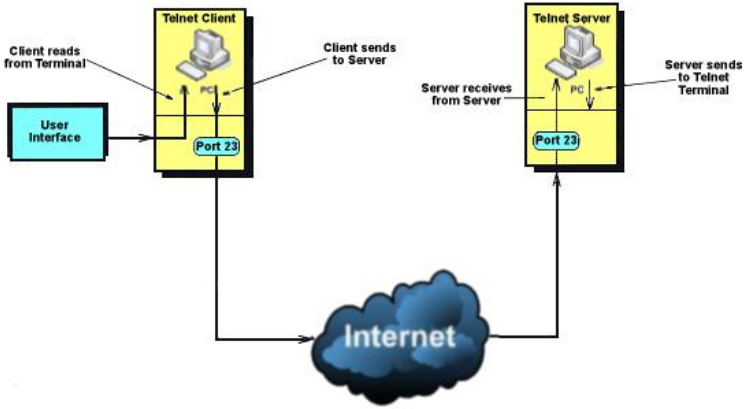
IP Address

Network Mask

Gateway IP Address

Apply Email Notification

TELNET/SSH SETUP



Telnet allows a computer to remotely connect to the WP54G CLI (Command Line Interface) for control and monitoring.

SSH (Secure Shell Host) establishes a secure host connection to the WP54G CLI for control and monitoring.

Telnet/SSH Setup

1

Click [Telnet/SSH Setup](#) from the **CONFIGURATION** menu.

2

1. To enable Telnet Server: Select Telnet Server Enable and enter the Port Number.
2. To enable SSH server: Select SSH Server Enable and enter the Port Number.

Click [Apply](#).

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"/>

3

To add user:

1. Click Add button.

User Management

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

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

3. Click Apply.

Add User Entry

User Name

Password

Permission

To Delete User:

1. Select which user to Delete.
2. Click Delete.

User Management

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

User Management list refreshes to update users.

To Refresh User Management list:

Click Refresh to refresh User Management list.

User Management

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

TELNET COMMAND LINE INTERFACE

Telnet CLI (Command Line Interface)

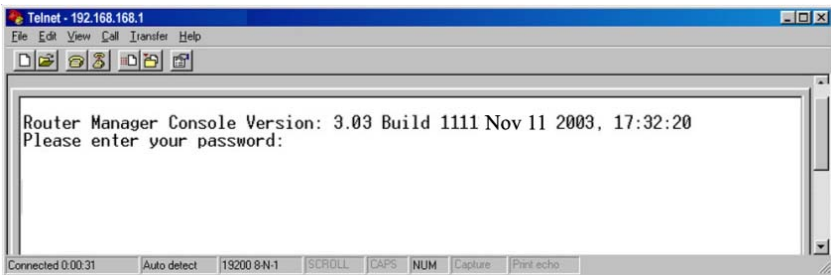
The user may connect to the CLI (Command Line Interface) via a TELNET session to the default IP, **192.168.168.1**. This section uses Microsoft TELNET command for instruction. You may use any TELNET client.

Connecting to CLI (Command Line Interface) via TELNET

1. Connect to CLI (Command Line Interface) with the following command at DOS prompt. The TELNET application will then be launched and connected.

C:\WINDOWS\TELNET 192.168.168.1

2. At the login prompt, type in “password” (default password) and press the <ENTER> key, as shown in Figure 2.4c. You will then login to the CLI.



NOTE

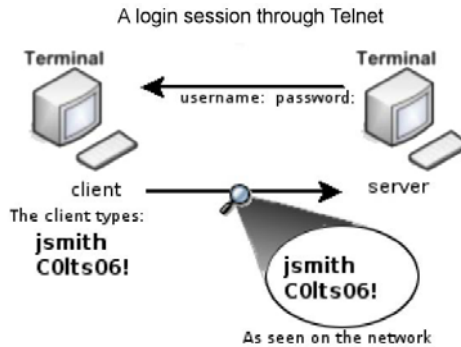
Please refer to Appendix IV for the list of commands available at the console.

SECURE SHELL HOST COMMAND LINE INTERFACE

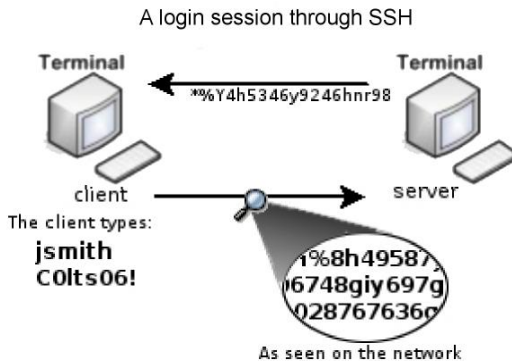
SSH CLI (Secure Shell Host Command Line Interface)

SSH is designed and created to provide the best security when accessing another computer remotely. Not only does it encrypt the session, it also provides better authentication facilities and features that increase the security of other protocols. It can use different forms of encryption and ciphers.

The first diagram below shows a telnet session.



The second diagram below shows how an encrypted connection like SSH is not viewable on the network. The server still can read the information, but only after negotiating the encrypted session with the client.



SSH CLI has a command line interface like shown below for example.

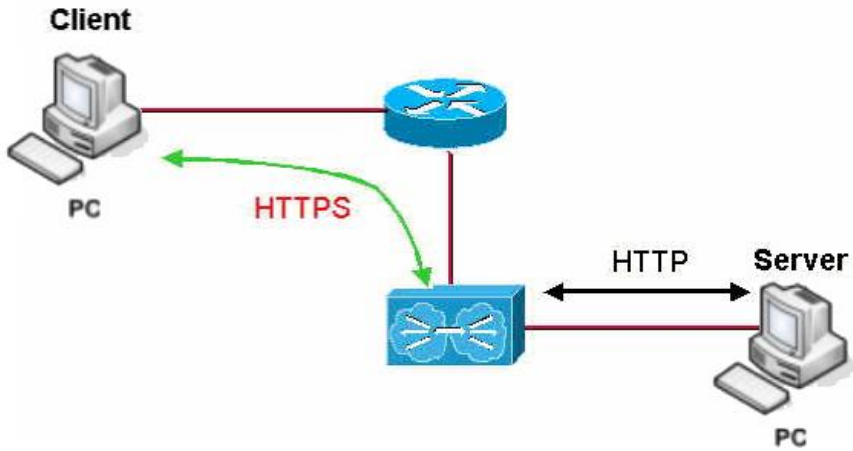
```
Generating public/private dsa key pair.  
Enter file in which to save the key (/home/localuser/.ssh/id_dsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/localuser/.ssh/id_dsa.  
Your public key has been saved in /home/localuser/.ssh/id_dsa.pub.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



NOTE

Please refer to Appendix V for the list of commands available at the console.

WEB MANAGEMENT SETUP



WP54G supports HTTPS (SSL) in addition to the standard HTTP.

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

Web Management Setup

1

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

2

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

Changes will be effected after reboot.

Web Management Setup

Mode

HTTP HTTPS (SSL)

Apply

SNMP SETUP

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

Step 1:

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



The screenshot shows a window titled "SNMP Setup". Inside the window, there are three fields: "SNMP State" with a dropdown menu set to "Enable", "Read Password" with a masked input field (dots), and "Read/Write Password" with a masked input field (dots). Below these fields is an "Apply" button.

Step 2:

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

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

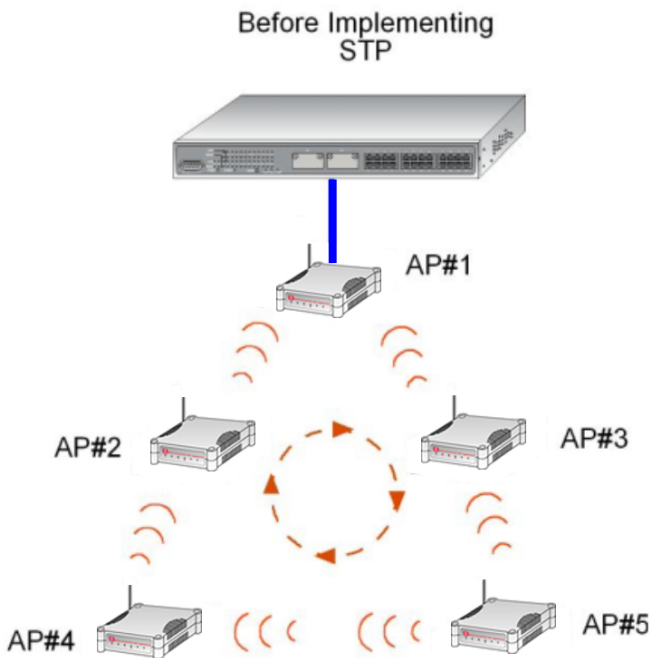
Step 3:

Click on the **Apply** button.

STP SETUP

(Only available in Access Point, Transparent Client, and Repeater Modes)

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

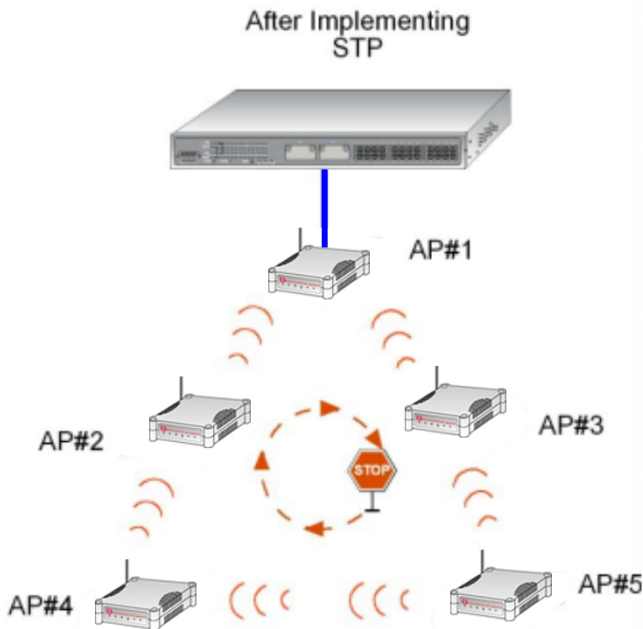


In short, the main purpose of activating STP is to prevent looping when you have redundant paths in the network. Without activating STP, redundant topology will cause broadcast storming.

To establish path redundancy, STP creates a tree that spans all of the devices in an extended network, forcing redundant paths into a standby, or blocked,

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

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



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

To explain the effect of STP on the wireless clients, we will compare 2 separate scenarios.

Scenario #1 – (No STP)

Referring to the illustration below, if the Spanning Tree Protocol (STP) is not implemented in a network, all clients (Notebook#1, #2, #3 & #4,) can access to one another, resulting in low level of data security. Due to the redundant paths found in this network, broadcast packets will be duplicated and forwarded endlessly resulting in a broadcast storm.



Scenario #2 – (With STP)

When STP is enabled, extra redundant network paths between APs will be disabled, hence preventing multiple active network paths in-between any two APs.

If one of the APs is down, the STP algorithm will reactivate one of the redundant paths so that the network connection will not be lost.

All wireless users will be able to communicate with each other if they are associated to the APs that are in the same zone.



Step 1:

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

Step 2:

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

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

This is the relative priority.

The lowest priority will be elected as the root.

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

This is the hello time.

Every (this number) seconds, a hello packet is sent out by.

Hello packets are used to communicate information about the topology throughout the entire STP network.

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

The forward delay is the time that is spent in the listening and learning state.

Max Age: (Default: 20, Range: 6 – 40)

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

Spanning Tree Protocol Setup

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

MAC FILTERING

MAC Filtering acts as a security measure by controlling the users accessing to the network through their MAC address. Each WLAN or radio card supports up to 16 virtual access points and has its own MAC address listing. The client MAC addresses entries can be set apply to all, or to only selected virtual access points.



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

ADD A MAC ADDRESS TO THE MAC ADDRESS LIST.

Step 1:

Select **MAC Filtering** from **WLAN Setup(a/b/g)**.
 MAC Address Filtering page displays.

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

Status	Policy
Enable ▾	Accept ▾

MAC Filtering set to **Enable** with Policy to **Accept** only the MAC addresses in the MAC Filter Address List and deny all other MAC addresses.

Status	Policy
Enable ▾	Deny ▾

MAC Filtering set to **Enable** with Policy to **Deny** all the MAC addresses in the MAC Filter Address List and accept all other MAC addresses.

Status	Policy
Disable ▾	Accept ▾

MAC Filtering set to **Disable**. Whether Policy is set to **Enable** or **Deny** does not matter.

Status	Policy
Disable ▾	Deny ▾

MAC Filtering set to **Disable**. Whether Policy is set to **Enable** or **Deny** does not matter.

Click **Edit**.
 (This displays the MAC Address List of individual virtual access points.)

MAC Address Filtering

Radio 1 MAC Filtering Options :

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

[View Complete MAC List](#)

(All changes will take effect after reboot)

Step 2:

MAC Filter Address List page displays.

Click the **Add** button.

MAC Filter Address List

MAC Address List
ESSID: "sampleRouter"

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

(All changes will take effect after reboot)

Step 3:

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 in the range 0-9 or a-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 AP.

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(a/b/g)**.
MAC Address Filtering page displays.

Click **View Complete MAC List**.
(This displays the MAC Address List of the radio card.)

MAC Address Filtering

Radio 1 MAC Filtering Options :

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

[View Complete MAC List](#)

(All changes will take effect after reboot)

Step 2:

MAC Filter Address List page displays.

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

Click the **Delete** button.

MAC Filter Address List

MAC Address List
Radio 1

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

(All changes will take effect after reboot)

Step 3:

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

MAC Filter Address List

MAC Address List
Radio 1

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

(All changes will take effect after reboot)

DELETE A MAC ADDRESS FROM INDIVIDUAL ACCESS POINT.

Step 1:

Select **MAC Filtering** from **WLAN Setup(a/b/g)**.
MAC Address Filtering page displays.

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

MAC Address Filtering

Radio 1 MAC Filtering Options :

AP Type	ESSID	Security	MACs	Status	Policy
Main AP	sampleRouter	NONE	Edit	Enable <input type="button" value="v"/>	Accept <input type="button" value="v"/>
Virtual AP	VAP1	NONE	Edit	Disable <input type="button" value="v"/>	Deny <input type="button" value="v"/>
Virtual AP	VAP2	NONE	Edit	Enable <input type="button" value="v"/>	Deny <input type="button" value="v"/>

[View Complete MAC List](#)

(All changes will take effect after reboot)

Step 2:

MAC Filter Address List page displays.

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

Click the **Delete** button.

MAC Filter Address List

MAC Address List
ESSID: "sampleRouter"

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

(All changes will take effect after reboot)

Step 3:

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	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(a/b/g)**.
MAC Address Filtering page displays.

Click **Edit**.

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

[View Complete MAC List](#)

(All changes will take effect after reboot)

Step 2:

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

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

(All changes will take effect after reboot)

Step 3:

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

Click **Save**.

Edit MAC Address

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

Comment

Apply to All

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

Step 4:

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

MAC Filter Address List

MAC Address List
ESSID: "VAP1"

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

(All changes will take effect after reboot)

Chapter 5: WLAN Security

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

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

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

Step 1:

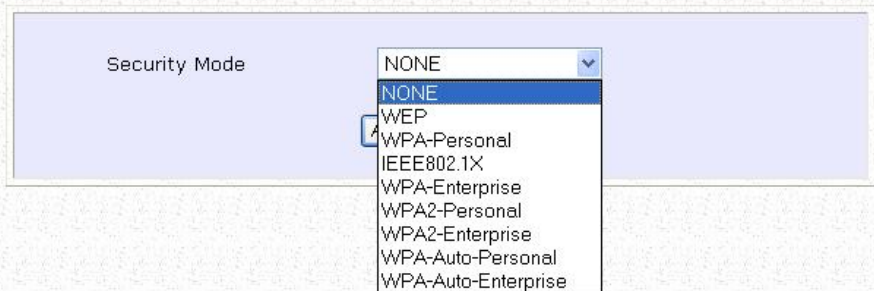
Click on **WLAN Setup** from the **CONFIGURATION** menu to select **Security**.

Step 2:

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

Click on the **Apply** button.

WLAN Security Setup

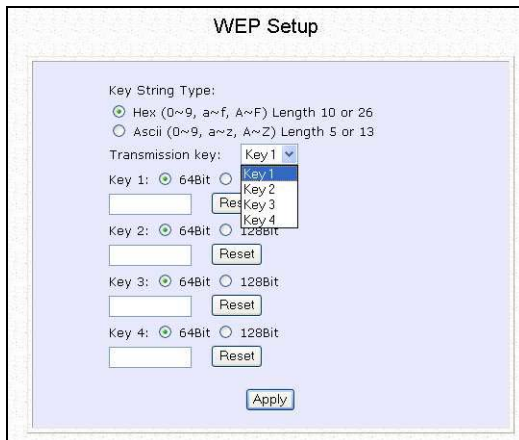


The screenshot shows a configuration page titled "WLAN Security Setup". A light blue box contains the "Security Mode" label and a dropdown menu. The dropdown menu is open, showing a list of security modes: NONE (highlighted in blue), WEP, WPA-Personal, IEEE802.1X, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise, WPA-Auto-Personal, and WPA-Auto-Enterprise.

HOW TO SET UP WEP

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

At the **WEP Setup** page,



The screenshot shows the 'WEP Setup' configuration page. It features a light blue background with the following elements:

- Key String Type:** Two radio button options: 'Hex (0~9, a~f, A~F) Length 10 or 26' (selected) and 'Ascii (0~9, a~z, A~Z) Length 5 or 13'.
- Transmission key:** A dropdown menu currently showing 'Key 1'.
- Key 1:** A radio button for '64Bit' (selected) and '128Bit'. Below it is a text input field and a 'Reset' button.
- Key 2:** A radio button for '64Bit' (selected) and '128Bit'. Below it is a text input field and a 'Reset' button.
- Key 3:** A radio button for '64Bit' (selected) and '128Bit'. Below it is a text input field and a 'Reset' button.
- Key 4:** A radio button for '64Bit' (selected) and '128Bit'. Below it is a text input field and a 'Reset' button.
- Apply:** A button located at the bottom center of the form.

Step 1:

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

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

Step 2:

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

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

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

Step 3:

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

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

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

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

HOW TO SET UP WPA-PERSONAL

(Only available in Access Point and Repeater modes)

The guidelines below will help you to set up the access point for using WPA-Personal. Please follow the steps below if you have activated **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: (60~9999)

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:

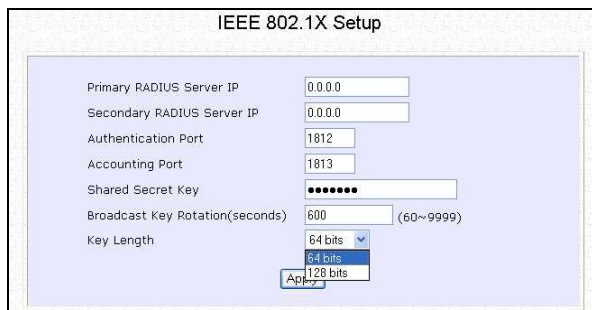
Press the **Apply** button and reboot your system, after which your settings will become effective.

HOW TO SET UP 802.1X/RADIUS

(Only available in Access Point and Repeater modes)

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

At the IEEE 802.1x Setup page,



The screenshot shows the IEEE 802.1X Setup configuration page. The page title is "IEEE 802.1X Setup". The configuration fields are as follows:

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 (dropdown menu)

The dropdown menu for Key Length is open, showing options: 64 bits, 64 bits, and 128 bits. An "Apply" button is visible at the bottom of the dropdown menu.

Step 1:

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

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

Step 2:

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

Step 3:

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

Step 4:

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

Step 5:

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

Step 6:

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

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

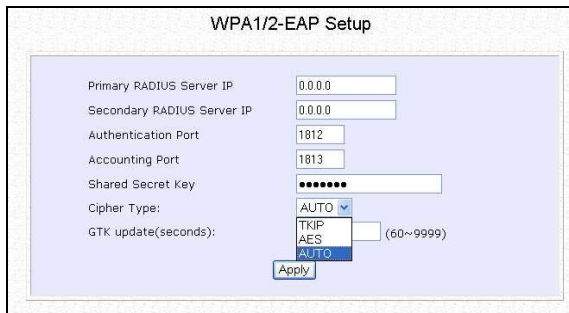
Step 7:

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

HOW TO SET UP WPA ENTERPRISE

(Only Access Point mode supports WPA2-Enterprise and WPA-Enterprise-AUTO)
The guidelines below will help you to set up the access point for using WPA- Enterprise. Please follow the steps below if you have selected the WPA or WPA1- Enterprise, WPA2- Enterprise or WPA- Enterprise -AUTO.

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



WPA1/2-EAP Setup

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

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

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

Step 6:

For WPA-Enterprise

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

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

For WPA2- Enterprise

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

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

For WPA- Enterprise -AUTO

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

Step 7:

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

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

Step 8:

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

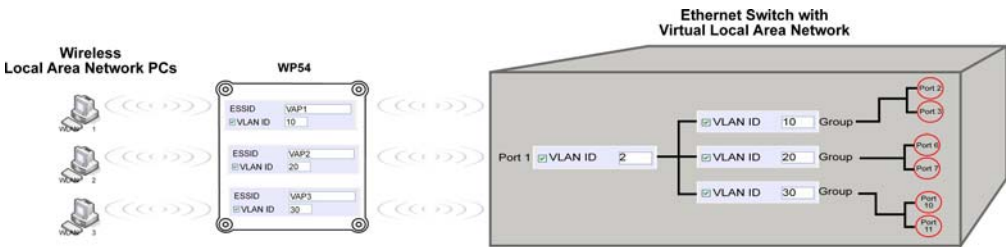
Chapter 6: Wireless Extended Features

This section illustrates how to configure the wireless extended features. To start with, follow the common preliminary steps described below.

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. Follow these steps to setup Virtual AP. Follow these steps to setup Virtual AP.

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

Follow these steps to setup Virtual AP.

Virtual AP

1

1. Click on **WLAN Setup (a/b/g)** from the **CONFIGURATION** menu.
2. Select **Virtual AP**.

Virtual AP List

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

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

(All changes will take effect after reboot)

2

Virtual AP List page displays.

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

Click Add to goto add Virtual AP page.

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.

PREFERRED APs (ONLY 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. Click on **WLAN Setup** from the **CONFIGURATION** menu.
2. Select **Preferred APs**.

Preferred Access Point MAC Address

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

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

LONG DISTANCE PARAMETERS

This setup allows the access point to calculate and display suggested values for certain parameters to use to ensure that wireless communication takes place efficiently and effortlessly between physically distant APs. The following steps demonstrate how to configure the Long Distance Parameters.

Step 1:

From **WLAN Setup** under Configuration, click on **Advanced**, which shows the **WLAN Advanced Setup** page.

Step 2:

Go to the **Extended Features** section, and click on the **Long Distance Parameters** button.

The image shows two screenshots from a network configuration interface. The top screenshot is titled "WLAN Advanced Setup" and contains the following settings:

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	▼
Radio Off When Ethernet Link Down	<input type="checkbox"/>	
Antenna Control	Auto	▼

Below the settings is an "Apply" button.

The bottom screenshot is titled "Extended Features" and contains three buttons: "Wireless Pseudo VLAN", "WDS Configuration", and "Long Distance Parameters".

Step 3:

As illustrated on the **Long Distance Parameters** Setup page, the **Outdoor** feature is disabled by default. Select **Enable** from the pull down menu.

Long Distance Parameters

Outdoor:

Distance(meter):

SlotTime(us):

ACKTimeOut(us):

CTSTimeOut(us):

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.

Step 4:

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 **Show Reference Data**.

Long Distance Parameters

Outdoor:

Distance(meter):

SlotTime(us):

ACKTimeOut(us):

CTSTimeOut(us):

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.

Microsoft Internet Explorer

Recommended slottime: 10 ;acknowdege timeout: 23; cts timeout:23

Step 5:

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

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

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

POINT-TO-POINT & POINT-TO-MULTIPOINT SETUP

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

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

Follow these steps to setup RootAP

RootAP Step 1:

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

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

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

WLAN Basic Setup

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

RootAP Step 2:

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

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

Field	Value
Card Status	enable
The Current Mode	Access Point
ESSID	sampleRouter
Wireless Profile	802.11a
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect
Tx Rate	Fully Auto
Closed System	<input type="checkbox"/>
Act as RootAP	<input checked="" type="checkbox"/>
VLANID	<input type="text"/>

Buttons: Change, Channel Survey, Apply

Follow these steps to setup Transparent Client/s.

Transparent Client Step:

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

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

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

WLAN Basic Setup

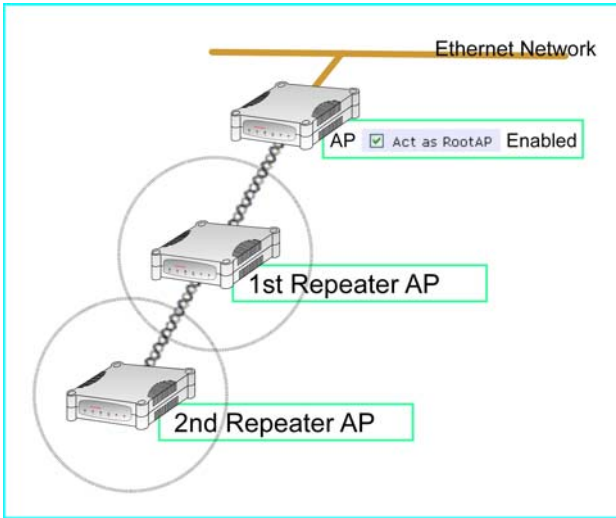
Card Status	enable
The Current Mode	Transparent Client Mode <input type="button" value="Change"/>
ESSID	sampleRouter <input type="button" value="Site Survey"/>
Wireless Profile	802.11a
Country	NO_COUNTRY_SET-(NA)
Tx Rate	Fully Auto

Link Information

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

REPEATER SETUP

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.



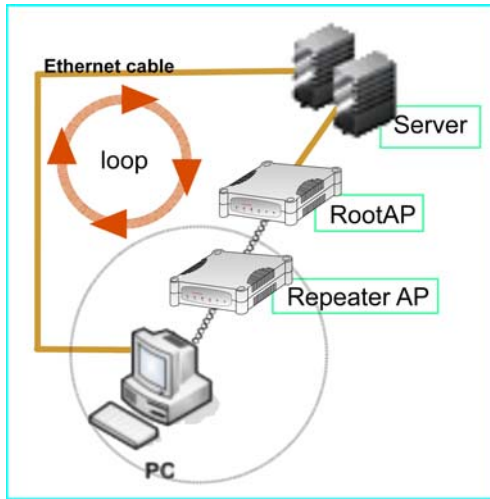
NOTE

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**.

WLAN Basic Setup

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

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. The settings are as follows:

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

Apply

Options for defining the root AP:

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

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

OR

- Enter the **Remote ESSID**.

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

OR

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

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

Click **Apply**.

Chapter 7: Advanced Configuration

ROUTING

(only supported by Wireless Routing Client and Gateway)

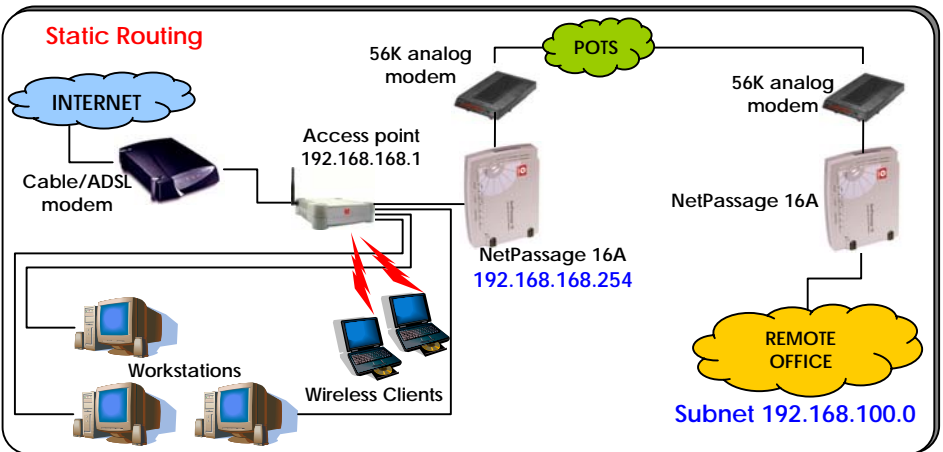
The access point allows the network administrator to add a static routing entry into its routing table so that the access point can re-route IP packets to another network access point. This feature is very useful for a network with more than one access point.



Important:

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

The diagram below illustrates a case in which you have two routers in the network. One router is used for broadband Internet sharing while another router connects to a remote office. You may then define a static routing entry in the access point to re-route the packets to the remote office.



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 NetPassage 16A (192.168.168.254). The remote office resides on a subnet 192.168.100.0.

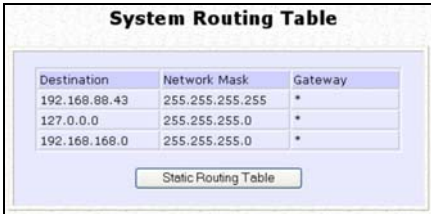
You may add a static routing entry into the access point's routing tables so that IP packets from the clients in the main office with a destination IP address of 192.168.100.X (where X is any number from 2 to 254) will be routed to the NetPassage 16A Router, which acts as the gateway to that subnet.

TO CONFIGURE STATIC ROUTING OF WP54G

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

Step 1:

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



System Routing Table

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

Static Routing Table



Static Routing Table

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

Add Back

Step 2:

Click on the **Static Routing Table** button above.

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



Static Routing Table

Destination IP Address : 192.168.100.0
Destination Net Mask : 255.255.255.0
Gateway IP Address : 192.168.168.254

Add Cancel

Step 3:

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

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

Destination	Network Mask	Gateway
192.168.100.0	255.255.255.0	192.168.168.254

NAT

(only supported by Wireless Routing Client and Gateway)

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

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

To learn more about NAT and its complementary technologies, please turn to the NAT Technology Primer found on the Product CD.

Learn more from our **NAT Technology Primer**

Step 1:

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



Step 2:

Click **Apply** to activate the setting.



Important:

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

TO CONFIGURE VIRTUAL SERVERS BASED ON DE-MILITARIZED ZONE HOST

Having gone through the NAT Technology Primer on the Product CD, you would now have a good understanding of how DMZ works to make a specific PC in a NAT-enabled network directly accessible from the Internet.

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

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



Step 1:

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

Step 2:

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

Step 3:

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



within the DMZ : 192.168.168.55

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

Remember to click the **Apply** button.



NOTE

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

TO CONFIGURE VIRTUAL SERVERS BASED ON PORT FORWARDING

Virtual Server based on Port Forwarding is implemented to forward Internet requests arriving at the access point's WAN interface, based on their TCP ports, to specific PCs in the private network. If you require more information on this function, please refer to the NAT Technology Primer on the Product CD.



Step 3:
Hit the **Add** button on the **Port Forward Entries** page.

Step 1:

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

Step 2:

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



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

Step 4:

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

For a more detailed explanation, please refer to the NAT Technology Primer found on the Product CD.

Learn more from our **NAT Technology Primer**

Known Server

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

Custom Server

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

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

Port Forward Entries

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

TO CONFIGURE VIRTUAL SERVERS BASED ON IP FORWARDING

When you have subscribed for more than one IP address from your ISP, you may define Virtual Servers based on IP Forwarding for which all Internet requests, regardless of ports, are forwarded to defined computers in the private network. If you require more information of its function, please refer to the NAT Technology Primer on the Product CD. Here are the steps to set it up:



Step 1:

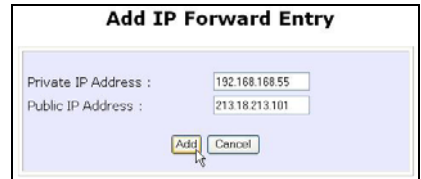
Under the **CONFIGURATION** command menu, click on **NAT**. You will find the **Advanced NAT Options** available near the bottom of the page.

Step 2:

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

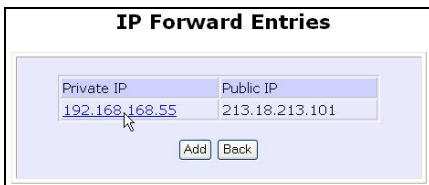
Step 3:

At the next screen **Add IP Forward Entry**, you have to specify a **Private IP Address** and a **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.



Step 4:

Click the **Add** button to continue.



Step 5:

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



NOTE

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

BANDWIDTH CONTROL

(only supported by Wireless Routing Client and Gateway)

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

TO ENABLE OR DISABLE BANDWIDTH CONTROL

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

Step 1:

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

Enable/Disable Bandwidth Control

Bandwidth Control Status : Enable Disable

Apply

WAN Bandwidth Control Setup

Upload/Download Bandwidth Setting

Download Total Rate(kbit):

Upload Total Rate(kbit) :

Apply

LAN Bandwidth Control Setup

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

Step 2:

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



Enable/Disable Bandwidth Control

Bandwidth Control Status : Enable Disable

TO CONFIGURE WAN BANDWIDTH CONTROL SETTING

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

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

Step 1:

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

Step 2:

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



WAN Bandwidth Control Setup

Upload/Download Bandwidth Setting

Download Total Rate(kbit):

Upload Total Rate(kbit) :

TO CONFIGURE LAN BANDWIDTH CONTROL SETTING

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

Step 1:

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

Step 2:

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

LAN Bandwidth Control Setup

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

Step 3:

Click **Add** 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 :

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

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

Step 3:

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



NOTE

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

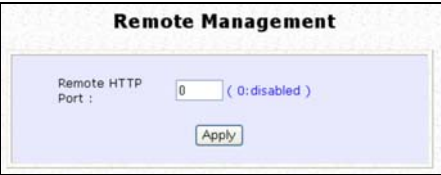
REMOTE MANAGEMENT

(only supported by Wireless Routing Client and Gateway)

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

TO SET UP REMOTE MANAGEMENT

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



Step 1:
Under the **CONFIGURATION** command menu, click on **Remote Management**, and you will be brought to the following screen.

Step 2:
To disable Remote Management, just enter 0 for **Remote Http Port** .

To enable **Remote Management**, enter a port number that is not being used by other applications in the network. Please take note that it is recommended not to use 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 the Ethernet port simply 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

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

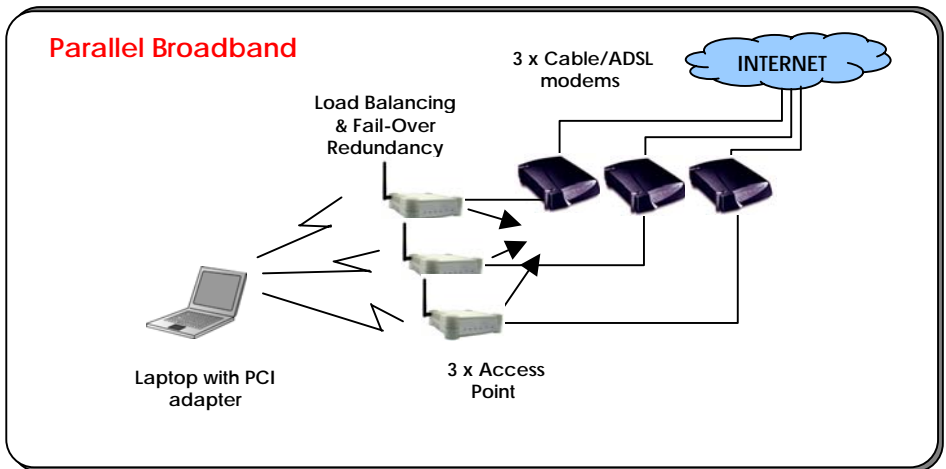
You are also advised to change this password from time to time to guard against malicious attackers.

PARALLEL BROADBAND

(only supported by Gateway)

The access point is equipped with the exclusive Parallel Broadband technology to provide scalable Internet bandwidth with Load Balancing and Fail-Over Redundancy.

By installing multiple units of the access point cascaded using Parallel Broadband, you may balance the Internet traffic generated from your private network over multiple broadband connections - providing the network with aggregated bandwidth! In the event of a particular broadband connection failing, the access point in cascade will use the remaining functional broadband channels, giving you an added peace of mind with its Fail-Over Redundancy capability.



To implement Parallel Broadband, you will need to install two or more access points in the network, each connected to its broadband Internet service account. There is no restriction to the type of broadband Internet accounts they are connected to (whether Cable or ADSL). You may thus have one Access point connected to Cable Internet, and another to an ADSL line.

When these access points operate in the Gateway mode using Parallel Broadband, you need to configure them by enabling Parallel Broadband and setting these access points to the same ESSID.

To learn more about Parallel Broadband, please read the whitepaper at www.cpx.com or www.complex.com.sg.

TO ENABLE PARALLEL BROADBAND ON WP54G

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

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

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

Step 1:

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

Step 2:

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

Step 3:

Repeat this for the other access points in your network and they will communicate with each other and assign each new user to the access point that has the smallest load, so that there is approximately the same number of users on each access point.





Important:

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

EMAIL NOTIFICATION

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

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

Step 1:

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

Step 2:

Click on the **Email Notification** button.

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

Step 3:

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

- **Email address of Receiver:**

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

- **IP address of Email Server:**

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

- **User Name:**

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

- **Password:**

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

- **Email address of Sender:**

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

Step 4:

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

Step 5:

Then click on the **Apply** button.

STATIC ADDRESS TRANSLATION

(only supported by Wireless Routing Client and Gateway)

If you use a notebook for work at the office, it is probable that you also bring it home to connect to the Internet and retrieve emails or surf the web. Since it is most likely that your office's and your home's broadband-sharing network subnets are differently configured, you would have to struggle with reconfiguring your TCP/IP settings each time you use the notebook in a different place. The access point provides the Static Address Translation (SAT) feature to enable its users to bypass this hassle.

Let's say that the IP address of your notebook is set to 203.120.12.47 at the workplace but the access point that is connecting your home network to the Internet, is using an IP address of 192.168.168.1. You have enabled SAT on your router and want to access the Internet without changing the IP address of the notebook as you have to use it at work again on the next day.

Since it is still set to the TCP/IP settings used in your office, the notebook will then try to contact the IP address of your office's gateway to the Internet. When the access point finds that the notebook is trying to contact a device that lies in a different subnet from that of the home network, it would then inform the notebook that the gateway to the Internet is in fact itself (Access Point).

Once the notebook has been informed that the gateway to the Internet is the access point, it will contact the latter (Access Point) to access the Internet, without any change to its TCP/IP settings required.



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:

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



Step 2:

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



DNS REDIRECTION

(only supported by Wireless Routing Client and Gateway)

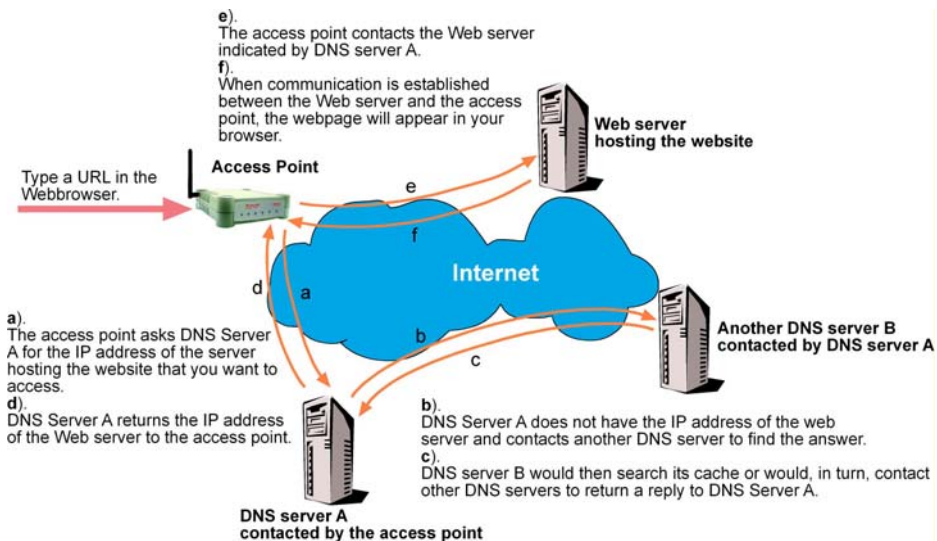
When you enter a URL in your Internet browser, the browser requests for a name-to-IP address translation from the Domain Name System (DNS) servers to be able to locate the web server

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

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

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

The DNS Redirection feature also provides better control to the network administrator. In case of a change in DNS servers, the latter can just indicate the IP address of the actual DNS server in the access point's LAN Setup and enable DNS Redirection, without having to re-configure the DNS settings of each LAN client.



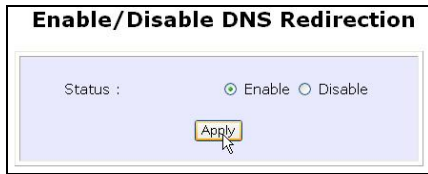
NOTE

For Internet access, please do NOT leave the DNS Server field of the PC's TCP/IP Properties blank. Simply key in any legal IP address for it (e.g. 10.10.10.10) even though you do not have the exact DNS IP address.

TO ENABLE/DISABLE DNS REDIRECTION

Step 1:

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



Step 2:

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

Step 3:

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

DYNAMIC DNS SETUP

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

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

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

If someone types in your address: **MyName.Domain.com** into their web browser, this request would go to the DDNS provider which would then re-direct that request to your computer, no matter what IP address it has been currently assigned by your ISP.

TO ENABLE/DISABLE DYNAMIC DNS SETUP

Step 1:

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

Step 2:

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




TO MANAGE DYNAMIC DNS LIST

Step 1:

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

Step 2:

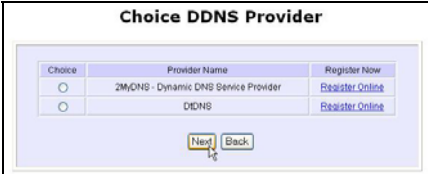
If you have already created a list earlier, click on the **Refresh** button to update the list.



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

Step 3:

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



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. Below the table, there are "Next" and "Back" buttons. A mouse cursor is pointing at the "Next" button.

Choice	Provider Name	Register Now
<input type="radio"/>	ZMYDNS - Dynamic DNS Service Provider	Register Online
<input type="radio"/>	DIDNS	Register Online

- **Choice :**

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

- **Provider Name :**

This is the name of your preferred DDNS provider.

- **Register Now :**

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

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

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

Step 1:

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

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

Step 2:

Enter your **Domain Name**.

Step 3:

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

Provider: 2MyDNS - Dynamic DNS Service Provider

Domain Name:

WAN IP: Auto Detect

Username:

Password:

Wildcard: YES NO

Mail Exchanger:

Backup Mail Exchanger: YES NO

For instance,

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

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

Step 4:

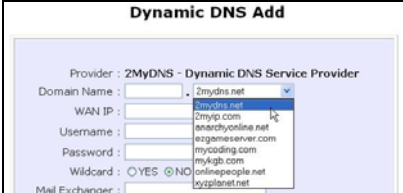
(Optional) If you enable the wildcard service, your hostname

would be allowed multiple identities.

For example, if you register: mydomain.2mydns.net, users looking for www.mydomain.2mydns.net or ftp.mydomain.2mydns.net can still reach your hostname.

Step 5:

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



Step 6:

Click on the Add button to save the new addition.


Step 7:

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



Step 8:

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



To select **DtDNS** as DDNS Service Provider

Step 1:

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

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

Next Back

Step 2:

Enter your **Domain Name**.

Step 3:

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

Provider : DtDNS

Domain Name : .

WAN IP : Auto Detect

Password :

Add Reset Back

For instance,

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

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

Step 4:

Then click on the **Add** button.

Step 5:

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



Chapter 8: Security Configuration

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

PACKET FILTERING

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

TO CONFIGURE PACKET FILTERING

Step 1:

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

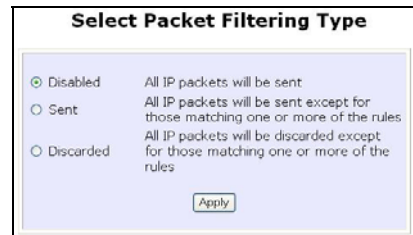


Packet Filter Configuration

Packet Filter Type : **Disabled**

Step 2:

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



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

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.



Packet Filter Configuration

Packet Filter Type : **Sent**

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

Step 4:

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

- 4a). Enter **Rule Name** for this new packet filtering rule. For example, *BlockCS*
- 4b). From the **IP Address** drop down list, select whether to apply the rule to:

- A **Range** of IP addresses

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

- A **Single** IP address

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

- **Any** IP address

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

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

- A **Range** of TCP ports

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

- A **Single** TCP port

Here, you need only specify

Add a new Packet Filter rule

Rule Name :

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

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

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

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

Rule Name :

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

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

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

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

the source port in the **(From)** field.

- **Any** IP port

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



Destination Port : Single
From : 25
To :



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

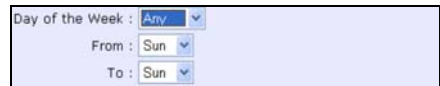
Here, you will have to select **(From)** which day **(To)** which day



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 :

IP Address :

From :

To :

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)

Step 6:

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

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

URL FILTERING

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

TO CONFIGURE URL FILTERING

Step 1:

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



Step 2:

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

Step 3:

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



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



Step 4:

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

FIREWALL CONFIGURATION

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

To learn more about SPI firewall, read our whitepaper at www.cpx.com or at www.compex.com.sg.

TO CONFIGURE SPI FIREWALL

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

Step 1:

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

Step 2:

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

Step 3:

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

Firewall Configuration

Warning: Incorrect configuration may cause undesirable behavior.

Firewall Status: Enable Disable

Allow user visit LAN from WAN port

Log Information

Accepted: TCP Packets UDP Packets
 ICMP Packets IGMP Packets

Denied: TCP Packets UDP Packets
 ICMP Packets IGMP Packets

No	Active	Name	Disposition Policy	Protocols	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"/>	ftp	Accept	UDP	Any	Any	53	Any
4	<input checked="" type="checkbox"/>	ftp (00-52)	Accept	TCP	Any	Any	Any	80-83
5	<input checked="" type="checkbox"/>	ftp (8000)	Accept	TCP	Any	Any	Any	8000
6	<input checked="" type="checkbox"/>	cdp	Accept	UDP	Any	Any	1645	Any
7	<input checked="" type="checkbox"/>	ftp (00-80)	Accept	UDP	Any	Any	81	88

Step 4:

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

Edit Firewall rule

Rule Number : 7
Rule Name : dhcp-bootp
Disposition Policy : Accept
Protocols : Udp

ICMP Types

<input type="checkbox"/> All Types	<input type="checkbox"/> Echo Reply
<input checked="" type="checkbox"/> Destination Unreachable	<input checked="" type="checkbox"/> Source Quench
<input type="checkbox"/> Redirect	<input type="checkbox"/> Echo Request
<input checked="" type="checkbox"/> Time Exceeded	<input checked="" type="checkbox"/> Parameter Problem
<input type="checkbox"/> Timestamp Request	<input type="checkbox"/> Timestamp Reply
<input checked="" type="checkbox"/> Information Request	<input checked="" type="checkbox"/> Information Reply
<input type="checkbox"/> Address Mask Request	<input type="checkbox"/> Address Mask Reply

Source IP Address : Any
(From) :
(To) :

Destination IP Address : Any
(From) :
(To) :

Source Port : Single
(From) : 67
(To) :

Destination Port : Single
(From) : 68
(To) :

Check Options : LSRR
Check TTL :
TTL value :

Save Delete Cancel

- Rule Name** : Enter a unique name to identify this firewall rule.
- Disposition Policy** : This parameter determines whether the packets obeying the rule should be accepted or denied by the firewall. Choose between Accept and Deny.
- Protocols** : Users are allowed to select the type of data packet from: TCP, UDP, ICMP, IGMP or ALL.
- Note: If users select either ICMP or IGMP, they are required to make further selection in the ICMP Types or IGMP Types respectively.
- ICMP Types** : This IP protocol is used to report errors in IP packet routing. ICMP serves as a form of flow control, although the receiving and transmitting of ICMP messages is not guaranteed.

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

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

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

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

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

range of IP addresses.

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

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

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

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

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

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

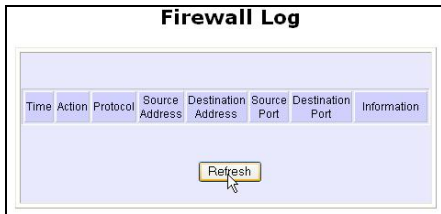
FIREWALL LOGS

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

TO VIEW FIREWALL LOGS

Step 1:

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



Step 2:

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

Chapter 9: System Utilities

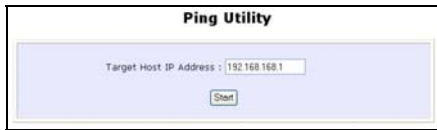
USING THE SYSTEM TOOLS MENU

PING UTILITY

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

Step 1:

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



Step 2:

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

Step 3:

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



Step 4:

The Ping messages will be displayed.

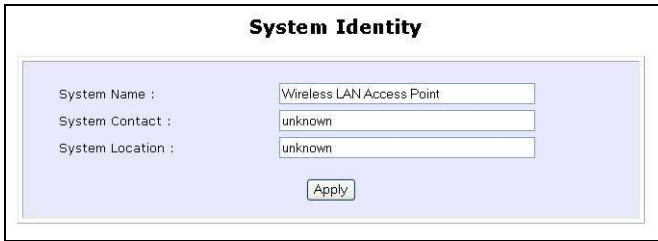
SYSTEM IDENTITY

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

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

Step 1:

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



The screenshot shows a window titled "System Identity" with a light blue background. It contains three text input fields and an "Apply" button. The first field is labeled "System Name :" and contains the text "Wireless LAN Access Point". The second field is labeled "System Contact :" and contains the text "unknown". The third field is labeled "System Location :" and contains the text "unknown".

Field Label	Value
System Name :	Wireless LAN Access Point
System Contact :	unknown
System Location :	unknown

Apply

Step 2:

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

Step 3:

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

Step 4:

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

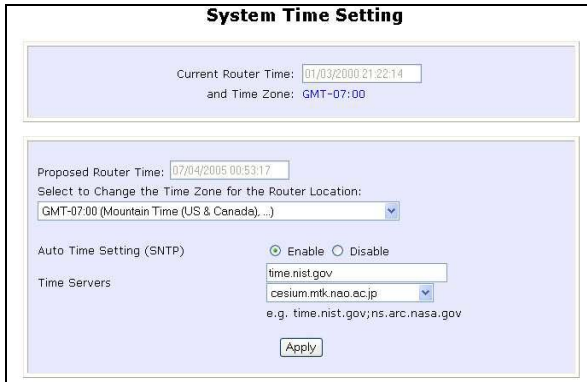
Step 5:

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

SYSTEM CLOCK SETUP

Step 1:

Click on **System Clock Setup** from the **SYSTEM TOOLS** menu.



The screenshot shows the 'System Time Setting' configuration page. At the top, it displays the 'Current Router Time' as 01/03/2006 21:22:14 and the 'Time Zone' as GMT-07:00. Below this, the 'Proposed Router Time' is shown as 07/04/2005 00:53:17. A section titled 'Select to Change the Time Zone for the Router Location:' contains a drop-down menu currently set to 'GMT-07:00 (Mountain Time (US & Canada)...)'. Underneath, the 'Auto Time Setting (SNTP)' section has two radio buttons: 'Enable' (which is selected) and 'Disable'. The 'Time Servers' field contains the text 'time.nist.gov' and a drop-down menu showing 'cesium.mtk.nao.ac.jp'. Below the drop-down menu, there is a small text example: 'e.g. time.nist.gov;ns.arc.nasa.gov'. At the bottom of the form is an 'Apply' button.

Step 2:

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

Step 3:

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

Step 4:

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

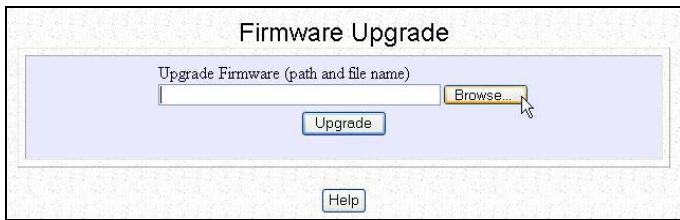
FIRMWARE UPGRADE

Keep your access point updated with the latest capabilities by downloading its latest firmware revision from either of Compex's corporate web sites at www.compex.com.sg or www.cpx.com before following the next steps. You can check the types and version of your firmware by clicking on **About System** from the **HELP** menu.

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

Step 1:

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



Step 2:

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

Step 3:

Click on the **Upgrade** button.

Follow the instructions given during the upgrading process.



Step 4:

You need to reboot the system after the firmware upgrade.



NOTE

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

BACKUP OR RESET SETTINGS

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

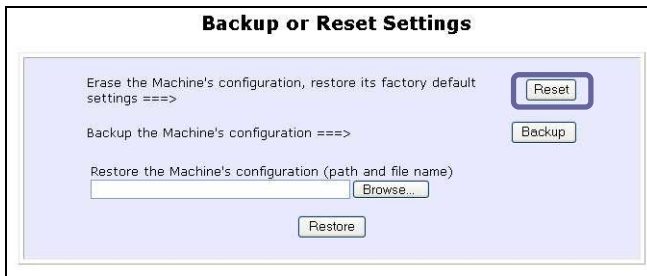
RESET YOUR SETTINGS

Step 1:

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

Step 2:

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



The screenshot shows a dialog box titled "Backup or Reset Settings" with a light blue background. It contains three options, each with a corresponding button:

- The first option is "Erase the Machine's configuration, restore its factory default settings ==>". To its right is a button labeled "Reset", which is highlighted with a blue border.
- The second option is "Backup the Machine's configuration ==>". To its right is a button labeled "Backup".
- The third option is "Restore the Machine's configuration (path and file name)". Below this text is a text input field and a "Browse..." button. Below the input field and "Browse..." button is a "Restore" button.

Step 3:

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

BACKUP YOUR SETTINGS

Step 1:

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

Step 2:

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



Step 3:

Next, save your configuration file to your local disk.



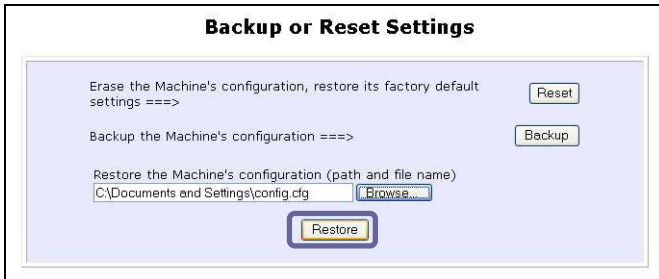
RESTORE YOUR SETTINGS

Step 1:

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

Step 2:

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



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

REBOOT SYSTEM

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

Step 1:

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

Step 2:

Click on the **Reboot** button.



Step 3:

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



CHANGE PASSWORD

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

Step 1:

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

Step 2:

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

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

Step 3:

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



The screenshot shows a web form titled "Change Password". It contains three input fields for "Current Password", "New Password", and "Confirm Password", each with a masked password field. Below the fields is an "Apply" button.

Change Password	
Current Password:	<input type="password"/>
New Password:	<input type="password"/>
Confirm Password:	<input type="password"/>
<input type="button" value="Apply"/>	

LOGOUT

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

Step 1:

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

Step 2:

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

Wireless LAN Access Point Management



Please enter your password:

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

USING THE HELP MENU

GET TECHNICAL SUPPORT

This page presents the contact information of Compex's technical support centres around the world.

Step 1:

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

Support Information

For technical support email to: support@compex.com.sg
For updates connect to the following Web Sites:
<http://www.cpx.com>
<http://www.compex.com.sg>

Regional Technical Support Centers

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

Compex Inc.
840 Columbia Street, Suite B, Brea, CA92821,USA
Tel : (714) 482-0333
Fax : (714) 482-0332
800 Line: (800) 279-8891
Support email: support@cpx.com

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

Compex Systems Pte. Ltd.
135, Joo Seng Road, #06-01,
PM Industrial Building
Singapore 368363
HotLine : (65) 6-286-1805
Fax : (65) 6-283-8337

The access point is a feature-packed device. If you require further information than provided in the manual or data sheet, please contact one of Compex's Technical Support Centres by mail, email, fax or telephone.

ABOUT SYSTEM

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

Step 1:

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

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

System Information

Device:	
System Up Time :	0 Days 00:14:25
BIOS/Loader Version :	2.1f (build 0310)
Firmware Version :	1.52 (build 0705)
NetWork Mode :	Inherent Bridge
Wireless:	
Hardware Address :	00-80-48-3d-0f-81
WLAN name (ESSID):	compex-wp54g
Operating frequency :	5240MHz
Operating Channel :	48
Security Mode :	None
Management Port:	
Hardware Address :	00-80-48-3d-0f-80
IP Address :	192.168.168.1
Network Mask :	255.255.255.0
DHCP Server :	Disabled

Appendix I: Firmware Recovery

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

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

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

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

Step 1:

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

Step 2:

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

Step 3:

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

Step 4:

Insert the WP54G 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** 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:\WP54G\WP54Axxx.IMG**, then replace the command with this new path and firmware name. In our example:

C:\WP54G\TFTP -i 192.168.168.1 PUT WP54Axxx.img

The recovery process will now take place. You can check the diagnostic LED to monitor the progress of the recovery process.

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

Appendix II: TCP/IP Configuration

Once the hardware has been set up, you need to assign an IP address to your PC so that it will be in the same subnet as the access point. By default, the access point's IP address is 192.168.168.1; and its subnet mask is 255.255.255.0. You need to configure your PC's IP address to 192.168.168.xxx; and its subnet mask is 255.255.255.0, where xxx can be any number from 2 to 254 excluding 1. Simply follow the procedures stated below to configure the TCP/IP settings of your PC.

FOR WINDOWS 95/98/98SE/ME/NT

Please note the following instructions are based on Windows 98.

Step 1:

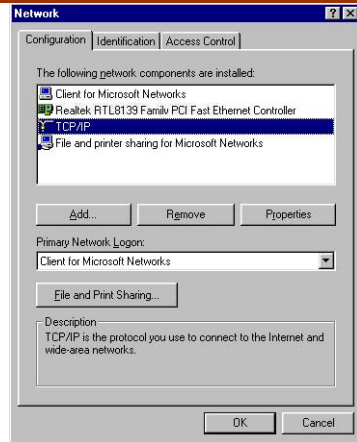
From your desktop, right click **Network Neighborhood** icon and select **Properties**.

Step 2:

Choose the network adapter that you are using; right click and select **Properties**.

Step 3:

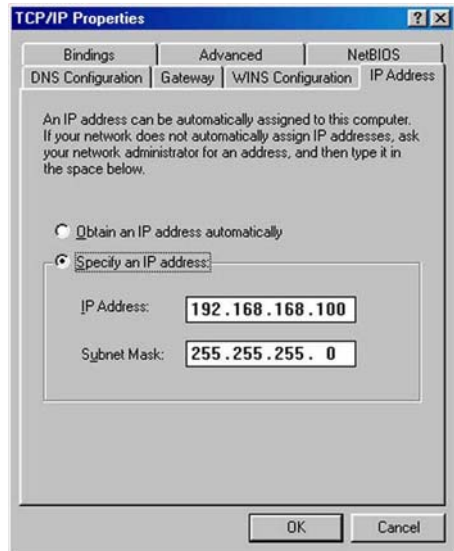
Highlight the **TCP/IP** and click on **Properties** button.



Step 4:

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

Enter the IP Address and Subnet Mask as 192.168.168.X and 255.255.255.0, where X can be any number from 2 to 254, except for 1. In this example, we are using 192.168.168.160 as the static IP Address.

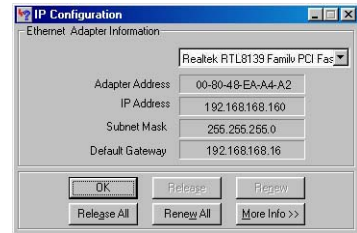


Step 5:

In order to check if the IP address has been assigned correctly to your PC, simply go to the **Start** menu, select **Run**, and enter the command *wiipcfg*.

Select your respective Ethernet Adapter from the drop down list and click **OK**.

Now, your PC is now ready to communicate with your access point.



FOR WINDOWS XP/2000

Step 1:

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

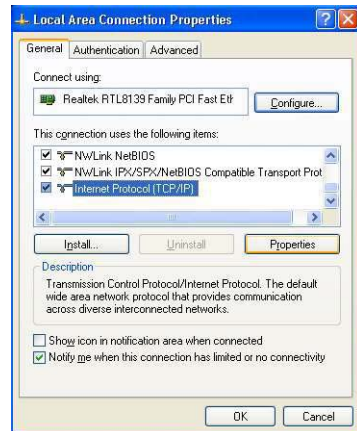
Step 2:

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



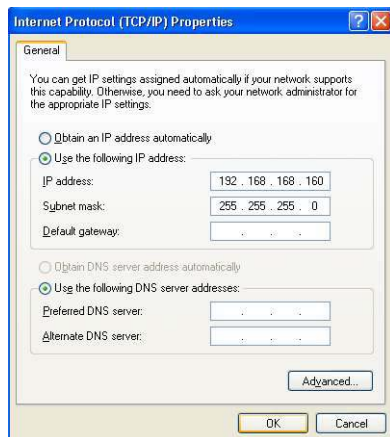
Step 3:

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



Step 4:

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

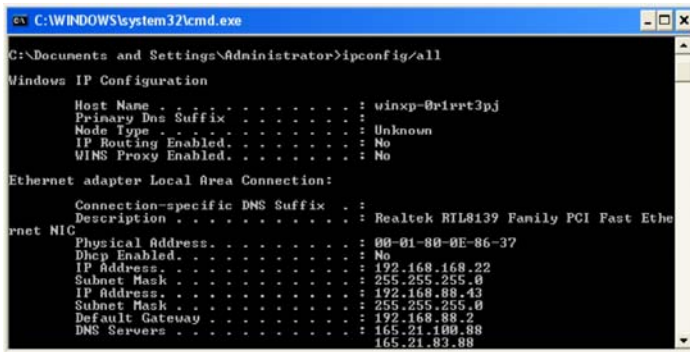


Step 5:

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

Step 6:

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



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

Windows IP Configuration

Host Name . . . . . : winxp-0r1rrt3pj
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

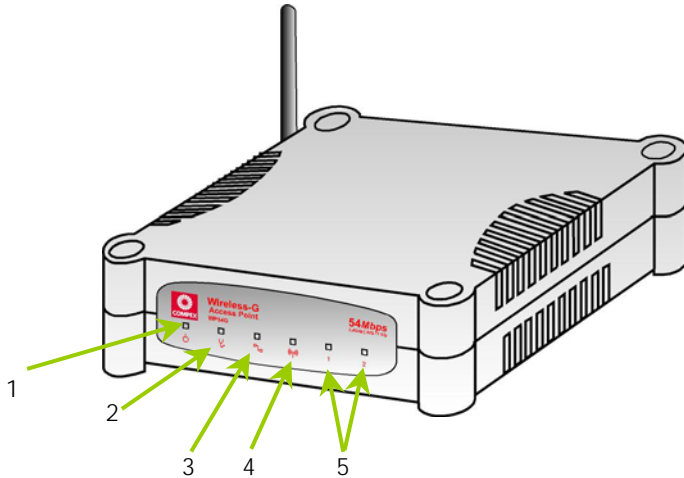
Ethernet adapter Local Area Connection:




    Connection-specific DNS Suffix  . :
    Description . . . . . : Realtek RTL8139 Family PCI Fast Eth
    eternet 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 . . . . . : 165.21.100.88
                           165.21.83.88
```



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

Appendix III: Panel Views & Descriptions

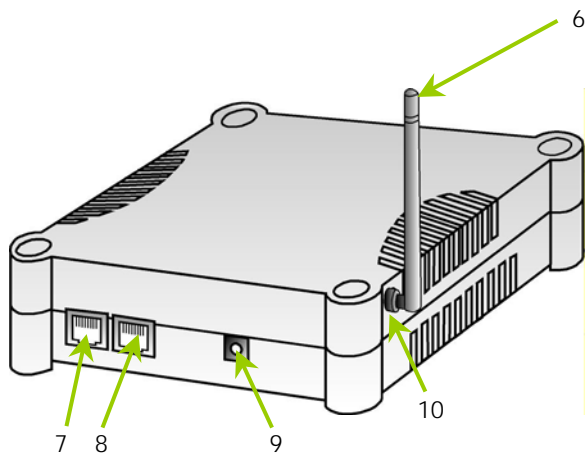
Front View of Access Point



	Name	Description	
1	 LED (Power)	Steady Blue	The device is powered up.
		Off	No power is supplied to the device.
2	 LED (Diagnostic)	Flashing Green	This indicates the flash during the power-up. The LED will go off when the diagnostic is passed.
3	 LED (WAN Link/Act)	Steady Green	WAN connection is established.
		Flashing Green	Data transmission at WAN connection.

4	 LED (WLAN Link/Act LED)	Steady Green	Wireless interface up and running. Ready for operation.
		Flashing Green	Activity is detected in the wireless network.
5	 LED (Port 1 & 2 LEDs)	Steady Green	Connection has been established between the device and the network.
		Flashing Green	Activity is detected in the network.
		Off	No network connection.

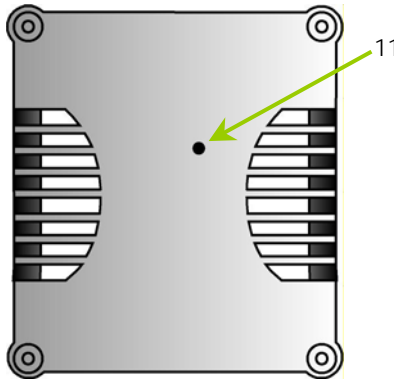
Back View of Access Point



	Name	Description
6	External Antenna	SMA antenna
7	Ethernet Port 2	Connection for computer with NIC (Network Interface Card) or Ethernet network card.

8	Ethernet Port 1	Connection for computer with NIC (Network Interface Card) or Ethernet network card. If using PoE, connect to this port - Ethernet Port 1.
9	DC jack	Power Input
10	Reverse SMA connector	To attach external antenna

Bottom View of Access Point



	Name	Description
11	Reset Push button	To reboot, press once. To reset password, press and hold the button for 5 seconds. The DIAG light will flash fast for about 5 flashes/sec before releasing the button. To restore the factory default settings, press and hold the button for more than 10 seconds. The DIAG light will flash slowly for about 10 flashes/sec before releasing the button.

Appendix IV: Command Line Interface Commands

Get Operation List

SYNTAX	DESCRIPTION
Get tasks	Display all active process/tasks.
Get sysinfo	Display system information.
Get apolist	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 stallist	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 (a/b/g)

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 distant option setup page.

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

TX Power

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

TX Rate

SYNTAX	DESCRIPTION
Set txrate <string>	Values are: (default auto)

	(802.11a)-- 6, 9, 12, 18, 24, 36, 48, 54, auto (802.11b/g mixed)-- 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54, auto (802.11b-only)-- 1, 2, 5.5, 11, auto
--	---

Wireless Mode

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

WEP Key

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

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

Add or Delete User

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

Country Code

SYNTAX	DESCRIPTION
Set countrycode <iso.name>	List of countries:
Set countrycode <2 letter string>	<pre>{0, "NA"}, {CTRY_ALBANIA, "AL"}, {CTRY_ALGERIA, "DZ"}, {CTRY_ARGENTINA, "AR"}, {CTRY_ARMENIA, "AM"}, {CTRY_AUSTRALIA, "AU"}, {CTRY_AUSTRIA, "AT"}, {CTRY_AZERBAIJAN, "AZ"}, {CTRY_BAHRAIN, "BH"}, {CTRY_BELARUS, "BY"}, {CTRY_BELGIUM, "BE"}, {CTRY_BELIZE, "BZ"}, {CTRY_BOLIVIA, "BO"}, {CTRY_BRAZIL, "BR"}, {CTRY_BRUNEI_DARUSSALAM, "BN"}, {CTRY_BULGARIA, "BG"}, {CTRY_CANADA, "CA"}, {CTRY_CHILE, "CL"}, {CTRY_CHINA, "CN"}, {CTRY_COLOMBIA, "CO"}, {CTRY_COSTA_RICA, "CR"}, {CTRY_CROATIA, "HR"}, {CTRY_CYPRUS, "CY"}, {CTRY_CZECH, "CZ"}, {CTRY_DENMARK, "DK"}, {CTRY_DOMINICAN_REPUBLIC, "DO"}, {CTRY_ECUADOR, "EC"}, {CTRY_EGYPT, "EG"}, {CTRY_EL_SALVADOR, "SV"}, {CTRY_ESTONIA, "EE"},</pre>

	{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"}, {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"}
--	---

	<pre>{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"},</pre>
--	--

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.

Appendix V: Virtual AP (Multi-SSID) FAQ

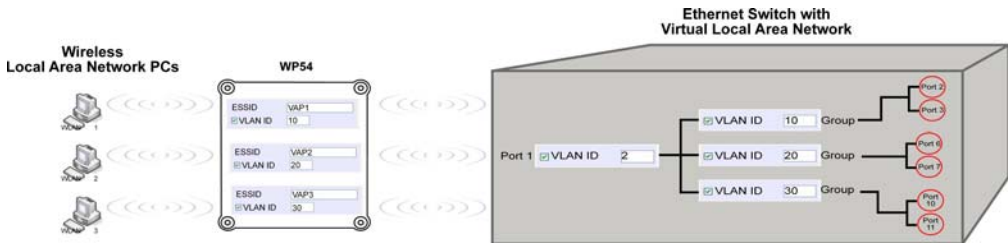
Q1) What is mSSID?

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 WP54G or WP54AG to this mSSID firmware?

Yes. You can retain your WP54G or WP54AG 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 WP54AG 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 VI: Technical Specifications

Safety and Electromagnetic Conformance	<ul style="list-style-type: none"> • FCC Part 15 SubPart B and SubPart C (for wireless module) • EN 300 328-2 • EMC CE EN 301 489 (EN300 826) • EN 55022 (CISPR 22)/EN 55024 Class B • EN 61000-3-2 • EN61000-3-3 • CE EN 60950
Standards	<ul style="list-style-type: none"> • IEEE 802.11b • IEEE 802.11g
Performance	<ul style="list-style-type: none"> • Network speeds dynamically shift between 1,2, 5.5, 11, 12, 18, 24, 36, 48, 54 Mbps • Indoor: 20 m (54 Mbps) • Outdoor: 80 m (54 Mbps)
Frequency Range IEEE 802.11b: IEEE 802.11g:	2.4 ~ 2.4835 GHz 2.4 ~ 2.497 GHz
Wireless Modes Operation	<ul style="list-style-type: none"> • Access Point Mode • Client Mode • Wireless Routing Client • Gateway Mode • Wireless Adapter Mode • Transparent Client Mode • Repeater Mode

Security	<ul style="list-style-type: none"> • 64 - bit / 128 - bit WEP • WPA-Enterprise, WPA-Personal, WPA2-Enterprise, WPA2-Personal, WPA-Auto-Enterprise, WPA-Auto-Personal • Tagged VLAN • IEEE 802.1x – TLS, TTLS, PEAP, EAP-SIM • Wireless MAC address filtering (in Access Point mode)
Network Interface	2 10/100 Mbps auto-negotiating Ethernet ports (RJ45)
Modulation Techniques	OFDM (BPSK, QPSK, 16-QAM, 64-QAM), DSSS (BPSK, QPSK, CCK)
Output Power IEEE 802.11b: IEEE 802.11g:	20 dBm 20 dBm
Operating Channels	<ul style="list-style-type: none"> • 11 Channels (US and Canada) • 13 Channels (Europe) • 14 Channels (Japan)
Advanced Wireless Features	<ul style="list-style-type: none"> • Virtual AP • Long Distance Parameters Setup • Adjustable transmit power control (in 1dB steps) • Smart Select • STP • HTTPS
Antenna	Detachable 2dBi antenna with SMA connector

Management	<ul style="list-style-type: none"> • Long Distance Parameters Setup • Adjustable transmit power control (in 1dB steps) • Smart Select • STP • HTTPS
Built-in DHCP Server	Yes
DHCP Reservation	By MAC address
Configuration Backup & Restore	Yes
Firmware Upgrade	Yes
Power Requirements Using Power Adapter:	Output 24VDC – 48 (localized to country of sale)
Using PoE:	802.11af PoE
Cable Length Requirement for PoE	100 meters (max)
Environment Requirements Operating Temp: Storage Temp: Operating Humidity:	-20°C to +70°C -65°C to +100°C 5% to 95% RH Humidity (RH – Relative Humidity):
Physical Dimensions	145mm x 132mm x 41mm (H x W x D)