



networks@work

USER'S MANUAL



COMPEX NETPASSAGE SERIES

WP54G 6e

WP54G 6e

WP54G 6e

WP54G 6e

WP54G 6e

Manual Number: U-0496-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-0496-V1.3C Version 1.3 October 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.

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) Tel: (65) 6286-2086 (Ext.199 Technical Support)
 Fax	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, Wireless Access Point with Integrated PoE, WP54G is a licensed product of Compex Systems Pte Ltd. This document contains instructions for installing, configuring and using WP54G. 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.compex.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 1.48.

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 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 Compex 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..... 1

Introduction.....	1
Features and Benefits.....	2
When to use which mode	3
Access Point Mode.....	3
Access Point Client Mode	4

CHAPTER 2: HARDWARE INSTALLATION 5

Setup Requirements	5
Hardware Installation	5
OPTION One: Using power adapter to supply power to the unit.....	5
OPTION Two: Using PoE to supply power to the unit.....	7
Optional: Mounting on the Wall.....	10

CHAPTER 3: ACCESS TO WEB-BASED INTERFACE 11

Access to the Web interface with uConfig.....	11
Manual access to web-based interface via Internet Explorer	15

CHAPTER 4: COMMON CONFIGURATION 20

Management Port Setup.....	20
Setting up your LAN	21
To view the active DHCP leases.....	24
To reserve specific IP addresses for predetermined DHCP clients.....	25
WLAN Setup	28
To configure the Basic setup of the wireless mode	29

To configure the Security setup of the wireless mode.....	40
To configure the Advanced setup of the wireless mode	40
Statistics.....	43
STP Setup.....	45
MAC Filtering.....	51
<i>Add a MAC address to the MAC Address List.....</i>	<i>52</i>
<i>Delete a MAC address from all access points.....</i>	<i>55</i>
<i>Delete a MAC address from individual access point.....</i>	<i>57</i>
<i>Edit MAC address from the MAC Address List.....</i>	<i>59</i>
CHAPTER 5: WLAN SECURITY	61
How to set up WEP.....	62
How to set up WPA-Personal.....	64
How to set up 802.1x/RADIUS.....	66
How to set up WPA Enterprise.....	68
CHAPTER 6: WIRELESS EXTENDED FEATURES	71
Access Control – The Wireless Pseudo VLAN.....	71
Wireless Pseudo VLAN Per Node	72
Wireless Pseudo VLAN Per Group.....	75
Wireless Setup - The Wireless Distributed System.....	79
Long Distance Parameters.....	85
CHAPTER 7: SYSTEM UTILITIES	88
Using the SYSTEM TOOLS Menu.....	88
System Identity.....	88
System Clock Setup	90
Firmware Upgrade.....	91
Backup or Reset Settings	93
Reboot System.....	96
Change Password.....	97
Logout	98
Using the HELP menu	99
Get Technical Support	99
About System.....	100

APPENDIX I: FIRMWARE RECOVERY	101
APPENDIX II: TCP/IP CONFIGURATION	103
For Windows 95/98/98SE/ME/NT	103
For Windows XP/2000.....	105
APPENDIX III: PANEL VIEWS & DESCRIPTIONS	108
APPENDIX IV: TECHNICAL SPECIFICATIONS.....	112

Chapter 1: Product Overview

INTRODUCTION



The high-performance access point (AP) is designed for enterprise and public access applications. Embedded with the Atheros chipset, it boasts network robustness, stability and wider network coverage. Based on 802.11g, 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 different modes: Access Point and Access Point Client, 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: Wireless Distribution System (WDS) to wirelessly link associated access points together and extend network coverage, 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; and Pseudo VLAN which enables the creation of wireless isolated nodes or workgroups of wireless clients to enhance security in a public access wireless network.

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.

Wireless Distribution System (WDS)

This feature allows linking of several access points, virtually creating a larger network infrastructure that allows mobile users to roam wirelessly, while still being able to access network resources.

Wireless Pseudo VLAN

The Complex unique Wireless Pseudo VLAN technology is a feature that allows wireless clients to be segmented individually or into workgroups, thus blocking access to another user's/group's PCs, and enhancing the privacy of the wireless clients. This is especially useful in public hotspot deployment.

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-PSK for SOHO users and WPA2-EAP 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

Complex'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.

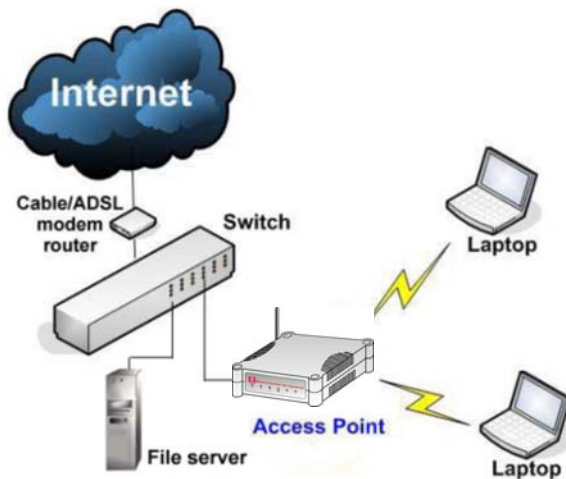
WHEN TO USE WHICH MODE

The access point is versatile in the sense that it may operate in 2 different types of modes: **Access Point Mode** and **Client 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 the access point. The **Access Point** mode enables you to bridge wireless clients to access the wired network infrastructure and to communicate with each other.

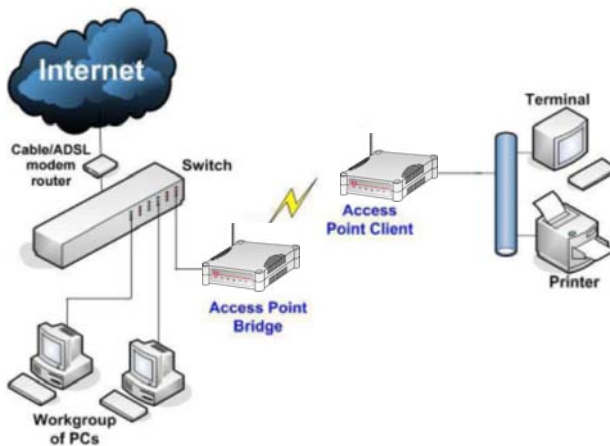


In the example above, the wireless users will be able to access the file server connected to the switch through the access point in Access Point mode.

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.

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

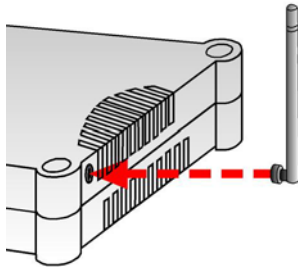
HARDWARE INSTALLATION

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

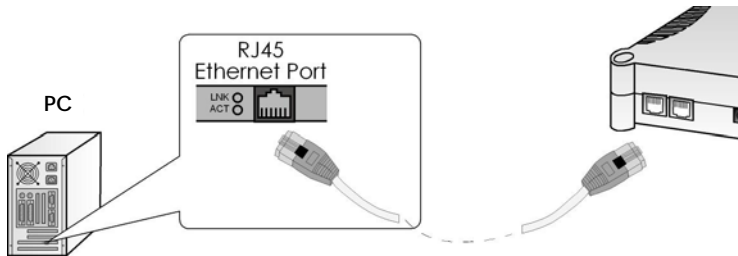
Step 1:

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



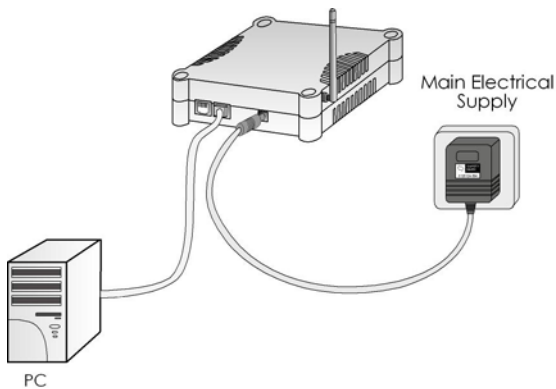
Step 2:

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.

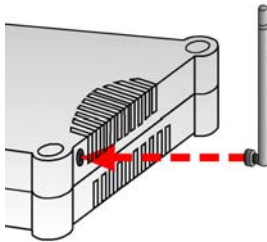
OPTION TWO: USING PoE TO SUPPLY POWER TO THE UNIT

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:

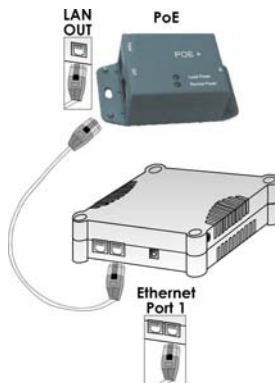
Step 1:

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



Step 2:

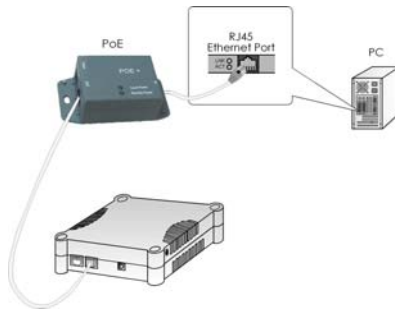
Use an RJ45 Ethernet cable to connect one end of the cable to the LAN OUT port of the Injector and the other end to Ethernet port 1 of the access point.



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.

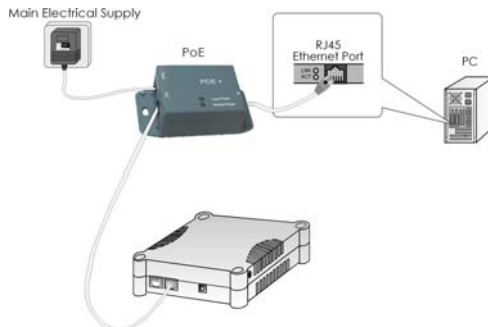


Step 4:

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.



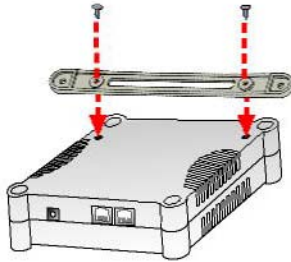
Step 5:

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.



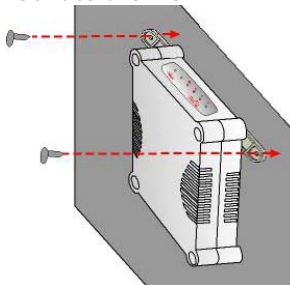
Step 2:

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 the 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 the 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 the 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:

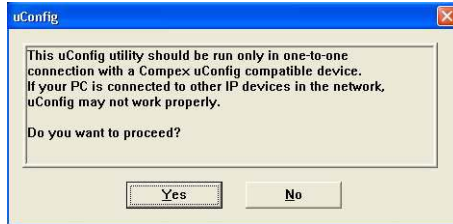
Insert the Product CD into your CD-ROM drive. The CD will run automatically.

Step 2:

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

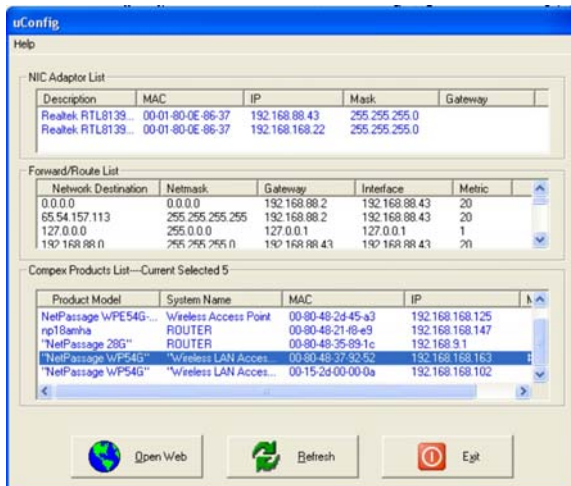
Step 3:

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



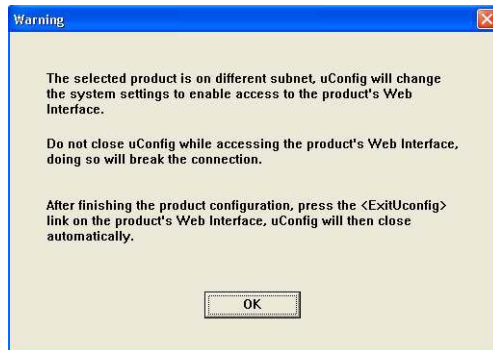
Step 4:

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.



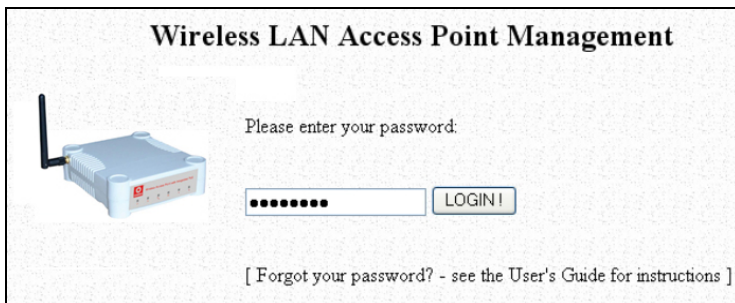
Step 5:

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.



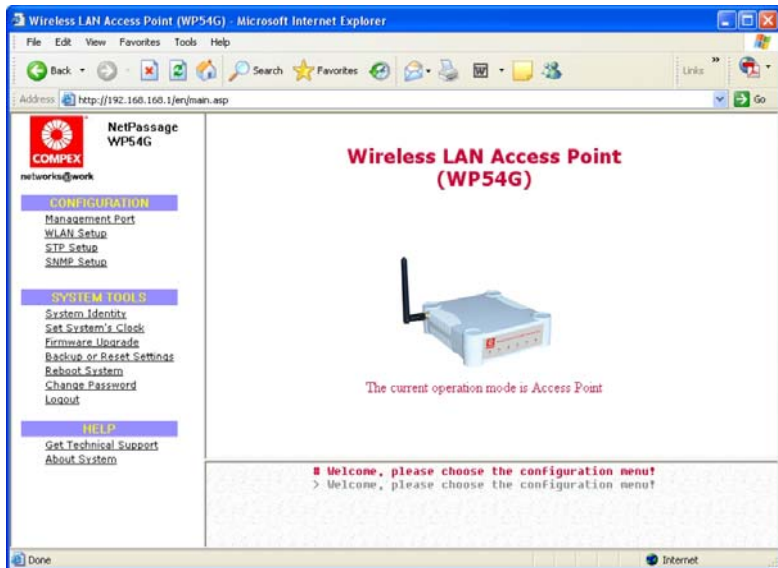
Step 6:

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 the 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**.

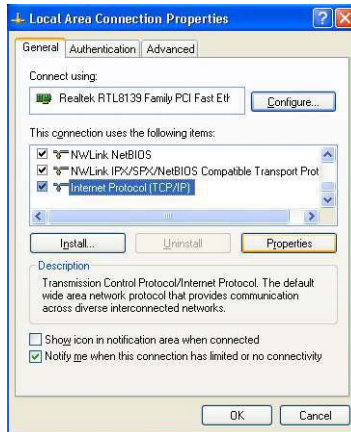
Step 2:

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



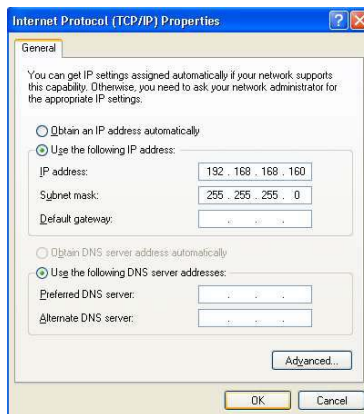
Step 3:

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.

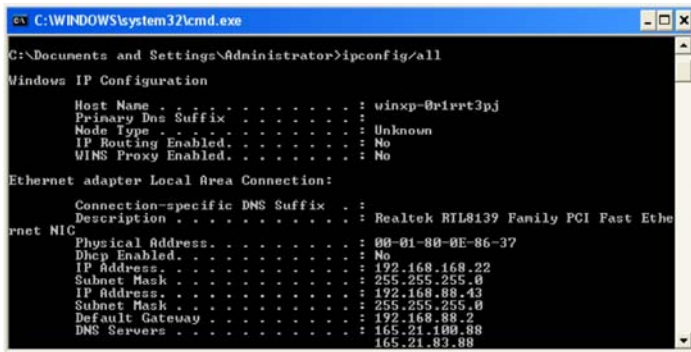


Step 5:

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 the access point.

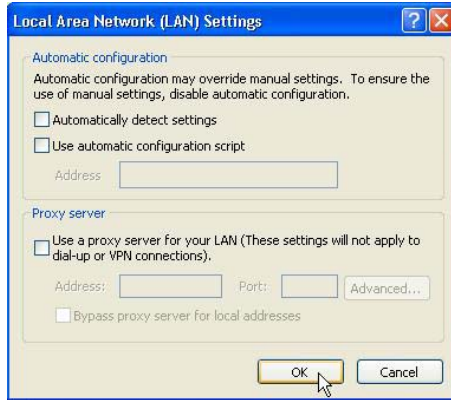
Step 7:

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.

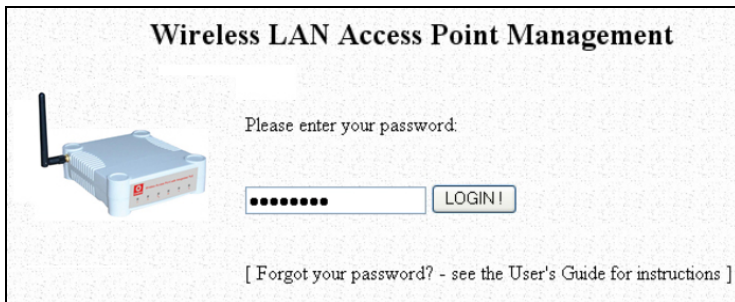


Step 9:

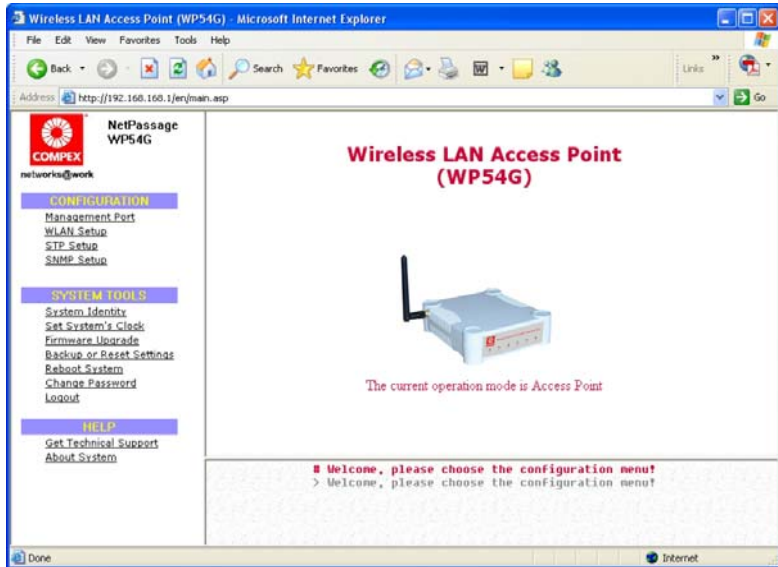
At the **Address** bar, enter `http://192.168.168.1` and press **Enter** on your keyboard.

Step 10:

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



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



Chapter 4: Common Configuration

This chapter illustrates the following features, which are available in ALL the operating modes of the 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 the access point to suit the needs of your network. It also explains how to make use of the built-in DHCP server of the access point.

SETTING UP YOUR LAN

You can opt to adjust the default values of the 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 the 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

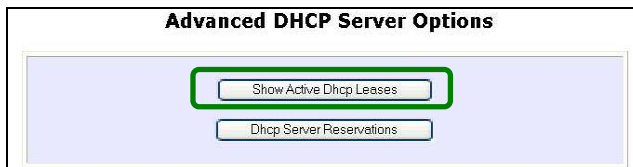
The following will guide you to a page display of the active IP address leases that have been allocated by the built-in DHCP server of the access point.

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

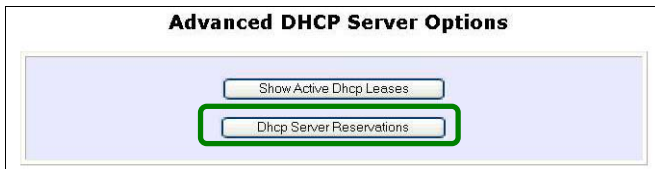
Making an IP address reservation lets you inform the DHCP server to exclude that specific address from the pool of free IP addresses it draws on for dynamic IP address allocation.

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*.



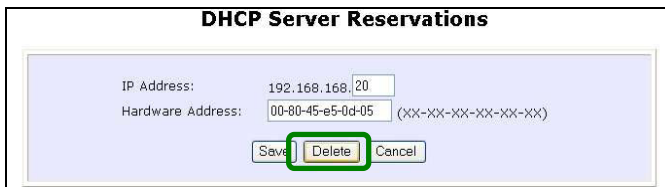
The screenshot shows a table titled "DHCP Server Reservations". The table has two columns: "IP Address" and "Hardware Address". The first row contains the values "192.168.168.20" and "00-80-45-e5-0d-05". The "192.168.168.20" cell is highlighted with a green box. Below the table are "Add" and "Back" buttons.

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

Buttons: Add, Back

Step 2:

Click on the **Delete** button.



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

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

Buttons: Save, Delete, Cancel

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 the wireless modes of operation: **Access Point mode** and **AP Client mode**.

Security:

This function performs data encryption and protection for the router.

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

Advanced:

This function furthers the basic configuration of the router by setting the system's additional parameters: **Wireless Pseudo VLAN**, **WDS Configuration** 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 mode):

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:

Double-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 the access point is the **Access Point** mode.

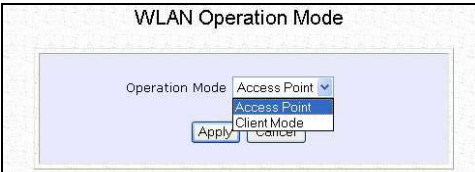


The screenshot shows the "WLAN Basic Setup" configuration page. It includes the following fields and controls:

- The Current Mode:** Access Point (with a "Change" button next to it).
- ESSID:** compex-wp54g1e
- Wireless Profile:** 802.11b/g mixed
- Country:** NO_COUNTRY_SET-(NA)
- Channel:** SmartSelect
- Tx Rate:** Fully Auto
- Closed System:** disable enable
- Buttons:** "Apply" at the bottom center and "Channel Survey" on the right side.

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.



The screenshot shows the "WLAN Operation Mode" configuration page. It includes the following fields and controls:

- Operation Mode:** A dropdown menu with "Access Point" selected. The dropdown list is open, showing "Access Point" and "Client Mode".
- Buttons:** "Apply" and "Cancel" buttons are located below the dropdown menu.

Step 3:

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

Note that the **WLAN Basic Setup** page for the Client mode is different from that of the **AP** mode.

The screenshot shows the 'WLAN Basic Setup' interface. At the top, it indicates 'The Current Mode' is 'Client Mode' with a 'Change' button. Below this, there are several configuration fields: 'ESSID' with the value 'compex-wp54g1e' and a 'Site Survey' button; 'Wireless Profile' set to '802.11b/g mixed'; 'Country' set to 'NO_COUNTRY_SET-(NA)'; and 'Tx Rate' set to 'Fully Auto'. An 'Apply' button is located below these fields. At the bottom of the page, there is a 'Link Information' section with a 'Show Link Information' button.

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 router can operate in two modes:</p> <ul style="list-style-type: none">AP modeClient 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>

Parameters	Description
Site Survey (Only in Client mode)	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.
Wireless Profile	<p>A selection of network environment types in which to operate the access point:</p> <p>802.11b only This mode supports wireless B clients with data rates of up to 11Mbps in the frequency range of 2.4GHz.</p> <p>802.11b/g mixed This mode supports both wireless B and G clients.</p> <p>802.11g only This mode supports wireless-G clients that offer transmission rates of up to 54Mbps in the 2.4GHz frequency band.</p>
Country	Choose the Country where you are located.
Channel (Only in AP mode)	This option allows you to select a frequency channel for the wireless communication.
Tx Rate	Allow you to choose the rate of data transmission from 2 Mbps to Auto.
Closed System	The access point will not broadcast its WLAN name (ESSID) when Closed system is enabled. By default Closed system is disabled.
Channel Survey	<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 mode supports this feature.</p>

SCAN FOR SITE SURVEY (ONLY FOR CLIENT MODE)

Step 1:

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



The image shows the 'WLAN Basic Setup' configuration page. It includes fields for 'The Current Mode' (Client Mode), 'ESSID' (complex-wp54g1e), 'Wireless Profile' (802.11b/g mixed), 'Country' (NO_COUNTRY_SET-(NA)), and 'Tx Rate' (Fully Auto). A 'Site Survey' button is highlighted with a green box. Below the configuration fields is an 'Apply' button and a 'Link Information' section with a 'Show Link Information' button.

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



The image shows the 'Site Survey' results page. It displays a table with columns for Bssid, SSID, Chan, Auth, Alg, and Signal. Below the table are 'Apply', 'Refresh', and 'Back' buttons.

Bssid	SSID	Chan	Auth	Alg	Signal
<input type="radio"/> 008048396769	wireless-AP	10	OPEN	WEP	94
<input type="radio"/> 00804839bd45	ts-np27g-1P1	1	OPEN	WEP	94
<input type="radio"/> 008048003472	PMD-28G	2	OPEN	WEP	10
<input type="radio"/> 00804835891e		10	OPEN	NONE	17
<input type="radio"/> 0080482be51d	BYSTROVANY	2	OPEN	NONE	12
<input type="radio"/> 008048358861	complex-np28g	10	OPEN	NONE	6
<input type="radio"/> 00804830b51b	BYSTROVANY	2	OPEN	NONE	0
<input type="radio"/> 00804821f7e4	GGG-2	5	OPEN	NONE	0
<input type="radio"/> 00804824c675	Any	3	OPEN	NONE	3
<input type="radio"/> 0080483780d7	27g-0705	6	WPA-PSK	TKIP	94

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-PSK, 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.

SHOW LINK INFORMATION (ONLY FOR 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.

The screenshot shows the 'WLAN Basic Setup' interface. At the top, it indicates 'The Current Mode' is 'Client Mode'. Below this are several configuration fields: ESSID (complex-wp54g1e), Wireless Profile (802.11b/g mixed), Country (NO_COUNTRY_SET-(NA)), and Tx Rate (Fully Auto). A 'Site Survey' button is located to the right of the ESSID field. At the bottom of the configuration area is an 'Apply' button. Below the configuration area, there is a 'Link Information' section with a 'Show Link Information' button highlighted by a green border.

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)

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 **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.

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 2:

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

Step 3:

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.

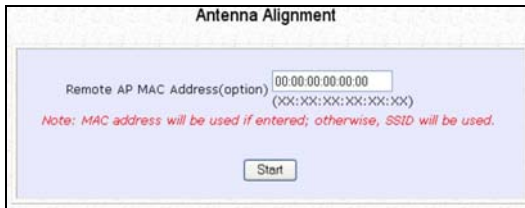
Parameters	Description
Freq	Refers to the frequency of the channel at which your access point is operating.
Channel	Refers to the channel of the access point being used for transmission depending on its origin of country.
MyQuality	Indicates the interference level of the respective channel with this 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-menu expanded under **WLAN Setup**. Click on **Antenna Alignment**. The **Antenna Alignment** page can act as a diagnostic tool to check the communication with a remote device. The remote AP MAC Address is preset to all zeros by default.

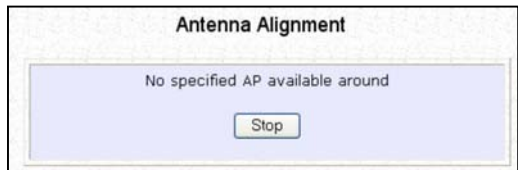


The screenshot shows the 'Antenna Alignment' configuration page. It features a text input field for 'Remote AP MAC Address(option)' with the value '00:00:00:00:00:00' and a placeholder '(XX:XX:XX:XX:XX:XX)'. Below the field is a red note: 'Note: MAC address will be used if entered; otherwise, SSID will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

Step 2:

If you wish to specify the MAC address of the remote AP, 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. It displays the message 'No specified AP available around' in the center. At the bottom of the screen is a 'Stop' button.



NOTE

If no MAC address is entered, the **Antenna Alignment** tool will make use of the SSID to align the antenna. Please 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:

Double-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	<p>The Radio Off When Ethernet Link Down function detects when the Ethernet link is down and disables the radio card automatically.</p>

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 AP MODE

Step 1:

Double-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

Step 1:

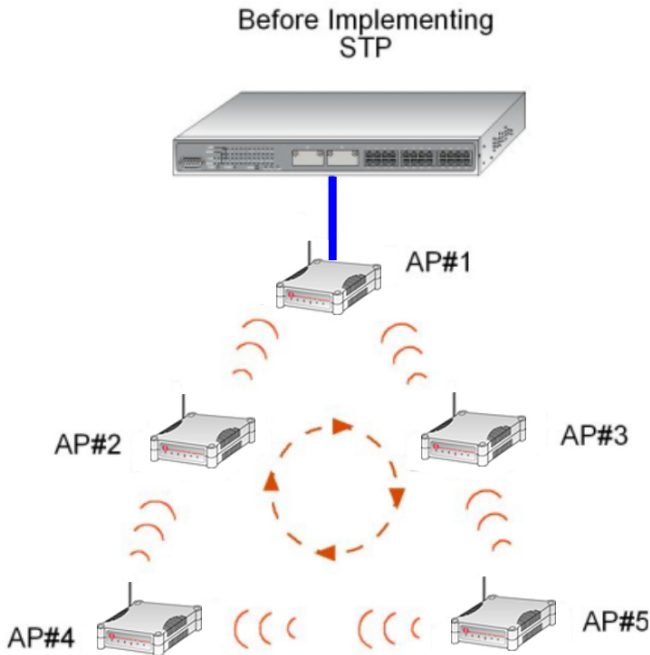
Double-click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Statistics**.

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.

STP SETUP

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.

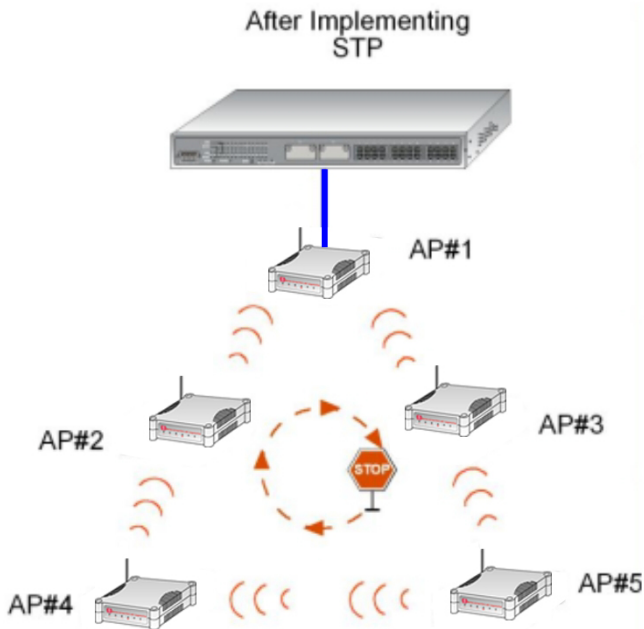


In short, the main purpose of activating STP is to prevent looping when you have redundant paths in the network. Without activating STP, redundant topology will cause broadcast storming.

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 & Pseudo VLAN on the wireless clients, we will compare 3 separate scenarios.

Scenario #1 – (No STP, No Pseudo VLAN)

Referring to the illustration below, if the Spanning Tree Protocol (STP) and Pseudo VLAN are 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, No Pseudo VLAN)

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

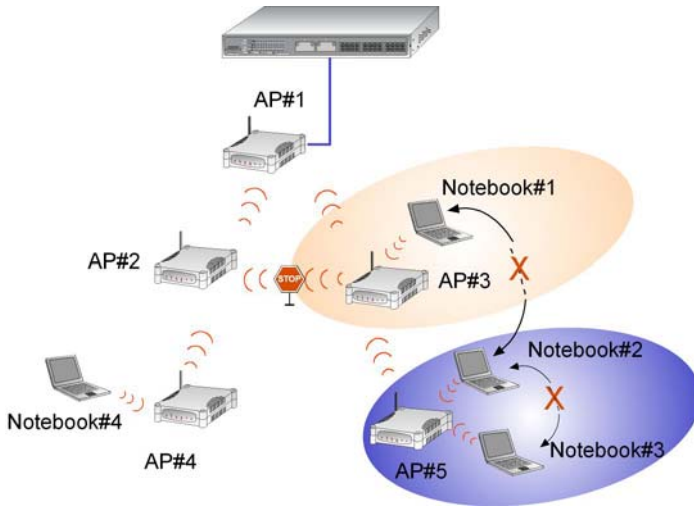
If one of the APs is down, the STP algorithm will reactivate one of the redundant paths so that the network connection will not be lost.

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



Scenario #3 – (With STP and Pseudo VLAN)

In this example, both STP and Pseudo VLAN Per Node are implemented in this network. When Pseudo VLAN Per Node is activated, the wireless users will be unable to access one another.



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.

Please note that MAC Filtering only filters wireless client MAC addresses. It does not filter the MAC addresses of computers connected to the Ethernet port, or the Ethernet network connection.

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 ▾

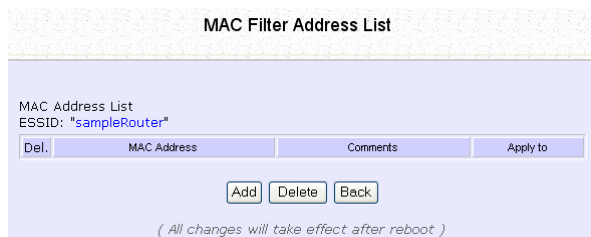
[View Complete MAC List](#)

(All changes will take effect after reboot)

Step 2:

MAC Filter Address List page displays.

Click the **Add** button.



The screenshot shows the "MAC Filter Address List" page. At the top, it says "MAC Filter Address List". Below that, it displays "MAC Address List" and "ESSID: 'sampleRouter'". There is a table with three columns: "Del.", "MAC Address", and "Comments". To the right of the table is an "Apply to" button. Below the table are three buttons: "Add", "Delete", and "Back". At the bottom, there is a note: "(All changes will take effect after reboot)".

Step 3:

Add MAC Address page displays.



The screenshot shows the "Add MAC Address" page. It has a form with the following fields: "MAC Address" (with a placeholder "(XX-XX-XX-XX-XX-XX)"), "Comment", and "Apply to All" (with a checked checkbox). Below the form is a table with three columns: "Selected", "AP ESSID", and "Security". The table has three rows: the first row has a checked checkbox, "sampleRouter", and "NONE"; the second row has an unchecked checkbox, "VAP1", and "NONE"; the third row has an unchecked checkbox, "VAP2", and "NONE". At the bottom are "Apply" and "Cancel" buttons.

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 ▾	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
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:

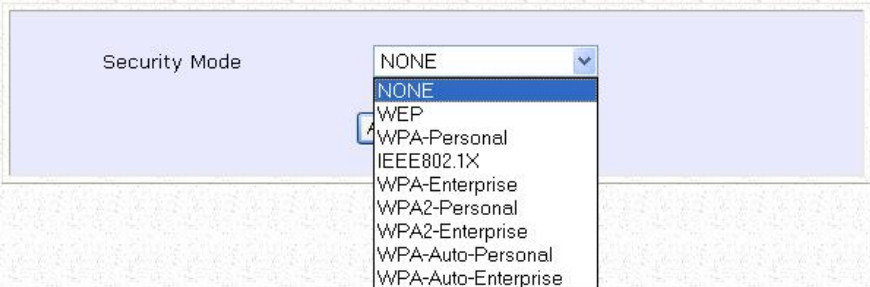
Click on **WLAN Setup** from the **CONFIGURATION** menu to select **Security**.

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

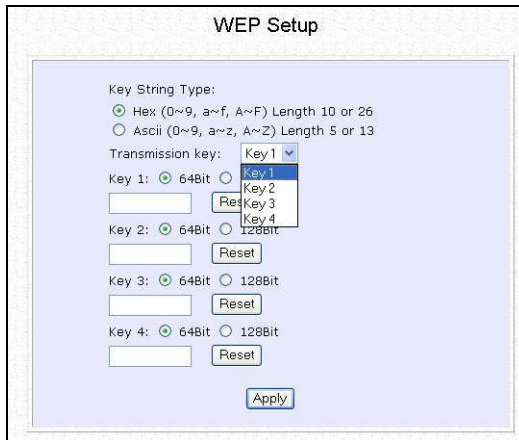


The screenshot shows the 'WLAN Security Setup' configuration page. The 'Security Mode' dropdown menu is open, displaying the following options: NONE (selected), WEP, WPA-Personal, IEEE802.1X, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise, WPA-Auto-Personal, and WPA-Auto-Enterprise.

HOW TO SET UP WEP

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

At the **WEP Setup** page,



The screenshot shows the 'WEP Setup' configuration page. It includes 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'. A list of options is visible: 'Key 1', 'Key 2', 'Key 3', and 'Key 4'.
- Key 1:** A radio button for '64Bit' (selected) and '128Bit'. Below it is an empty text input field and a 'Reset' button.
- Key 2:** A radio button for '64Bit' (selected) and '128Bit'. Below it is an empty text input field and a 'Reset' button.
- Key 3:** A radio button for '64Bit' (selected) and '128Bit'. Below it is an empty text input field and a 'Reset' button.
- Key 4:** A radio button for '64Bit' (selected) and '128Bit'. Below it is an empty 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 mode)

The guidelines below will help you to set up the access point for using WPA-PSK. 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: 11111111

Cipher Type: AUTO

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 **WPA-PSK** (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 2:

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 3:

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 4:

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 mode)

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

At the IEEE 802.1x Setup page,

IEEE 802.1X Setup

Primary RADIUS Server IP	0.0.0.0
Secondary RADIUS Server IP	0.0.0.0
Authentication Port	1812
Accounting Port	1813
Shared Secret Key
Broadcast Key Rotation(seconds)	600 (60~9999)
Key Length	64 bits

Step 1:

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

The RADIUS authentication server MUST be in the same subnet as your 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-EAP and WPA-EAP-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	0.0.0.0
Secondary RADIUS Server IP	0.0.0.0
Authentication Port	1812
Accounting Port	1813
Shared Secret Key	*****
Cipher Type:	AUTO
GTK update(seconds):	TKIP AES AUTO (60~9999)
Apply	

Step 1:

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

You can optionally add in the IP address of a **Secondary RADIUS Server**, if any. The RADIUS authentication server MUST be in the same subnet as your 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 2:

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 6:

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 7:

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.

ACCESS CONTROL – THE WIRELESS PSEUDO VLAN

(Only in Access Point mode)

A **VLAN** is a group of PCs or other network resources that behave as if they were connected to a single network segment although they may be physically located on different segments of a LAN.

Those stations which are assigned to the same VLAN share network resources and bandwidth as if they were connected to the same segment. Conversely, only the stations within the same VLAN can access each other.

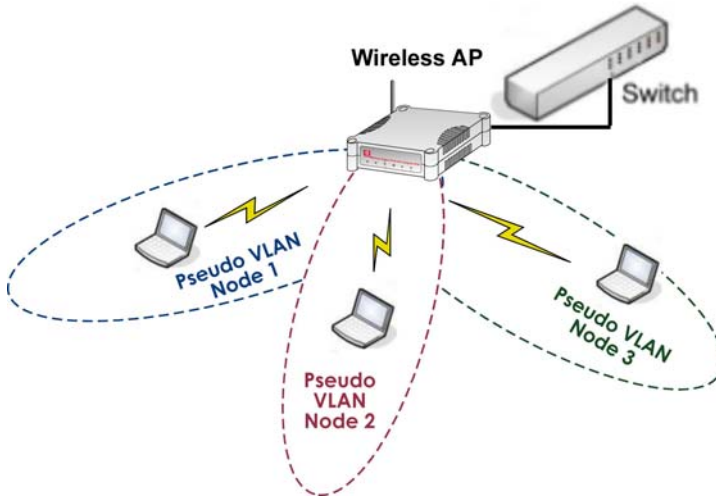
A **Wireless Pseudo VLAN** acts by segregating a single wireless LAN into multiple VLANs so that communication is possible only among wireless clients within the same VLAN.

When operating in the **Access Point** mode, the access point allows you to define *Wireless Pseudo VLAN Per Node* and *Wireless Pseudo VLAN Per Group*.

To learn more about Compex's exclusive **Wireless Pseudo VLAN**, please refer to the white paper available online at www.cpx.com or www.compex.com.sg.

WIRELESS PSEUDO VLAN PER NODE

When implemented, this mode isolates each wireless client into its own pseudo VLAN. Wireless clients can therefore access resources on the wired network but are unable to see each other or access each other's data.



The following steps demonstrate how to set up a Wireless Pseudo VLAN per Node.

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 **Wireless Pseudo VLAN** button.

The screenshot displays the 'WLAN Advanced Setup' configuration page. It features several input fields and dropdown menus for various parameters:

- Beacon Interval: 100 (range: 100-1000)
- Data Beacon Rate (DTIM): 1 (range: 1-16384)
- RTS/CTS Threshold: 2312 (range: 2312-2312)
- Frag Threshold: 2346 (range: 2346-2346)
- Transmit Power: Maximum (dropdown menu)
- Radio Off When Ethernet Link Down:
- Antenna Control: Auto (dropdown menu)

Below these settings is an 'Apply' button. At the bottom of the page, the 'Extended Features' section is visible, containing three buttons: 'Wireless Pseudo VLAN', 'WDS Configuration', and 'Long Distance Parameters'.

Step 3:

The **Wireless Pseudo VLAN** function is disabled by default. Click on the **Change** button to make your selection of the type of Pseudo VLAN to implement.

Step 4:

Select the **Per node** radio button and click on the **Apply** button.

Select Wireless Pseudo VLAN Type

Disable
 Per node
 Per group

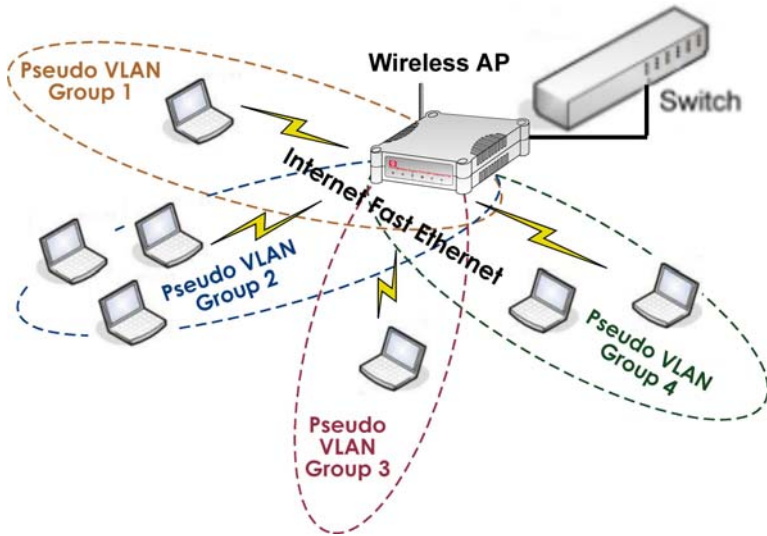
The Wireless Pseudo VLAN has configured as Per node.

Wireless Pseudo VLAN

Type : Per node

WIRELESS PSEUDO VLAN PER GROUP

The access point can configure up to four 'groups' of wireless clients identified by their MAC address. Whenever a wireless client requests network access, the access point will first verify whether its MAC address is present in any of the Pseudo VLAN groups. If it is, the access point will grant it access to the wired system resources and to all other wireless clients belonging to the same Pseudo VLAN group only.

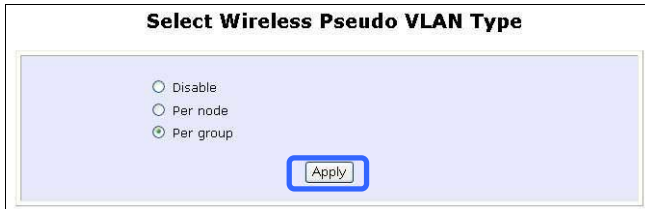


The following steps demonstrate how to set up Wireless Pseudo VLAN Groups.

CREATE A CLIENT IN A PSEUDO VLAN GROUP

Step 1:

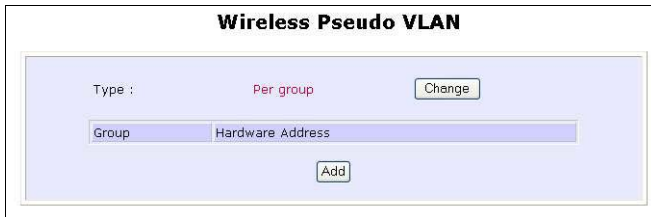
From the **Select Wireless Pseudo VLAN Type** page, select **Per group** and click on the **Apply** button.



The screenshot shows a configuration page titled "Select Wireless Pseudo VLAN Type". It contains three radio button options: "Disable", "Per node", and "Per group". The "Per group" option is selected. Below the options is an "Apply" button.

Step 2:

Click on the **Add** button to create a client in the Wireless Pseudo VLAN group.



The screenshot shows a configuration page titled "Wireless Pseudo VLAN". It displays "Type : Per group" with a "Change" button next to it. Below this is a table with two columns: "Group" and "Hardware Address". An "Add" button is located below the table.

Step 3:

Select a group number from the **Group** drop-down list.

Add Wireless Pseudo VLAN Entry

Group:

Hardware Address: (xx-xx-xx-xx-xx-xx)

Step 4:

Fill in the **Hardware Address** field with the MAC address of the client in the format **xx-xx-xx-xx-xx-xx**, where x is any value within the range 0-9 or a-f.

Step 5:

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

The Pseudo VLAN group has been added to the list as shown below.

Wireless Pseudo VLAN

Type : Per group

Group	Hardware Address
01	00-80-45-e5-0d-05



NOTE

A client can be a member of more than one Pseudo VLAN group. For instance, if a client is a member of wireless Pseudo VLAN groups 01 and 02, it will be able to communicate with the other clients in both groups.

ADD ANOTHER CLIENT IN A PSEUDO VLAN GROUP

Follow the procedures mentioned in Steps 3-5. You can create up to 32 members per Wireless Pseudo VLAN group.

EDIT/DELETE A CLIENT IN A PSEUDO VLAN GROUP

Step 1:

Click on the **MAC address** in the table as shown below.

Group	Hardware Address
01	00-80-45-e5-0d-05

Step 2:

From the **Edit Wireless Pseudo VLAN Entry** page,

Click on the **Delete** button to remove the client from the group, or Click on the **Save** button after you had edited the entry.

Group: group 01
Hardware Address: 00-80-45-e5-0d-05 (XX-XX-XX-XX-XX-XX)

Save Delete Cancel

WIRELESS SETUP - THE WIRELESS DISTRIBUTED SYSTEM

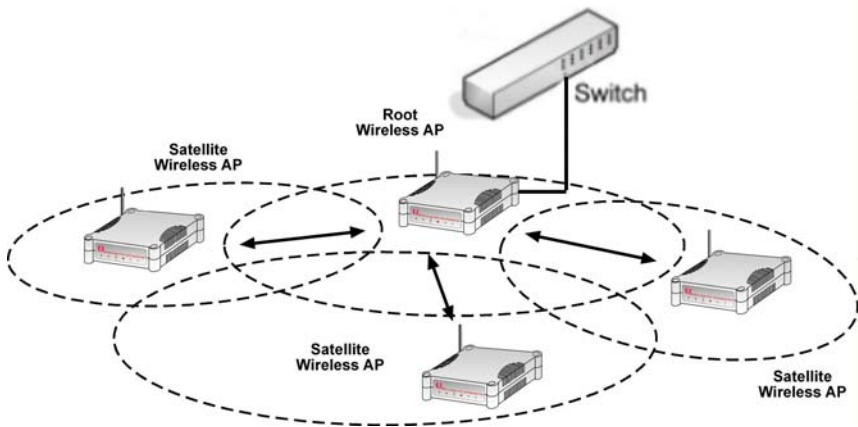
(Only in Access Point mode)

A wireless distribution system creates a wider network in which mobile users can roam while still staying connected to the available network resources by linking up several access points.

In a WDS, the access point can drive a cell of wired and wireless clients while at the same time, connecting to other access points. This requires the operational frequency channel to be the same within the cell controlled by your access point as well as for its wireless links to the other access points.

Star Configuration WDS

In a star configuration WDS, links are established between one root access point and several satellite wireless APs positioned to increase the area covered.

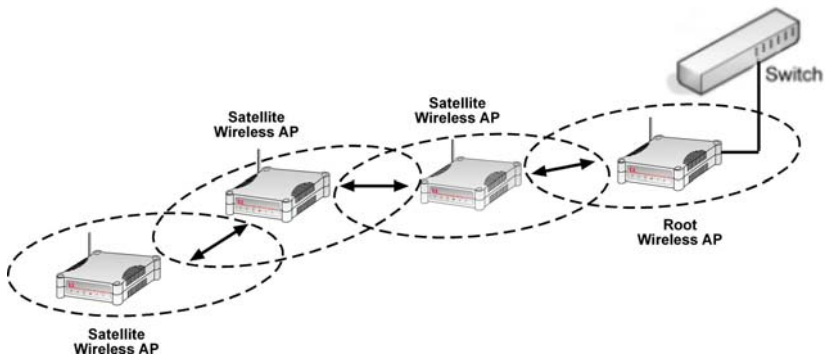


Here, the root Wireless AP connects to the wired network and maintains three WDS links while each satellite Wireless AP (Access Point) maintain a WDS link for communication with the root.

Chain Configuration WDS

A chain configuration WDS spans an area in length, for instance a long corridor. Satellite access points are chained together starting from a root access point.

The access point at either end of the chain will have only one WDS link enabled, while the access points in the middle will have two WDS links configured to associate with the neighboring access point upward and downward in the chain.



The following steps will guide you in setting up WDS in your access point.

CREATE A CLIENT IN A WDS

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 **WDS Configuration** button.

The image shows a screenshot of a web interface for configuring WLAN settings. The top section is titled "WLAN Advanced Setup" and contains several configuration fields:

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 these fields is an "Apply" button.

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

Step 3:

As illustrated on the **WDS Setup**, the **WDS** feature is disabled by default. Click on the **Change** button.



WDS Configuration

WDS Status : Disable Change

Step 4:

From the **Enable/Disable WDS** page, select **Enable** and click on the **Apply** button.



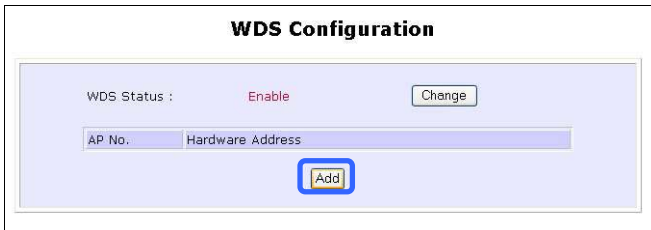
Enable/Disable WDS

Enable Enable the wireless wds function
 Disable Disable the wireless wds function

Apply

Step 5:

Click on the **Add** button to create a MAC address of a client.



WDS Configuration

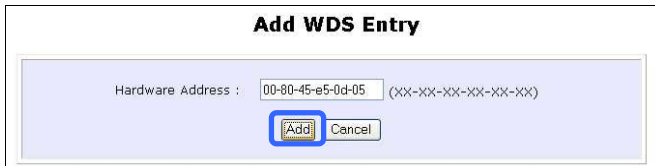
WDS Status : Enable Change

AP No. Hardware Address

Add

Step 6:

Fill up the **Hardware Address** field with the wireless MAC address of the device to include in your WDS, using the format xx-xx-xx-xx-xx-xx, where x can take any hexadecimal value 0-9 or a-f.



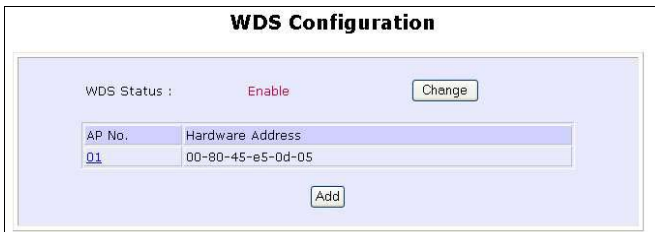
Add WDS Entry

Hardware Address : (xx-xx-xx-xx-xx-xx)

Click on the **Add** button to update the table.

Step 7:

From the **WDS Configuration** page, notice that the MAC Address has been added to the table as shown below.



WDS Configuration

WDS Status : Enable

AP No.	Hardware Address
01	00-80-45-e5-0d-05



NOTE

To configure WDS, all your access points must use the same channel and security mode and both access points at opposite ends of a WDS link must have each other's wireless MAC address

ADD ANOTHER CLIENT IN A PSEUDO VLAN GROUP

Follow the procedures mentioned in Step 5 to Step 7.

EDIT/DELETE A CLIENT IN A WDS

Step 1:

Click on the **MAC address** in the table as shown below.

WDS Configuration

WDS Status : Enable

AP No.	Hardware Address
01	00-80-45-e5-0d-05

Step 2:

From the **Edit WDS Entry** page,

Click on the **Delete** button to remove the client from the WDS, or
Click on the **Save** button after you have edited the entry.

Edit WDS Entry

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

LONG DISTANCE PARAMETERS

This setup allows the WP54G 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 web interface. The top screenshot is titled "WLAN Advanced Setup" and contains the following configuration options:

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 these options 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: Enable

Distance(meter): 120

SlotTime(us): 9

ACKTimeOut(us): 18

CTSTimeOut(us): 18

Show Reference Data

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.

Apply

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: Enable

Distance(meter): 100

Show Reference Data

Microsoft Internet Explorer

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

OK

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 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 the 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.

Chapter 7: System Utilities

This chapter provides guidelines in using:
The **SYSTEM TOOLS** menu
The **HELP** menu

USING THE SYSTEM TOOLS MENU

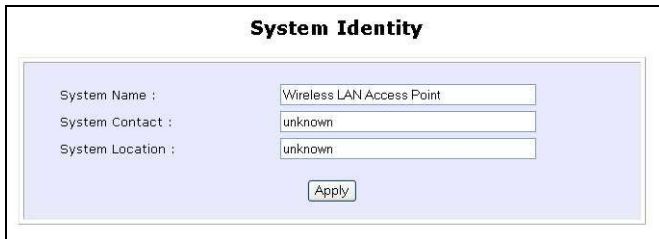
SYSTEM IDENTITY

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 the 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 fields are labeled "System Name :", "System Contact :", and "System Location :". The values entered in the fields are "Wireless LAN Access Point", "unknown", and "unknown" respectively.

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.

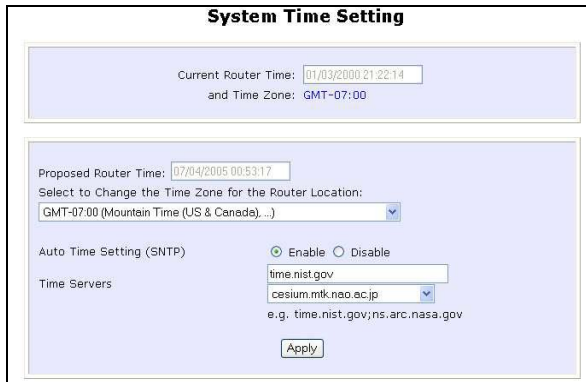
Step 5:

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 'time.nist.gov' and a drop-down menu showing 'cesium.mtk.nao.ac.jp'. Below the drop-down, 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.

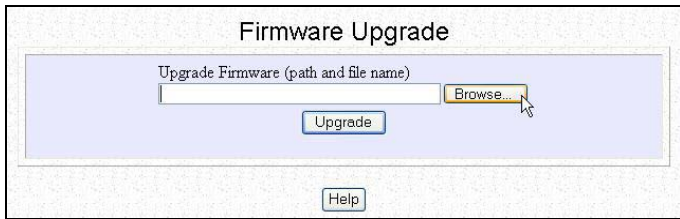
FIRMWARE UPGRADE

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.

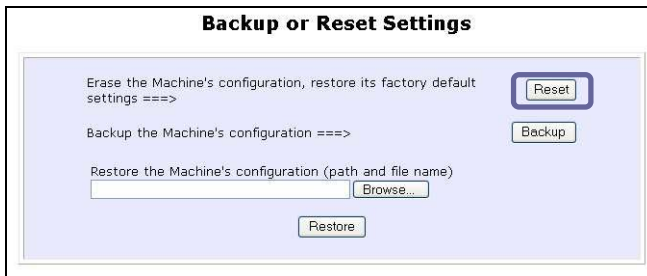
RESET YOUR SETTINGS

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.

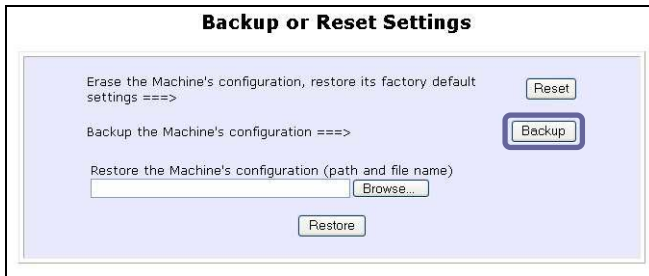
BACKUP YOUR SETTINGS

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.



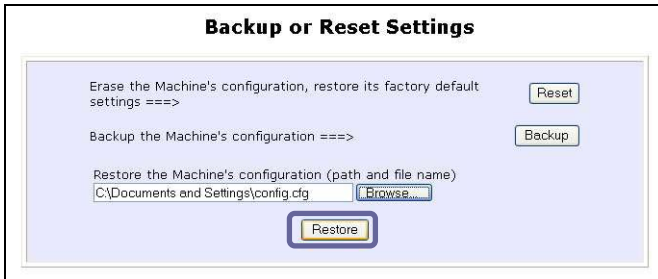
RESTORE YOUR SETTINGS

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

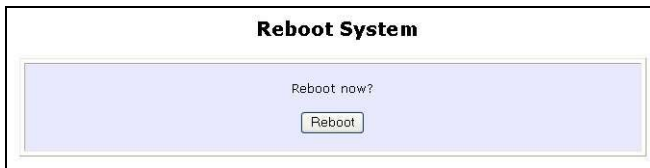
Most of the changes you make to the system's settings require a system reboot before the new parameters can take effect.

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: "Current Password:", "New Password:", and "Confirm Password:". Each field is filled with a series of dots representing masked text. Below the fields is a yellow "Apply" button.

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.



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 the access point's configuration settings.

System Information

Device:

System Up Time :	0 Days 00:09:11
BIOS/Loader Version :	2.1f (build 0310)
Firmware Version :	1.43 (build 0628)
NetWork Mode :	Inherent Bridge

Wireless:

Hardware Address :	00-80-48-3d-0f-81
WLAN name (ESSID):	compex-wp54g
Operating frequency :	5180MHz
Operating Channel :	36
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 (LED 1).

State	Diagnostic LED (LED 1) State
Corrupted firmware - the 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 crossover 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. The computer will obtain an IP address of **192.168.168.100** from the access point. Otherwise, configure your computer's IP address to 192.168.168.100 and its network mask to 255.255.255.0.

Step 4:

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

Firmware Recovery

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\wp54gxxxx.IMG**, then replace the command with this new path and firmware name. In our example:

C:\WP54G\TFTP -I 192.168.168.1 PUT wp54gxxx.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 your 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:

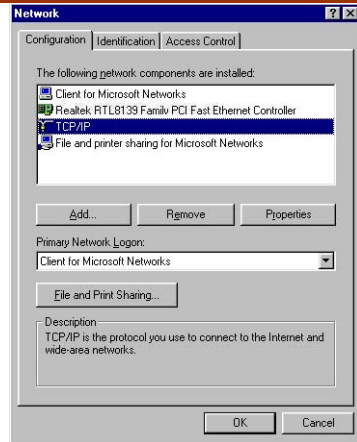
From your desktop, right click **Network Neighborhood** icon and select **Properties**.

Step 2:

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

Step 3:

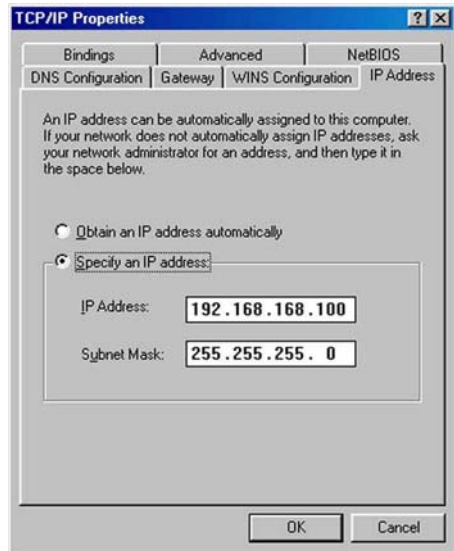
Highlight the **TCP/IP** and click on **Properties** button.



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.

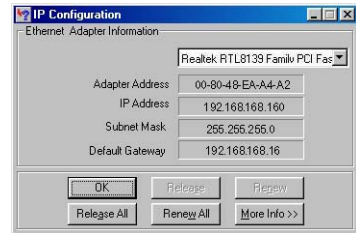


Step 5:

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 *winipcfg*.

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

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



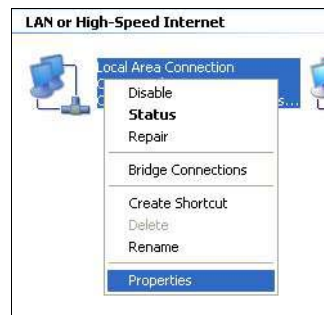
FOR WINDOWS XP/2000

Step 1:

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

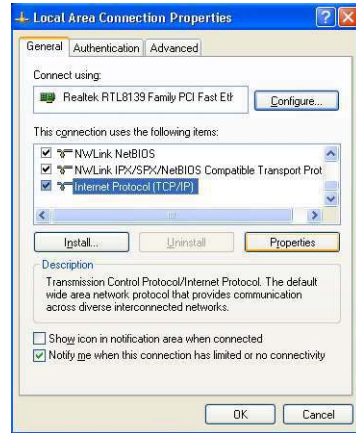
Step 2:

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



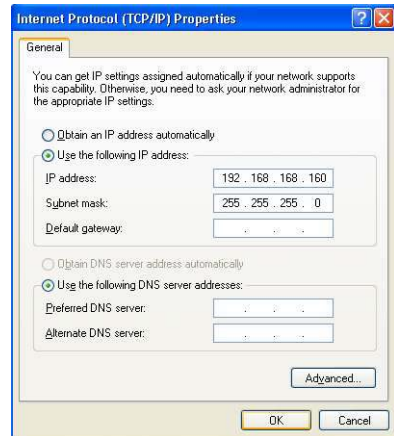
Step 3:

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.

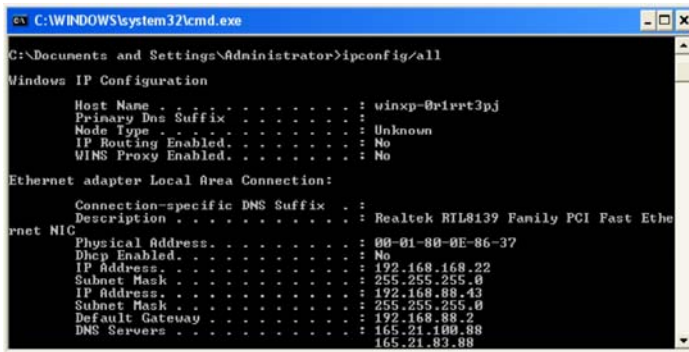


Step 5:

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

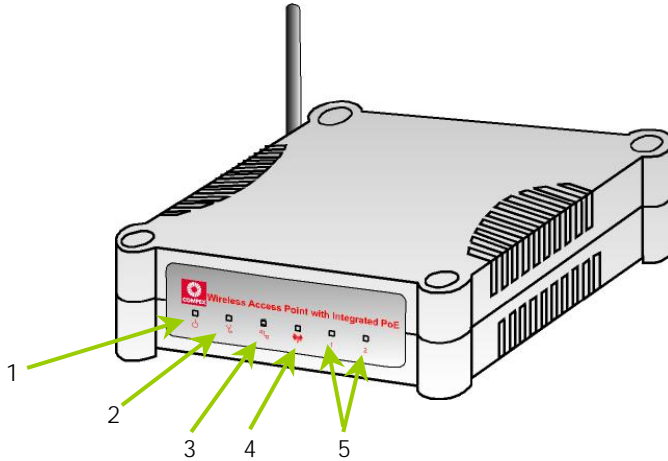
Ethernet adapter Local Area Connection:





   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 the access point.

Appendix III: Panel Views & Descriptions

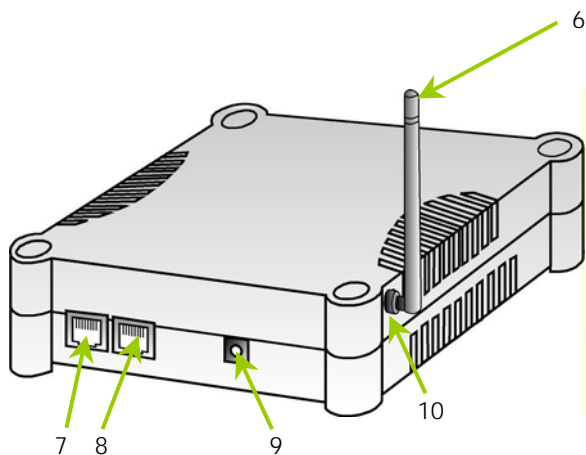
Front View of the Access Point



	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 goes off when the diagnostic is passed.
3	 LED (LAN Link/Act)	Steady Green	LAN connection is established.
		Flashing Green	Data transmission at LAN connection.
4	 LED	Steady Green	Wireless interface up and running. Ready for operation.

	(WLAN Link/Act LED)	Flashing Green	Activity is detected in the wireless network.
	Name	Description	
5	1 2 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.

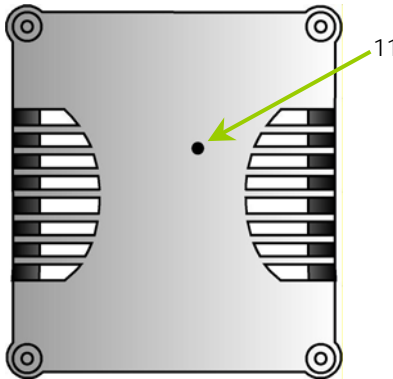
Back View of the Access Point



	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 the 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: Technical Specifications

Safety and Electromagnetic Conformance	FCC Part 15 SubPart B and SubPart C [for wireless module] EN 300 328-2 [for wireless module] EN 301 489 (EN300 826) [for wireless module] EN 55022 (CISPR 22)/EN 55024 Class B EN 61000-3-2 EN61000-3-3 CE EN 60950
Industrial Standards	IEEE 802.11b IEEE 802.11g IEEE 802.3 IEEE 802.3u
Wireless Operation Range IEEE 802.11b: IEEE 802.11g:	80m (54Mbps outdoor), 20m (54Mbps indoor) 300m (11Mbps outdoor), 100m (11Mbps indoor)
Frequency Range IEEE 802.11b: IEEE 802.11g:	2.4 ~ 2.4835 GHz 2.4 ~ 2.497 GHz
Wireless Operation Modes	Access Point Access Point Client
Security	64 - bit / 128 - bit WEP WPA-Enterprise, WPA-Personal, WPA2-Enterprise, WPA2-Personal, WPA-Auto-Enterprise, WPA- Auto-Personal Pseudo Virtual LAN IEEE 802.1x – TLS, TTLS, PEAP, EAP-SIM
Network Interface	10/100 Mbps auto-negotiating Ethernet ports

Modulation Techniques	OFDM (BPSK, QPSK, 16-QAM, 64-QAM) DSSS (BPSK, QPSK, CCK)
Receiver Sensitivity	Up to -90dBm
Output Power IEEE 802.11b: IEEE 802.11g:	20 dBm 20 dBm
Operating Channels	11 Channels: US and Canada 13 Channels: Europe 14 Channels: Japan
Advanced Wireless Features	Wireless Distribution System (WDS) Long Distance Parameters Setup Wireless Pseudo VLAN <ul style="list-style-type: none"> - Per Node - Per Group - Tagged VLAN pass-through Adjustable transmit power control (in 1dB steps) Smart Select STP
Antenna	Detachable 2dBi antenna with SMA connector
Built-in DHCP Server	Yes
DHCP Reservation	By MAC address
Profile Backup & Restore	Yes
Firmware Upgrade	Yes
Power Requirements Using Power Adapter: Using PoE:	Output 24VDC – 48VDC (localized to country of sale) 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 148mm x 41m (with antenna)