

Wireless-G Dual-Band Network Access Point
Wireless-G Dual-Band Network Access Point



networks@work

USER'S MANUAL



COMPEX NETPASSAGE SERIES

WPE54G

WPE54G

WPE54G

WPE54G

WPE54G

Manual Number: U-0436-V1.1 C

© 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-0436-V1.1C Version 1.1, November 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:

1. This device may not cause harmful interference, and
2. 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: Compex Wireless-A/G Dual-Band Network Access Point

Model No.: Compex WPE54AG conforms to the following Product Standards:

Radiated Emission Standards:

ETSI EN 300 328-2: July 2000; FCC: 47 CFR Part 15, Subpart B, ANSI C63.4-1992; 47 CFR Part 15, Subpart C (Section 15.247), ANSI C63.4-1992.

Conducted Emission Standards:

ETS 300 826: Nov. 1997.

Immunity Standards:

IEC 801-2; IEC 801-3; IEC 801-4

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.

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

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)
 Fax	Tel: +1 (800) 279-8891 (Ext.122 Technical Support) Fax: +1 (714) 482-0332
Asia, Australia, New Zealand, Middle East and the rest of the World	
 Write	Compex Systems Pte Ltd 135, Joo Seng Road #08-01, PM Industrial Building Singapore 368363
 Call	Tel: (65) 6286-1805 (8 a.m.-5 p.m. local time)
 Fax	Tel: (65) 6286-2086 (Ext.199 Technical Support) Fax: (65) 6283-8337
Internet access/	E-mail: support@compex.com.sg FTPsite: ftp.compex.com.sg
Website:	http://www.cpx.com or http://www.compex.com.sg

About This Document

The product described in this document, Compex Wireless-G Network Access Point, Compex WPE54G is a licensed product of Compex Systems Pte Ltd. This document contains instructions for installing, configuring and using Compex WPE54G. 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 Compex WPE54G.

Firmware

This manual is written based on Firmware version 2.07

Conventions

In this document, special conventions are used to help and present the information clearly. The Compex Wireless-A/G Dual-Band Network Access Point is often referred to as Compex WPE54G 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.....	9
1.1 Introduction.....	9
1.2 Features and Benefits	9
1.3 When to use which mode	11
1.3.1 The Access Point Mode	12
1.3.2 The Access Point Client Mode.....	13
1.3.3 The Gateway Mode.....	14
1.3.4 The Wireless Routing Client Mode	16
1.3.5 The Wireless Ethernet Adapter Mode.....	17
1.3.6 The Wireless Bridge Link Mode.....	17
Chapter 2 Hardware Installation	18
2.1 Setup Requirements	18
2.2 Hardware Installation	19
Chapter 3 Access to Web-based Interface	20
3.1 Access to the Web interface with uConfig	20
3.2 Direct access to web-based interface via Internet Explorer.....	23
Chapter 4 Common Configuration.....	27
4.1 Management Port Setup	27
4.1.1 To view the active DHCP leases.....	30
4.1.2 To reserve specific IP addresses for predetermined DHCP clients	31
4.2 WLAN Setup.....	34
4.2.1 To configure the Basic setup of the wireless mode.....	35
4.2.2 To configure the Advanced setup of the wireless mode.....	38
4.3 Scan for Site Survey.....	41
4.3.1 Show Link Information.....	43

4.4	Wireless Extended Features	44
4.4.1	Access Control – The Wireless Pseudo VLAN.....	44
4.4.2	Wireless Setup - The Wireless Distributed System (WDS)	52
4.4.3	WMM Parameters.....	58
4.4.4	Long Distance Parameters	61
4.5	WLAN Security	63
4.5.1	How to set up WEP.....	64
4.5.2	How to set up WPA-PSK.....	66
4.5.3	How to set up 802.1x/RADIUS	68
4.5.4	How to set up WPA EAP.....	69
4.6	STP Setup.....	71
4.7	SNMP Setup.....	79
4.8	MAC Filtering.....	79
 Chapter 5 Further Configuration.....		 81
5.1	Setting up uConfig	81
5.2	Configuring WAN Setup.....	82
5.2.1	Dynamic IP.....	83
5.2.2	Static IP	84
5.2.3	PPPoE.....	85
5.2.4	Singapore ADSL.....	87
5.2.5	Australia BPA Cable.....	88
5.2.6	PPTP	89
5.3	Using NAT.....	90
5.3.1	To set up a De-Militarised Zone host.....	91
5.3.2	To set up port forwarding	92
5.4	Routing 96	
5.4.1	Static Routing	97
5.4.2	Dynamic Routing.....	98
5.5	Implementing IP Filtering	99
5.6	Applying Remote Management.....	104
5.7	Enabling Parallel Broadband.....	105
5.7.1	Load balancing.....	105
5.7.2	Fail-Over Redundancy.....	106
5.7.3	To enable Parallel Broadband	107
 Chapter 6 System Utilities		 108
6.1	Using the SYSTEM TOOLS Menu.....	108
6.1.1	System Identity	108
6.1.2	WLAN Station List.....	109
6.1.3	Set System's Clock	110
6.1.4	Firmware Upgrade	111
6.1.5	Save or Reset Settings.....	112

6.1.6	Reboot System.....	113
6.1.7	Change Password.....	114
6.1.8	Logout.....	115
6.2	Using the HELP menu.....	116
6.2.1	Get Technical Support	116
6.2.2	About System	117
Appendix I Troubleshooting.....		118
AI	Solutions to Common Problems	118
Appendix II Firmware Recovery		122
AII	How to recover the access point from failed firmware	122
Appendix III TCP/IP Configuration.....		123
AIII.1	Configure dynamic IP Address in Windows 98SE/ME.....	123
AIII.2	Configure dynamic IP Address in Windows XP/2000	127
AIII.3	Configure static IP Address in Windows 98SE/ME.....	129
AIII.4	Configure static IP Address in Windows XP/2000	130
Appendix IV Panel Views and Descriptions		131
Appendix V Technical Specifications.....		cxxxiii

1.1 Introduction

The Compex NetPassage WPE54G is a 54Mbps wireless access point that is interoperable with all standard based 802.11g and 11b wireless devices. The Compex NetPassage WPE54G is a compact and high performance access point that is designed with support for high security features like Wi-Fi Protected Access (WPA), IEEE 802.1x Authentication and 64-bit or 128-bit Wired Equivalent Privacy. Compex exclusive wireless LAN technology Wireless Pseudo VLAN further enhances security in wireless hotspot networks in isolating different users into their own VLANs. The NetPassage WPE54G is capable of operating in 5 different modes: Access Point Bridging, Access Point Client, Gateway, Wireless Routing Client and Wireless Ethernet Adapter; making it suitable for all kinds of wireless applications.

1.2 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 the access point's full potential

Wireless Distribution System

This unique feature allows linking of several access points, virtually creating a larger wireless network infrastructure that allows desktops or laptops that are connected to the access point to share their network resources wirelessly.

Pseudo Virtual LAN

The unique Wireless Pseudo Virtual LAN technology is a feature that allows a wireless client or groups of wireless client to be segmented wirelessly into its individual workgroup or individual node thus enhancing the privacy of the wireless clients. This is especially useful in public hotspot deployment.

Secured Wireless Authentication

The access point supports the latest wireless security standard—Wi-Fi Protected Access. The wireless users now enjoy the freedom of wireless roaming without worrying important data being exposed to outsiders. WPA has two different modes: WPA-PSK for SOHO users and WPA-EAP for Enterprise users. The access point supports WPA-EAP using IEEE 802.1x-based Extensible Authentication Protocol (EAP) for secure and centralized user-based authentication. The wireless clients are now able to authentication through a RADIUS server to the authorized network through highly secured authentication methods like EAP-TLS, EAP-TTLS, and EAP-PEAP.

Chapter 2 Hardware Installation

Smart Select

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

Wireless Routing Client Capability

The Wireless Routing Client mode enables Internet Service Provider (ISP) or offices to send their data packet wirelessly and these network packets will be routed to a wired Local Area Network via the access point.

Wireless Ethernet Adapter

The Wireless Ethernet Adapter mode enables any computers with an Ethernet interface to be connected to the wireless LAN without the need to install any driver software. This is extremely useful for machines with limited driver support, e.g. Apple Macintosh machines and Linux machines.

Parallel Broadband

This unique feature allows bandwidth aggregation and fail-over redundancy capability when set to gateway mode which uses wireless distribution system to wirelessly link all associated access point gateway together.

Universal Configuration Software

The uConfig software allows users to get onto the web based configuration interface of the access point without the need to further manipulate the TCP/IP setup of the workstation.

Web-based Management Interface

Embedded with a HTTP server allows the configuration of the access point features via a user-friendly web-based management interface. In addition, firmware upgrade can be done through this interface as well.

IEEE 802.1x Authentication and Wi-Fi Protected Access (WPA)

The access point supports latest wireless security Wi-Fi Protected Access (WPA) using both Pre-Share Key and 802.1x EAP authentication. A wide range of IEEE 802.1x authentication methods like EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP for strong mutual authentication and data encryption is supported.

Wireless Pseudo Virtual LAN

Allows the creation of wireless virtual nodes or workgroups for wireless clients to increase the privacy in a wireless LAN installation.

SNMP

For easy remote management and monitoring of the access point through standard SNMP software.

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.

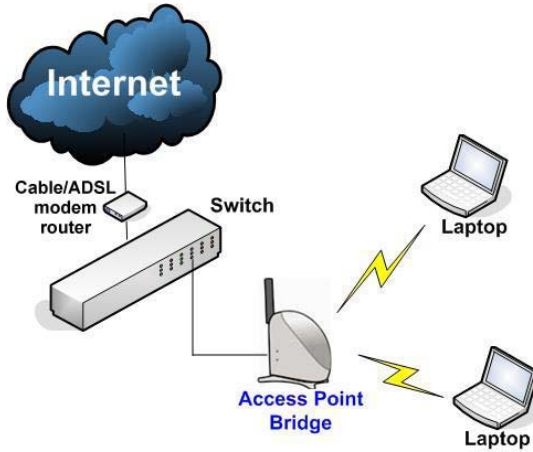
1.3 When to use which mode

The access point is unique in the sense that it may operate in up to 5 different complex modes in order to best suit any type of network application that you require.

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

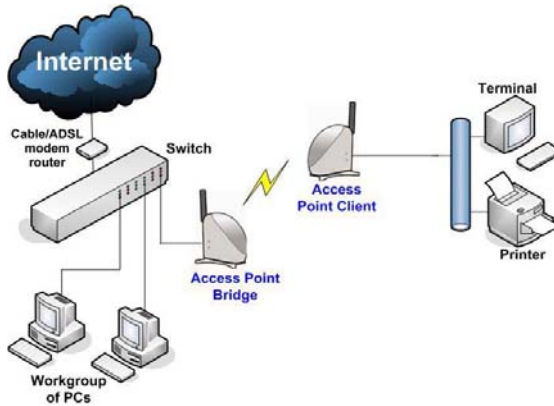
1.3.1 The Access Point Mode

This is the default mode of the access point. The **Access Point** mode enables you to bridge wireless clients to the wired network infrastructure.



1.3.2 The Access Point Client Mode

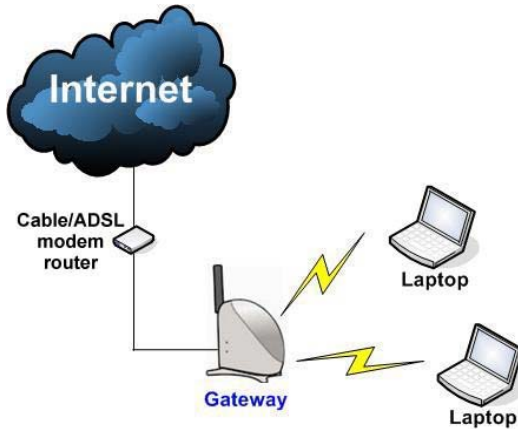
In **Access Point Client** mode, the access point acts as a wireless client that can operate wirelessly with another access point to perform transparent bridging between two Fast Ethernet networks.



1.3.3 The Gateway Mode

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

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



Static IP address

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

Dynamic IP address

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

This type of connection applies for instance, to:

- Singapore Cable Vision subscribers
- @HOME Cable Service users

Chapter 2 **Hardware Installation**

PPP over Ethernet (PPPoE)

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

For instance:

If you are in Germany which uses T-1 connection or

If you are using SingNet Broadband or Pacific Internet Broadband in Singapore:

Singapore ADSL (Ethernet 512K)

This applies to ADSL subscribers in Singapore including SingTel Magix SuperSurf users.

Australia BPA Cable

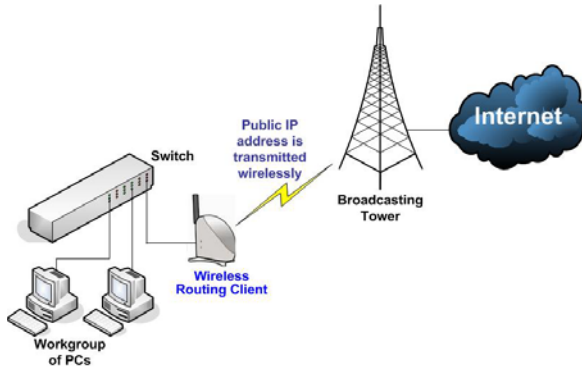
This connection type is customised for Big Pond Cable Internet users in Australia.

PPTP

The Point-to-Point Tunneling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks.

1.3.4 The Wireless Routing Client Mode

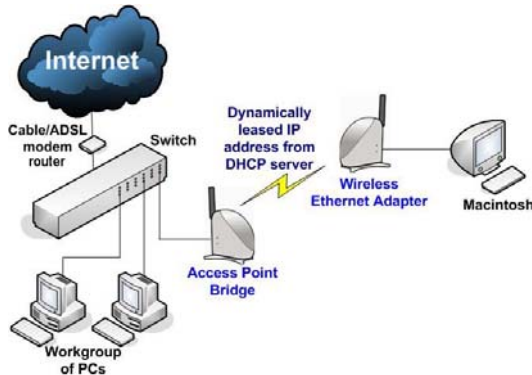
An application of this mode would be for the Ethernet port of the **Wireless Routing Client** to be used for connection with other devices on the network while access to the Internet would be achieved through wireless communication with wireless ISP.



1.3.5 The Wireless Ethernet Adapter Mode

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

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



1.3.6 The Wireless Bridge Link Mode

The **Wireless Bridge Link** mode allows point-to-point communication between different buildings. It enables you to bridge wireless clients that are kilometres apart (eg. within 100 metres between two buildings) while unifying the networks. In this scenario, you may configure two of the access point units to perform transparent bridging between two buildings.

2.1 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

2.2 Hardware Installation

In three simple steps, you may power ON and begin configuring the access point.

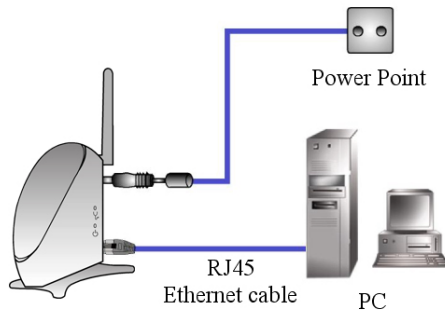
Step 1

Use the RJ45 cable to connect the Ethernet port of the access point to your PC.

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

Step 2

Next, attach the power adapter supplied in the packaging to the main power supply and connect its power plug into the DC jack of the access point.



Step 3

Power ON your PC. Notice that the **Power** and **LAN** LEDs of the access point have lighted up. This indicates that the connection has been established successfully between the AP and your PC.

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

- **Through our Utility – uConfig**
You can access to the web-based interface directly without the need to assign an IP address to your PC.
- **Enter 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.xxx, where **x** can take any value from 2 to 254.so that it is in the same subnet as the access point.

3.1 Access to the Web interface with uConfig

The powerful uConfig utility has been developed to provide you hassle-free access to the web-based configuration page. It has been designed to give you direct access to the Web interface.

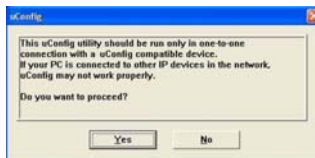
Step 1

Insert the Product CD into your CD-ROM drive.

Step 2

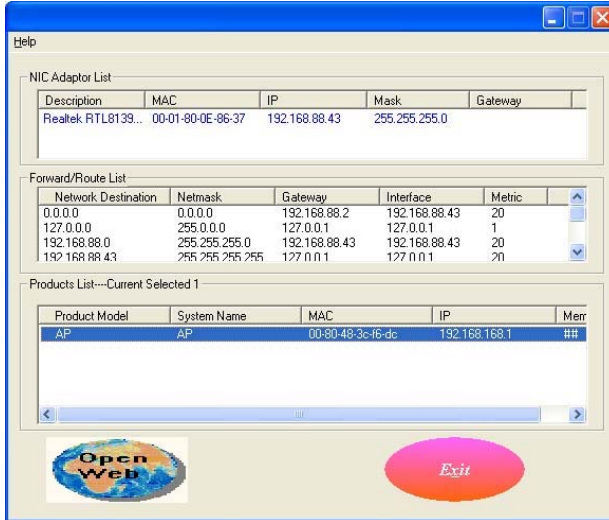
From the **Software** section, select to install the **uConfig** utility to your hard disk.

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



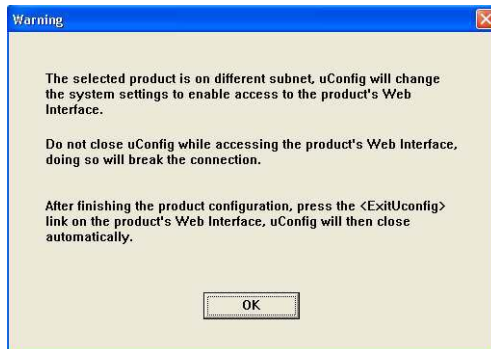
Step 3

Select the access point from the products list and click on **Open Web** button.



Step 4

This screen prompts you not to exit your uConfig program while accessing to your Web interface, or else you will fail to connect to your device. Click on **OK** to proceed.

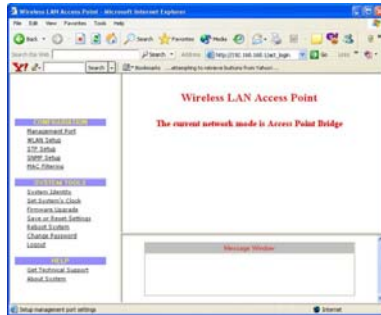


Step 5

At the authentication page, click on the **Log On!** button to enter the main configuration page.



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



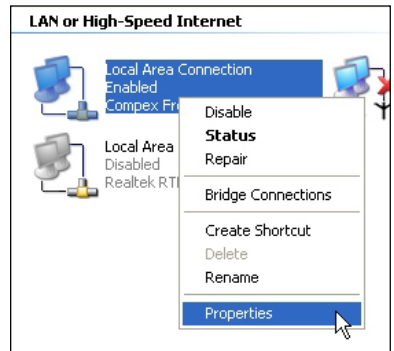
3.2 Direct access to web-based interface via Internet Explorer

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

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



2. Right click on your Ethernet adapter and select **Properties**.

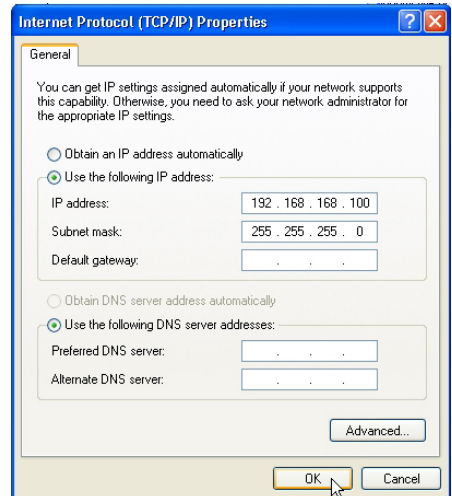


Chapter 3 Access to Web-based Interface

- Next, select on **Internet Protocol (TCP/IP)** and click on **Properties** button.



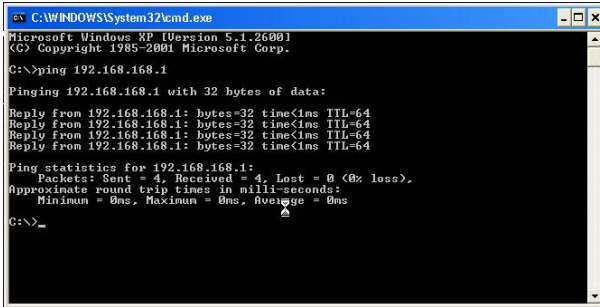
- Since the default IP address for the access point is 192.168.168.1, we need to set your PC's IP address to be the same subnet as your access point. Therefore, in this example, we assign an IP address of *192.168.168.100* and subnet mask as *255.255.255.0*.
- Click **OK** button to update the changes.



- Now, you may open the MS-DOS prompt window and type in *ping 192.168.168.1* to verify whether your PC can communicate with the access point.

Chapter 3 Access to Web-based Interface

7. If your TCP/IP settings are correct, you will get replies to the ping command:



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ping 192.168.168.1

Pinging 192.168.168.1 with 32 bytes of data:

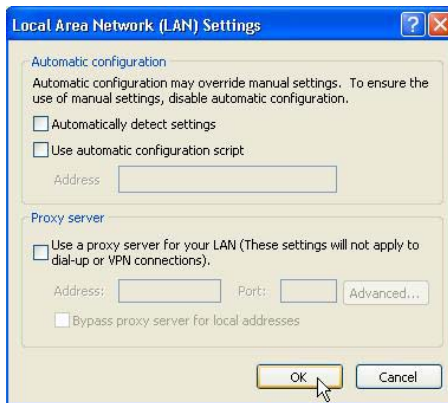
Reply from 192.168.168.1: bytes=32 time<1ms TTL=64
Reply from 192.168.168.1: bytes=32 time<1ms TTL=64
Reply from 192.168.168.1: bytes=32 time<1ms TTL=64
Reply from 192.168.168.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.168.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>_
```

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

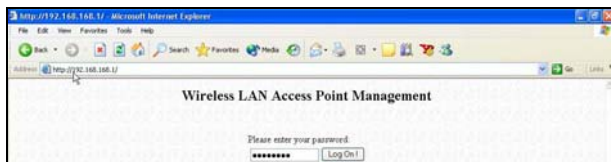


9. Open the **Connections** tab and in the **LAN Settings** section, disable all the option boxes. Click **OK** button to update the changes.



Chapter 3 Access to Web-based Interface

10. At the **Address** bar, enter `http://192.168.168.1` and press **Enter** from your keyboard.
11. At the login page, click the **Log On!** button to enter the configuration pages.



2. 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**

4.1 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.

LAN SETUP

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.

IP Address	192	168	168	1
Network Mask	255	255	255	0
Management Gateway Ip	0	0	0	0
DHCP Start IP Address	192	168	168	100
DHCP End IP Address	192	168	168	254
DHCP Gateway IP Address	0	0	0	0
<input type="checkbox"/> Always use these DNS servers:				
Primary DNS IP Address	0	0	0	0
Secondary DNS IP Address	0	0	0	0
DHCP Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			

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

Chapter 4 Common Configuration

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

Parameters	Description
IP Address	<p>The LAN IP address of the access point is set by default to 192.168.168.1.</p> <p>When the DHCP server of the AP is enabled (unless you set a different DHCP Gateway IP Address), this LAN IP Address would also be allocated as the Default Gateway of the DHCP client.</p>
Network Mask	<p>The Network Mask serves to identify the subnet in which the access point resides. The default network mask is 255.255.255.0.</p>
Management Gateway IP	<p>(Optional) 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 unit from the Internet or from a router on the LAN, you can set the IP address of the router as the Management Gateway IP.</p> <p>The Management Gateway IP address of the 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 the access point. For example, if the IP address and network mask of the 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 the access point. For instance, if the IP address and network mask of the 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>
DHCP Gateway IP	<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 DHCP Gateway IP Address, which will be allocated as the Default Gateway 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, when the unit 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 enable the DHCP server of the access point and set the 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>

Chapter 4 Common Configuration

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 PC in your network.

4.1.1 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.

View Active DHCP Leases

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

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

Advanced DHCP Server Options

The **DHCP Active Leases** table displays:

- The **IP Address** that has been allocated to the DHCP client
- The **Host Name** of the DHCP client
- Its Hardware (MAC) Address
- The date and time at which the IP address leased **expires**

DHCP Active Leases

IP Address	Host Name	Hardware Address	Expires
------------	-----------	------------------	---------



NOTE

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

Chapter 4 Common Configuration

4.1.2 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.

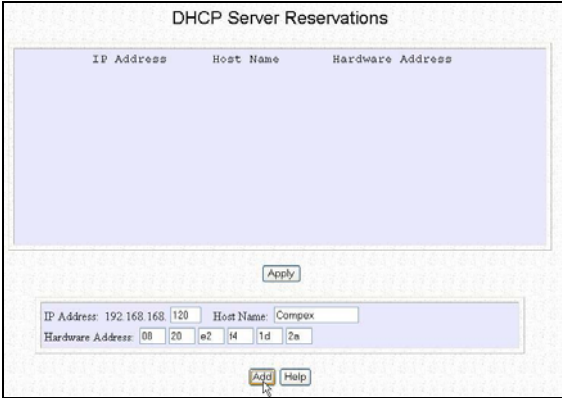
Reserve Specific IP addresses

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

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



Fill in:
The host portion of the **IP Address** to reserve.
The **Host Name**, if there is any, else, leave it blank.
The **Hardware Address**, in pairs of two hex values



Click on **Add** button.

Chapter 4 Common Configuration

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

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

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



Delete DHCP Server Reservation

Select the reserved IP address to delete.

Click on **Delete**.

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



NOTE

- When creating a DHCP reservation, you can opt to key in either the Host Name or the Hardware Address of the DHCP client.
- If you have entered both, the DHCP server will first check the hardware address.

If a match in hardware address has been found, the Host Name will then be ignored.

4.2 WLAN Setup

This section shows how to perform the following functions:

Basic:

This function performs a basic setup of the wireless modes of operation.

Security:

This function performs data encryption and protection for the router.

Advanced:

This function furthers the basic configuration of the router by setting the system's additional parameters such as Access Control, WDS, WMM and Long Distance Parameters.

Statistics:

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

It also covers the **Show Link Information** option featured ONLY in **wireless client mode**.

Chapter 4 Common Configuration

4.2.1 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.

It also covers the **Show Link Information** option featured ONLY in **wireless client mode**.

Basic Setup Wireless Mode

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 is the **Access Point** mode.

Regardless of the current operating mode, you can pick a different mode by clicking on the **Change** button (available in all operating modes).

The screenshot shows the "Access Point Setup" window. At the top, it says "The Current Mode" is "Access Point" with a "Change" button. Below this are several configuration fields: "Access Point Name" (text box with "Access Point"), "ESSID" (text box with "Access Point"), "Wireless Profile" (dropdown menu with "802.11b/g mixed"), "Country" (text box with "NO_COUNTRY_SET" and an "Edit Country Setting" button), "Channel" (dropdown menu with "SmartSelect" and a "Site Survey" button), "Tx Rate" (dropdown menu with "Fully Auto"), and "Closed System" (dropdown menu with "Disable"). At the bottom, there is a red note: "Note: Changes made will only take effect after rebooting." and three buttons: "Save", "Reboot", and "Help".

Make your selection from the **Network Mode** drop-down list.

Click on the **Apply** button to access the setup page of your selected mode.

The screenshot shows the "Network Mode Setup" window. A "NetWork Mode" dropdown menu is open, showing a list of options: "Access Point", "Access Point", "Access Point Client", "Gateway", "Wireless Routing Client", "Wireless Ethernet Adapter", and "Wireless Bridge Link". A mouse cursor is pointing at the "Wireless Bridge Link" option. Below the dropdown is an "Apply" button. A red note says "Note: NetMode switched will" followed by "em.". The "NetWork Mode" text box above the dropdown contains "Access Point".

Chapter 4 Common Configuration

In the **Mode Setup** page:

The Current Mode: **Access Point**

Access Point Name:

ESSID:

Wireless Profile:

Country:

Channel:

Tx Rate:

Closed System:

Note: Changes made will only take effect after rebooting.

The **Access Point Name** field appears when the access point is in AP/Gateway mode and refers to the identity of the device.

Access Point Name

When the access point is operated in wireless client mode, this field is referred to as Station Name instead.

Station Name

Each name is case-sensitive and can reach a maximum of 32 alphanumeric characters.

It is a good practice to name the access points uniquely, particularly when there are several devices in the network.

In AP/Gateway mode, the ESSID uniquely identifies each WLAN.

ESSID

When the access point is operated in **wireless client mode**, this field is referred to as **SSID** instead.

SSID

This case-sensitive entry can consist of a maximum of 32 characters and should be the same for any device connecting to the same network.

Chapter 4 Common Configuration

The **Wireless Mode** drop-down list provides a selection of network environment types in which to operate the access point:

- 802.11b only;
- 802.11b/g mixed, when both b and g clients are present;
- 802.11g only

Choose a **Country** that you are located. Click on the **Edit** button to select your country.

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

Wireless Profile	802.11b/g mixed	ET
Country	802.11b only	
Channel	802.11b/g mixed	
	802.11g only	

Country	SINGAPORE	Edit
---------	-----------	------



Country Setup

Country	SINGAPORE-SG	X
	LIECHTENSTEIN-LI	X
	LITHUANIA-LT	
	LUXEMBOURG-LU	
	MACAU-MO	
	MEXICO-MX	
	MONACO-MC	
	NETHERLANDS-NL	
	NEW ZEALAND-NZ	
	NORWAY-NO	
	PANAMA-PA	
	PHILIPPINES-PH	
	POLAND-PL	
	PORTUGAL-PT	
	PUERTO RICO-PR	
	SINGAPORE-SG	
	SLOVAK REPUBLIC-SK	
	SLOVENIA-SI	
	SOUTH AFRICA-ZA	
	SPAIN-ES	
	SWEDEN-SE	
	SWITZERLAND-CH	
	TAIWAN-TW	
	THAILAND-TH	
	TRINIDAD & TOBAGO-TT	
	TUNISIA-TN	
	TURKEY-TR	
	UNITED KINGDOM-GB	
	UNITED STATES-US	
	URUGUAY-UY	
	VENEZUELA-VE	

Configuration Please Click Edit more

Chapter 4 Common Configuration

4.2.2 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.

Advanced Setup Wireless Mode

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

In the **WLAN Advanced Setup** page:

WLAN Advanced Setup

Beacon Interval	<input type="text" value="100"/>	(100:20-1000)
Data Beacon Rate (DTIM)	<input type="text" value="1"/>	(1:1-16384)
RTS/CTS Threshold	<input type="text" value="2346"/>	(2346:256-2346)
Frag Threshold	<input type="text" value="2346"/>	(2346:256-2346)
Transmit Power	<input type="text" value="Maximum"/>	
Radio Off When Ethernet No Link	<input type="text" value="Disable"/>	
Auto Reboot Timer	<input type="text" value="00:00"/>	<input type="text" value="Disable"/>

Note: Changes made will only take effect after rebooting.

Extended Features

Chapter 4 Common Configuration

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 access points. It also sends information, such as timestamp, SSID, and other parameters regarding the access point to other access points that are within the specified range. The access point needs the beacon interval to know when to receive the beacon from the other access point.

Beacon Interval 100 (100:20-1000)

The **Data Beacon Rate (DTIM)** determines how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them. If the beacon period is set at 100, its default setting, and the data beacon rate is set at 1, its default setting, then the access point sends a beacon containing a DTIM every 100 Kμsecs. One Kμsec equals 1,024 microseconds.

Data Beacon Rate (DTIM) 1 (1-1-16384)

The **RTS/CTS Threshold** value determines the minimum size of a packet in bytes that would trigger the RTS/CTS mechanism.

RTS/CTS Threshold 2346 (2346:256-2346)

The **Frag Threshold** value indicates the maximum size that a packet can reach without being fragmented. This value ranges from 256 to 2346 bytes.

Frag Threshold 2346 (2346:256-2346)

This value extends from 256 to 2346 bytes, where a value of 0 indicates that all the packets should be transmitted using RTS.

The **Transmit Power** drop-down list lets you pick from a range of transmission power.

Transmit Power Maximum

Enabling **Radio Off When Ethernet No Link** option allows your AP to turn off the radio signal so that no wireless clients can connect to it. This might occur when you

In AP/Gateway mode ONLY:

Radio Off When Ethernet No Link Disable
Disable
Enable

Chapter 4 Common Configuration

Ethernet cable is disconnected to the network)

If this function is enabled, the wireless radio will be turned off if there is no Ethernet connection. The wireless radio will be turned back on when the Ethernet link is restored.

The turning ON or OFF delay takes about 60 seconds after detecting whether the Ethernet link is UP or DOWN respectively.

The **Auto Reboot Timer** is the time setting for the access point to automatically reboot.

Auto Reboot Timer	00:00	Disable ▾
-------------------	-------	-----------



NOTE

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

Chapter 4 Common Configuration

4.3 Scan for Site Survey

(For Wireless Client Mode Only)

This feature only available in **wireless client mode** (**Access Point Client**, **Wireless Routing Client** and **Wireless Ethernet Adapter**).

When one of the access points is connected to wired network and a set of wireless stations, it is referred to as a **Basic Service Set (BSS)**. The MAC address of the access point is used as entry here.

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.

Scan For Site Survey

In the **Mode Setup** page, click on the **Scan** button.

The Current Mode: **Access Point Client**

Station Name:

SSID:

Wireless Profile:

Country:

Tx Rate:

Note: Changes made will only take effect after rebooting.

Chapter 4 Common Configuration

The **Site Survey** provides a list of the **BSS** and **SSID** available, the **Chan** (channels), **Auth** (Authentication), **Alg** (Algorithm) being used, and the strength of the **Signal** received.

To configure to a different SSID:

Select the radio button corresponding to the SSID you want to configure to.

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

Click on the **Refresh** button.


Site Survey					
BSS	SSID	Chan	Auth	Alg	Signal
<input type="radio"/> 008048223c43	GoldenTree-2	1	OPEN	NONE	50%
<input type="radio"/> 00804824c675	wb11-cpx	1	OPEN	NONE	58%
<input type="radio"/> 00804835220d	pure-client	1	OPEN	NONE	62%
<input type="radio"/> 0080482b8d72	RD-Pserver	1	OPEN	WEP	70%
<input type="radio"/> 0080482aca60	26g-1118	6	WPA-PSK	TKIP	62%
<input type="radio"/> 0080482bcd7	ts-AP54G-55 Test	6	OPEN	WEP	56%
<input type="radio"/> 0080482be465	ts-AP54G-56 Test	6	OPEN	WEP	50%
<input type="radio"/> 000b6b31c947	ts-np18-22 RC (Do not connect)	11	OPEN	NONE	22%
<input type="radio"/> 000b6b31c93d	ts-np18-23 RC (Do not connect)	11	OPEN	NONE	20%
<input type="radio"/> 000b6b31c94d	ts-np18-20 RC (Do not connect)	11	OPEN	NONE	8%
<input type="radio"/> 000b6b33cb44	ts-np18-21 RC (Do not connect)	11	OPEN	NONE	8%
<input type="radio"/> 008048335467	No Ethernet	11	OPEN	WEP	8%

4.3.1 Show Link Information
(For Wireless Client Mode Only)

This function offers a summary of the link data when the access point is in the **wireless client mode**, i.e., either of the *Access Point Client*, *Wireless Routing Client* or the *Wireless Ethernet Adapter* mode.


Show Link Information

In the Mode **Setup** page, go to the **Link Information** section.



Click on the **Show Link Information** button. When an access point is connected to a wired network and a set of wireless stations, it is referred to as a **Basic Service Set (BSS)**.

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



Link Information	
State	Associated BSS ID=00:80:4B:2B:E3:27
Current Channel	1
Signal Strength	68%

State refers to the MAC address of the BSS.

Current Channel is the channel being presently used for transmission.

Signal Strength, given in percentage form, shows the intensity of the signal received and hence the connection strength

4.4 Wireless Extended Features

The **Wireless Extended Features** are ONLY available when the access point operates in all modes as tabulated below:

Features	Mode
Access Control	Access Point and Gateway
Wireless Distributed System (WDS)	Access Point and Gateway
WMM Parameters	All modes except for Wireless Bridge Link
Outdoor Parameters	All modes

4.4.1 Access Control – The Wireless Pseudo VLAN

A **VLAN** is a group of PCs or other network resources that behave as if they were connected to a single network segment.

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.

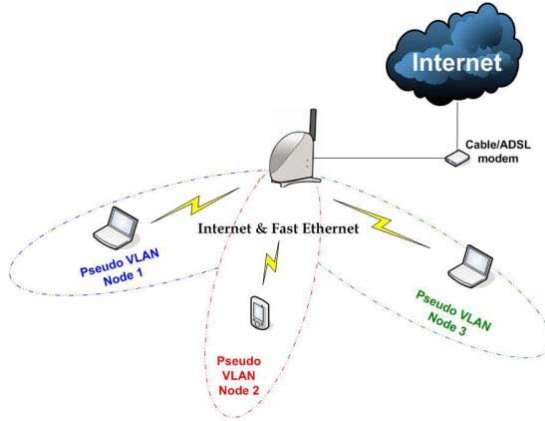
A **Wireless Pseudo VLAN** acts by segregating a single wireless LAN into multiple virtual LANs so that communication is possible only among wireless clients within the same VLAN.

When operating in the **Gateway** mode, the access point lets you create VLANs containing either a single user, and referred to as *Wireless Pseudo VLAN Per Node*, or a group of users, termed *Wireless Pseudo VLAN Per Group*.

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

4.4.1.1 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*.

Wireless Pseudo VLAN – Per Node

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

Go to the **Extended Features** section, and click on the **Access Control** button

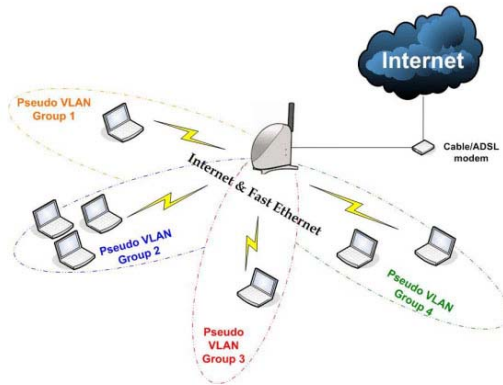
The **Wireless Pseudo VLAN** function is *Disabled* by default.

Select **Per Node** from the drop-down list.

Click on the **Apply** button.

4.4.1.2 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 all 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.

Wireless Pseudo VLAN – Per Group

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

Click on the **Access Control** button.

The **Wireless Pseudo VLAN** function is *Disabled* by default.

Select **Pseudo VLAN** from the drop-down list.

Click on the **Apply** button.

The screenshot shows the 'WLAN Advanced Setup' page. Under the 'Extended Features' section, the 'Access Control' button is highlighted. Below this, the 'Access Control Setup' section is visible, showing a dropdown menu with 'Pseudo VLAN' selected. Other options in the dropdown include 'Per Node', 'Disable', and 'Tag VLAN'.

Chapter 4 Common Configuration

The **MAC Address List** enables you to manage specific VLAN groups by adding or deleting clients through their MAC address.

Click on the **Add** button.

The screenshot shows the "Pseudo VLAN" configuration page. It features a "Mac address list" section with four groups: Group1 (checked), Group2, Group3, and Group4. Each group has a checkbox and a dropdown menu. Below the groups are "Add" and "Delete" buttons. At the bottom of the page are "Save", "Reboot", and "Help" buttons. A red note states: "Note: Changes made will only take effect after rebooting."

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

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

The screenshot shows the "Add MAC address" dialog box. It has a "GroupID" dropdown menu with options 1, 2, 3, and 4. The "Mac Addr" field contains the value "aa-bb-cc-dd-ee-ff". Below the fields are "Apply", "Cancel", and "Help" buttons.

Click on the **Apply** button.

The updated **Mac Address List** page will appear as shown.

The screenshot shows the updated "Pseudo VLAN" configuration page. The "Mac address list" section now shows Group1 with a checked checkbox and a dropdown menu displaying "aa-bb-cc-dd-ee-ff". Groups 2, 3, and 4 remain unchecked. The "Add" and "Delete" buttons are still present. At the bottom are "Save", "Reboot", and "Help" buttons. The red note remains: "Note: Changes made will only take effect after rebooting."

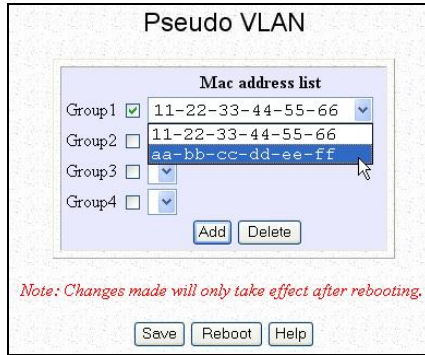
Chapter 4 Common Configuration

Delete client from a group

If you want to delete a particular client from a group:

Select the client to delete from the **Mac Address List**.

Click on the **Delete** button.



The screenshot shows the 'Pseudo VLAN' configuration page. It features a table titled 'Mac address list' with four rows. The first row is selected, and the 'Delete' button is highlighted. Below the table are 'Add' and 'Delete' buttons. At the bottom of the page are 'Save', 'Reboot', and 'Help' buttons. A red note states: 'Note: Changes made will only take effect after rebooting.'

Group	Mac address
Group1 <input checked="" type="checkbox"/>	11-22-33-44-55-66
Group2 <input type="checkbox"/>	11-22-33-44-55-66
Group3 <input type="checkbox"/>	aa-bb-cc-dd-ee-ff
Group4 <input type="checkbox"/>	

Note: Changes made will only take effect after rebooting.

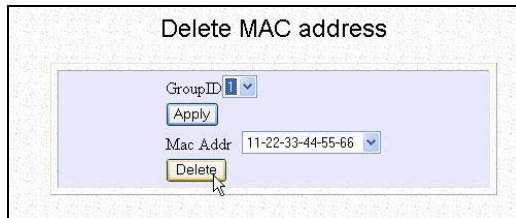
This **Delete MAC Address** page will appear to confirm whether you want to delete the selected client.

If you do not want to delete the client:

Click on **Apply** button.

If you want to remove the client from the group:

Click on **Delete** button.



The screenshot shows the 'Delete MAC address' confirmation page. It includes a 'GroupID' dropdown menu, an 'Apply' button, a 'Mac Addr' dropdown menu showing '11-22-33-44-55-66', and a 'Delete' button.

Chapter 4 Common Configuration

4.4.1.3 Tag VLAN

- [Available in Access Point mode ONLY]

While a port-based VLAN is limited in size since it can only exist within the confines of a single Ethernet switch, a Tag VLAN is designed to extend the wired VLAN to individual wireless clients.

Here, each VLAN is identified by a 'tag', which the switch associates with specific ports. The switch will then pass this tag information with every data packet transmitted. By using the same tag on each access point in the network, full client roaming can be implemented while complying with VLAN integrity.

Wireless Pseudo VLAN – Tag VLAN

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

Go to the **Extended Features** section.

Click on the **Access Control** button.

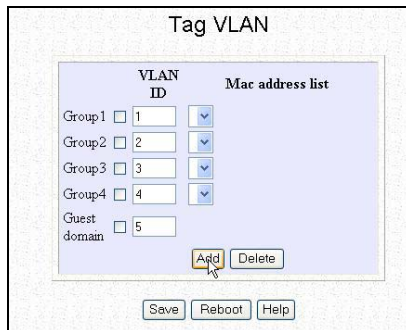
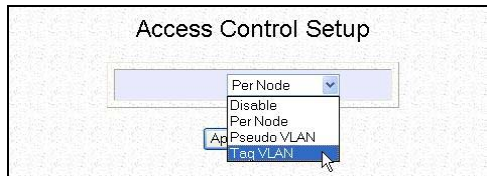
The Wireless Pseudo VLAN function is *Disabled* by default.

Select Tag VLAN from the drop-down list.

Click on the **Apply** button.

The **Tag VLAN** page enables you to manage specific VLAN groups by adding or deleting clients through their MAC address.

Click on the **Add** button.



Chapter 4 Common Configuration

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

Fill in the **Mac Addr** field with the MAC address of the client in the format **xx:xx:xx:xx:xx** or **xx-xx-xx-xx-xx**, where x is any value between 0-9 and a-f.

Click on the **Apply** button.

The updated **Mac Address List** page will appear as shown on the right.

Repeat Step 4 if you need to add more clients or to configure more groups.



The screenshot shows a window titled "Add MAC address". It contains a "GroupID" dropdown menu with options 1, 2, 3, and 4. Option 1 is selected. To the right is a "Mac Addr" text field containing "aa-bb-cc-dd-ee-ff". Below these fields are three buttons: "Apply", "Cancel", and "Help". A mouse cursor is pointing at the "Apply" button.



The screenshot shows a window titled "Tag VLAN". It has two columns: "VLAN ID" and "Mac address list". Under "VLAN ID", there are five entries: "Group1" with a checkbox and input field containing "1", "Group2" with a checkbox and input field containing "2", "Group3" with a checkbox and input field containing "3", "Group4" with a checkbox and input field containing "4", and "Guest domain" with a checkbox and input field containing "5". Each input field has a small blue downward arrow on its right side. Under "Mac address list", there is a dropdown menu showing "aa-bb-cc-dd-ee-ff". Below the list are "Add" and "Delete" buttons. At the bottom of the window are "Save", "Reboot", and "Help" buttons. A mouse cursor is pointing at the "Save" button.

Chapter 4 Common Configuration

Delete client from a Tag VLAN

If you want to delete a particular client from a group:

Select the client to delete from the **Mac Address List**.

Click on the **Delete** button.

	VLAN ID	Mac address list
Group 1 <input type="checkbox"/>	1	aa-bb-cc-dd-ee-ff
Group 2 <input type="checkbox"/>	2	
Group 3 <input type="checkbox"/>	3	
Group 4 <input type="checkbox"/>	4	
Guest domain <input type="checkbox"/>	5	

Buttons: Add, Delete, Save, Reboot, Help

The **Delete MAC Address** page will appear to confirm whether you want to delete the selected client.

If you want to remove the client from the group:

Click on **Delete**.

Else click on **Apply**.

Click on the corresponding **Group** checkbox to enable a particular VLAN.

If you enable **Guest domain**, even those stations which are not identified in the **MAC address list** will still be allowed to access the Internet though they will not be able to communicate with each other

GroupID: 1

Apply

Mac Addr: e1-08-a2-bb-2e-f4

Delete

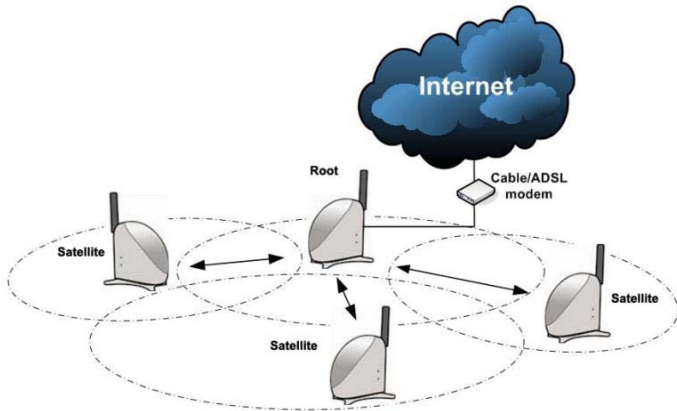
4.4.2 Wireless Setup - The Wireless Distributed System (WDS)

A distribution system links up several of the access points and the areas they serve, creating a wider network in which mobile users can roam while still staying connected to the available network resources.

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

4.4.2.1 Star Configuration WDS

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

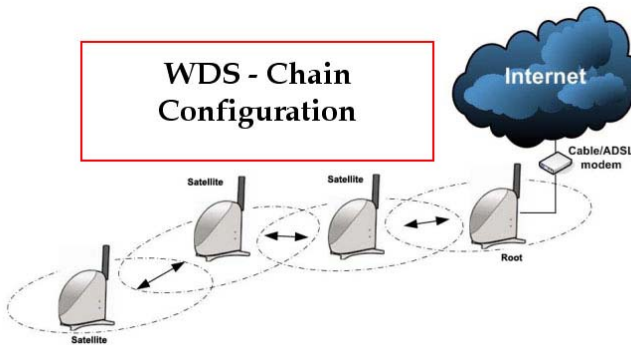


Here, the root gateway connects to the Internet and maintains three WDS links while each satellite gateway uses one port only for communication with the root.

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



Chapter 4 Common Configuration

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

WDS Configuration Setup

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

Go to the **Extended Features** section. Click on the **WDS Configuration** button.

As illustrated on the **WDS Setup**, the **WDS** feature is *Disabled* by default.

Select **Enable** from the **WDS Global Control** drop-down list to operate WDS.

Click on the **Apply** button.

At the **WDS Status** page:

Click on the **Add** button to expand your WDS.

Please note that if you auto select your frequency channel (**SmartSelect**), you are not allowed to activate WDS Global Control.

WDS link	Partner Address	Status
----------	-----------------	--------

WDS Statistics Info

Show Statistics Info




NOTE

To configure WDS, all your access points must be in the same channel; and both your access points at opposite WDS link must have each other's wireless MAC address

Chapter 4 Common Configuration

On the **Add WDS Link** screen that appears:

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



The screenshot shows the 'Add WDS Link' configuration page. It features a form with two fields: 'Partner Address' containing the value '11-22-33-44-55-66' and 'Status' with a dropdown menu set to 'Enable'. Below the form are two buttons: 'Apply' and 'Help'.

Use the **Status** option to control whether you want to **Enable** this particular WDS link or to **Disable** it.

Click on the **Apply** button.

The **WDS Status** page will be updated as shown on the right.

If you want to modify the status entry for a WDS link:

Select the radio button on the left of that particular link as illustrated below left.



The screenshot shows the 'WDS Status' page. It contains a table with the following data:

WDS link	Partner Address	Status
1	11-22-33-44-55-66	Enable

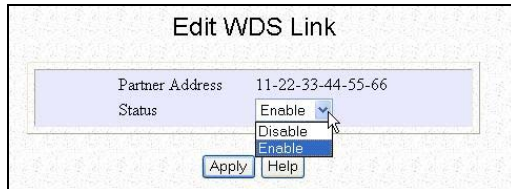
Below the table are three buttons: 'Add', 'Remove', and 'Edit'. Underneath is a section titled 'WDS Statistics Info' with a 'Show Statistics Info' button.

Click on the **Edit** button.

At the **Edit WDS Link** page which shows:

Select whether to enable or to disable the WDS link.

Click on the **Apply** button for the changes you made to take effect.



The screenshot shows the 'Edit WDS Link' configuration page. It features a form with two fields: 'Partner Address' containing the value '11-22-33-44-55-66' and 'Status' with a dropdown menu. The dropdown menu is open, showing options 'Enable', 'Disable', and 'Enable'. Below the form are two buttons: 'Apply' and 'Help'.

Chapter 4 Common Configuration

If you want to delete a WDS link:

Select the radio button on the left of that particular link.

Click on the **Remove** button.

An updated **WDS Status** page will be displayed.

To view **WDS Statistics Info**:
Click on the hyperlink of the selected Partner Address.

The **Link (Partner Address) Statistics** table shown on the left will be displayed.

Click on the **Back** button to return to the **WDS Status** page.

WDS Status		
WDS link	Partner Address	Status
<input checked="" type="radio"/> 1	11:22:33:44:55:66	Enable
<input type="radio"/> 2	ab.cd:11:22:aa:ff	Enable

WDS Status		
WDS link	Partner Address	Status
<input type="radio"/> 1	ab.cd:11:22:aa:ff	Enable

WDS Status		
WDS link	Partner Address	Status
<input type="radio"/> 1	11:22:33:44:55:66	Enable

Link(11:22:33:44:55:66) Statistics						
State		Power Save				
joined		off				
Encryption	Advertised Cipher	Unicast Cipher	Multicast Cipher			
yes	None	None	None			
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	0	0	0
Transmit	0	0	0	0	0	0
	Signal Strength (RSSI)			Data Rate (Mbps)		
Receive	295			1		
Transmit	2			1 1		
Receive Errors	Discarded Frames	Duplicate Frames	CRC Errors	Decrypt Errors	PHY Errors	DMA Errors
0	0	0	0	0	0	0
Transmit	Discarded	Excessive		DMA		



NOTE

- If **WDS Global Control** is Disabled, every WDS link will be closed regardless of its status.

When **WDS Global Control** is set to Enabled, the status of every WDS link that you want to include still needs to be individually Enabled.

- In the WDS Statistics table:
Each entry corresponds to a particular WDS link and for each link, the parameters listed are:
WDS Link: identifier assigned to the link
rxTotal: total number of packets received (inclusive of *rxUni* & *rxMulti*)
rxUni: number of unicast packets received
rxMulti: number of multicast or broadcast
- Although the WDS nodes may belong to different SSIDs, they MUST be configured in the same channel and use the same WEP keys (if the encryption feature is enabled) to be able to communicate with one another.

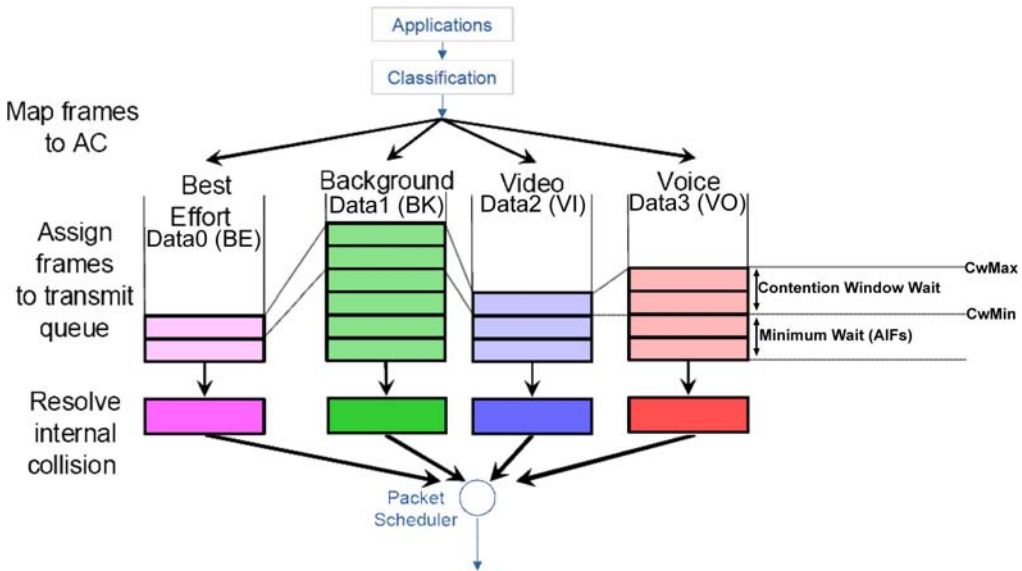
If the WDS-enabled access points are required to support too many operational wireless clients, you may find end-to-end throughput to be low (depending on the applications). For instance, end-to-end latency may become an issue in a very long WDS chain configuration.

Chapter 4 Common Configuration

4.4.3 WMM Parameters

(available in all modes except for Wireless Bridge Link)

Wireless Multimedia (WMM) is a QoS (Quality of Service) standard in IEEE802.11E that we have adopted to improve and support the user experience for multimedia, video, and voice applications by prioritizing data traffic. QoS can be realized through 4 different Access Categories (AC). Each AC type consists of an independent transmit queue, and a channel access function with its own parameters.



Chapter 4 Common Configuration

The following steps demonstrate how to configure these WMM Parameters.

WMM Parameters

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

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

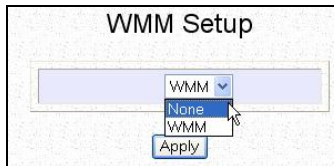


The **WMM Setup** function is **WMM** by default.

Select **WMM** from the drop-down list



Click on the **Apply** button.



AP WMM Parameters

AC TYPE	CWMin	CWMax	AIFS	TxopLimit	ACM	Ack-policy
AC_BE(0)	4	6	3	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BE(1)	4	10	7	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI(2)	3	4	1	3008	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO(3)	2	3	1	1504	<input type="checkbox"/>	<input type="checkbox"/>

BSS WMM Parameters

AC TYPE	CWMin	CWMax	AIFS	TxopLimit	ACM
AC_BE(0)	4	10	3	0	<input type="checkbox"/>
AC_BE(1)	4	10	7	0	<input type="checkbox"/>
AC_VI(2)	3	4	2	3008	<input type="checkbox"/>
AC_VO(3)	2	3	2	1504	<input type="checkbox"/>

Note: Changes made will only take effect after rebooting.

Chapter 4 Common Configuration

Depending on the mode you set up, you have to select either AP (Access Point) or BSS (Basic Service Set) WMM Parameters. For instance, if the mode is AP, select AP WMM Parameters. The following parameters are described :

WMM Parameters (for advanced users)	
AIFs (Arbitrary Inter-Frame Space)	Arbitrary Inter-Frame Space is the minimum wait time interval between the wireless medium becoming idle and the start of transmission of a frame over the network.
Cwmin (Contention Window Minimum)	Contention Window Minimum is the minimum random wait time drawn from this interval or window for the backoff mechanism on the network.
CwMax (Contention Window Maximum)	Contention Window Maximum is the maximum random wait time drawn from this interval or window for the backoff mechanism on the network.
TxOp limit (Transmit Opportunity Limit)	Transmit Opportunity limit specifies the minimum duration that an end-user device can transmit data traffic after obtaining a transmit opportunity. TxOp limit can be used to give data traffic longer and shorter access.
ACM (Admission Control Mandatory)	Admission Control Mandatory enables WMM on the radio interface. When ACM is enabled, associated clients must complete the WMM admission control procedure before access.

Chapter 4 Common Configuration

4.4.4 Long Distance Parameters (available in all modes)

These parameters determine the distance between wireless clients to ensure that the wireless point-to-point communication takes place efficiently and effortlessly.

The following steps demonstrate how to configure these Long Distance Parameters.

Long Distance Parameters

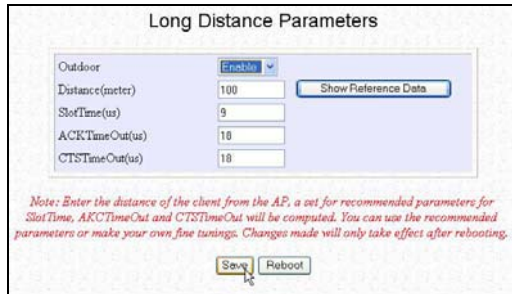
From **WLAN Setup** under **Configuration**, click on **Advanced**, which shows the **WLAN Advanced Setup** page.

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



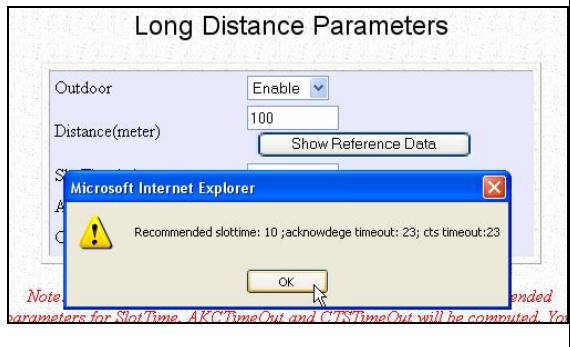
The **Long Distance Parameters** function is *Disable* by default.

Select **Enable** from the drop-down list



Click on the **Apply** button.

To copy the reference data, click on **Show Reference Data**.



Chapter 4 Common Configuration

The parameters are described below:

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 specified.

Distance:

This parameter determines the distance between different buildings. It should be entered in meters.

Slot Time:

This parameter determines the slot time allocated by each wireless client (that is, the sending and the receiving clients) to initiate and/or receive data transmission.

ACK Timeout:

This parameter determines the timeout allowed for the sending client to receive the acknowledgment response from the receiving client.

CTS Timeout:

This Clear-to-Send time is the one in which the wireless clients are ready to initiate and/or receive data transmission within a specified timeout.

Chapter 4 Common Configuration

4.5 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.

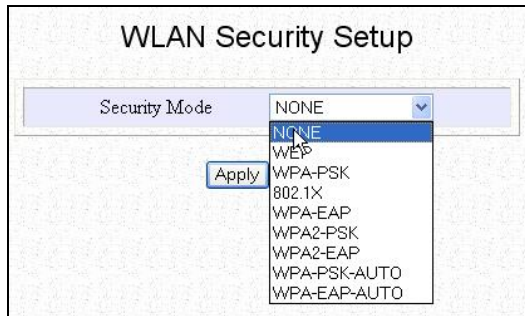
Selecting Security Mode

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

Make a selection from the **Security Mode** drop down menu.

The **Security Mode** is set to **NONE** by default.

Click on **Apply**.



Chapter 4 Common Configuration

4.5.1 How to set up WEP [Available in ALL modes]

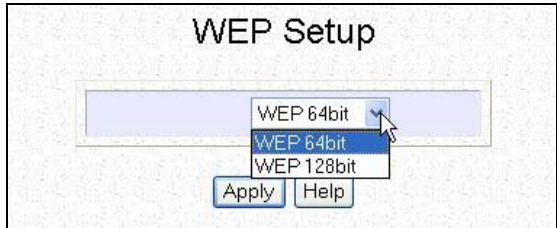
The guidelines below will help you to set up the access point for using WEP.

Security Mode -WEP

At the **WEP Setup** page:

Select whether to use WEP 64bit or WEP 128 bit.

Click on **Apply**.



The access point lets you define up to four different WEP keys.

Specify the key entry format, by selecting either:

- Use Alphanumeric Characters
- Use Hexadecimal

Enter your WEP keys in the **Key** fields.

When using 64-bit encryption:

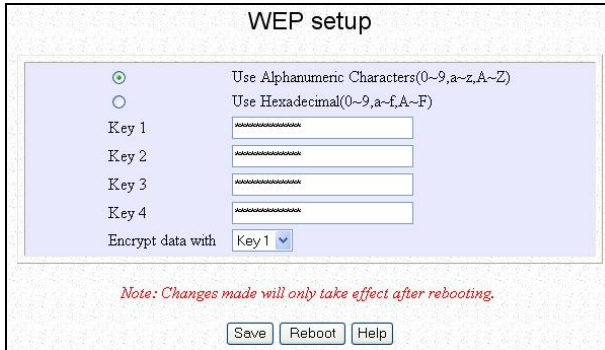
Your WEP key has to be either **5** alphanumeric characters or **10** hex characters long.



Chapter 4 Common Configuration

When using 128-bit encryption:

Your WEP key has to be either **13** alphanumeric characters or **26** hex characters long.



WEP setup

Use Alphanumeric Characters(0~9,a~z,A~Z)
 Use Hexadecimal(0~9,a~f,A~F)

Key 1
Key 2
Key 3
Key 4

Encrypt data with Key 1

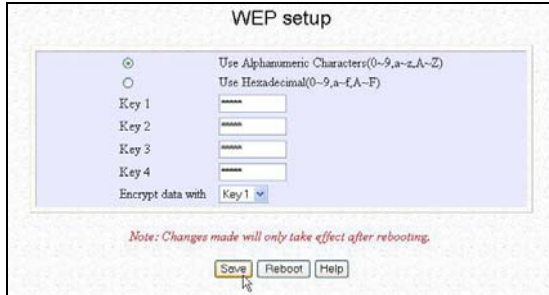
Note: Changes made will only take effect after rebooting.

Save Reboot Help

Select which of the keys defined to **Encrypt data with**.

Click on **Save** and **Reboot** the access point.

A **Hexadecimal** value can only take in numbers **0-9** and letters **A-F** and is NOT case-sensitive.



WEP setup

Use Alphanumeric Characters(0~9,a~z,A~Z)
 Use Hexadecimal(0~9,a~f,A~F)

Key 1
Key 2
Key 3
Key 4

Encrypt data with Key 1

Note: Changes made will only take effect after rebooting.

Save Reboot Help

Chapter 5 Further Configuration

4.5.2 How to set up WPA-PSK

[Available in AP/Gateway mode ONLY]

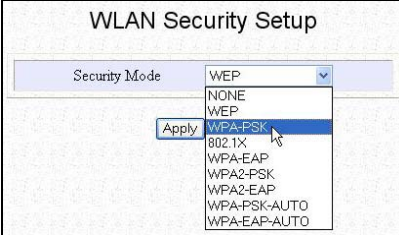
The guidelines below will help you to set up the access point for using WPA-PSK. Please take note that the **WPA-PSK**, **WPA2-PSK** and **WPA-PSK-AUTO** security modes share the same functions).

Security Mode –WPA-PSK, WPA2-PSK, WPA-PSK-AUTO

At the **WLAN Security Setup** page:

Select **WPA-PSK** mode.

Click on **Apply** button.

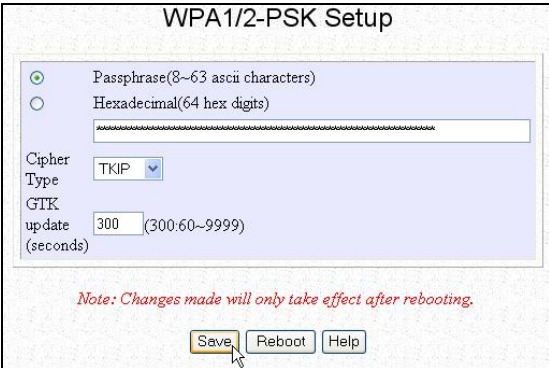


The screenshot shows the 'WLAN Security Setup' page. A dropdown menu for 'Security Mode' is open, displaying options: NONE, WEP, WPA-PSK (highlighted), 802.1X, WPA-EAP, WPA2-PSK, WPA2-EAP, WPA-PSK-AUTO, and WPA-EAP-AUTO. An 'Apply' button is visible to the left of the dropdown.

Specify the key entry format by selecting either:

- Passphrase (Alphanumeric characters)
- Hexadecimal

Fill in the pre-shared network key.



The screenshot shows the 'WPA1/2-PSK Setup' page. The 'Passphrase(8-63 ascii characters)' radio button is selected. Below it is a text input field for the passphrase. The 'Cipher Type' is set to TKIP. The 'GTK update (seconds)' field is set to 300. A note at the bottom states: 'Note: Changes made will only take effect after rebooting.' There are 'Save', 'Reboot', and 'Help' buttons at the bottom.

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.

The **Cipher Type** is set to **TKIP**.

Define the **GTK update** (Group Transient Key update), or the length of time after which the access point will automatically generate a new master key.

Chapter 5 Further Configuration

Press the **Save** button.

Click on **Reboot** to restart the system, after which your settings will become effective.

A **Hexadecimal** value can only take in numbers **0-9** and letters **A-F** and is NOT case-sensitive.

For selecting WPA2-PSK and WPA-PSK-AUTO, you can use the above procedure of selecting WPA-PSK. However, for WPA (actually is the same as WPA1) , AES is not mandatory whereas AES is mandatory for WAP2.

Chapter 5 Further Configuration

4.5.3 How to set up 802.1x/RADIUS [Available in Access Point mode ONLY]

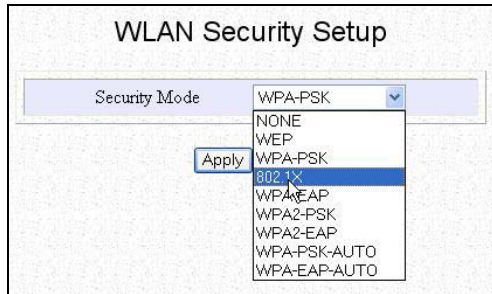
The guidelines below will help you to set up the access point for using 802.1x/RADIUS.

Security Mode –802.1x/RADIUS

At the **WLAN Security Setup** page:

Select **802.1x** mode.

Click on **Apply** button.



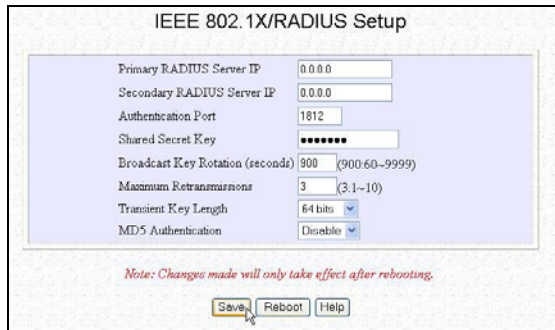
WLAN Security Setup

Security Mode: WPA-PSK (dropdown menu open showing options: NONE, WEP, WPA-PSK, 802.1X, WPA-EAP, WPA2-PSK, WPA2-EAP, WPA-PSK-AUTO, WPA-EAP-AUTO)

Apply

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.



IEEE 802.1X/RADIUS Setup

Primary RADIUS Server IP: 0.0.0.0

Secondary RADIUS Server IP: 0.0.0.0

Authentication Port: 1812

Shared Secret Key: [masked]

Broadcast Key Rotation (seconds): 300 (900:60-9999)

Maximum Retransmissions: 3 (3:1-10)

Transient Key Length: 64 bits

MD5 Authentication: Disable

Note: Changes made will only take effect after rebooting.

Save Reboot Help

[Refer to the section on **How to set up WEP.**]

Press the **Save** button.

Click on **Reboot** to restart the system, after which your settings will become effective.

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

Chapter 5 Further Configuration

4.5.4 How to set up WPA EAP [Available in Access Point mode ONLY]

The guidelines below will help you to set up the access point for using WPA-EAP. (Please take note that the WPA or WPA1-EAP, WPA2-EAP and WPA-EAP_AUTO have the same functions).

Security Mode – WPA-EAP, WPA2-EAP, WPA-EAP-AUTO

At the **WLAN Security Setup** page:

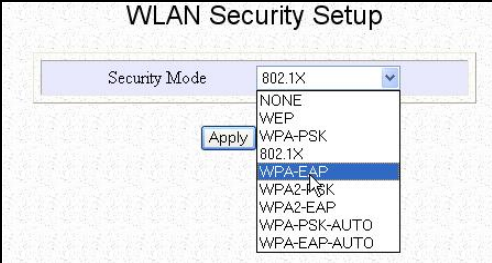
Select **WPA-EAP** mode.

Click on **Apply** button.

The **Cipher Type** is set to TKIP.

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.

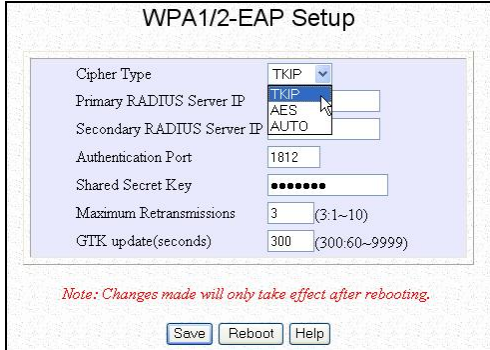


WLAN Security Setup

Security Mode: 802.1X

Apply

NONE
WEP
WPA-PSK
802.1X
WPA-EAP
WPA2-PSK
WPA2-EAP
WPA-PSK-AUTO
WPA-EAP-AUTO



WPA1/2-EAP Setup

Cipher Type: TKIP

Primary RADIUS Server IP:

Secondary RADIUS Server IP:

Authentication Port: 1812

Shared Secret Key:

Maximum Retransmissions: 3 (3~10)

GTK update(seconds): 300 (300~9999)

Note: Changes made will only take effect after rebooting.

Save Reboot Help

You can key in a different Authentication Port but it **MUST** match the corresponding port of the RADIUS server.

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

Specify the **Maximum Retransmissions**. For greater security, key in the minimum permissible 1, else the maximum allowed is 10.

Define the **GTK update** (Group Transient Key update), or the length of time after which the access point will automatically generate a new master key.

Press the **Save** button.

Click on **Reboot** to restart the system, after which your settings will become effective.

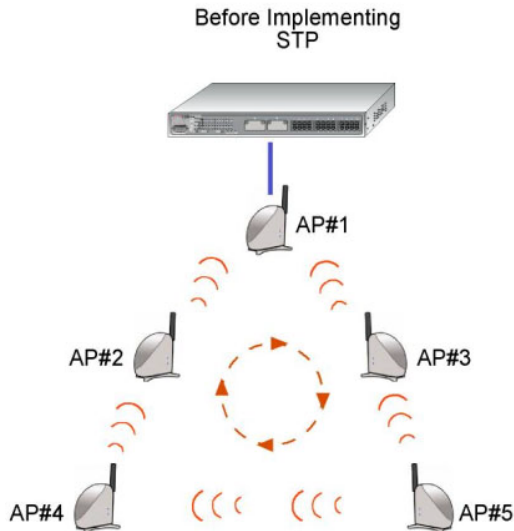
The RADIUS authentication server **MUST** be in the same subnet as the access point.

For selecting WPA2-EAP and WPA-EAP-AUTO, you can use the above procedure of selecting WPA-EAP. However, for WPA (actually is the same as WPA1) , AES is not mandatory whereas AES is mandatory for WPA2

4.6 STP Setup

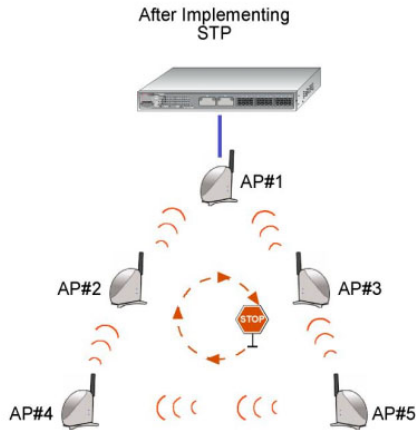
Spanning Tree Protocol (STP) is a link management protocol that helps to prevent undesirable loops occur in the network. For an Ethernet network to function properly, only one active path can exist between two stations. If a loop exists in the network topology, duplication of messages will occur and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



Chapter 5 Further Configuration

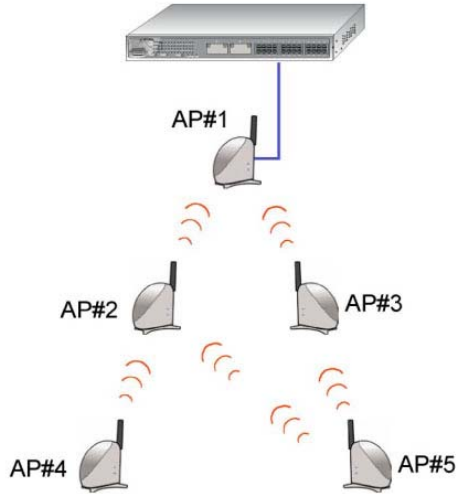
To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and re-establishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections 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.

Chapter 5 Further Configuration

The figure shown below explains the implementation of STP in a network. AP#1 is physically connected to a switch whilst another 4 access points (AP#2, AP#3, AP#4 and AP#5) are connected to AP#1 wirelessly. Redundant paths were found in this network, without enabling STP function, broadcast storm will occur in this network, resulted duplicated frames to be forwarded.



Chapter 5 Further Configuration

When STP is enabled, the STP-enabled access points will first try to find the root access point using the following criteria:

- use the access point that is configured with the smallest STP priority. Default priority set in the access points is 32768.
- If the STP priority values are the same, the access point with smallest MAC address will be chosen as root.



Once the root access point is determined, the STP algorithm will start to calculate the path cost from each access point to the root access point. Based on the path cost in the following table,

Bandwidth	STP Cost
4Mbps	250
10Mbps	100
16Mbps	62
45Mbps	39
100Mbps	19
155Mbps	14
622Mbps	6
1Gbps	4
10Gbps	2

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

Chapter 5 Further Configuration

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 low level of data security. If redundant paths were found in this network, broadcast packets will be duplicated and forwarded endlessly resulting in a broadcast storm.



Chapter 5 Further Configuration

Scenario #2 – (With STP, No Pseudo VLAN)

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

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

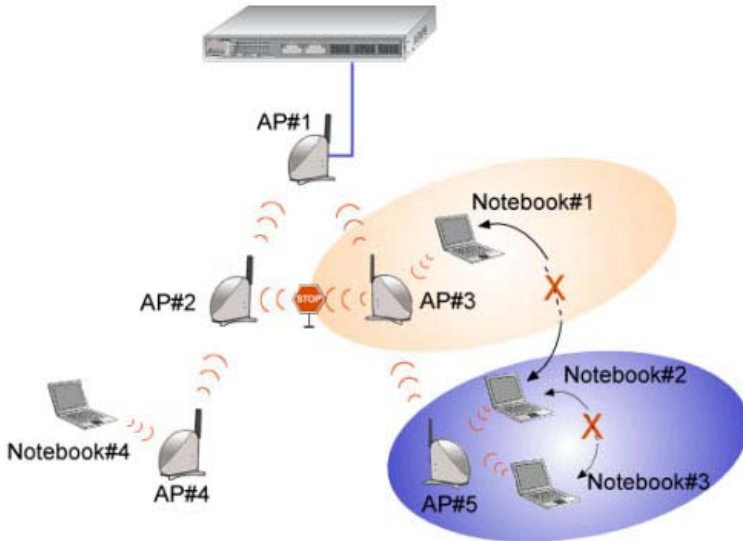
All wireless users will be able to communicate with each other if they are associated to the access points of the same WDS zone.



Chapter 5 Further Configuration

Scenario #3 – (With STP and Pseudo VLAN)

In this example, both STP and Pseudo VLAN are implemented in this network. All wireless users are unable to communicate with one another. This is one of the measures to ensure data privacy between wireless users in the network.



Enabling STP Setup

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

Select **Enable** from the **STP State** radio button.

STP State:

Activate Spanning Tree Protocol (STP) function makes your network more resilient to link failure and also provides a protection from loop.

Field	Value
STP Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
STP Designated Root	4
Priority (0 - 65535)	32768
Hello Time (1 - 10)	2
Forward Delay (4 - 30)	15
Max Age (6 - 40)	20

Note: Changes made will only take effect after rebooting.

Buttons: Save, Reboot, Help

Priority:

Specify the configurable value that is appended as the most significant portion of a AP.

This value specifies which access point acts as the central reference point, or Root AP, for the STP system — the lower the priority value, the more likely the access point is to become the Root AP. If the priority values are all the same, then the system will search for the smallest MAC address of the access point and set it as the Root AP.

Hello Time:

Specify the time in seconds that elapses between the configuration messages (also known as Hello BPDUs) generated by an AP that assumes itself to be the Root AP.

Forwarding Delay:

Specify the time in seconds that an AP spends in the listening and learning states, that is, listening for configuration messages.

Max Aging Time:

Specify the maximum age in seconds at which the stored configuration message information is judged to be too old and is discarded.

If an AP does not receive a configuration message after the Max Aging Time, the system will assume that the link between itself and the Root AP has gone down and will then reconfigures the network to cater for the change.

Click on the **Apply** button.

4.7 SNMP Setup

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

Enabling SNMP

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

A screenshot of the 'SNMP Setup' configuration window. The window has a title bar 'SNMP Setup'. Inside, there are three fields: 'SNMP State' with a dropdown menu showing 'Enable', 'Read Password' with a text box containing 'public', and 'Read/Write Password' with a text box containing 'private'. Below these fields is an 'Apply' button with a mouse cursor over it.

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

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

Click on the **Apply** button.

4.8 MAC Filtering

MAC Filtering acts as a security measures by controlling the users from accessing to the network. This can be easily done by adding the user's MAC address to the listing and from there, you can choose whether the particular user is allowed to access to the network or not. Simply click on the radio button besides **Allow PCs listed to access network**, or **Prevent PCs listed from accessing network** to activate the function.

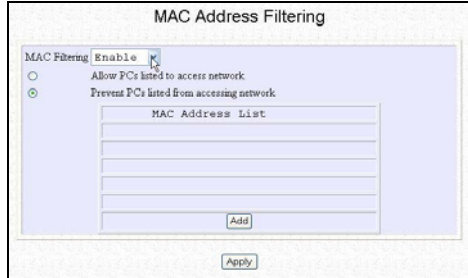
Chapter 5 Further Configuration

Enabling MAC Filtering

Click on **MAC Filtering** from the **CONFIGURATION** menu.

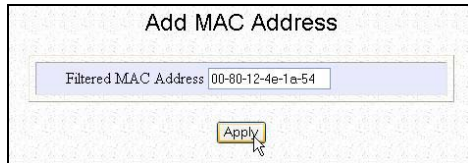
Select **Enable** from the **MAC Filtering** drop-down list.

Click on the **Add** button to add in the MAC address of the user.



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

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



Referring to the figure shown on the right, notice that the MAC Address has been added to the list.

Next, you can choose whether you wish to allow/prevent the user to/from access to the network.

Simply click on the radio button besides Allow PCs listed to access network, or Prevent PCs listed from accessing network.

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



NOTE

When Mac Filtering is enabled with allow access policy, the Mac Address list cannot be empty.

Chapter 5 Further Configuration

This chapter provides guidelines in:

- **Setting up uConfig (only in Gateway mode)**
- **Configuring WAN Setup (only in Gateway or Wireless Routing Client mode)**
- **Using NAT**
- **Routing**
- **Implementing IP Filtering**
- **Applying Remote Management**
- **Enabling Parallel Broadband**

5.1 Setting up uConfig (only in Gateway mode)

This option is ONLY available when the access point operates in **Gateway** mode.

uConfig Set up


Click on **uConfig IP Setup** from the **CONFIGURATION** menu.

Fill in the IP Address.

Key in the **Network Mask**.

Click on **Save** button.

Reboot the system to make your changes effective.



5.2 Configuring WAN Setup

(only available in Gateway and Wireless Routing Client mode)

The WAN setup allows you to set up the access point for broadband Internet connection.

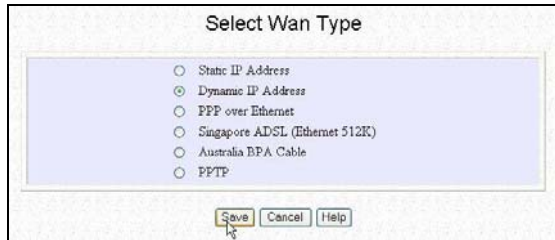
Described below are the common steps you should start with to select or change the broadband connection type.

Changing WAN Type

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

The setup page of the WAN type that you have last implemented will be displayed.

Since the access point operates in **Dynamic IP** Address Allocation mode by default, initially the **Dynamic IP** setup page will appear.



Press the **Change** button (which appears on the setup pages of all the WAN Types), to reach the **Select WAN Type** page.

Select the **WAN type** you want to switch to.

Click on **Save**.

The setup page of the WAN type that you have selected will then appear.

5.2.1 Dynamic IP

In the default **dynamic IP** addressing mode, your ISP automatically assigns the IP address of the access point to it.

This type of connection applies to most Cable Internet subscribers, for instance:

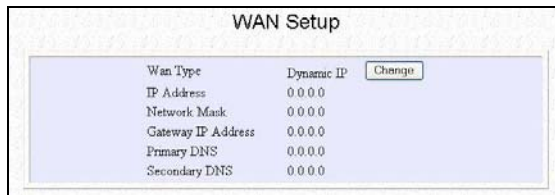
- Singapore Cable Vision subscribers.
- @HOME Cable Service users.

Changing WAN Type – Dynamic IP Configuration

At the **Dynamic IP WAN Setup** page:

You can review the:

- IP Address
- Network Mask
- Gateway IP Address
- Primary DNS
- Secondary DNS



The screenshot shows a 'WAN Setup' window with a table of configuration parameters. The 'Wan Type' is set to 'Dynamic IP', and there is a 'Change' button next to it. The other parameters are all set to '0.0.0.0'.

Wan Type	Dynamic IP	Change
IP Address	0.0.0.0	
Network Mask	0.0.0.0	
Gateway IP Address	0.0.0.0	
Primary DNS	0.0.0.0	
Secondary DNS	0.0.0.0	

Your ISP dynamically allocates these parameters to the access point.

Chapter 5 Further Configuration

5.2.2 Static IP

If you have subscribed to a specific IP address or to a fixed range of IP addresses from your ISP, follow the procedure summarized below.

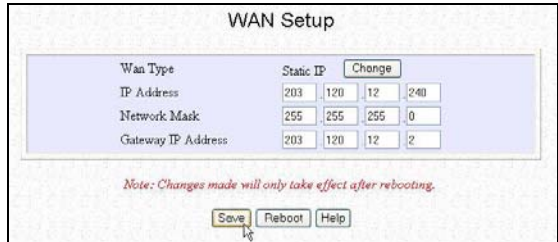
Changing WAN Type – Static IP Configuration

At the **Static IP WAN Setup** page:

Replace the default **IP Address**, **Network Mask** and **Gateway IP Address** fields with the relevant values given by your ISP.

Click on the **Save** button.

Click on the **Reboot** button to restart the system and let the changes to take effect.



The screenshot shows the 'WAN Setup' interface. At the top, there is a 'Wan Type' dropdown menu set to 'Static IP' and a 'Change' button. Below this is a table for configuration:

Wan Type	Static IP				Change
IP Address	203	120	12	240	
Network Mask	255	255	255	0	
Gateway IP Address	203	120	12	2	

Below the table, a red note reads: *Note: Changes made will only take effect after rebooting.* At the bottom, there are three buttons: 'Save', 'Reboot', and 'Help'. A mouse cursor is pointing at the 'Save' button.

Chapter 5 Further Configuration

5.2.3 PPPoE

Select this connection type if you have subscribed to ADSL in a country utilizing standard PPPoE for authentication, for instance:

- If you are in Germany which uses T-1 connection.
- If you are a SingNet Broadband or Pacific Internet Broadband user in Singapore.

The next steps will guide you in setting up the access point.

Changing WAN Type – PPPoE Configuration

At the **PPPoE WAN Setup** page:

Fill in the relevant fields following the parameters of your broadband Internet account.

The **Status** section gives you a summary of your connection settings such as:

- IP address
- Network Mask
- Gateway IP Address
- Primary & Secondary DNS

The screenshot shows the 'WAN Setup' configuration page. The 'Wan Type' is set to 'PPPoE' with a 'Change' button. The 'MTU(1400 - 1492)' is set to '1482 (default 1462)'. There are input fields for 'Username' and 'Password' (masked with asterisks). The 'Service Name' field is empty. Under 'Service Name', there are radio buttons for 'On-Demand' (selected) and 'Always-On'. The 'On-Demand' section has 'Idle Timeout (0.Disable)' set to '0' seconds and 'Reconnect Time Factor' set to '30' seconds. There is a checkbox for 'Use non-standard PPPOE ethernet type' which is unchecked. The 'Status' is 'Disconnected' with a 'Connect' button. Below the status, there are fields for 'IP Address', 'Network Mask', 'Gateway IP Address', 'Primary DNS', and 'Secondary DNS', all showing '0.0.0.0'. At the bottom, there are 'Save', 'Reboot', and 'Help' buttons. A note at the bottom reads: 'Note: Changes made will only take effect after rebooting.'

If you are offline, pressing the **Connect** button will immediately initiate a connection.

Click on the **Save** button.

Click on the **Reboot** button to restart the system and allow the changes to take effect.

Chapter 5 Further Configuration

PPPoE Parameter	Description
MTU	The MTU or Maximum Transmission Unit is the largest packet size allowed by the ISP. It is set by default to 1462 though it can vary between 1400 and 1492.
Username	This refers to your broadband account username.
Password	This refers to your broadband account password.
Service Name	This optional field allows you to key in the service name of your ADSL subscription.
On-Demand	If enabled, the router will automatically connect to the ISP whenever a LAN client makes an Internet request.
Idle Timeout	<p>This field is relevant only if the On-Demand option is enabled and allows you to specify a maximum lapse of idle time allowed before the router automatically goes offline. It will only re-connect when a LAN client makes an Internet request.</p> <p>If the field is set to 0, this feature will be disabled and the access point will remain online unless disconnected by the ISP.</p>
Always-On	If this feature is enabled, the access point will remain permanently connected to the Internet.
Reconnect Time Factor	This field is relevant only if the Always-On option is enabled and allows you to specify a maximum lapse of offline time following which, the unit should automatically reconnect to the Internet. The default value has been set to 30 seconds.
Use non-standard PPPoE Ethernet type	This applies to certain Ethernet-based ADSL modem requiring non-standard PPPoE for authentication. In case of doubts, do <u>NOT</u> enable this checkbox.

Chapter 5 Further Configuration

5.2.4 Singapore ADSL

Other ADSL subscribers in Singapore, including SingTel Magix SuperSurf users, should opt for this type of connection.

Changing WAN Type – Singapore ADSL Configuration

At the **Singapore ADSL WAN Setup** page:

Key in the **Username** of your Internet account.

Insert your account **Password**.

Enter an **Idling Timeout** value, in the range of 30-3600 seconds. Entering **0** will disable this feature.

WAN Setup	
Wan Type	Singapore ADSL(Ethernet 512K) <input type="button" value="Change"/>
Username	<input type="text" value="Username@INT512"/>
Password	<input type="password" value="*****"/>
Idle Timeout (30-3600, 0=Disable)	<input type="text" value="300"/> seconds
Status	Disconnected <input type="button" value="Connect"/>
IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Note: Changes made will only take effect after rebooting.

The **Status** section gives you a summary of your connection settings such as:

- IP address
- Network Mask
- Gateway IP Address
- Primary & Secondary DNS

If you are offline, pressing the **Connect** button will immediately initiate a connection.

Click on the **Save** button.

Press the **Reboot** button to restart the system and allow the changes to take effect.

Chapter 5 Further Configuration

5.2.5 Australia BPA Cable

This type of connection has been especially customized for Big Pond Cable Internet users in Australia

Changing WAN Type – Singapore ADSL Configuration

At the **Australia BPA WAN Setup** page:

Key in the **Username** of your Internet account.

Insert your account **Password**.

Enter the **IP address** of your Authentication Server, as defined by your ISP.

Fill in an **Idling Timeout** value, in the range of 30-3600 seconds.

Entering **0** will disable this feature.

The Status section gives you a summary of your connection settings such as:

- IP address
- Network Mask
- Gateway IP Address
- Primary & Secondary DNS

If you are online, pressing the **Disconnect** button will immediately end your connection.

Click on the **Save** button.

Press the **Reboot** button to restart the system and allow the changes to take effect.

The screenshot shows a web-based configuration interface titled "WAN Setup". The "Wan Type" is set to "Australia BPA Cable". The "Username" field contains "Username" and the "Password" field contains "*****". The "Authentication Server" field is empty. The "Idle Timeout (30-3600, 0 Disable)" is set to "0" seconds. The "Status" is "Disconnected" with a "Connect" button. The "IP Address", "Network Mask", "Gateway IP Address", "Primary DNS", and "Secondary DNS" are all set to "0.0.0.0". A "Change" button is next to the "Wan Type". At the bottom, there are "Save", "Reboot", and "Help" buttons. A note at the bottom reads: "Note: Changes made will only take effect after rebooting."

Field	Value
Wan Type	Australia BPA Cable
Username	Username
Password	*****
Authentication Server	
Idle Timeout (30-3600, 0 Disable)	0 seconds
Status	Disconnected
IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Chapter 5 Further Configuration

5.2.6 PPTP

The Point-to-Point Tunneling Protocol (PPTP) is a networking technology which, enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks, enabling remote users to access corporate networks securely at a lower cost

Changing WAN Type – PPTP Configuration

At the **PPTP WAN Setup** page:

Key in the **Client IP address**.

Enter the Network Mask.

Fill in the **Username** of your Internet account.

Insert your account **Password**.

Enter the **IP address** of your VPN Server.

Fill in an **Idling Timeout** value, in the range of 30-3600 seconds.

Entering **0** will disable this feature.

Click on the **Save** button.

Press the **Reboot** button to restart the system and let the changes take effect.

The screenshot shows the 'WAN Setup' configuration page. At the top, 'Wan Type' is set to 'PPTP' with a 'Change' button next to it. Below this, there are several input fields: 'Client IP' (293, 120, 12, 240), 'Net Mask' (255, 255, 255, 0), 'Username' (empty), 'Password' (masked with asterisks), and 'VPN Server' (empty). A note says 'Pls input IP of the server. e.g. 100.100.100.100'. Below these are 'Idle Timeout (30-3600, 0:Disable)' set to 0 seconds, 'Status' set to 'Disconnected' with a 'Connect' button, and several other fields for IP Address, Network Mask, Gateway IP Address, Primary DNS, and Secondary DNS, all set to 0.0.0. At the bottom, there are 'Save', 'Reboot', and 'Help' buttons. A red note at the bottom of the form states: 'Note: Changes made will only take effect after rebooting.'

5.3 Using NAT

(Only available in Gateway and Wireless Routing Client mode)

NAT, also known as Network Address Translation, functions by transforming the private IP address of packets originating from hosts on your network so that they appear to be coming from a single public IP address and by restoring the destination public IP address to the appropriate private IP address for packets entering the private network. The multiple PCs on your network would then appear as a single client to the WAN interface.

Enabling NAT

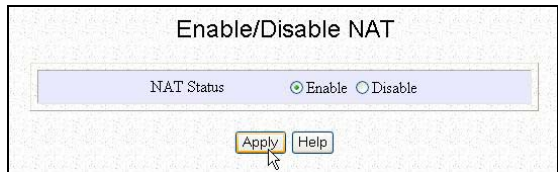
Click on **NAT** from the **CONFIGURATION** menu.

By default, the **NAT Status** radio button is enabled.

To change the **NAT Status**:

Select the appropriate radio button.

Click on the **Apply** button.



NOTE

Disabling NAT will disable Internet Sharing. Broadband Internet sharing requires this option to be Enabled.

When NAT is enabled, your network is not accessible to the WAN. However, implementing **virtual servers** allows you to host Internet servers such as Web servers, FTP servers or Mail servers on your network, in spite of NAT.

5.3.1 To set up a De-Militarised Zone host

A De-Militarised Zone host, or DMZ host, is a separate neutral client sitting between your private network and the WAN.

It initiates WAN connections upon request from your network clients, and forwards the request packets. Similarly, outside users can access only the DMZ host.


You can host Web pages or public information that can be served to the outside world, on the DMZ host.

Setting up DMZ

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

Ensure the **NAT Status** is enabled.

At the **Advanced NAT** Options section:



The screenshot shows a configuration window titled "Nat DMZ Ip Address". It contains a text input field labeled "Private IP Address" with the value "192.168.168.55" entered. Below the field is a yellow "Apply" button with a mouse cursor hovering over it.

Click on **DMZ**.

Key in the **IP address** of the PC you wish to place within the DMZ in the **Private IP Address** field.

The default Private IP Address is set to 0.0.0.0. For illustration, we entered **192.168.168.55**

Click on the **Apply** button to confirm your entry.

Disable DMZ

Enter 0.0.0.0 as the Private IP Address.

Click on the **Apply** button.



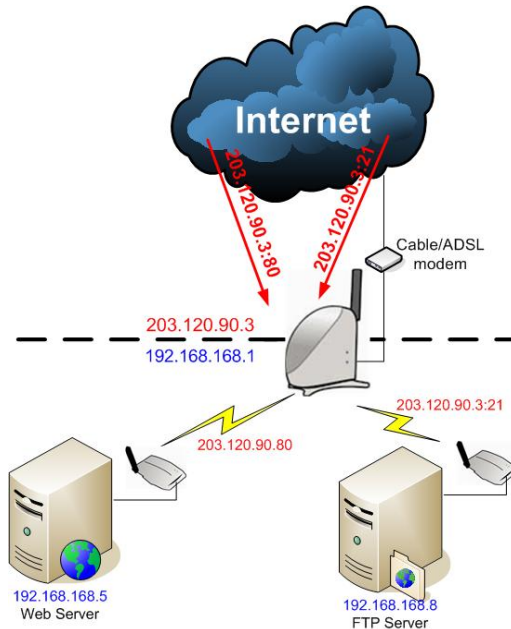
The screenshot shows a configuration window titled "Nat DMZ Ip Address". It contains a text input field labeled "Private IP Address" with the value "0.0.0.0" entered. Below the field is a yellow "Apply" button with a mouse cursor hovering over it.

5.3.2 To set up port forwarding

Port forwarding allows the access point to redirect any incoming Internet request bearing a public IP address to a specific PC on your network, based on the incoming packet's TCP/UDP port number.

You can thus use TCP port forwarding to hide your web-server behind the access point for added security while using UDP port forwarding lets you run a secure multiplayer game server.

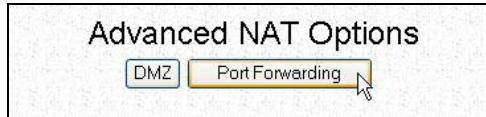
The following diagram shows the access point with a public IP address of 203.120.90.3 and a private IP address of 192.168.168.1. All incoming packets with port number 80 will be forwarded to the Web server, known on the LAN as 192.168.168.5, while those with port number 21 will be directed to the FTP server which has a private IP address of 192.168.168.8.



Set up Port Forwarding – For Known Server

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

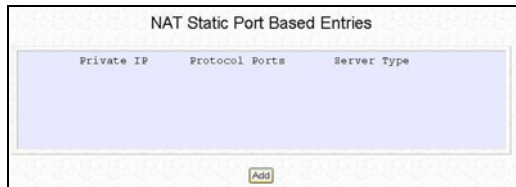
Ensure whether the **NAT Status** is enabled.



At the Advanced NAT Options section:

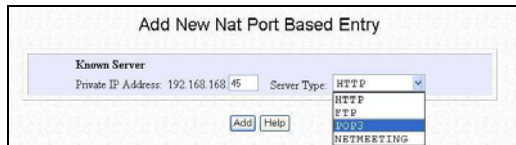
Click on Port Forwarding.

The **NAT Static Port Based Entries** table illustrated by the screen shot displays the list of current port-based entries.



Click on the **Add** button.

For standard server applications: **HTTP/FTP/POP3/Netmeeting**, go to the **Known Server** section:



Complete the **Private IP Address** field.

Pick the appropriate selection from the **Server Type** drop down list.

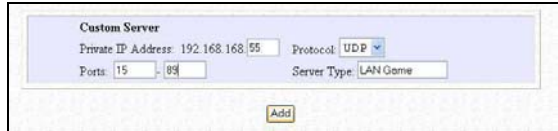
Click on **Add** button.

We illustrated with a **POP3** server having **Private IP Address** of **192.168.168.45**.

Chapter 5 Further Configuration

Set up Port Forwarding – For Custom Server

Otherwise, in order to set up Internet applications which are not defined in the **Known Server** section, go to **Custom Server**:



The screenshot shows a form titled "Custom Server" with the following fields: "Private IP Address" (192.168.168.55), "Protocol" (UDP), "Ports" (15-89), and "Server Type" (LAN Game). An "Add" button is located at the bottom right of the form.

Key in the Private IP Address.

Define the **Port numbers** to use.

Select the relevant **Protocol** from the drop down list.

Identify the **Server Type**.

Click on **Add** button.

We entered a **Private IP Address** of **192.168.168.55**, defined ports **15** to **89** as the application **Ports**, selected **UDP** from the **Protocol** drop-down list and labelled the **Server Type** as **LAN Game**.

The updated **NAT Static Port Based Entries** will reflect your new entry.

If you want to assign more servers in your LAN, click on the **Add** button.

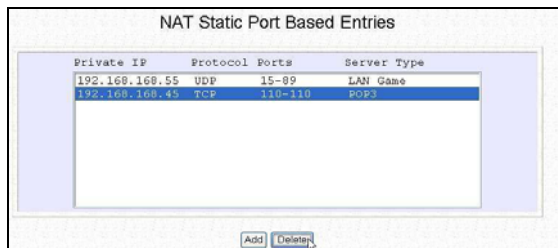
Delete a table entry

If you want to delete any of the table entries:

Select the entry to delete.

Click on the **Delete** button.

The table will be refreshed.



The screenshot shows a table titled "NAT Static Port Based Entries" with the following data:

Private IP	Protocol	Ports	Server Type
192.168.168.55	UDP	15-89	LAN Game
192.168.168.45	TCP	110-110	POP3

An "Add" button and a "Delete" button are located at the bottom right of the table.

Chapter 5 Further Configuration

The following is a non-exhaustive list of well-known port numbers:

Application	Port Number
Echo	7
Daytime	13
FTP	21
SMTP (Simple Mail Transfer, i.e., email)	25
Telnet	23
Time	37
Name server	42
Gopher	70
WWW (World Wide Web)	80

5.4 Routing

(Only available in Gateway and Wireless Routing Client mode)

The access point supports both static routing so that you can manually add entries into its routing table and dynamic routing, where it will automatically update the routing table, whenever necessary.



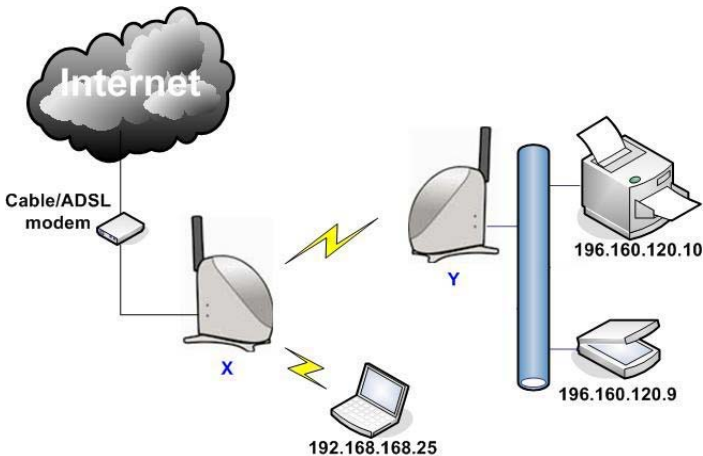
NOTE

The default settings of the access point are sufficient to allow broadband Internet sharing. There is NO need to configure any further routing information.

Please note that improper routing settings will cause undesired effects!

The diagram illustrates one of the access points (**X**) functioning as Internet gateway to wireless clients while another of the access points (**Y**) connects to the office's remote resources.

The routing table of **X** can be modified so that if its wireless clients intend to use the remote office resources, data packets are automatically redirected to **Y**.



Chapter 5 Further Configuration

5.4.1 Static Routing

The following will show you how to add entries to your gateway's routing table so that it may re-route IP packets to another network, which is very useful if your network has more than one router.

Static Routing

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

The **IP Routing Table** illustrated by the screen shot on the left displays the list of current routing entries.

If you want to add a static route in the **IP Routing Table**:

Click on the **Add** button.

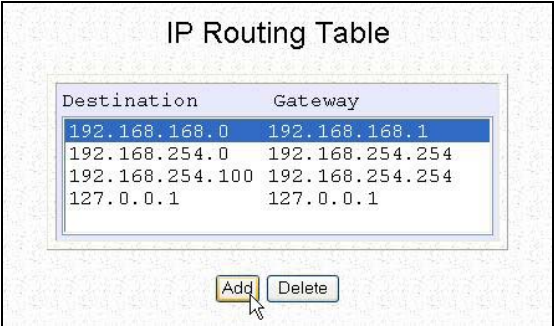
Specify the **Destination IP Address** of your new entry.

Fill in the Gateway IP Address.

Click on **Apply**.

The new entry will appear in the updated **IP Routing Table**.

If you want to add more routes, click on the **Add** button.



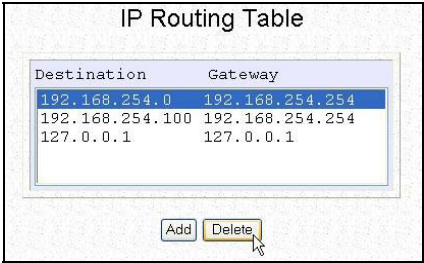
Destination	Gateway
192.168.168.0	192.168.168.1
192.168.254.0	192.168.254.254
192.168.254.100	192.168.254.254
127.0.0.1	127.0.0.1

Delete Static Routing

If you want to delete any of the table routes:

Select the entry to delete. Click on the **Delete** button.

The table will be refreshed.



Destination	Gateway
192.168.254.0	192.168.254.254
192.168.254.100	192.168.254.254
127.0.0.1	127.0.0.1

Chapter 5 Further Configuration

5.4.2 Dynamic Routing

When using dynamic routing, the access point can continuously update its routing table with the latest routing information, thus automatically adjusting to any physical changes in the network topology.

The access point supports RIP1 (Routing Information Protocol) and RIP2 (Routing Information Protocol version 2), and periodically broadcasts its routing tables to neighboring routers. The best route is chosen if there are multiple routes to a destination.

The next steps will guide you in setting up dynamic routing.

Dynamic Routing

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

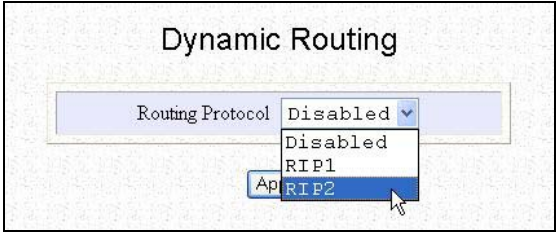
By default, **Dynamic Routing** is disabled.

Select which dynamic routing protocol to implement from the **Routing Protocol** drop down list.

Click on the **Apply** button.

Reboot the system.

From then on, the **IP Routing Table** will be dynamically updated.



5.5 Implementing IP Filtering

(Only available in Gateway and Wireless Routing Client mode)

Enabling the IP Filtering function causes the access point to decide, according to predefined rules, whether to block all outgoing packets or to let them pass.

The access point provides granularity and latitude in monitoring the traffic in your network by allowing you to define IP filtering rules, based on these 3 factors:

- **Source IP Address**

This would allow you to selectively restrict Internet activity originating from a specific PC or group of PCs.

- **TCP Port**

You may choose to prevent certain applications such as FTP or Telnet, which use a commonly known port number.

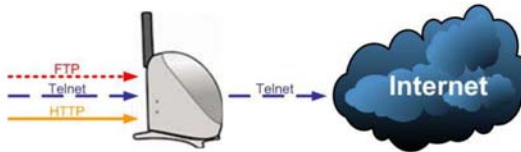
- **Time frame**

For example, you may restrict Internet access from your children's PC to certain time frames such as between 19H30 and 21H45.

For instance, let us assume that an IP filtering rule has been defined as:

TCP Port **23** from **any** IP on **any** day at **any** time (Port 23 is usually used for **Telnet**).

If the **sent** radio button is selected, all outgoing packets will be sent except those belonging to **Telnet** sessions. On the other hand, if the **discarded** radio button is selected, all outgoing packets will be blocked except for those belonging to **Telnet** sessions. We illustrated the second case below.



Chapter 5 Further Configuration

IP Filtering

Click on **IP Filtering** from the **CONFIGURATION** menu.

Select either the **Sent** or **Discarded** radio button to accept or reject any packet conforming to the rules.

Click on the **Add** button to set the new rule in the **IP Filter Configuration** GUI.

 sent discarded except for those matching one or more of the following rules.' A table with columns: 'Select to Edit', 'Rule Name', 'IP Address(es)', 'Destination Port(s)', 'Day of the Week', and 'Time of the Day'. Below the table, a text line says: 'If the system loses its time settings, ignore accept the access time settings in the above rules.' At the bottom are buttons: 'Apply', 'Add', 'Delete', 'Edit', and 'Help'."/>

Insert a **Rule Name** for this new packet filtering rule.

From the **IP Address** drop down list, select whether to apply the rule to:

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

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

Any IP address
You may here, leave both, the **(From)** as well as the **(To)** fields, blank.

Chapter 5 Further Configuration

At the **Destination Port** drop down list, select either:

Destination Port	Single
(From)	Any
(To)	Range
	Single

A Range of TCP ports

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

Destination Port	Range
(From)	25
(To)	61

A Single TCP port

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

Destination Port	Single
(From)	25
(To)	

Any IP port

You may here, leave both, the **(From)** as well as the **(To)** fields, blank.

Destination Port	Any
(From)	
(To)	

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

Day of the Week	Range
(From)	Any
(To)	Range
	Thu

A Range of days

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

Day of the Week	Range
(From)	Mon
(To)	Thu

Any day

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

Day of the Week	Any
(From)	Sun
(To)	Sun

Chapter 5 Further Configuration

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

Time of the Day	Range	(hh: 00-23, mm: 00-59)
(From)	Any	(hh:mm)
(To)	15:00	(hh:mm)

A Range of time

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

Time of the Day	Range	(hh: 00-23, mm: 00-59)
(From)	08:00	(hh:mm)
(To)	15:00	(hh:mm)

Any time

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

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

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

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

If you want to define more **IP Filtering** rules, click on the **Add** button.

Chapter 5 Further Configuration

Delete IP Filtering

We illustrated deleting the rule called **Finance**.

To delete an existing IP filtering rule:

Select the radio button corresponding to the rule to delete.

Click on **Delete**.

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

Filtering Configuration

Warning: Incorrect configuration may cause undesirable behavior.

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

Select to Edit	Rule Name	IP Address(es)	Destination Port(s)	Day of the Week	Time of the Day
<input checked="" type="radio"/>	Finance	192.168.168.12-192.168.168.16	1-5	Mon-Fri	08:00-15:00
<input type="radio"/>	Purchasing	192.168.168.20-192.168.168.30	14-24	Mon-Sat	09:00-22:00

If the system loses its time settings, ignore accept the access time settings in the above rules.

We illustrated editing the rule called **Purchasing**.

If you want to edit an existing IP filtering rule:

Select the radio button corresponding to the rule to edit.

Click on **Edit**.

You will then return to the **IP Filtering Configuration** GUI, from which you can re-define the rule.

Filtering Configuration

Warning: Incorrect configuration may cause undesirable behavior.

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

Select to Edit	Rule Name	IP Address(es)	Destination Port(s)	Day of the Week	Time of the Day
<input type="radio"/>	Finance	192.168.168.12-192.168.168.16	1-5	Mon-Fri	08:00-15:00
<input checked="" type="radio"/>	Purchasing	192.168.168.20-192.168.168.30	14-24	Mon-Sat	09:00-22:00

If the system loses its time settings, ignore accept the access time settings in the above rules.

Chapter 5 Further Configuration

5.6 Applying Remote Management

(Only available in Gateway and Wireless Routing Client mode)

Making use of remote management, you only require Internet access to be able to manage your network.

This feature is especially helpful for those who work away from the office or from home.

Remote Management

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

Specify the **HTTP Port number** and the **Telnet Port number**.

The standard entry for HTTP Port is 80 and 23 for Telnet Port.

Click on **Save** button.

Press the **Reboot** button to restart the system so that the changes can take effect.

The screenshot shows the 'Remote Management' configuration interface. It has a title 'Remote Management' at the top. Below it, there are two input fields: 'HTTP Port' with the value '80' and '(Standard=80)', and 'TELNET Port' with the value '23' and '(Standard=23)'. Below these fields is a note: '(Enter 0 to disable remote management)'. At the bottom, there is a red note: 'Note: Changes made will only take effect after rebooting.' and two buttons: 'Save' and 'Reboot'.

If you want to disable the **Remote Management** feature:

Key in **0** for both the **HTTP Port** and the **TELNET Port**.

Click on **Save** button.

Press the **Reboot** button to restart your computer so that the changes can take effect.

The screenshot shows the 'Remote Management' configuration interface. It has a title 'Remote Management' at the top. Below it, there are two input fields: 'HTTP Port' with the value '0' and '(Standard=80)', and 'TELNET Port' with the value '0' and '(Standard=23)'. Below these fields is a note: '(Enter 0 to disable remote management)'. At the bottom, there is a red note: 'Note: Changes made will only take effect after rebooting.' and two buttons: 'Save' and 'Reboot'.

5.7 Enabling Parallel Broadband (Only available in Gateway mode)

The access point is equipped with the exclusive **Parallel Broadband** technology, which translates into scalable Internet bandwidth as well as Load Balancing and Fail-Over Redundancy features.

Since there is no restriction to the type of broadband Internet account that the access point can connect to, your network may run with one of the access points on Cable Internet, while the rest connect to ADSL.

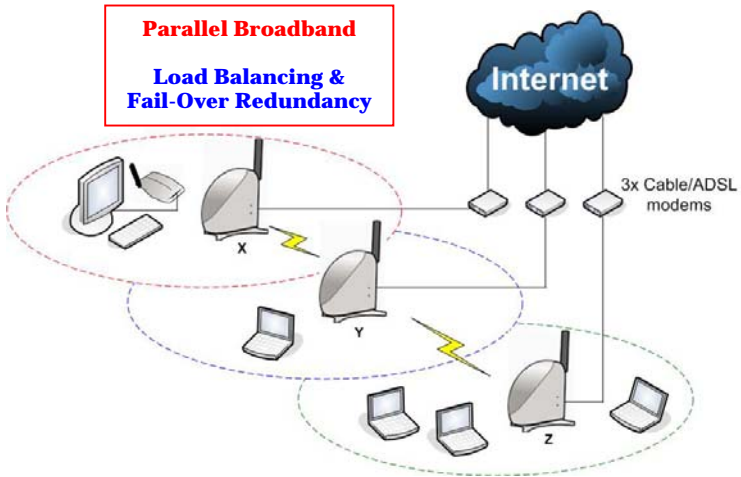
The diagram below illustrates an application of Parallel Broadband in a network with 3 of the access points, **X**, **Y** and **Z**.

5.7.1 Load balancing

Building your network around multiple access points arranged in cascade and running under Parallel Broadband, creates an aggregate bandwidth and enables you to balance the Internet traffic generated by your private network over multiple broadband connections. For instance, **Z** might share its load with **X** and **Y** so that each of the access points serves approximately the same number of users.

5.7.2 Fail-Over Redundancy

In case one of your broadband connections should fail, the affected access point will automatically switch over to other operational broadband channels so that your network is not disrupted. For instance, when the WAN connection to **Z** is down, **Z** will redirect its traffic to **Y**, and hence providing Fail-Over Redundancy of Internet access to wireless clients of **Z**.



5.7.3 To enable Parallel Broadband

Before enabling the Parallel Broadband feature, verify whether:

- Each of the access points is correctly configured to connect to its specific broadband Internet account.
- You need to enable DHCP on all of the access points in Parallel broadband. It is recommended that each of the access points leases IP in a non-overlapping IP address pool.
- All of the access points are interconnected in a chain manner using WDS as illustrated in the section on **WLAN Basic Setup**.
- Each of the access points is running in Gateway mode with the Parallel Broadband option enabled.

Enable Parallel Broadband

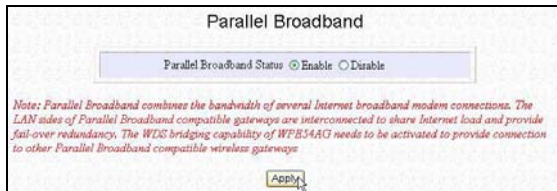
Click on **Parallel Broadband** from the **CONFIGURATION** menu.

By default the **Parallel Broadband** feature is disabled.

Enable the Parallel Broadband Status.

Click on **Apply** button.

Repeat this for the other access points in your network.



This chapter provides guidelines in using:

- The **SYSTEM TOOLS** menu
- The **HELP** menu

6.1 Using the SYSTEM TOOLS Menu

6.1.1 System Identity

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

In certain cases, your Internet Service Provider might request for a **System Name** before allowing you to access the Internet. This **System Name** also serves as a **DHCP Client ID** during negotiations with the DHCP Server for dynamic IP address allocation.

You can define the **System Identity** of the access point to be also utilized as **System Name** or as **DHCP Client ID**.

System Identity


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

Enter the **DHCP Client ID** assigned by your ISP in the **System Name** field.

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

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

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



Chapter 6 System Utilities

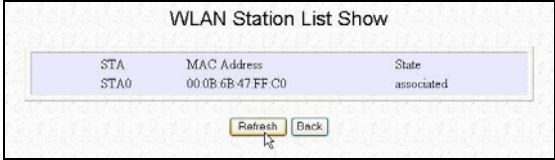
6.1.2 WLAN Station List (Only available in AP mode/Gateway mode)

This option allows you to view the wireless clients in the wireless network.

WLAN Station List

Click on **WLAN Station List** from the **SYSTEM TOOLS** menu.

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



STA	MAC Address	State
STA0	00:0B:6E:47:FF:C0	associated

Refresh Back

6.1.3 Set System's Clock

Synchronizing the built-in clock of the access point with the time kept by your workstation will enable you to effectively manage and operate the time-based functions provided by the access point.

Set System's Clock

Click on **Set System's Clock** from the **SYSTEM TOOLS** menu.


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

Enable the Auto Time Setting (SNTP) radio button.

SNTP stands for Simple Network Time Protocol and is used to synchronies computer clocks in the Internet.

Fill in the **Time Servers** field.

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



6.1.4 Firmware Upgrade

Our products are designed for upgradeability. You can check the current 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.

Firmware Upgrade

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

Key in the path and file name of the downloaded file in the **Upgrade Firmware (path and file name)** field.

Alternatively, click on the **Browse** button to locate the file.

Click on the **Upgrade** button.

Follow the instructions given during the upgrading process.

Reboot the system.

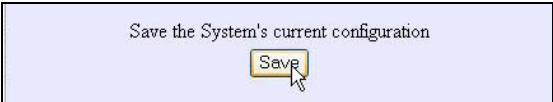
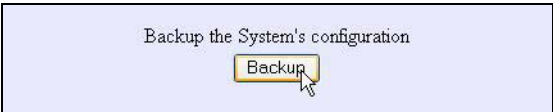

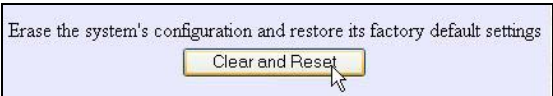


NOTE

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

6.1.5 Save 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.

Save Your Settings	
Click on Save or Reset Settings from the SYSTEM TOOLS menu.	
Click on the Save button.	
Reboot the system.	
Backup Your Settings	
If you want to back up the current settings of the access point onto your hard disk drive:	
Click on the Backup button.	
Restore Your Settings	
Or you may directly type in the path name of the file at Restore the Machine's configuration (path and file name) .	
Click on the Restore button.	
Reset Your Settings to Factory Default	
To discard <u>ALL</u> the configuration you have made and restore the access point to its initial factory settings:	
Click on Clear and Reset button.	

6.1.6 Reboot System

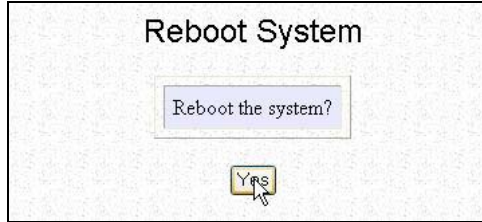
Most of the changes you make to the system's settings require a system reboot before the new parameters can take effect.

Reboot Your device

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

You will be prompted to confirm whether to execute a system reboot.

Click on the **Yes** button whenever you are ready to restart.



6.1.7 Change Password

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


Changing your Password

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

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.

Click on the **Change Password** button.



The screenshot shows a web interface titled "Change System Password". It contains three input fields: "Current Password" with 8 dots, "New Password" with 6 dots, and "Confirm Password" with 6 dots. Below the fields is a "Change Password" button with a mouse cursor pointing to it.

6.1.8 Logout

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

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

Click the **Logon** button to access the configuration interface again.

6.2 Using the **HELP** menu

6.2.1 Get Technical Support

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

Get Technical Support

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

This is a feature-packed device. If you require further information than provided in the manual or data sheet, please contact a Technical Support Centres by mail, email, fax or telephone.

6.2.2 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.

Get Technical Support

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

The **System Information** page will supply information concerning the access point configuration settings.

AI Solutions to Common Problems

In this section, we list suggested steps to rectify some common problems that may arise during the installation and operation of the access point.

3. I want to know whether the access point is connected to the Internet.

A. Open a Command Prompt

For *Windows 98/98SE/ME*, please click the **Start** button and **Run**. In the **Open** field within the **Run** dialog box, type in **command**. Press the **Enter** key or click the **OK** button.

For *Windows 2000 and XP*, please click the **Start** button and **Run**. In the **Open** field within the **Run** dialog box, type in **cmd**. Press the **Enter** key or click the **OK** button.

B. In the Command Prompt, type ping 192.168.168.1 and press the Enter key. You will get a reply if the PC is communicating with the gateway.

If you do NOT get a reply, ensure that your settings are correct before trying again. Your computer MUST be in the same subnet as the access point.

C. In the Command Prompt, type ping www.yahoo.com and press the Enter key.

Obtaining a reply means that you are connected to the Internet.

Otherwise, you may want to ping another known host.

Getting no reply from any of the other hosts that you have tried, suggests that your connection may be having problems.

4. I am not getting an IP address and am unable to surf the Internet.

- A. Make sure that the Ethernet cable is properly connecting your Cable/ADSL modem to the WAN port of the gateway, and verify whether the gateway has a valid IP address from the **About System** page. Then refer to suggested steps A, B & C to Problem 1 described above, to verify the connectivity of the gateway.
- B. Ensure that the WAN settings are relevant to your broadband connection. In case of doubt, you should contact your network administrator/ISP to enquire about your Internet connection type.
- C. Power off your computer, the gateway and the Cable/ADSL modem. Turn on the Cable/ADSL modem then wait for 1 minute before turning on the gateway. Lastly, turn on your computer. Verify whether you have been allocated an IP address and are able to surf the web.

5. I am not able to access the Web interface of the access point

- D. Refer to Problem 1 and follow suggested steps A and B to verify your connectivity to the gateway.
- E. If you are a PPPoE user, you will need to remove the proxy settings or the dial-up pop-up window.
- F. If you are not using the uConfig utility, you may need to change the settings of your Web browser.

For Microsoft Internet Explorer 5.0 or later versions

From the **Tools** menu bar, select **Internet Options** and then click on the **Connections** tab. Click on the **LAN Settings** button. Uncheck any options from that dialog box. Press the **OK** button to return to the previous screen.

For PPPoE users, click the radio box option **Never dial a connection** to remove any dial-up pop-ups. Press the **OK** button to finish.

For Netscape 4.7 or later versions

Start Netscape Navigator. From the **Edit** menu bar, select **Preferences**, then **Advanced**, and finally **Proxies**.

Make sure that the **Direct connection to the Internet** option is selected.

Close all windows to finish.

Appendix I Troubleshooting

6. I want to set the access point to its factory default settings.

- G. Power up the gateway.
- H. Depress the **Reset** button situated at the back of the device and hold it for **2 to 10** seconds before releasing it.

7. My laptop is not able to access the AP.

- I. In the Command Prompt, type ping 192.168.168.1 and press the Enter key.

If you get a reply, your laptop is communicating with the gateway.

If you do NOT get a reply, please continue with the following steps.

- J. Ensure whether your wireless card and driver have been properly installed.

Open the **Control Panel**. Double-click the **System** icon. Inside the **Device Manager** window, expand the **Network Adapters** listing and verify whether the name of your wireless card is listed.

If it does not, power down your laptop. Remove the wireless card from its slot and re-insert it, ensuring that it properly fits into the slot. Reboot your computer.

If it does, click on it and press the **Properties** button. Check whether **Device Status** displays this message “*This device is working properly*”. If it does not, you will need to uninstall and re-install the software driver.

- K. Verify whether your gateway and your laptop and/or other wireless clients have been configured with the same SSID, which is the case-sensitive name of the wireless network that you are trying to access, and the same WEP settings.
- L. Check whether your gateway and your laptop are using the same frequency channel.

Appendix I Troubleshooting

8. **My network contains several of the access points but they are unable to connect to each other.**

M. If you are running the **Parallel Broadband** feature:

Though they may belong to different SSIDs, the gateways MUST operate in the same frequency band.

N. If you are trying to implement a **WDS**:

Verify that the gateways are functioning in the same frequency band.

Check whether the MAC address that you have added as WDS link corresponds to the wireless MAC address displayed in the **About System** page of your gateway.

Appendix III TCP/IP Configuration

Appendix II 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 **DIAG** LED will light up and remain ON.

Table 1 below illustrates the behaviour of the **DIAG** LED.

Operation State	DIAG LED
Corrupted firmware – The access point switches to loader mode	Blinks very fast
Recovery in progress	ON
Successful recovery	Blinks very slowly

AII How to recover the access point from failed firmware

Before starting, check the status of the **DIAG** LED against Table 1 above to verify whether firmware failure has occurred.

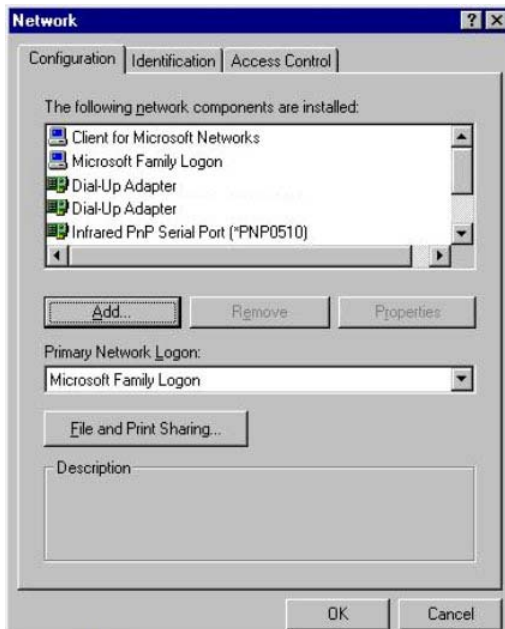
- Power the access point off and disconnect it from the network.
- Use a MDI cable (cross-connect for the access point) to connect the LAN port of the access point to the LAN port of your computer.
- Power the access point on, and then start up your computer. The computer will obtain an IP address of **192.168.168.100** from the access point.
- Insert the access point Product CD into the CD drive of your computer.
- From the computer, click **Start**, then **Run** and type in the following command:
X:TFTP -i 192.168.168.1 PUT X: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.
- If you have downloaded a newer firmware and have saved it in your local hard disk as for example, **C:\accesspoint\accesspointxxx.IMG**, then replace **X:\image_name.IMG** with this new path and firmware name.
- The recovery process will now take place. You can check the **DIAG** LED against Table 1 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 III TCP/IP Configuration

This chapter discusses the configuration of your TCP/IP connection of the access point. Upon the successful installation of the access point, the network adapter will be added to your network folder. To configure TCP/IP connection settings for the access point, please follow the steps listed below. If you are using Windows 2000/XP, please go to section AIII.2.

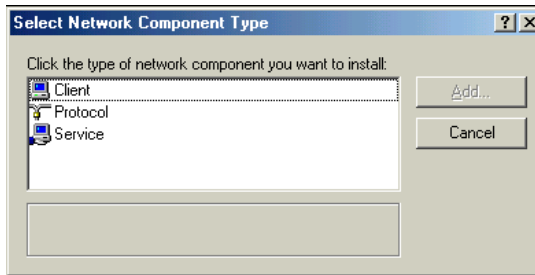
AIII.1 Configure dynamic IP Address in Windows 98SE/ME

1. From the Windows 98SE/ME **Start** Button, select **Settings**, and then **Control Panel**.
2. Double-click on the **Network** icon and a Network screen will appear as shown.

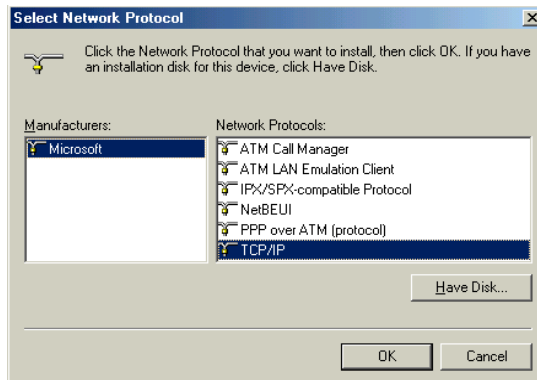


Appendix III TCP/IP Configuration

3. Go through the list of Network Components in the Network window Configuration tab. If TCP/IP is not installed, click on **Add** to start the installation
4. Select **Protocol** and click **Add**.



5. Select **Microsoft** and TCP/IP in the **Manufacturers** and **Network Protocols** columns respectively. Click **OK**.

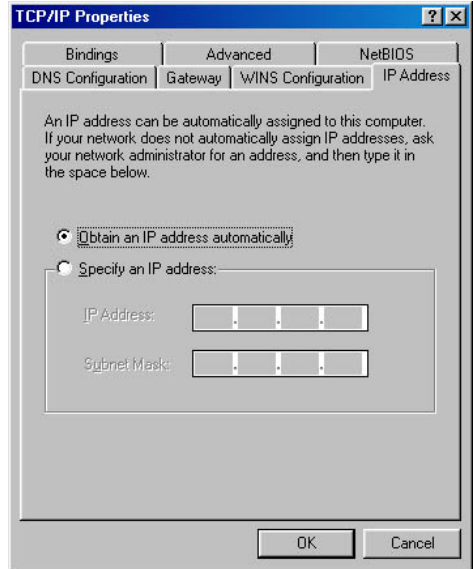


Appendix III TCP/IP Configuration

6. After TCP/IP is installed, go back to the Network screen and select TCP/IP in the list of Network Components.



7. Click **Properties**, and configure the settings in each of the TCP/IP Properties window.



NOTE

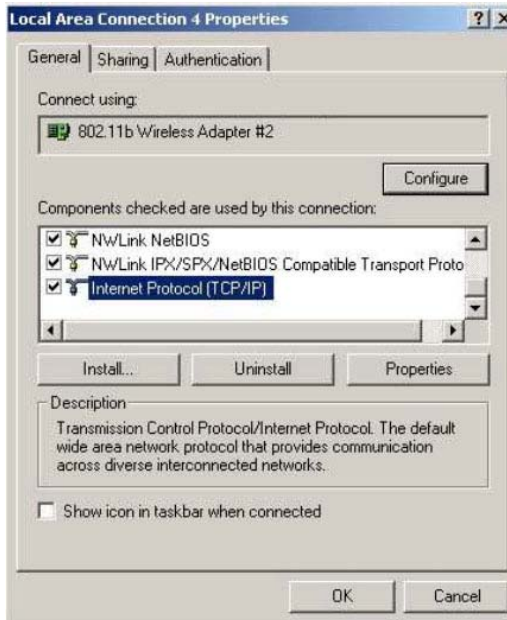
Please check with your system administrator or Internet Service Provider for more information on the TCP/IP parameters.

Appendix III TCP/IP Configuration

AIII.2 Configure dynamic IP Address in Windows XP/2000

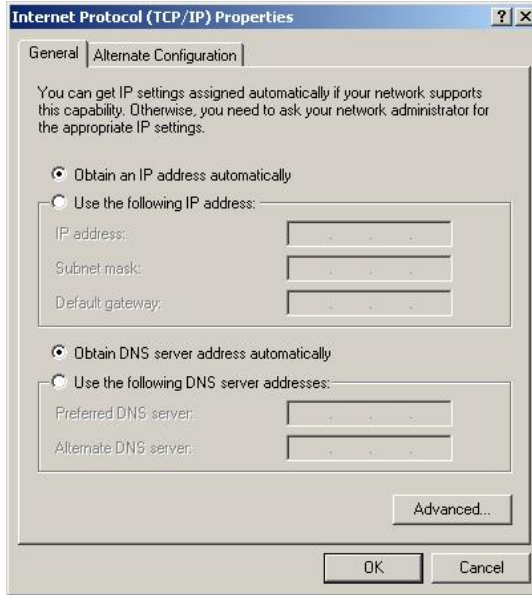
For Windows XP users, you do not need to add the TCP/IP protocol, as it is already setup when a network card is installed. Therefore only the configuration for TCP/IP is needed.

1. From the Windows 2000 **Start** menu, click **Control Panel**, followed by **Network and Internet Connections**. Then click **Network Connections**.



Appendix III TCP/IP Configuration

2. Right click on the **Wireless Network Connections** with the access point and click on **Properties**. Select the **Internet Protocol (TCP/IP)** and click **Properties**.



3. Configure your IP address and the rest of the parameters so that you can be connected to the network.
4. If your access point is configured as a DHCP server, you have to select **Obtain an IP address automatically**.
5. If your access point (AP) has a certain IP address. In order to communicate with the AP, you would have to assign an IP address with the same first 3 sets of numbers and a different set of number for the last set to differentiate your laptop and the access point in the network. The **subnet mask** would be 255.255.255.0



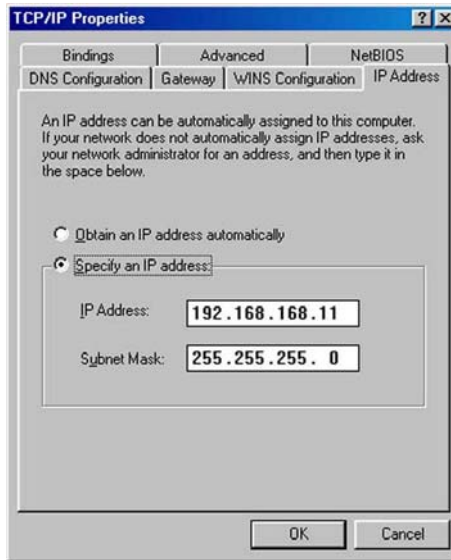
NOTE

Please check with your system administrator or Internet Service Provider for more information on the TCP/IP parameters.

Appendix III TCP/IP Configuration

AIII.3 Configure static IP Address in Windows 98SE/ME

1. Follow Step 1 to 6 in **Section AIII.1 “Configure dynamic IP Address in Windows 98SE/ME”** on Page 88.
2. Click **Properties**, and configure the settings in each of the TCP/IP Properties window.

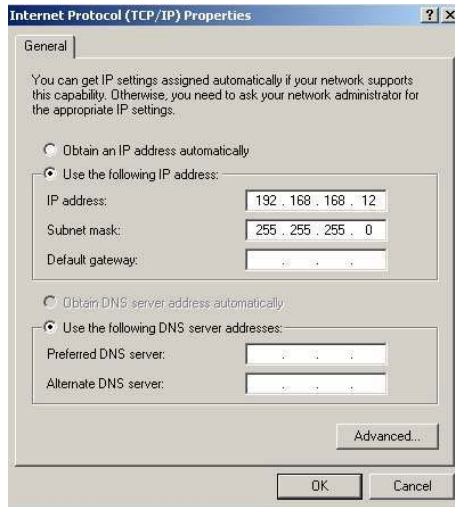


3. Click **OK** to update the changes.

Appendix III TCP/IP Configuration

AIII.4 Configure static IP Address in Windows XP/2000

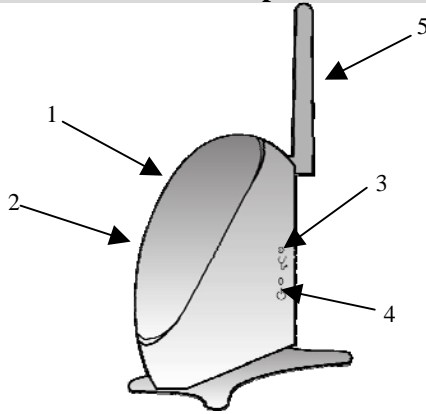
1. Follow Step 1 to 6 in **Section AIII.2 “Configure dynamic IP Address in Windows XP/2000”** on Page 91.
2. Right click on the **Wireless Network Connections** with the access point and click on **Properties**. Select the **Internet Protocol (TCP/IP)** and click **Properties**.



3. Configure your IP address and the rest of the parameters so that you can be connected to the network.
4. Click **OK** to update the changes.

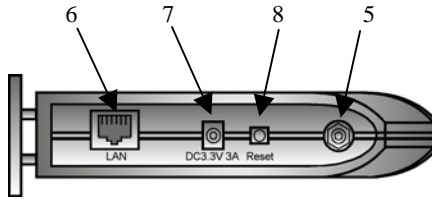
Appendix IV Panel Views and Descriptions

Appendix IV Panel Views and Descriptions



Features		Status and Indications	
1	LAN Link/Act LED	Steady Yellow	The access point is operating at the speed of 10Mbps.
		Steady Green	The access point is operating at the speed of 100Mbps.
2	WLAN Link/Act LED	Steady Green	More than 1 wireless client is present in the wireless network.
		Blinking Green	Activity is detected in the wireless network.
3	Diagnostic LED	Steady Green	The device is in access point or gateway mode.
		Blinking Green	The device is booting.
		Off	The device is in Client mode.
4	Power LED	Steady Blue	Power is supplied to the device.
		Off	No power is supplied to the device.
5	Antenna	2dbi antenna	

Appendix IV Panel Views and Descriptions



Features		Status and Indications
6	LAN RJ45 Ethernet Port	Using RJ45 Ethernet cable for connection.
7	DC 3.3V 3A	Power input of 3.3VDC
8	Reset button	Push button: <ul style="list-style-type: none">• 2s to reboot your device• between 2s to 10s to restore to its factory default• 10s for operating mode switch

Appendix V Technical Specifications

Appendix V Technical Specifications

Industrial Standards	<ul style="list-style-type: none">• IEEE 802.11b• IEEE 802.11g
Performance	<ul style="list-style-type: none">• Network speeds dynamically shift between 1,2, 5.5, 11, 12, 18, 24, 36, 48, 54 Mbps• Indoor: 20 m (54 Mbps)• Outdoor: 80 m (54 Mbps)
Frequency Range IEEE 802.11b: IEEE 802.11g:	2.4 ~ 2.4835 GHz 2.4 ~ 2.497 GHz
Wireless Operation Modes	<ul style="list-style-type: none">• Access Point Bridge• Access Point Client• Gateway• Wireless Routing Client• Wireless Ethernet Adapter• Wireless Bridge Link
Security	<ul style="list-style-type: none">• 64 - bit / 128 - bit WEP• WPA1/2-PSK / WPA1/2-EAP• Pseudo Virtual LAN• Tagged VLAN• IEEE 802.1x – TLS, TTLS, PEAP, EAP-SIM
Network Interface	1 x RJ45 10/100 Mbps auto-negotiating Ethernet port
Modulation Techniques	OFDM (BPSK, QPSK, 16-QAM, 64-QAM), DSSS (BPSK, QPSK, CCK)
Output Power IEEE 802.11b: IEEE 802.11g:	20 dBm 19 dBm
Operating Channels	<ul style="list-style-type: none">• 11 Channels: US and Canada• 13 Channels: Europe• 14 Channels: Japan
Resiliency	Parallel Broadband (in Gateway mode using WDS)

Appendix V Technical Specifications

SNMP	<ul style="list-style-type: none">• SNMP (RFC 1157)• MIB II (RFC 1213)
LED Indicators	<ul style="list-style-type: none">• Power• Diagnostic• LAN Link/Activity• WAN Link/Activity
Power Requirements	<ul style="list-style-type: none">• Input Voltage Options: 3.3VDC• Current Ratings: 3 A (max)
Antenna	Detachable 2dBi antenna with SMA connector
Management	<ul style="list-style-type: none">• Telnet Command Console• HTTP Web Management
Built-in DHCP Server	Yes
DHCP Reservation	By MAC address
Load Balancing	Parallel Broadband
Fail-Over Redundancy	Parallel Broadband
Virtual Server	IP and Port Forwarding, De-Militarised Zone
IP Packet Filtering	<ul style="list-style-type: none">• Time-based• By TCP Port• By Source IP
IP Routing	Static & Dynamic Routing
VPN Client Pass-Through	PPTP, IPsec
Configuration Interface	Web-based Configuration Menu
Profile Backup & Restore	Yes
Firmware Upgrade	Yes
Electromagnetic Emissions	<ul style="list-style-type: none">• FCC Part 15 SubClass B• CE R&TTE

Appendix V Technical Specifications

Electromagnetic Immunity	<ul style="list-style-type: none">• EN 55022 (CISPR 22)/EN 55024 Class B• EN 61000-3-2• EN61000-3-3
Safety	<ul style="list-style-type: none">• CE Mark• EN 60950
Power Requirements Input Voltage: Current Ratings:	3.3VDC 3 A (max)
Environment Requirements Operating Temp: Storage Temp: Operating Humidity:	0°C to 70°C -15°C to 70°C 5% to 95% RH Humidity (RH – Relative Humidity):
Physical Dimensions	88mm x 24mm x 88mm (H x W x D)

Manual Number:
U-0436-V1.1C
Version 1.1
November 2006

