COMPEX

networks@work

USER'S MANUAL

COMPEX NETPASSAGE SERIES

NetPassage 18A

Wireless A+G VPN Internet Router

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-0453-V1.3C   Version 1.3, October 2006

Disclaimer

Compex, Inc. provides this manual without warranty of any kind, either, 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.

i

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.

Declaration of Conformity

Compex, Inc. declares the following:

Product Name: **Dual Band Wireless A+G VPN Internet Router, NetPassage 18A**

Model No: **NetPassage 18A** conforms to the following Product Standards:

The device complies with the Electromagnetic Compatibility Directive (89/336/EEC), Low Voltage Directive (73/23/EEC) and the Amendment Directive (93/68/EEC) issued by the Commission of the European Community. Compliance with these directives implies conformity to the following European Norms (in brackets are the equivalent international standards).

EN 55022 (CISPR 22) – Electromagnetic Interference (Conduction and Radiation)

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

EN 61000-3-2 (IEC610000-3-2) – Power Line Harmonics

EN 61000-3-3 (IEC610000-3-3) – Product Safety

Therefore, this product is in conformity with the following regional standards:

FCC Class B — following the provisions of FCC Part 15 directives,

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 Centre.

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 A Brea, CA 92821, USA	
☎ Call 🖨️Fax	Tel:	+1 (714) 482-0333 (8 a.m.-5 p.m. Pacific time)
	Tel:	+1 (800) 279-8891 (Ext.122 Technical Support)
	Fax:	+1 (714) 482-0332
Europe		
✉ Write	ReadyLINK Networktechnology Gmbh Albert Einstein Straβe 34/M21 63322 Rödermark, Germany	
☎ Call 🖨️ Fax	Tel:	+49 (0) 6074 - 98017 (8 a.m.-5 p.m. local time)
	Fax:	+49 (0) 6074 - 90668
	Support Email: readylink@compex.com.sg	
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 🖨️ Fax	Tel:	(65) 6286-1805 (8 a.m.-5 p.m. local time)
	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 products described in this document, **Compex Dual Band Wireless A+G VPN Internet Router, NetPassage 18A** series are licensed products of Compex Systems Pte Ltd.

Information provided: This document contains instructions for installing, configuring and using all two versions of the Compex NetPassage 18A series. It also gives an overview of key applications and networking concepts relevant to the products.

We feature the four devices interchangeably in our illustrations since this document is applicable for all four models, unless stated otherwise.

Audience: This documentation is intended for both network administrators and end users who possess some basic knowledge of networking structures and protocols.

Assumptions: Procedures listed in the document are intended for *Microsoft Windows* users. If you are running a different operating system, you may need to refer to your operating system's documentation for relevant networking instructions.

Firmware

Please take note that this User's Manual is written based on NetPassage 18A Firmware Version 2.

Conventions

The class inclusive of all model versions in this series is often denoted as either *NetPassage 18A* or *NP18A*.

TABLE OF CONTENTS

Chapter 1: Introduction

Introducing the Router

THis is a Dual Band Wireless A+G VPN Internet Router. It does not merely operate in wired network environments, it additionally upholds simultaneous IEEE802.11a and IEEE802.11b/g connections, as is often required in hotspots and other public Internet access deployment.

Advanced Features

- New **54Mbps** 802.11a & 802.11g **5X faster** than 802.11b!

- Secure your wireless data transmissions with **WPA protocol, IEEE 802.1x authentication** and **64/128-bits WEP Encryption**!

Read on and find out more about these features!

Designed to support state-of-the-art security standards such as the Wi-Fi Protected Access (WPA) protocol, the 802.1x authentication standard and 64/128-bits Wired Equivalent Privacy (WEP) encryption, the router also sports built-in hardware encryption and embedded VPN support that can create multiple IPSec tunnels to remote locations, thus promoting increased scalability within a robust security infrastructure.

This high-performance router also bears advanced features such as Load Balancing, Fail-Over Redundancy, and exclusives: uConfig and Parallel Broadband. A full-fledged gateway with built-in DHCP server, the router further supports Virtual Servers based on IP and Port Forwarding, De-Militarized Zone hosts, Packet Filtering and much more!

- Quickly access your network device's Web administration setup with **uConfig**!

- Have you heard of **Parallel Broadband**?

If not, keep reading and discover the ultimate Internet solution is delivered!

Chapter 2: Getting to know your Router

The following will help you get more acquainted with the rich suite of features offered by the router so that you are better able to exploit your router's full potential.

Key features

Compatible with IEEE 802.11g/b and IEEE 802.11a standards

Adopting the 802.11g standard, the **router** provides you the fastest wireless access within your office or home network. Since it is fully backward compatible with 802.11b, you can safeguard your existing network investments.

Easy Management & Configuration

You can browse or **uConfig** to the web interface for effortless configuration. Additionally, you can make use of these features:

- HTTPS (SSL) is supported in addition to the standard HTTP. HTTP (SSL) features additional authentication and encryption for secure communication.

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

- SSH (Secure Shell Host) establishes a secure host connection to the CLI for control and monitoring. SSH is designed and created to provide the best security when accessing another computer remotely. Not only does it encrypt the session, it also provides better authentication facilities and features that increase the security of other protocols. It can use different forms of encryption and ciphers.

- **SNMP** feature for managing the network performance.

Virtual AP (Multiple SSID)

Virtual AP implements mSSID (Multi-SSID)

This allows a single wireless card to be set up with up to 16 virtual AP connections with different SSIDs or BSSID (Basic Service Set Identifier) and security modes.

WMM

WMM (Wireless Multimedia) improves the user experience for audio, video, and voice applications by prioritizing data traffic.

Point-to-Point & Point-to-MultiPoint Support

Point-to-Point and Point-to-MultiPoint communication between different buildings enables you to bridge wireless clients that are kilometres apart while unifying the networks.

Antenna Alignment

Antenna Alignment function finds the best alignment for the unit antenna by measuring the quality of the signal.

Security Features

You will be glad to learn about the security elements we have put in place to better protect your data and privacy.

WPA (Wi-Fi Protected Access) Standard & 802.1x Authentication

The router supports the **WPA** standard for enhanced security in your wireless network. The **WPA** protocol combines two mechanisms: *Dynamic Key Encryption* and *Mutual Authentication* for enhanced security in the wireless LAN. This combination ensures that all users are authenticated through a central authority before being allowed network access.

WPA Modes:

- WPA Personal
- WPA Enterprise
- WPA2 Personal
- WPA2 Enterprise
- WPA Auto Personal
- WPA Auto Enterprise

Detailed information on the WPA Modes can be found in Chapter 5: Setting Up A WLAN – How to Make Your WLAN More Secure

64/128-bit WEP encryption

The router supports the WEP (Wired Equivalent Privacy) protocol with key lengths of 64-bit and 128-bit to protect data communication in your wireless network.

Additional Features

These features reveal the comprehensive range of advanced functionalities when the router is further configured.

Static IP, Dynamic IP, PPPoE, PPTP, and L2TP WAN types

Whether you have subscribed to fixed IP, dynamic IP or PPPoE, you can use the router for broadband cable /ADSL Internet connection sharing.

Parallel Broadband

The unique Parallel Broadband technology features improved load balancing and fail-over Internet connectivity.

Built-in "NAT" firewall & Packet filtering

Since it handles the incoming and outgoing data packet transactions between your LAN and the external network, the router can validate individual packet information before passing it on to a LAN client. To complement NAT, you can use the packet filtering features to regulate Internet access and control the transmission of TCP, UDP, ICMP or IGMP packets to and from your LAN clients.

Virtual Servers based on Port-forwarding, IP-forwarding and DMZ's

The router lets you set up Internet application servers such as FTP file servers and HTTP web servers based on Port-forwarding, IP-forwarding and Demilitarised Zone hosts.

When to use which router

- **NetPassage 18A IB11US**, **1A13EU**, **IB11US**, and **1B13EU** are dualband wireless A+G VPN Internet router offering simultaneous support of IEEE 802.11a and IEEE 802.11g/b wireless LAN connections.
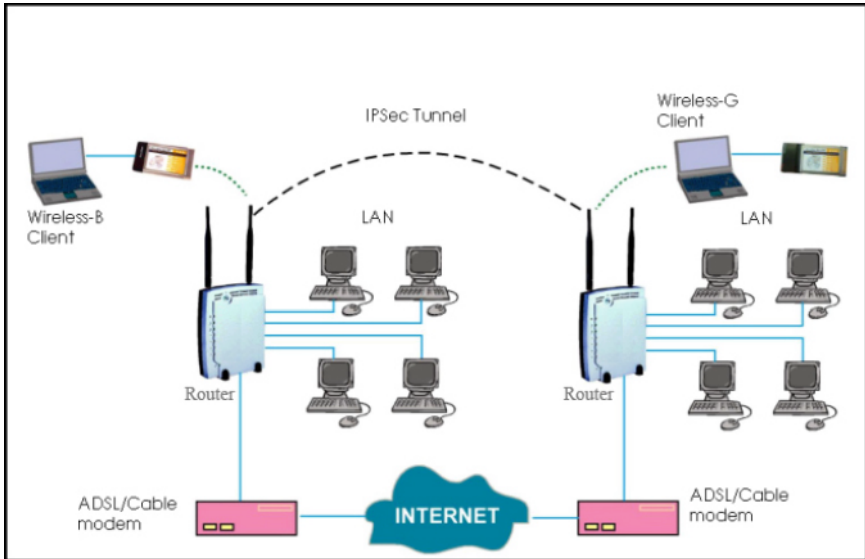
- **NetPassage 18A 1A00US**, **1A00EU**, **18A 1B00US**, and **1B00EU** are VPN Internet routers used only in wired environments.
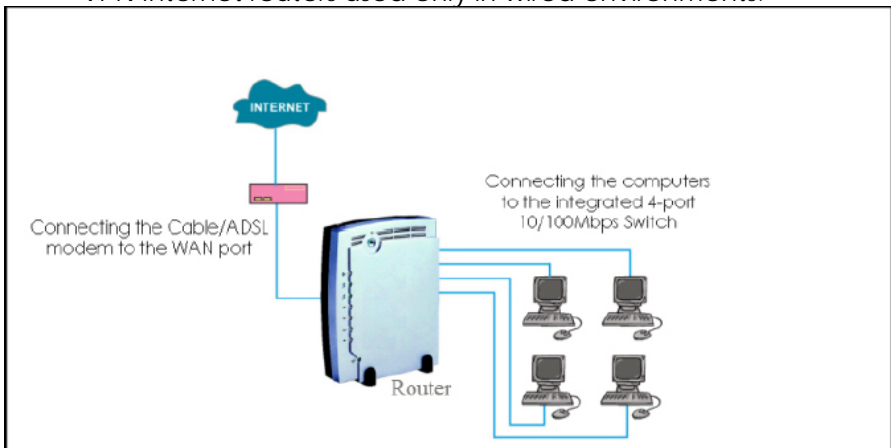
Panel Views

The router has been designed such that it can either be placed on a desktop or mounted onto a wall.

LED indicators denoting network status and activity, are situated on the front edge of the router for easy visibility. Moreover, two plastic feet support the router in a standing arrangement, thus minimising desktop clutter and ensuring better organization when setting up the hardware.

NOTICE: Actual product appearance may slightly differ depending on the hardware version.

Rest feet attached to the bottom of the router
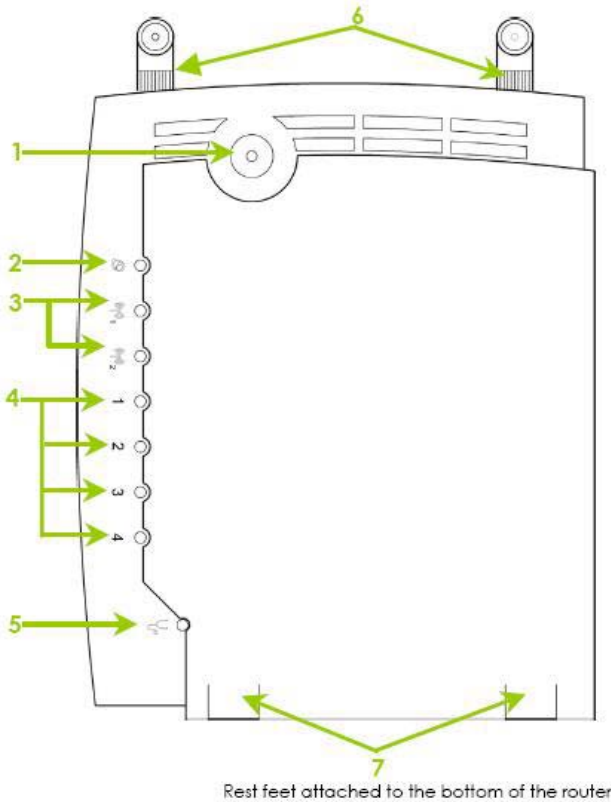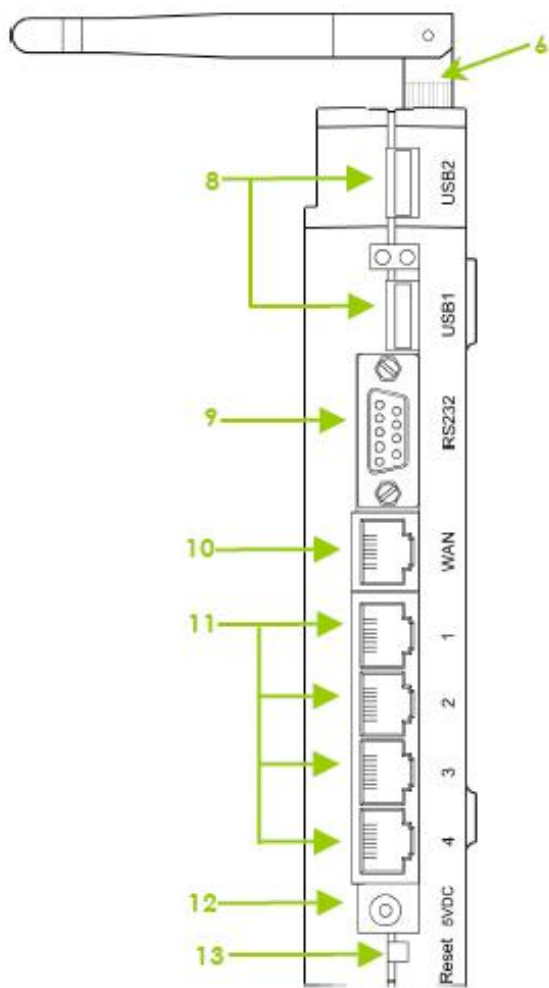
Panel Description

	Name	Description	
1	**Power** (LED)	Steady Green	The device is powered up.
		Off	No power is supplied to the device.
2	**WAN** (Link/Activity LED)	Steady Green	The WAN connection is ON.
		Flashing Green	Data transmission at WAN connection.
3	**WLAN (1), (2)** (Link/Activity LED)	Steady Green	Wireless interface up and running. Ready for operation.
		Flashing Green	Activity is detected in the wireless network.
4	**1, 2, 3, 4** (Link/Activity/Speed LEDs)	These LEDs reflect the status of the integrated Fast Ethernet Switch. They will light up when connected with an Ethernet cable.	
		Steady Green	There is a connectivity link of 100Mbps.
		Flashing Green	100Mbps data transmission is detected at the port concerned.
		Steady Amber	There is a connectivity link of 10Mbps.
		Flashing Amber	10Mbps data transmission is detected at the port concerned.
5	DIAG (LED)	This LED is reserved for diagnostic purposes.	

6	External Antennas	SMA antennas
7	Rest Feet	These rest feet hold the router in the standing position.
8	**USB1, USB2** USB Ports (NP18A 1A, NP18A 2A)	These ports support printers, webcams, or hard drives.
9	R232 (Integrated Serial Interface)	Not in use. Reserved for future update.
10	**WAN** (Ethernet Port)	10/100Base-T Port connects to Cable/ADSL modem.
11	**1, 2, 3, 4** (Ethernet Ports)	Integrated 3-port 10/100Mbps Switching. Ports 1, 2, 3, and 4 all function as normal Ethernet ports except that Port 4 supports PoE connection. Connect Port 4 to PoE Injector if you wish to use it to supply power to the unit.
12	**DC Jack**	Direct Current jack. If using power adapter to supply power to the unit, attach the power adapter to the main electrical supply and connect the power plug into the **DC Jack** of the router.

13	**Reset** (Push Button)	The table below illustrates the use of the **Reset** button.

Reset Push Button	Diagnostic LED	Router Behavior
Less than 3 sec	On	Reboots.
5 sec	Fast Blinking	Restores the default login password, which is 'password'.
Between 8 sec and 10 sec	Slow Blinking	Restores all the default factory settings including password.
More than 10 sec	Off	Reset cancelled.

NOTE:

Although the Ethernet ports are numbered 1 to 4, they <u>DO NOT</u> have to be connected sequentially.

For example: in a network of two computers, you can choose to connect one computer to Port 2 and another to Port 4.

Chapter 3: Hardware Setup

Step 1

Before attaching a pair of external antennas to the router, take note of the 'A' marking on one of the two antennas.

The antenna with the 'A' marking is the Dualband AG Antenna.
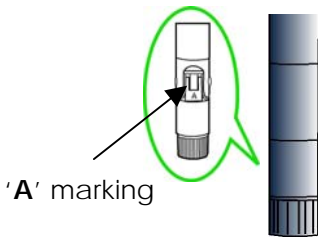
'A' marking

The antenna without the marking is the single-band G Antenna.

Connect the single-band G antenna to Ant-2 on the RIGHT.

Connect the Dualband AG antenna to Ant-1 on the LEFT.

Important: To ensure proper functionality of the router, these two antennas MUST NOT be swapped.

Step 2

Insert one end of the RJ45 Ethernet cable to any of the LAN ports (1, 2, 3, or 4) on the router and the other end to your PC's Ethernet network adapter.
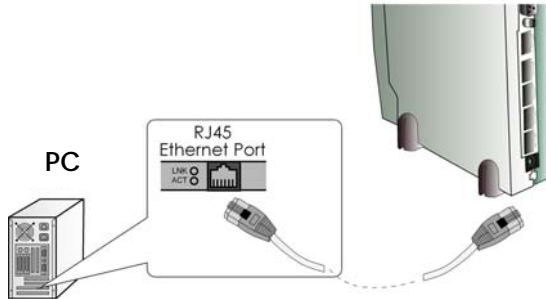
Step 3

Attach the power adapter to the main electrical supply and connect the power plug into the socket of the router.
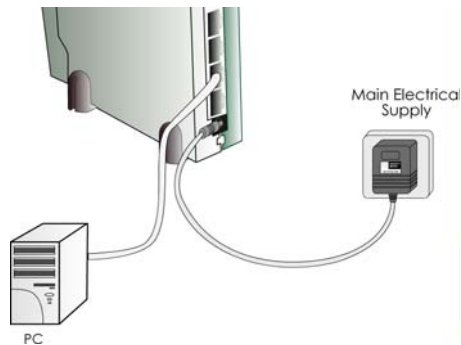
Step 4

Power on your PC.
Notice that the **Power** and the corresponding port LEDs have lighted up.
This indicates that connection has been established successfully between the router and your PC.

Chapter 4: Accessing the Web interface

This chapter consists of the following:

- ❑ Overview of alternatives to access the web interface
- ❑ How to uConfig to the web interface
- ❑ How to browse to the web interface

Overview of alternatives

The router can be configured with the web interface.

After connecting the router to your PC, there are two methods of accessing its web interface:

- ▪ Installing and running the **uConfig** utility.
- ▪ Changing your web browser settings.

How to uConfig to the Web Interface *exclusive!*

The **uConfig** utility has been developed to allow access to the web interface of your product without having to change the TCP/IP settings of your PC.

Installing uConfig

1

Insert the Product CD into the CD-ROM drive.
It will automatically run and display the web page.

2

1. Click on **Utilities**.

2. Select to install the **uConfig** utility on your hard disk.

3. After installation, double-click on the **uConfig** icon to run the program.

After installation, your PC will automatically detect connected products.

Double-click on the **uConfig** utility icon to run the program.

Running uConfig

1

1. Ensure that the router is selected under the **Products List.**

2. Click on **Open Web.**

   This opens the router's login screen.
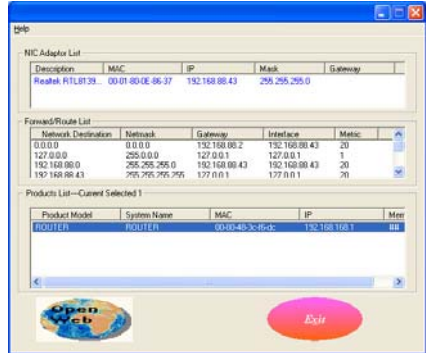
2

This screen prompts you not to exit uConfig while accessing the web interface or else connection to the device will fail.
Click on the **OK** button to proceed.

Warning

The selected product is on different subnet, uConfig will change the system settings to enable access to the product's Web Interface.

Do not close uConfig while accessing the product's Web Interface, doing so will break the connection.

After finishing the product configuration, press the <ExitUconfig> link on the product's Web Interface, uConfig will then close automatically.

OK

3

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

Note: The default password is "password"

Management

Please enter your password:

•••••••   Log On !

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

How to Browse to the Web Interface

Browsing to the web interface

Open your Command prompt window and type in: **ping 192.168.168.1** to verify that your PC can communicate with the router.
If your TCP/IP settings are correct, you will get replies to this ping command.
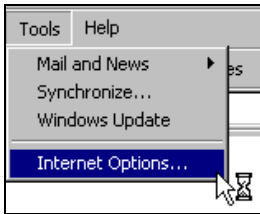
1. Launch your web browser.
2. Under the **Tools** tab, select **Internet Options**.
3. Open the **Connections** tab.
4. In the **LAN Settings** section, disable all the option boxes.

1. At the address bar, type: **http://192.168.168.1**

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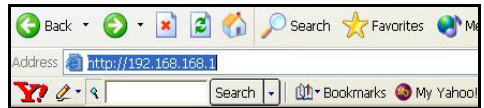
Note: The default password is "password"

You will then reach the home page of the router's web interface.

Chapter 5: Setting Up a WLAN

This chapter applies exclusively to **Wireless Setup (a/b/g)** and **Wireless Setup (b/g)**.

Wireless Setup (a/b/g) supports IEEE 802.11a and IEEE 802.11g/b wireless LAN connections simultaneously.

Wireless Setup (b/g) supports IEEE 802.11b and IEEE 802.11g wireless LAN connections simultaneously.

Whether you're a home user or a network administrator, a WLAN implementation will allow your roaming users to enjoy network resources anywhere, anytime. It also provides convenience, and cost savings, since deploying WLANs is less costly than setting up cables.

The next sections involve the following:
- WLAN Setup
- Wireless Security Settings
- Advanced Settings

The steps featured are common to both **Wireless Setup (a/b/g)** and **Wireless Setup (b/g),** unless otherwise stated.

Operation Modes

Access Point Mode

This is the default mode of your access point. The **Access Point** mode enables you to bridge wireless clients to access the wired network infrastructure and to communicate with each other.
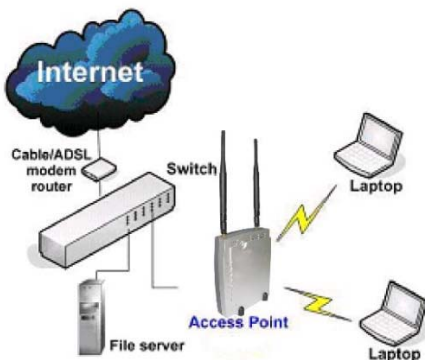
In the example above, the wireless users will be able to access the file server connected to the switch through the access point in **Access Point** mode.

Client Mode

In **Client** mode, the device acts as a wireless **Client**.
When connected to an access point, it will create a network link
between the Ethernet network connected at this **Client** device, and
the wireless and Ethernet network connected at the access point.

In this mode it can only connect with an access point. Other wireless
clients cannot connect with it directly unless connected to the same
access point - allowing them to communicate with all devices
connected at the Ethernet port.
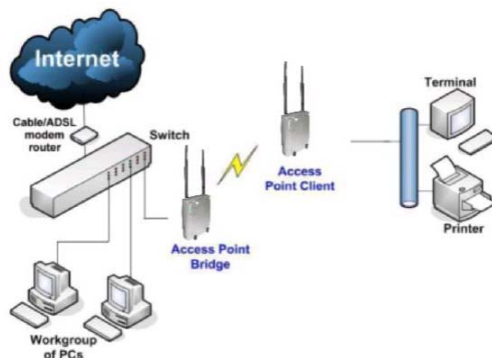
In the example above, the workgroup PCs will be able to access the
printer connected to the access point in **Access Point Client** mode.

Transparent Client Mode

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

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

This mode is generally used for outdoor connections over long distances, or for indoor connections between local networks.
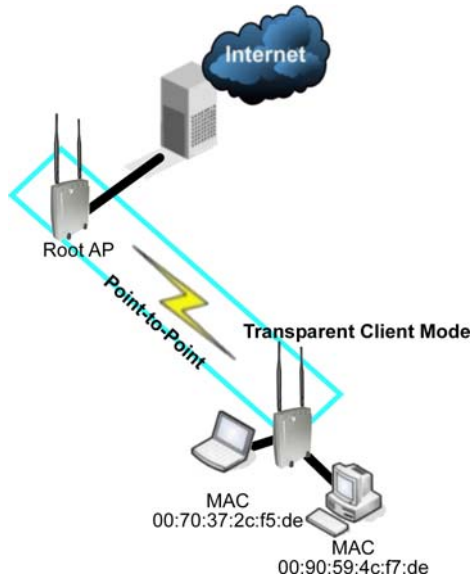
Difference Between other client modes and Transparent Client Mode	
Other client modes	Transparent Client Mode
Connectivity with any standard APs.	Connectivity with RootAP-supported APs.
All devices connected to the Ethernet ports use a common MAC address for communications with the AP.	Devices connected to the Ethernet ports flow through freely and transparently without the MAC address restriction.

Transparent Client Mode is more transparent, making it more suitable for linking two networks as point-to-point, or point-to-multi-point network connection.
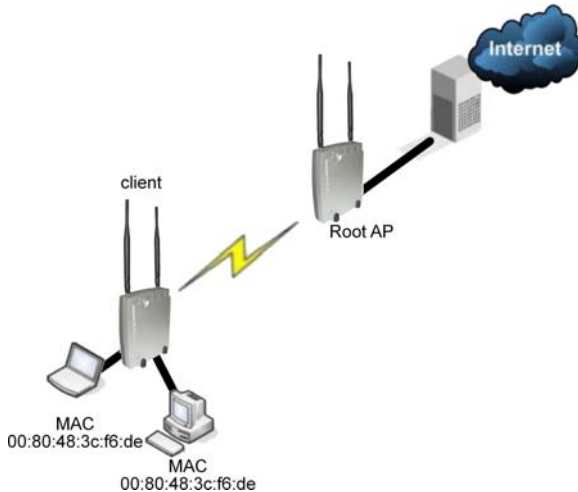
To Set Up a Wireless LAN

Follow these steps to setup your wireless LAN for IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g.

WLAN Setup (a/b/g)

1

Click on **WLAN Setup(a/b/g)** from the **CONFIGURATION** menu.

2

Select **Basic** to make changes.

If you disable the card, you will not be able to use the features of this wireless card.

If you wish to disable the card, click on the **Click to Disable This Wireless Card** button.

Click **Reboot** in **Reboot System** page.

Rebooting page displays and machine reboots.

The **Wireless Card Disabled** screen indicates that the wireless card has been disabled.

3 The router supports wireless LAN connectivity that is fully compliant with the IEEE 802.11g, IEEE 802.11a, and IEEE 802.11b standards.

It also employs different security modes to secure the data transmission of the wireless clients within your network.

The **Current Mode** is defaulted to **Access Point**.
To change the mode, click on the **Change** button.

WLAN Basic Setup

The Current Mode	Access Point	Change
ESSID	sample	
Wireless Profile	802.11a	
Country	NO_COUNTRY_SET-(NA)	
Channel	SmartSelect	Channel Survey
Tx Rate	Fully Auto	
Maximum Associations	32 (32:1-128)	

☐ Closed System
☐ Act as RootAP
☐ VLANID

Apply

4 To change the wireless mode, make a selection from the drop-down box.

WLAN Basic Setup

The Current Mode	Access Point	Change
ESSID	sample	
Wireless Profile	802.11a	
Country	802.11a	T-(NA)
	802.11b only	
Channel	802.11b/g mixed	Channel Survey
	802.11g only	
Tx Rate	Fully Auto	
Maximum Associations	32 (32:1-128)	

☐ Closed System
☐ Act as RootAP
☐ VLANID

Apply

Operation Mode : The router supports three types of modes such as Access Point, Client, and Transparent Client.

WLAN name (ESSID) : Enter a preferred name for the wireless network.
Your wireless clients must be configured with the same ESSID (sometimes referred to as SSID).

Wireless mode	:	Select from the list of wireless modes available:
		802.11a (not supported by WLAN Setup for b/g) This mode supports wireless A clients with data rates of up to 54Mbps in the frequency range of 5.4GHz.
		802.11b only This mode supports wireless B clients with data rates of up to 11Mbps in the frequency range of 2.4Hz.
		802.11g only This mode supports wireless G clients with data rates of up to 54Mbps in the frequency range of 2.4Hz.
		802.11b/g mixed This mode supports both wireless B and G clients. The basic rates are: 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, and 54Mbps.
Country Code	:	Choose the Country where you are located.
Channel	:	This option allows you to select a frequency channel for wireless communication.
		Select SmartSelect to automatically scan and recommend the best channel that can be utilised.
Tx Rate	:	Allow you to choose the rate of data transmission from 1Mbps to Fully Auto.
Maximum Associations	:	Allow you to limit the number of WLAN associations that can be made from 1 to 128. Default: 32
Closed system	:	The router will suppress and not broadcast its **WLAN name (SSID)** when **Closed system** is enabled. **Closed system** is disabled by default.
Act as RootAP	:	The router will connect with one or multiple Transparent Clients to create a point-to-point and point-to multi-point connections network with 2 or more APs. This connection method is fully compliant with 802.1h standards.
VLANID	:	Select and specify the VLANID. This is a number to identify the different virtual network segments to which the network devices are grouped. This can be any number from 1 to 4094.

Point-to-Point & Point-to-MultiPoint Setup

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

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

Follow these steps to setup RootAP

RootAP Step 1:

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

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

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

WLAN Basic Setup

Card Status	enable
The Current Mode	Access Point [Change]
ESSID	sampleRouter
Wireless Profile	802.11a
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect [Channel Survey]
Tx Rate	Fully Auto
	☐ Closed System
	☐ Act as RootAP
	☐ VLANID

[Apply]

RootAP Step 2:

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

WLAN Basic Setup

Card Status	enable
The Current Mode	Access Point [Change]
ESSID	sampleRouter
Wireless Profile	802.11a
Country	NO_COUNTRY_SET-(NA)
Channel	SmartSelect [Channel Survey]
Tx Rate	Fully Auto
	☐ Closed System
	☑ Act as RootAP
	☐ VLANID

[Apply]

Follow these steps to setup Transparent Client/s.

Transparent Client Step 1:

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

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

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

WLAN Basic Setup

Card Status	enable
The Current Mode	Transparent Client [Change]
ESSID	sampleRouter [Site Survey]
Remote AP MAC	☐
Wireless Profile	802.11a
Country	NO_COUNTRY_SET-(NA)
Tx Rate	Fully Auto

[Apply]

Transparent Client Step 2:

Select the **Remote AP MAC** checkbox.

Enter the **Remote AP MAC**.

WLAN Basic Setup

Card Status	enable
The Current Mode	Transparent Client [Change]
ESSID	sampleRouter [Site Survey]
Remote AP MAC	09-00-2B-23-00-00 ☑
Wireless Profile	802.11a
Country	NO_COUNTRY_SET-(NA)
Tx Rate	Fully Auto

[Apply]

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

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

How to Make Your WLAN More Secure

All your network clients <u>MUST</u> share the same wireless settings as your router to be able to communicate.

The router offers 8 types of security modes:

- **WEP**
Short for Wired Equivalent Privacy, WEP is a security protocol basing on a secret key to encrypt data packets before they are transmitted.
You <u>MUST</u> remember to apply the same WEP settings and key to the router as well as to all your wireless clients.

- **802.1x**
This mode conforms to the IEEE 802.1x authentication standard that ensures that a client is not given access to network resources unless it has been successfully authenticated.
There <u>MUST</u> be a RADIUS server on your LAN for this security mode to function.

- **WPA Personal**
WPA, or Wi-Fi Protected Access, is a protocol for authorising and authenticating users onto the wireless network and implements the majority of the IEEE 802.11i standard.
WPA Personal mode implements a shared network password for clients and access points.
The only interaction is between the router and the client, therefore, a RADIUS server is <u>NOT</u> required.

- **WPA Enterprise**
WPA Enterprise mode implements the 802.1X authentication.
There <u>MUST </u>be a RADIUS server on your LAN for this security mode to function.

- **WPA2 Personal**

WPA2 Personal mode implements the full IEEE 802.11i standard with a shared network password for clients and access points.

The only interaction is between the router and the client, therefore, a RADIUS server is <u>NOT</u> required.

- **WPA2 Enterprise**

WPA2 Enterprise mode implements the full IEEE 802.11i standard and 802.1X authentication.

There <u>MUST </u>be a RADIUS server on your LAN for this security mode to function.

- **WPA Auto Personal**

WPA Auto Personal mode implements a shared network password for clients and access points and if there are no WPA enabled access points available with the given SSID in WPA Personal mode, the unit will attempt to associate with a non-WPA point with the given SSID, if available.

The only interaction is between the router and the client, therefore, a RADIUS server is <u>NOT</u> required.

- **WPA Auto Enterprise**

WPA Auto Enterprise implements 802.1X authentication and if there are no WPA enabled access points available with the given SSID in WPA Enterprise mode, the unit will attempt to associate with a non-WPA point with the given SSID, if available.

There <u>MUST </u>be a RADIUS server on your LAN for this security mode to function.

The subsequent sections illustrate how to configure each security mode.

Begin with following the two common preliminary steps shown below to select the most appropriate security mode to protect your wireless communications.

Selecting a security mode

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

WLAN Security Setup

Security Mode
NONE
NONE
WEP
WPA-Personal
IEEE802.1X
WPA-Enterprise
WPA2-Personal
WPA2-Enterprise
WPA-Auto-Personal
WPA-Auto-Enterprise
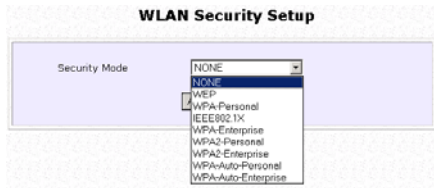
2 1. Make a selection from the **Security Mode** drop down menu.

The **Security Mode** is disabled by default.

2. Click on **Apply**.

How to Setup WEP

WEP

1. You can define up to 4 WEP keys.

   For each key, you can specify:
   - The **Key Entry Method**, by selecting either:
     - Hexadecimal
     - ASCII text
   - The encryption level, from the dropdown list:
     - 64-bit
     - 128-bit

   Click **Edit** to set the keys, and then click **Apply**.
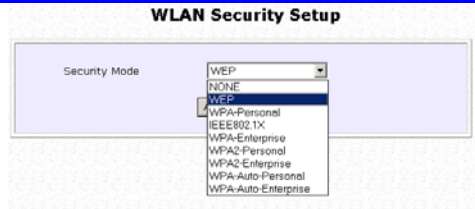
WEP Key Setup

Key String Type:
- ⦿ Hex (0~9, a~f, A~F) Length 10 or 26
- ◯ ASCII (0~9, a~z, A~Z) Length 5 or 13

Key 1: ⦿ 64Bit ◯ 128Bit
[   ] [Reset]
Key 2: ⦿ 64Bit ◯ 128Bit
[   ] [Reset]
Key 3: ⦿ 64Bit ◯ 128Bit
[   ] [Reset]
Key 4: ⦿ 64Bit ◯ 128Bit
[   ] [Reset]

[Apply] [back]

2   For hexadecimal key entry:

1.   Select the **Hex** radio button.

2.   Select the radio button of the key to be entered.

3.   Select the key encryption mode from the drop down menu.

4.   Fill in the key value.

A hexadecimal value is made of digits **0-9** and letters **A-F**, and is NOT case-sensitive.

For **64**-bit encryption:
Your WEP key has to be **10** hex digits long.

For **128**-bit encryption:
Your WEP key has to be **26** hex digits long.

5.   Click on **Apply**.

6.   If the key format is valid, the page will refresh and the key will appear in encrypted form.

3 For **ASCII** key entry:

1. Select the **ASCII** radio button.

2. Select the radio button of the key to be entered.

3. Select the key encryption mode from the drop down menu.

4. Fill in the key value.

An **ASCII** value can take in any alphanumeric character and is NOT case-sensitive.

For **64**-bit encryption:
Your WEP key has to be **5** characters long.
For **128**-bit encryption:
Your WEP key has to be **13** characters long.

5. Click on **Save**.

6. If the key format is valid, the page will refresh and the key will appear in encrypted form.

WEP Key Setup

Key String Type:
○ Hex (0~9, a~f, A~F) Length 10 or 26
◉ ASCII (0~9, a~z, A~Z) Length 5 or 13

Key 1: ◉ 64Bit ○ 128Bit
[____] Reset
Key 2: ◉ 64Bit ○ 128Bit
[____] Reset
Key 3: ◉ 64Bit ○ 128Bit
[____] Reset
Key 4: ◉ 64Bit ○ 128Bit
[____] Reset

Apply back

WEP Key Setup

Key String Type:
○ Hex (0~9, a~f, A~F) Length 10 or 26
◉ ASCII (0~9, a~z, A~Z) Length 5 or 13

Key 1: ◉ 64Bit ○ 128Bit
[******] Reset
Key 2: ◉ 64Bit ○ 128Bit
[******] Reset
Key 3: ◉ 64Bit ○ 128Bit
[******] Reset
Key 4: ◉ 64Bit ○ 128Bit
[******] Reset

Apply back

4 To add more hexadecimal WEP keys, repeat step 2.
To add more ASCII WEP keys, repeat step 2.

You can set a maximum of 4 WEP keys using different key entry methods and encryption levels.

To specify which key to use:

1. Select the radio button of the key to be used.

2. Click on **Apply**, then on **Reboot** to apply the changes.

How to Setup 802.1x

802.1x

1 1. Key in the IP address of the **Primary RADIUS Server** in your WLAN.
Optional: You may also key in a Secondary RADIUS Server, if any.

Note: The RADIUS server <u>MUST</u> be in the same subnet as your router.

2. The **Authentication Port** is preset as **1812,** but another port number can be used.

Note: The Authentication Port <u>MUST</u> match the corresponding port of the RADIUS server.

3. Enter the **Shared Secret Key**, known only to you and the RADIUS server.

4. The **Accounting Port** is preset as **1813**, but another port number can be used.

5. You can opt for a **Key Length** of either **64 bits** (10 hex / 5 ASCII values) or **128 bits** (26 hex / 13 ASCII values).

6. Click on **Apply**.

7. Click on **Reboot** to restart the system, after which the settings will be effective.

WLAN Security Setup

Security Mode   IEEE802.1X
NONE
WEP
WPA-Personal
IEEE802.1X
WPA-Enterprise
WPA2-Personal
WPA2-Enterprise
WPA-Auto-Personal
WPA-Auto-Enterprise

IEEE 802.1X Setup

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

Apply

How to Setup WPA Enterprise Modes

Follow these steps to setup the router to use WPA Enterprise, WPA2 Enterprise, and WPA Auto Enterprise.

WPA Enterprise

1

1. Select the **Cipher Type** to implement:
   - **TKIP**
   - **AES**
   - **AUTO**

   The **Cipher Type** is set to **AUTO by default** so that the router can automatically detect which cipher type can be supported by the client.
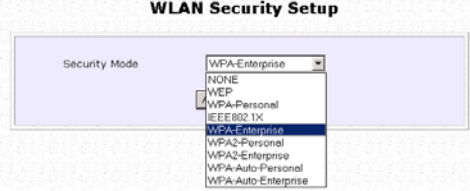
2. Key in the IP address of the **RADIUS Server** in your WLAN.

   Note: The RADIUS server <u>MUST</u> be in the same subnet as your router.

3. The **Authentication Port** is preset as **1812,** but another port number can be used.

   Note: The Authentication Port <u>MUST</u> match the corresponding port of the RADIUS server.

4. Enter the **Shared Secret Key**, known only to you and the RADIUS server.

5. The **Accounting Port** is preset as **1813**, but another port number can be used.

WLAN Security Setup

Security Mode: WPA-Enterprise
- NONE
- WEP
- WPA-Personal
- IEEE802.1X
- WPA-Enterprise
- WPA2-Personal
- WPA2-Enterprise
- WPA-Auto-Personal
- WPA-Auto-Enterprise

WPA1/2-EAP Setup

Primary RADIUS Server IP: 192.168.168.85
Secondary RADIUS Server IP: 0.0.0.0
Authentication Port: 1812
Accounting Port: 1813
Shared Secret Key: •••••••
Cipher Type: TKIP
GTK update(seconds): 600 (60~9999)

[Apply]

6. Click **Apply**.

7. Click on **Reboot** to restart the system, after which your settings will become effective.
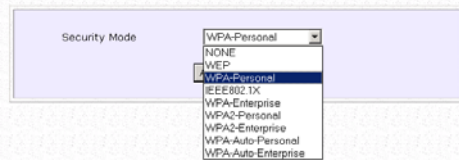
How to Setup WPA Personal

Follow these steps to setup the router for using WPA Personal, WPA2 Personal, and WPA Auto Personal.

WPA Personal

1

1. Fill in the **Passphrase** or pre-shared network key.

2. Select the **Cipher Type** to implement:
   a. **TKIP**
   b. **AES**
   c. **AUTO**.

   The **Cipher Type** is set to **AUTO by default** so that the router can automatically detect which cipher type can be supported by the client.

WLAN Security Setup

Security Mode   WPA-Personal

NONE
WEP
WPA-Personal
IEEE802.1X
WPA-Enterprise
WPA2-Personal
WPA2-Enterprise
WPA-Auto-Personal
WPA-Auto-Enterprise

WPA1/2-PSK Setup

Key String Type:
○ Hexadecimal(64 hex digits)
⊙ Passphrase(8~63 ascii characters)
WPA-PSK: 11111111
Cipher Type: TKIP
GTK Update(seconds): 600   (60~9999)

Apply

2

1. Click **Apply**.

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

Advanced WLAN Settings

Follow these steps to change the radio settings of your router.

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

2. Select **Advanced**.

WLAN Advanced Setup

2

Beacon Interval	200 (200:200-1000)
Data Beacon Rate (DTIM)	1 (1:1-16384)
RTS/CTS Threshold	2312 (2312:1-2312)
Frag Threshold	2346 (2346:256-2346)
Transmit Power	Maximum
Station Isolation	☐
Antenna Control	MAIN
DFS	⦿ Enable ○ Disable

Apply

1. Set the **Beacon Interval** (the time lapse between every beacon sent) to any value between 200 and 1000.
    It is preset as 200 seconds.

2. Set the **Data Beacon Rate** from 1 to 16384.
    This determines how often the beacon should contain a **Delivery Traffic Indication Message** (**DTIM**) that tells power-save clients that a packet is waiting for them.

3. Set the **RTS/CTS Threshold** from 256 to 2346.
    It is preset to 2346.

4. Set the **Frag Threshold** from 256 to 2346.
    It is preset to 2346.

5. Transmission Power Control (TPC) offers the flexibility to set the **Transmit Power**. (802.11h compliant)
    It is set to **Maximum** by default, but should be reduced if there is more than one unit using the same channel frequency.
    It can be set from Minimum to Maximum, 1dBm to 20dBm, in increments or 1dBm per step.

6. Select whether to enable **Station Isolation**.
This security feature implements isolation, in order to prevent network clients from attacking other network clients.

7. The **Antenna Control** function allow you to control whether to use the:
   - MAIN antenna (Default)
   - AUX (Auxiliary) antenna
       OR
   - Diversity, to monitor the signal from each antenna and automatically switch to the one with the better signal.

   For **Antenna Control** recommended settings, please refer to the next section.

8. **Dynamic Frequency Selection** (DFS) support provides flexible selection of the best frequency channel for the wireless communication to allow mobility among networks.
It reduces interference by detecting and avoiding other frequencies in use.
(DFS is a component of, and compliant with 802.11h specifications.)

   DFS is enabled by default.
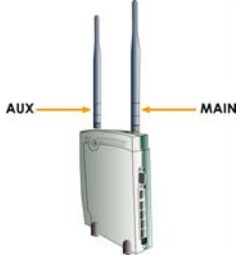
3

1. Click **Apply.**

Changes will be enabled after reboot.

Antenna Control

These are the recommended antenna control settings.

Antenna Control
If both antennas are connected: set antenna control to **Diversity**
  If antenna is connected to main: set antenna control to **MAIN**
If antenna is connected to auxiliary: set antenna control to **AUX**

Long Distance Parameters

It is necessary to adjust the long distance parameters, only if the distance is 100 meters and beyond.

Follow these steps to change the long distance parameters of your router.

Editing Long Distance Parameters

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

WLAN Advanced Setup

Beacon Interval	200	(200:200-1000)
Data Beacon Rate (DTIM)	1	(1:1-16384)
RTS/CTS Threshold	2312	(2312:1-2312)
Frag Threshold	2346	(2346:256-2346)
Transmit Power	Maximum	
Station Isolation	☐	
Antenna Control	MAIN	
DFS	⊙ Enable ○ Disable	

Apply

Extended Features

Long Distance Parameters   WMM Settings

2
1. Click **Long Distance Parameters.**

3

1. Select whether to Enable or Disable Outdoor operation.
2. Enter Distance of the unit in meters.
3. Enter the SlotTime.
4. Enter the acknowledgement timeout.
5. Enter the CTS timeout.
6. Click Apply.

To view recommended long distance parameters:
Click Show Reference Data button.

Long Distance Parameters

OutDoor	Disable ▾	
Distance(meter)	100	Show Reference Data
SlotTime(us)	9	
ACKTimeOut(us)	10	
CTSTimeOut(us)	18	

Note: Enter the distance of the client from the AP, a set for recommended parameters for SlotTime, AKCTimeOut and CTSTimeOut will be computed. You can use the recommended parameters or make your own fine tunings. Changes made will only take effect after rebooting.

Apply

This dialog box displays if the Distance entered is less than 100 meters.

Microsoft Internet Explorer

⚠ Only the distance is beyond 100 meters, it is neccessary to adjust the following parameters

OK

WMM
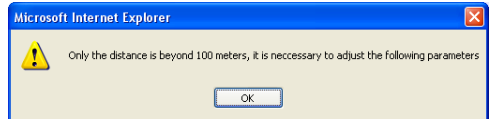
Wireless Multimedia (WMM) is a feature specially developed to improve the user's experience for audio, video, and voice applications by prioritizing data traffic.
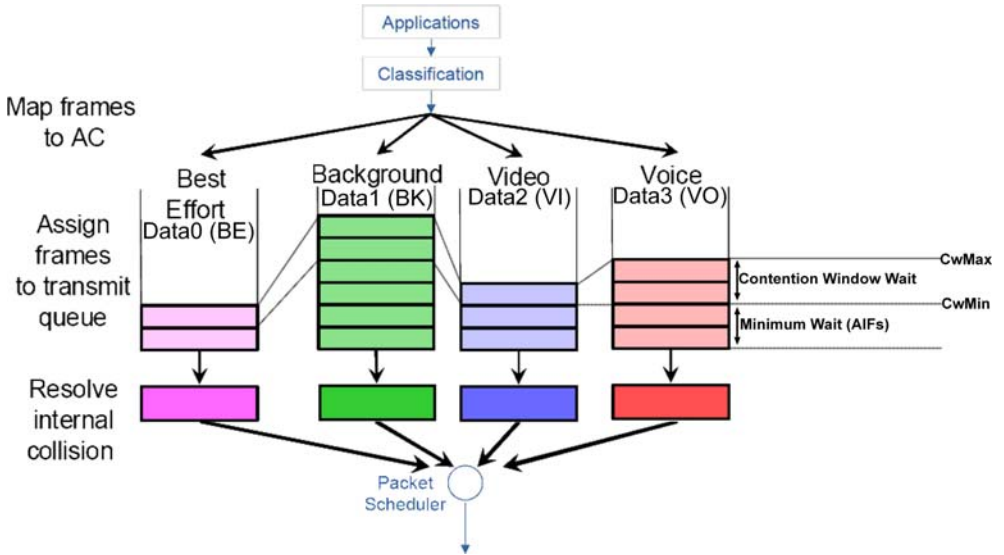
Follow these steps to change the setup Wireless Multimedia on your access point.

Setting WMM

1

3. Click on **WLAN Setup (a/b/g)** from the **CONFIGURATION** menu.

4. Select **Advanced**.

Extended Features

[Long Distance Parameters]   [WMM Settings]

2 Click **WMM Settings**.

Wireless Multimedia (WMM)   ⊙ Enable   ○ Disable

AP WMM Parameters:

	AIFs	cwMin	cwMax	TxOp limit	NoAck
Data0 (BE)	3	15	63	0	☐
Data1 (BK)	7	15	1023	0	☐
Data2 (VI)	1	7	15	3008	☐
Data3 (VO)	1	3	7	1504	☐

Station WMM Parameters:

	AIFs	cwMin	cwMax	TxOp limit	ACM
Data0 (BE)	3	15	1023	0	☐
Data1 (BK)	7	15	1023	0	☐
Data2 (VI)	2	7	15	3008	☐
Data3 (VO)	2	3	7	1504	☐

[Apply] [Default] [Back]

(All changes will take effect after reboot)

3

1. Select to Enable **Wireless Multimedia (WMM)**

2. Enter the desired WMM parameters. Using the default parameters is recommended.

3. Click **Apply** to apply the WMM settings, click **Default** to reset all parameters to default, or click **Back** to discard any changes and return to WLAN Basic Setup page.

WMM Parameters (for advanced users)	
AIFs (Arbitrary Inter-Frame Space)	Arbitrary Inter-Frame Space is the fixed wait time for different data traffic to access the network.
Cwmin (Contention Window Minimum)	Contention Window Minimum is the minimum random wait time for different data traffic to access the network.
CwMax (Contention Window Maximum)	Contention Window Maximum is the maximum random wait time for different data traffic to access the network.
TxOp limit (Transmit Opportunity Limit)	Transmit Opportunity limit specifies the duration that an end-user device can transmit data traffic. TxOp limit can be used to give data traffic longer and shorter access.
NoAck (No Acknowledgement)	No Acknowledgement provides control of the reliability of traffic flow. Usually an acknowledge packet is returned for every packet received, increasing traffic load and decreasing performance. Enabling No Acknowledgement cancels the acknowledgement. This is useful for data traffic where speed of transmission is important.
ACM (Admission Control Mandatory)	Admission Control Mandatory enables WMM on the radio interface. When ACM is enabled, associated clients must complete the WMM admission control procedure before access.
BE (Best Effort)	Parameters for Data0 Best Effort. Best Effort data traffic has no prioritization and applications equally share available bandwidth.
BK (Background)	Parameters for Data1 Background. Background data traffic is de-prioritized and is mostly for backup applications, or background transfers like backup applications or background transfers like bulk copies that do not impact ongoing traffic like Internet downloads.
VI (Video)	Parameters for video data traffic.
VO (Voice)	Parameters for voice data traffic.

Statistics

Follow these steps to view the WLAN detailed connections statistics per WLAN station.

Statistics

1

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

2. Select **Statistics**.

WLAN Connection List

ID	MAC Address	RSSI	TxRate
AP	00:80:48:3c:f6:de		
AP	00:80:48:6c:f3:de		

Refresh   Back

2
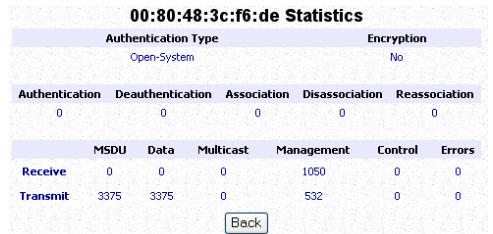
1. Select the WLAN connection to view statistics of.

- Click Refresh to refresh the WLAN Connection List.
- Click Back to return to the WLAN Basic Setup page.

3

The WLAN connection's statistics displays.

Click Back to return to WLAN Basic Setup page.

00:80:48:3c:f6:de Statistics

Authentication Type		Encryption	
Open-System		No	

Authentication	Deauthentication	Association	Disassociation	Reassociation
0	0	0	0	0

	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	1050	0	0
Transmit	3375	3375	0	532	0	0

Back

Virtual AP (Multiple SSID)

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

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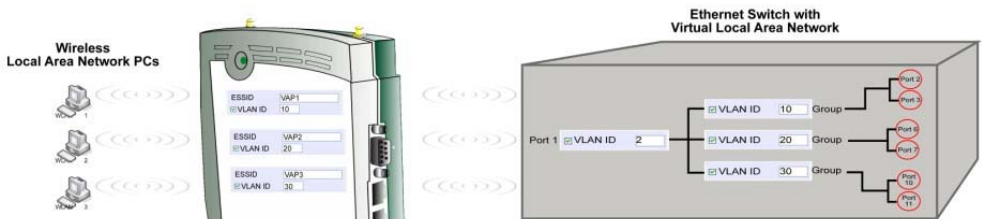
How it Works

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

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

Follow these steps to setup Virtual AP.

Virtual AP

1

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

Virtual AP List

En	ESSID	BSSID	Statistics	Security	
☑	Main	XX-XX-XX-XX-XX-XX	View	NONE	Delete
☑	Sub	XX-XX-XX-XX-XX-XX	View	NONE	Delete

Apply Add Clear Back

(All changes will take effect after reboot)

2

Virtual AP List page displays.

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

Click Add to goto add Virtual AP page.

Virtual AP

ESSID [   ]

☐ VLAN ID [   ]

☐ Closed System

☐ RootAP

Security Mode: NONE ▼

Apply Back

3

1. Enter ESSID name.
2. Settings:
   - VLAN ID
   - Closed System
   - RootAP

3. Select Security Mode
4. Click Apply to make changes or click Back to return to Virtual AP List page.

Preferred APs (Only available in Client Mode)

When there is more than one AP with the same SSID, the Preferred APs function allows you define the MAC address of the APs in order of preference.
The MAC address at the top of the Preferred APs list has the highest connection preference, and the MAC address at the bottom has the lowest connection preference.

Follow these steps to specify your preferred APs.

Preferred APs

1

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

2. Select **Preferred APs**.

Preferred Access Point MAC Address

Access Point 1	09:10:4A:B9:E2:A4	(XX:XX:XX:XX:XX:XX)
Access Point 2	08:00:07:A9:2B:FC	(XX:XX:XX:XX:XX:XX)
Access Point 3		(XX:XX:XX:XX:XX:XX)
Access Point 4		(XX:XX:XX:XX:XX:XX)

Apply

2

1. Enter the MAC addresses of the preferred APs.

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

Antenna Alignment

The antenna alignment function helps you find the best alignment for the antenna by measuring the quality of the signal.

For best results during the antenna alignment, turn off all wireless networking devices within range except the device with which you are trying to align the antenna.

Follow these steps to setup your wireless LAN.

Antenna Alignment

1

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

2. Select **Antenna Alignment**.

2

1. Enter the Remote AP MAC Address you wish to align with.

2. Click Start to perform antenna alignment.

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

Chapter 6: Configuration

This chapter describes the different features of your router and explains how to customise them to meet your network requirements.

- ❑ Setting up the router in your LAN
- ❑ SNMP (Simple Network Management Protocol) Setup

Setting Up the Router in Your LAN

The following table lists out the parameters relevant to your LAN setup. You can replace the default settings with appropriate values to suit the needs of your LAN.

LAN Parameters	Description
IP Address	The IP address of your router access point is **192.168.168.1** by default. When the DHCP server of the access point is enabled, this LAN <IP address> would be allocated as the Default Gateway of the DHCP client unless you set a different <DHCP Gateway IP address>
Network Mask	The Network Mask identifies the subnet in which your router resides. The default network mask is **255.255.255.0**.
Management Gateway IP	(Optional) As a bridge router, the router does not usually communicate with devices on other IP subnets. However, the Management Gateway here acts as the equivalent of the Default Gateway of a PC, to allow the router to communicate with devices on different subnets. For instance, if you want to access the router from the internet or from the router on the LAN, you can set the IP address of the router as the Management Gateway IP. The Management Gateway IP address of your router is set to Nil by default.
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.	
DHCP Start IP Address	This is the first IP address that the DHCP server will assign. The value you enter should belong to the same subnet as your router. For example if the IP address and network mask of your router are 192.168.168.1 and 255.255.255.0 respectively,

51
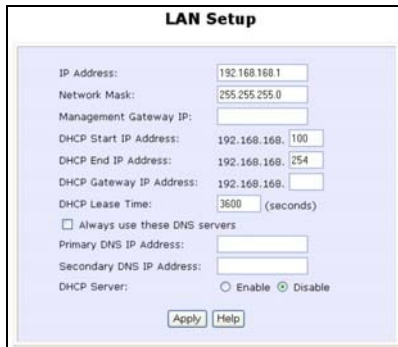
	the DHCP Start IP Address should be 192.168.168.X where X is any value from 2 to 254. It is preset to **192.168.168.100**.
DHCP End IP Address	This is the last IP address that the DHCP server can assign. The value you enter should also belong to the same subnet as your router. For example if the IP address and network mask of your router are 192.168.168.1 and 255.255.255.0 respectively, the DHCP End IP Address should be 192.168.168.X where X is any value from 2 to 254. It is preset as **192.168.168.254.**
DHCP Gateway IP Address	Enter the IP address of the gateway to Internet or of the router if this access point is the one connecting to the Internet. If your network uses multiple gateways / access points, you may wish the router to act as DHCP server to a LAN segment while another access point connects to the Internet or to another LAN. Though the DHCP server usually acts as the Default Gateway of the DHCP client, you can 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 router but will access the Internet or the other LAN through the Default Gateway defined by the <DHCP Gateway IP address>.
Always use these DNS servers	Enable this option if you want the router to use only the DNS server you have specified.
Primary DNS IP Address	Your ISP usually provides the IP address of the DNS server.
Secondary DNS IP Address	This optional field is for the IP address of a secondary DNS server.
DHCP Server	If DHCP server is disabled you will need to manually configure the TCP/IP parameters of each computer in your LAN.

Setting Up Your LAN

Follow these steps to change the values and customise them for your LAN settings.

LAN Setup

1 Click **LAN Setup** from the **CONFIGURATION** menu.

2 2. Amend the relevant fields in the **LAN Setup** page.

3. Click **Apply**, to apply the changes.

To view the active DHCP leases

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

① 1. Click **LAN Setup** from the **CONFIGURATION** menu.

2. In **LAN Setup** page, go to **Advanced DHCP Server Options**.

3. Click **Show Active DHCP leases**.

Advanced DHCP Server Options

Show Active DHCP Leases

DHCP Server Reservations
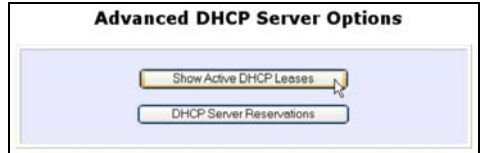
② The **DHCP Active Leases** table displays:
- The **IP Address** that has been allocated to the DHCP client.
- The **Host Name** of the DHCP client.
- The **Hardware Address** (MAC) of the DHCP client.
- The date and time when the IP address leased **expires.**

DHCP Active Leases

Host Name	IP Address	Hardware Address	Lease Expiry Time

Refresh Help Back

> ⚠ **NOTE:** Invalid date and time displayed in the **Expires** column indicates that the clock of your router has not been set. Please refer to the **SYSTEM TOOLS** section for more details on how to set the router's clock.

<u>To reserve specific IP addresses for predetermined DHCP clients</u>

The ability to make IP reservations enables you to assign a fixed IP address to a predetermined client (identified by its MAC address), thus informing the DHCP server to exclude that specific address from the pool of free IP addresses it draws on for its dynamic 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 modify the settings of the built-in DHCP server.

Advanced DHCP Options

1

1. Click **LAN Setup** from the **CONFIGURATION** menu.

2. In **LAN Setup** page, go to **Advanced DHCP Server Options**.

3. Click **DHCP Server Reservations.**

4. Click **Add.**

Advanced DHCP Server Options

Show Active DHCP Leases

DHCP Server Reservations

DHCP Server Reservations

| IP Address | Hardware Address |

Add Back

DHCP Server Reservations

IP Address: 192.168.168.

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

Add Cancel

2
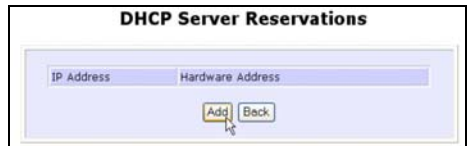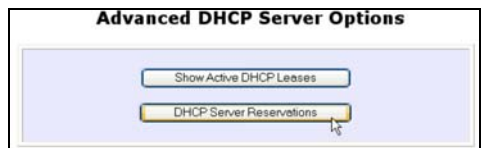
1. Enter:
   - The host portion of the **IP Address** to reserve.
   - The **Hardware Address**, in 6 pairs of two hex values

2. Click **Add** effect the changes.

3. The DHCP Reservations table will refresh to display the currently reserved IP addresses.

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

1. Select the reserved IP address to delete.

2. Click **Delete**.

3. The DHCP Reservations table will refresh to reflect the changes.

DHCP Server Reservations

IP Address	Hardware Address
192.168.168.25	00-80-45-e5-0d-05

Add Back

DHCP Server Reservations

IP Address: 192.168.168. 25

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

Save   Delete   Cancel

Bandwidth Control for WAN

Bandwidth Control allows you to decide the available bandwidth in levels of 1kbit.

Follow these steps to setup Bandwidth Control for WAN.

Bandwidth Control for WAN

1

Click **Bandwidth Control** from the **CONFIGURATION** menu.

Enable/Disable Bandwidth Control

Bandwidth Control Status :   ○ Enable ● Disable

Apply

2
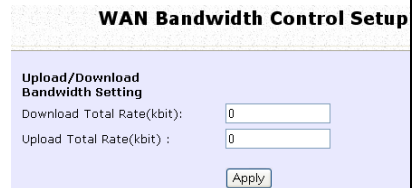
Select whether to Enable or Disable Bandwidth Control and click Apply.

3

To apply Bandwidth Control on WAN, in WAN Bandwidth Control Setup:

1. Enter the Download Total Rate in kbit. This restricts the bandwidth available for downloading.

2. Enter the Upload Total Rate in kbit. This restricts the bandwidth available for uploading.

3. Click Apply.

WAN Bandwidth Control Setup

Upload/Download Bandwidth Setting
Download Total Rate(kbit):   [0]
Upload Total Rate(kbit) :   [0]

Apply

Bandwidth Control for LAN

Bandwidth Control allows you to decide the available bandwidth in levels of 1kbit.

Follow these steps to setup Bandwidth Control for LAN.

Bandwidth Control for LAN

1

Click **Bandwidth Control** from the **CONFIGURATION** menu.

Enable/Disable Bandwidth Control

Bandwidth Control Status : ○ Enable ⊙ Disable

[Apply]

2

Select whether to Enable or Disable Bandwidth Control and click Apply.

3

Click Add to add a Bandwidth Control Entry

LAN Bandwidth Control Setup

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

[Add]

Add Bandwidth Control Entry

Bandwidth Control Rule

Rule Name :

Committed Rate(kbit) :

Ceil Rate(kbit) :

Rule type   DownLoad By IP Address ▼

IP/MAC Address

[Add] [Cancel]

3

1. Enter the Bandwidth Control Rule Name.
2. Enter the Committed Rate in kbit. This sets the bandwidth committed.
3. Enter the Ceil Rate in kbit. This is the ceiling rate which sets the maximum bandwidth allowed.
4. Enter the Rule Type

Rule Types:
- Download by IP Address
- Download by MAC Address
- Upload by IP Address
- Upload by MAC Address

5. Enter the IP or MAC Address according to the Rule Type selected.
6. Click Add to add this Bandwidth Control Entry or click Cancel to cancel to disregard your entry.

STP Setup

Spanning Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations.

Multiple active paths between stations cause loops in the network. If a loop exists in the network topology, the potential exists for duplication of messages. When loops occur, some switches see stations appear on both sides of the switch. This condition confuses the forwarding algorithm and results in duplicate frames being forwarded.

Enabling Spanning Tree Protocol

1

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

2

Select **Enable**, and click **Apply** to allow spanning tree protocol to be activated on the router.

Spanning Tree Protocol Setup

Status :   ⊙ Enable ○ Disable
Apply

STP Status:
Spanning Tree Protocol (STP) function makes your network more resilient to link failure and avoids loop formation.

Spanning Tree Protocol Setup

STP Status	○ Enable ⊙ Disable	
STP Designated Root		
Priority	32768	(32768:0-65535)
Hello Time	2	(2:1-10)
Forward Delay	15	(15:4-30)
Max Age	20	(20:6-40)

Apply

Priority:
Specify the priority given to the AP.

This value determines 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 access point with the smallest MAC address and set it as the Root AP.

Hello Time:
Specify the time in seconds that elapses between the generation of configuration messages (also known as Hello BPDUs) by an AP that assumes itself that it's the Root AP.

Forwarding Delay:
Specify the time in seconds an AP spends in the listening and learning states (listening for configuration messages.)

Max Aging Time:
Specify the maximum age in seconds of stored configuration message information, after which it is judged as too old and are discarded.

Note: If an AP does not receive another configuration message after the Max Aging Time, the system assumes that the link between itself and the Root AP has gone down and reconfigures the network accordingly.

After specifying the values, click **Apply** to apply changes.

SNMP Setup

SNMP (Simple Network Management Protocol) is a set of protocols that facilitates the exchange of management information between network devices. It enables network administrators to manage network performance, detect and solve network problems, and plan for network growth.

Follow these steps to setup SNMP.

SNMP Setup

1 Click **SNMP Setup** from the **System Tools** menu.

2

3. From the **SNMP** drop-down list, select **Enable**.

   Read Password is set to *public* and **Read/Write Password** set to *private* by default.

4. Enter the SNMP **EngineID**.

5. Press **Apply**.

6. Click **Reboot**.

   You are recommended to change to a different password.
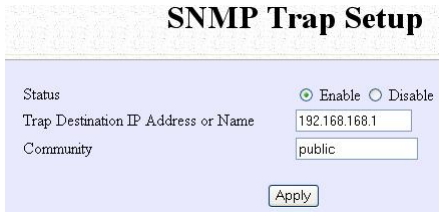
SNMP Trap

The SNMP Trap provides notification of significant network events through unsolicited SNMP messages. This results in substantial savings of network resources by eliminating the need for unnecessary SNMP requests.

Follow these steps to setup SNMP Trap.

SNMP Trap

1 Click **SNMP Setup** from the **CONFIGURATION** menu.

SNMP Trap Setup

2

Status	⦿ Enable ○ Disable
Trap Destination IP Address or Name	192.168.168.1
Community	public

Apply

1. Select whether to **Enable** or **Disable** the SNMP Trap.

2. Enter the **Trap Destination IP Address or Name**. This is the IP address of the SNMP manager.

3. Enter the **Community**. This is used to authenticate messages and is included in every packet that is transmitted between the SNMP manager and agent.

4. Click **Apply**.

Chapter 7: Enabling and Disabling Router

This chapter describes the switching capability of the unit to operate either as a router or access point.

Setting Up Router

By default, the unit is operating as a router.
The simple procedure to enable the router is described.

Enable Router

1 Click **Enable Router** from the **CONFIGURATION** menu.

Enable Router Function

Notice:
If you want to set router function, Press the button, and
it will reboot, To proceed, click the button.

[Enable Router]

2 The **Enable Router Function** appears. Click on the **Enable Router** button.

Setting Up Access Point

Follow these steps to disable the router and switch back as an access point.

Disable Router

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

Disable Router Function
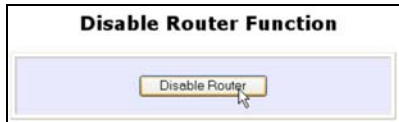
Disable Router

2 Click **Disable Router**.

3 The Disable Router Function screen appears. Click **Disable Router** again.

Disable Router Function

Notice:
This button will disable the router function.
To proceed, click the button and it will reboot.

Disable Router

Chapter 8: Router Setup

This chapter describes the different features of your unit when it is set to operate as a router.

- ❑ Broadband Internet
- ❑ Using NAT
- ❑ Routing
- ❑ Remote Management
- ❑ Parallel Broadband
- ❑ DDNS (Dynamic Domain Name System) Setup

Features unsuitable for office network:

- ❑ Universal Plug and Play
- ❑ DNS (Domain Name System) Redirection

> ⚠️ **NOTE:** Universal Plug and Play and DNS Redirection features are not designed for operation in an office network.
>
> To ensure proper functionality of the router, these features should not be activated when connected to an office network.

Broadband Internet

Setting up the router in your network enables you to share a single cable or ADSL Internet account among multiple LAN clients.

As the router supports several types of broadband Internet connections and WAN protocols, you should verify your broadband Internet subscription type to set up your router correctly.

WAN Setup

The configuration for each type of broadband Internet connection is shown in the following individual sections.
The system has to be restarted to effect changes in settings.

Start with these common steps to set the broadband connection type.
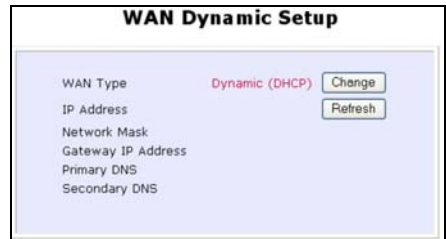
Changing the WAN Type

1

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

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

As the router operates in **Dynamic (DHCP) Address Allocation** mode by default, initially the **WAN Dynamic Setup** page will appear.

2

Clicking **Change** (which appears on the setup pages of all the WAN Types), displays the **Select WAN Type** page.

WAN Dynamic Setup

WAN Type	Dynamic (DHCP) [Change]
IP Address	[Refresh]
Network Mask	
Gateway IP Address	
Primary DNS	
Secondary DNS	

3

From **Select WAN Type** page, select the WAN type to apply and click **Apply**.

The setup page of the selected WAN type displays.

Select WAN Type

○ Static IP Address
◉ Dynamic IP Address
○ PPP over Ethernet
○ PPTP

[Apply] [Cancel] [Help]

Static IP

If you have subscribed to a specific IP address or to a fixed range of IP addresses from your ISP, follow these steps.

Static IP Configuration

1

Select **Static IP Address** from **Select WAN Type** page and click **Apply**.

2

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

1. Enter the **IP Address**, **Network Mask**, and **Gateway IP Address** provided by your ISP.

2. Click **Apply**.

3. Click **Reboot System** to restart the system and let the changes take effect.

Dynamic IP

This is the default WAN Type of your router.

In this connection mode, your ISP will automatically assign its IP address.
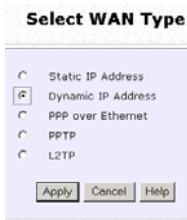
This connection mode applies to most cable Internet subscribers, for instance:
- Singapore Cable Vision subscribers.
- @HOME Cable Service users.

Follow these steps to setup Dynamic IP.

Dynamic IP Configuration

1

Select WAN Type

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

[Apply] [Cancel] [Help]

Select **Dynamic IP Address** as **WAN Type**.
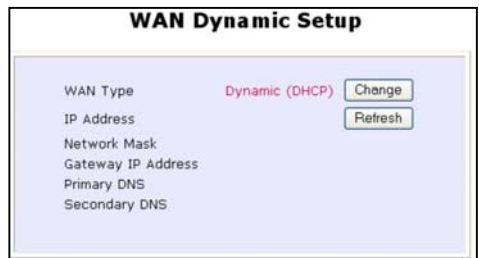
2

At **Dynamic IP WAN Setup** page:

1. You can review the:
   - IP Address
   - Network Mask
   - Gateway IP Address
   - Primary DNS
   - Secondary DNS

The DHCP server of your ISP dynamically allocates these parameters.

Click **Reboot System** to allow the new WAN type to take effect.

WAN Dynamic Setup

WAN Type	Dynamic (DHCP)	[Change]
IP Address		[Refresh]
Network Mask		
Gateway IP Address		
Primary DNS		
Secondary DNS		

PPPoE

Select this connection type if you have subscribed to ADSL in a country utilising 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.

These are the parameters in the PPPoE setup.

PPPoE Parameter	Description
Username	This refers to your broadband account username.
Password	This refers to your broadband account password.
On-Demand	If enabled, the router will automatically connect to the ISP whenever a LAN client makes an Internet request.
Idle Timeout	This field is relevant only if **On-Demand** is enabled. It allows you to specify an idle time allowed before the router automatically goes offline. It will only reconnect when a LAN client makes an Internet request. If the field is set to **0**, this feature will be disabled, and the router will remain online unless disconnected by the ISP. The default value is preset to **30** seconds.
Always-On	If this feature is enabled, the router will remain permanently connected to the Internet.
Reconnect Time Factor	This field is relevant only if **Always-On** is enabled and allows you to specify an offline time allowed, before the router automatically reconnects to the Internet. The default value is preset to **30** seconds.

Follow these steps to setup PPPoE.

PPPoE Configuration

Select WAN Type

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

[Apply] [Cancel] [Help]

1

Select **PPP over Ethernet** from the **Select WAN Type** menu.

2

WAN PPPoE Setup

WAN Type :	PPPoE	[Change]
Username	guest	
Password		
○ On-Demand	Idle Timeout (0:disabled) 30 seconds	
◉ Always-On	Reconnect Time Factor 30 seconds	
Status :	Connecting	[Refresh Status]
IP Address		
Network Mask		
Default Gateway		
Primary DNS		
Secondary DNS		

[Apply] [Email Notification] [Help]

At the **PPPoE WAN Setup** page:

1. Enter your broadband Internet account parameters in the relevant fields.

2. The **Status** section displays your connection settings such as:
   - IP Address
   - Network Mask
   - Gateway IP Address
   - Primary & Secondary DNS

3. If you are online, clicking **Disconnect** will disconnect your connection.

4. Click **Apply**.

5. Click **Reboot System** button to restart the system and allow the WAN type changes to take effect.

To use **Email Notification**, please refer to **Chapter 8: Router Setup – Broadband Internet Through the router – WAN Setup Email Notification**

PPTP

The Point-to-Point Tunneling Protocol (PPTP) enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks, enabling secure remote access at lower cost.

Follow these steps to setup PPTP.

PPTP Configuration

1

Select **PPTP** as your **WAN Type** at **Select WAN Type** page.

2

At the PPTP WAN Setup page:

1. Select whether to enable DHCP.

2. Enter Client **IP Address**.

3. Enter **Network Mask**.

4. Enter the **Gateway**.

5. Enter the **Username** of your Internet account.

6. Enter the **Password** of your Internet account.

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

8. Enter an **Idle Timeout** value between 30-3600 seconds. Entering **0** will disable this feature.

9. The **Status** section gives you a summary of your connection settings such as:
   - IP address
   - Network Mask
   - Gateway IP Address

To use **Email Notification**, please refer to **Chapter 8: Router Setup – Broadband Internet Through the router – WAN Setup Email Notification**

10. If you are online, clicking **Disconnect** will disconnect your connection.
11. Click **Apply**.
12. Click **Reboot** button to restart the system and allow the changes to take effect.

L2TP

L2TP (Layer 2 Tunneling Protocol) is an extension to the PPP protocol used for Virtual Private Networks (VPNs) that supports multiple protocols and unregistered and privately administered IP addresses over the Internet.

Follow these steps to setup L2TP

L2TP Configuration

Select WAN Type

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

[Apply] [Cancel] [Help]

1

Select **L2TP** as your **WAN Type** at **Select WAN Type** page.

2

WAN L2TP Setup

WAN Type	l2tp	[Change]
IP Address		☑ DHCP
Network Mask		
Gateway		
Username		
Password		
VPN Server		
Idle Timeout	0	(30-3600, 0:disabled)
Status	**Disconnected**	[Refresh Status]
IP Address		
Network Mask		
Gateway IP Address		

[Apply] [Email Notification]

At the WAN L2TP Setup page:

1. Select whether to enable DHCP.
2. Enter Client **IP Address**.
3. Enter **Network Mask**.
4. Enter the **Gateway**.
5. Enter the **Username** of your Internet account.
6. Enter the **Password** of your Internet account.
7. Enter the IP address of your **VPN Server**.
8. Enter an **Idle Timeout** value between 30-3600 seconds. Entering **0** will disable this feature.
9. The **Status** section gives you a summary of your connection settings such as:
   - IP address
   - Network Mask
   - Gateway IP Address
10. If you are online, clicking **Disconnect** will disconnect your connection.
13. Click **Apply**.
14. Click **Reboot** button to restart the system and allow the changes to take effect.

Email Notification

This feature notifies you by email if there is a change in the WAN IP address.
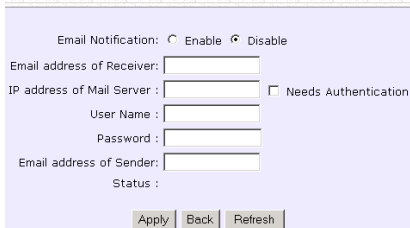
Follow these steps to setup Email Notification.

Email Configuration

1

After applying **WAN PPPoE Setup, WAN PPTP Setup, or L2TP.**
The WAN Setup screen of the WAN Type displays. (PPPoE shown in this example.

Click **Email Notification**.

2

Click **Enable** and enter the following fields:

Email address of Receiver:
The email will be sent to this address.

IP address of Email Server:
This is the IP address of the SMTP server through which the message would be sent out.
Note: It is recommended to use your ISP's SMTP server).

User Name:
This is the email account user's name that should be entered if authentication is required.

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

Email address of Sender:
This is the email address that will appear as the sender.

Needs Authentication specifies whether the SMTP server requires authentication, and is not selected by default.

Click **Apply**.

Using NAT

NAT (Network Address Translation) functions by transforming the private IP address of packets originating from hosts on your LAN 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 LAN would then appear as a single client to the WAN interface.

Enabling/Disabling NAT

NAT

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

Enable/Disable NAT

NAT Status :   ⦿ Enable ○ Disable

[Apply] [Help]

Advanced NAT Options

[DMZ] [Port Forwarding] [IP Forwarding]

2 The **NAT Status** radio button is enabled by default.

To change **NAT Status**:
1. Select the appropriate radio button.
2. Click **Apply**.

NOTE: Disabling NAT will disable Internet Sharing. Broadband Internet sharing requires this option to be ENABLED.

When NAT is enabled, your LAN 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 LAN, in spite of NAT.

To Setup a De-Militarised Zone Host

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

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

You may wish to set up a DMZ host if you intend to use a special-purpose Internet Service such as an online game for which no port range information is available.

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

DMZ

1
1. Click **NAT** from the **CONFIGURATION** menu.

2. Ensure that **NAT Status** is set to **Enable**.

At the **Advanced NAT Options** section:

3. Click **DMZ.**

Enable/Disable NAT

NAT Status : ⊙ Enable ○ Disable

Apply Help

Advanced NAT Options

DMZ Port Forwarding IP Forwarding

NAT DMZ IP Address

Private IP Address : 0.0.0.0

Apply Back

2
1. In the **Private IP Address** field, enter the IP address of the PC you wish to place within the DMZ.

Private IP Address is set to 0.0.0.0 by default.

2. Click **Apply**.

3 To disable **DMZ**:
3. In **Private IP Address** field enter **0.0.0.0**.

4. Click **Apply**.

Nat DMZ Ip Address

Private IP Address: 0.0.0.0

Apply

NOTE:
1. The Static IP Address configuration is recommended for the DMZ host when DMZ is enabled, as the address may change if allocated by DHCP, causing improper functioning of the DMZ.

2. The DMZ host is not invulnerable to malicious attacks from the Internet as DMZ exposes ALL of the host's ports.

To Setup Port Forwarding

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

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

The following diagram shows a router with a public IP address of 203.120.90.3 and a private IP address of 192.168.168.1. Using appropriate port forwarding settings, 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 can be directed to the FTP server, which has a private IP address of 192.168.168.8.
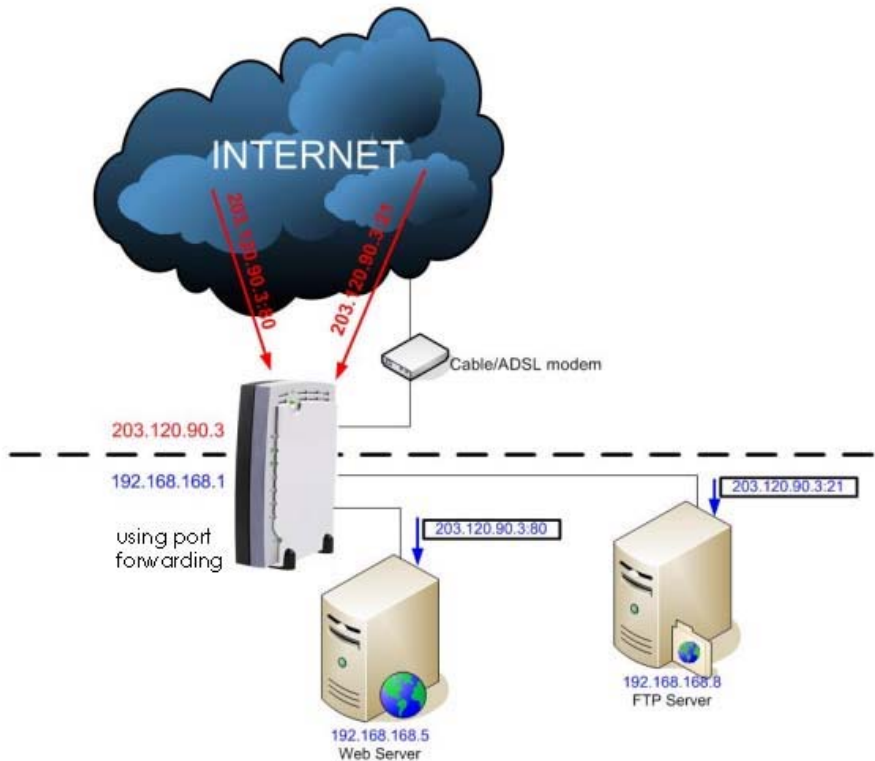
Follow these steps to setup port forwarding.

Port Forwarding

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

2. Ensure that **NAT Status** is set to Enable.

At the **Advanced NAT Options** section:

3. Click **Port Forwarding.**

2 The **Port Forward Entries** table displays the list of current port-based entries.

Click **Add**.

3 For standard server applications (HTTP/FTP/POP3/Netmeeting), go to **Known Server**:

1. Enter the **Private IP Address**.

2. Pick the appropriate **Server Type**.

3. Enter the range in the **From:** and **To:** fields.

4. Click **Add**.

To set up Internet applications not included under **Known Server**, go to **Custom Server**:

1. Enter the **Private IP Address**.
2. Define the **Port** numbers to use.
3. Select the relevant **Protocol** from the drop down list.
4. Identify the **Server Type**.
5. Enter the **From:** and **To:** fields.
6. Click on **Add**.
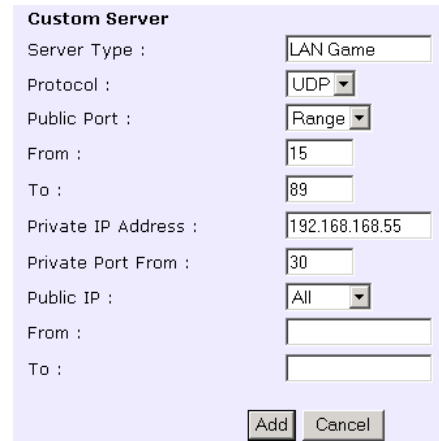
We entered a **Private IP Address** of **192.168.168.55**, defined ports **15** to **89** as the application **Ports**, selected **UDP** from the **Protocol** drop-down list and labeled the **Server Type** as **LAN Game**.

Port Forward Entries

Server Type	Protocol	Public Port	Private IP	Private Port
LAN Game	UDP	15-99	192.168.168.55	30-104

Add Back

Edit Port Forward Entry

Server Type :	LAN Game
Protocol :	UDP
Public Ports :	Range
From :	15
To :	99
Private IP Address :	192.168.168.55
Private Ports From :	30
Public IP :	All
From :	
To :	

Save Delete Cancel

NAT Static Port Based Entries reflects the new entry.

4 To assign more servers in your LAN:
1. Click **Add**.

This will bring you back to Add New NAT Port-Based Entry.

2. Repeat Step 3 above.

To delete table entries:
1. Select the entry to delete.

2. Click **Delete**.

The table will refresh.

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
Nameserver	42
Gopher	70
WWW (World Wide Web)	80

IP Forwarding

If you have subscribed to more than one IP address from your ISP, you may define Virtual Servers based on their IP address so that incoming Internet requests are forwarded to specific computers within the private network.

Assuming you subscribe to the range of Public IP addresses **203.120.12.1** to **203.120.12.62** from your ISP and the PC hosting a server has a LAN IP address of **192.168.168.100**:

To define the Internet Server as having an IP address of **203.120.12.62**, you can set a NAT Static IP Address Entry such that Internet requests to **203.120.12.62** are forwarded to **192.168.168.100** regardless of the TCP/UDP port.

Follow these steps to setup an IP-Forwarding Virtual Server.

IP Forwarding

1

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

2. Ensure **NAT Status** is set to **enable**.

3. At **Advanced NAT Options**:
   Click **IP Forwarding.**

Enable/Disable NAT

NAT Status :   ⊙ Enable ○ Disable

[Apply] [Help]

Advanced NAT Options

[DMZ] [Port Forwarding] [IP Forwarding]

IP Forward Entries

Private IP   Public IP

[Add] [Back]

2 The NAT Static IP Address Entries table displays the list of current port-based entries.

Click **Add**.

Add IP Forward Entry

Private IP Address : [   ]
Public IP Address :   [   ]

[Add] [Cancel]

3

1. Enter the **Private IP Address** of your virtual server as identified in your LAN.

2. Enter the **Public IP Address** of the server, as known outside your LAN.

3. Click **Add**.

Add IP Forward Entry

Private IP Address :   192.168.168.55
Public IP Address :   203.120.101.18

[Add] [Cancel]

IP Forward Entries

Private IP   Public IP
192.168.168.55   203.120.101.18

[Add] [Back]

Edit IP Forward Entry

Private IP Address :   192.168.168.55
Public IP Address :   203.120.101.18

[Save] [Delete] [Cancel]

4 NAT Static IP Address Entries reflects your new entry.

To assign more servers in your LAN:
1. Click **Add**.

This will bring you back to Add New NAT IP Address Entry.

2. Repeat Step 3 above.

To delete table entries:
1. Select the entry to delete.

2. Click **Delete**.

The table will refresh.

NOTE: Please ensure that the public IP address specified to forward from is the correct IP address to which you have subscribed.

Routing

The router supports both static routing for manual routing table entry addition, and dynamic routing for automatic routing table update.

> ⚠️ **NOTE:** The default settings of the router allow broadband Internet sharing so there is no need to configure any further routing information.
>
> **Improper routing settings might cause improper functioning.**

The following diagram illustrates a wireless LAN having subnet 192.168.168.0 in which a router **(X)** with IP address 192.168.168.1 functions as Internet access point while a router **(Y)** with IP address 195.165.150.2 connects to a remote office, of subnet 195.165.150.0.

In this scenario, if client A wants to communicate with the remote client D, when the router **(X)** sees the packets with the destination IP address of D, it will search for and send the routing table information to the router **(Y)** to route the packets to the specified destination.
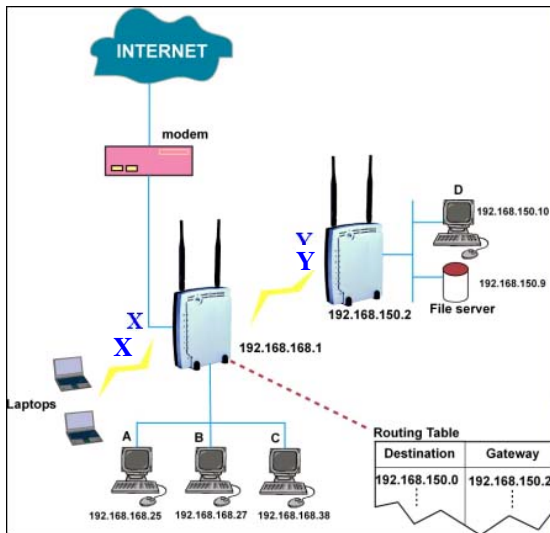
Static Routing

Follow these steps to add entries to your access point's routing table for rerouting of IP packets to another network.

Static Routing

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

System Routing Table

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

Static Routing Table

2 The IP Routing Table displays the list of current routing entries.

To add static route in the IP Routing Table click **Add**.

Static Routing Table

Destination	Network Mask	Gateway

Add   Back

3
1. Enter the Destination **IP Address** of your new entry.

2. Enter the **Gateway IP Address**.

3. Click **Apply**.

   The new entry will appear in the IP Routing Table.

Static Routing Table

Destination IP Address :
Destination Net Mask :
Gateway IP Address :

Add   Cancel

Static Routing Table

Destination	Network Mask	Gateway
192.168.88.21	255.255.255.0	192.168.88.1

Add | Back

Static Routing Table

Destination IP Address : 192.168.88.21
Destination Net Mask : 255.255.255.0
Gateway IP Address : 192.168.88.1

Save | Delete | Cancel

4 The IP Routing Table reflects the new entry.

To add more routes:
1. Click **Add**.

This will bring you back to **Add IP Route** GUI.

2. Repeat Step 3 above.

To delete a route:
1. Select the entry to delete.

2. Click **Delete**.

The table will refresh.

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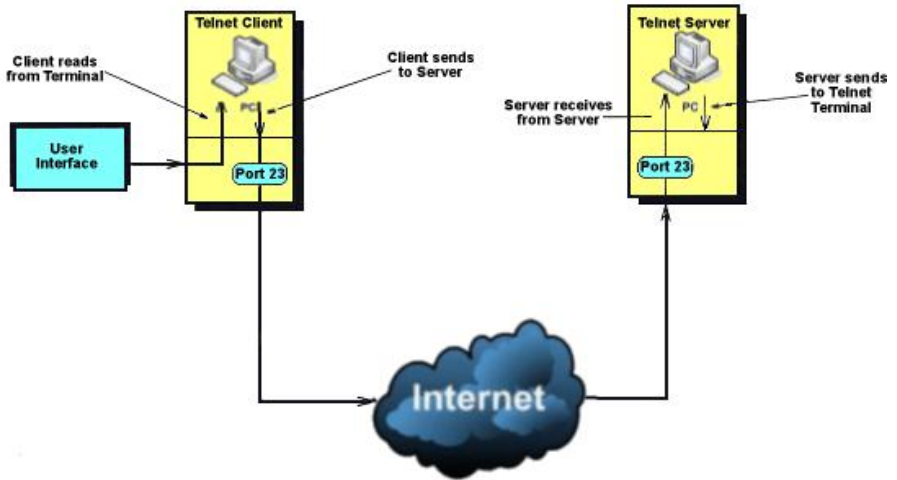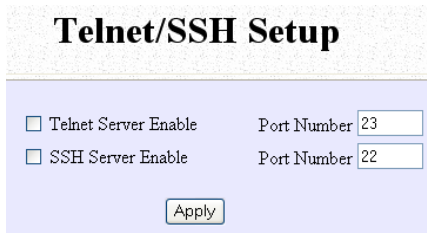
Telnet allows a computer to remotely connect to the CLI (Command Line Interface) for control and monitoring.

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

Follow these steps to setup Telnet/SSH.

Telnet/SSH Setup

1 Click **Telnet/SSH Setup** from the **Device Access Management** menu.

Telnet/SSH Setup

☐ Telnet Server Enable   Port Number 23

☐ SSH Server Enable   Port Number 22

[Apply]

2

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

TELNET CLI

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

Connecting to CLI (Command Line Interface) via TELNET

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

   C:\WINDOWS\TELNET 192.168.168.1

At the login prompt, type in "password" (default password) and press the <ENTER> key, as shown in Figure 2.4c. You will then login to the CLI.
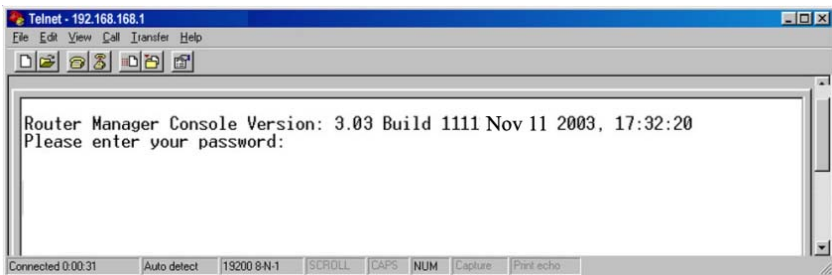
NOTE	**NOTE**
	Please refer to Appendix C for the list of commands available at the console.

91

SSH CLI

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

The first diagram below shows a telnet session.

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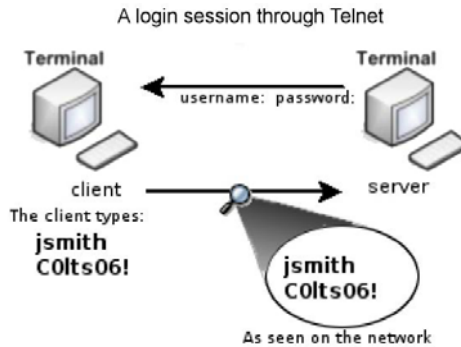
The second diagram below shows how an encrypted connection like SSH is not viewable on the network. The server still can read the information, but only after negotiating the encrypted session with the client.

A login session through SSH
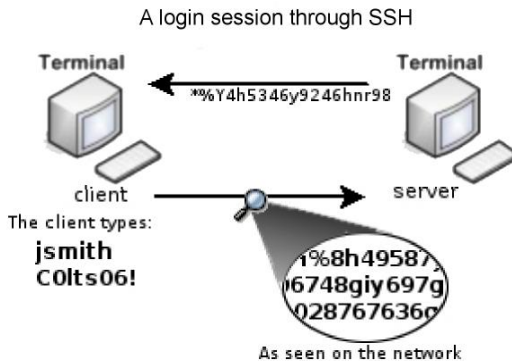
SSH CLI has a command line interface like shown below for example.

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

NOTE	**NOTE**
	Please refer to Appendix D for the list of commands available at the console.

User Management

1 Click **User Management** from the **Device Access Management** menu.

2

To add user:

1. Click Add button.

2. In Add User Entry Page, enter User Name, Password, Confirm Password, specify whether to allow Telnet/SSH, and specify whether user is granted permission to Read Only or Read/Write.
3. Click Apply.

To Delete User:

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

User Management list refreshes to update users.

User Management

Select	User Name	Telnet/SSH(Permission)

Add   Delete

Add a new Account

User Name :   [   ]
New Password :   [   ]
Confirm Password :   [   ]
☐ Telnet/SSH   Permission [Read Only ▼]

Apply   Cancel

User Management

Select	User Name	Telnet/SSH(Permission)
☐	userName	Yes(ReadWrite)
☑	secondUser	No(No)

Add   Delete

User Management

Select	User Name	Telnet/SSH(Permission)
☑	userName	Yes(ReadWrite)

Add   Delete

Web Management Setup
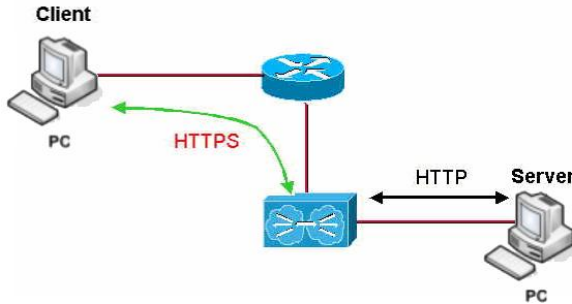
HTTPS (SSL) is supported in addition to the standard HTTP.

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

Follow these steps to setup web management.

Web Management Setup

1 Make selection from the **Device Access Management menu**.

Web Management Setup

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

2. Click **Apply**.

Mode   ⊙ HTTP ○ HTTPS (SSL)
[Apply]

3

Web service restarts automatically.
Web session logouts.

You may reconnect using the new web service using the relogin link displayed on the IP address or Web Mode changed page.

IP address or Web Mode changed.

please relogin from uConfig
uConfig
!

Remote Management

This feature is especially helpful for users who work away from the office or from home.
The user only requires Internet access to manage the network.

Remote Management

1 Click **Remote Management** from the **Device Access Management** menu.

Remote Management

Remote HTTP/HTTPS Port: 8088
(0 =disable, 80 =HTTP default, 443 =HTTPS default)

[Apply]

2

1. Specify the **HTTP / HTTPS Port** number.

   Note: Entering **0** would disable this feature. **80** is the default remote HTTP port. **443** is the default remote HTTPS port.

2. Click **Apply**.

3. Click **Reboot** to reboot the system to effect the changes.

To access the router from the Internet when Remote Management is enabled, open your Internet browser and enter the access point's WAN IP address, followed by a colon (:), and then followed by the HTTP port number.

For example: If your WAN IP address is 210.90.0.13 and you have set port 1111 for remote management, enter 210.90.0.13:1111

Universal Plug and Play (UPnP)

The following are issues that can arise when using NAT:

- Some network applications assume the IP address and port that the client has been assigned are global routable values that can be used on the Internet directly. Often, this is not the case as the client has been assigned a private IP address that can only be used on the LAN.
- Other network applications send requests using a socket on a port "A" and expect to receive the reply from a different listening socket on port "Z". When the NAT access point creates a port mapping for port "A", it won't know that it has to match it with the reply packets addressed to port "Z".
- A number of network protocols assume they will always be able to use certain globally routable well-known ports. However there are several clients in the LAN and at any given time, only one client can be allowed to use a specific well-known port. In the meantime, the other clients will not be able to run any web service requiring the same well-known port.

NAT traversal techniques have been developed as a workaround to allow network-aware applications to discover that they are behind a NAT-enabled device, to learn the external, globally-routable IP address and to configure port mappings to automatically forward packets from the external port of the NAT to the internal port used by the application – without the user having to manually configure port mapping.

NAT traversal relies on the discovery and control protocols that are part of the Universal Plug and Play (UPnP) architecture. The UPnP specification is based on TCP/IP and Internet protocols that let devices discover the presence and services offered by other UPnP devices in the network. It also supports the following, which are essential for NAT traversal:

- Learning public IP address
- Enumerating existing port mappings
- Adding and removing port mappings
- Assigning lease times to mappings

Although NAT traversal does not solve all NAT-related issues, it allows several applications to run behind NAT-enabled devices. It is recommended that you enable UPnP when running:

- Multi-player games
- Peer-to-peer connections
- Real-time communications
- Remote Assistance

UPnP

1 Click **UPnP Configuration** from the **Configuration** menu.

Universal Plug and Play (UPnP) is disabled by default.

Enable/Disable UPNP

Status :   ○ Enable ⊙ Disable
            [Apply]

2 1. Select the appropriate **UPnP Status**.

2. Click **Apply**.

3. Reboot the system for the new status to take effect.

Parallel Broadband *Exclusive!*

The router is equipped with the exclusive Parallel Broadband technology, which features scalable Internet bandwidth, Load Balancing, and Fail-Over Redundancy.

As there is no restriction to the type of broadband Internet account the router can connect to, your network can run with one router on Cable Internet, with the rest connected to ADSL at the same time.

Load Balancing

A network built around multiple units arranged in cascade, and running under Parallel Broadband creates an aggregate bandwidth, and balances the Internet traffic generated by your private network over multiple broadband connections.

Fail-Over Redundancy

In the case of one of your broadband connections failing, the affected access point will automatically switch over to broadband channels that are operational so that there is no network disruption.

<u>To Enable Parallel Broadband</u>

Parallel Broadband can be implemented when:

- More than one access point is interconnected (LAN port to LAN port) in your network.
- Each access point is connected to a broadband Internet account.

Parallel Broadband

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

Parallel Broadband is disabled by default.

Parallel Broadband Enable/Disable

Status : ○ Enable ⊙ Disable

Apply

2
1. Enable the Parallel Broadband Status.

2. Click **Apply**.

3. Repeat this for the other access points in your network.
This would enable them to intercommunicate and reassign users to the access point with the smallest load, so that the users are distributed equally among the access points.

Static Address Translation

(Only supported by Wireless Routing Client and Gateway)

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

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

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

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

NOTE	**NOTE** For SAT to function properly:

1. The IP address of the notebook should belong to a different subnet from the LAN IP address of your access point.

2. The <Default Gateway> in the TCP/IP settings of your notebook should NOT be left blank.

1

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

2

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

Enable/Disable Static Address Translation

Status :   ⊙ Enable ○ Disable

Apply

DNS Redirection

DNS Redirection allows you to redirect DNS requests to a local or closer DNS server. This improves the response time and enables true plug-and-play accessibility, especially if your DNS server is behind a firewall or is situated on your private LAN.

DNS Redirection

1 Click **DNS Redirection** from the **Home User Features** menu.

Enable/Disable DNS Redirection

Status : ○ Enable ◉ Disable

[Apply]

2 DNS redirection is disabled by default.

1. Set **DNS Redirection** status to enable.
2. Click **Apply**.

Dynamic DNS Setup

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

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

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

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

The Dynamic DNS service is ideal for a home website, file server, or just to keep a pointer back to the USB storage disk connected to your router so you can access those important documents while you are at work.

Dynamic DNS Setup

1 Click **Dynamic DNS Setup** from the **Configuration** menu.

2

On **Enable/Disable Dynamic DNS** page, **Dynamic DNS Status** is disabled by default.
If you have already created a list earlier, click **Refresh** to update the list.

Enable/Disable Dynamic DNS

Dynamic DNS Status : ○ Enable ⊙ Disable

[Apply]

Dynamic DNS List

Domain Name   Update Status

[Add] [Refresh]

3

To add a new Dynamic DNS to the list, click **Add**.

Dynamic DNS List

Domain Name   Update Status

[Add] [Refresh]

Choice DDNS Provider page displays. There are two default providers that you can use.
The parameters are explained below:

Choice DDNS Provider

Choice	Provider Name	Register Now
○	2MyDNS - Dynamic DNS Service Provider	Register Online
○	DtDNS	Register Online

[Next] [Back]

Choice:
This allows you to select your preferred DDNS provider.

Provider Name:
This is the name of your preferred DDNS provider.

Register Now:
This allows you to go to the website of your preferred DDNS provider to register your account.

There are two predefined DDNS providers.
Please note that you need to be connected to the Internet to register your DDNS account.

1

Under the **Choice** column in the **Choice DDNS Provider** check the radio button for **2MyDNS – DNS Service Provider**.
Click **Next**.
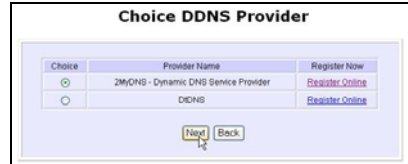
2

At the Dynamic DNS Add page:

1.   Enter your **Domain Name**.

2.   Select **Auto Detect** to detect your current WAN IP address. Enter your DDNS account **Username** and **Password**.
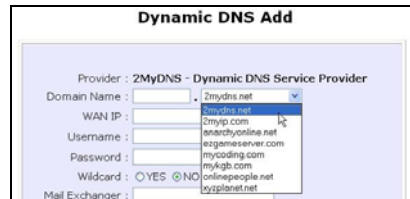
3

Optional: If you enable the wildcard service by selecting **Yes,** your hostname would be allowed multiple identities.
For example, if you register: **mydomain.2mydns.net** users looking for www.mydomain.2mydns.net or ftp.mydomain.2mydns.net can still reach your hostname.

107

4

Optional: In the Mail Exchanger field, enter the Static WAN IP address of the mail server configured to handle email for your domain.

Select **Backup Mail Exchanger** to enable this service.

Click Add button to save the new addition.

5

Dynamic DNS list table displays the new domain.

Dynamic DNS List

Domain Name	Update Status
My Coding.mycoding.com	
people.onlinepeople.net	

Add   Refresh

6

It will appear as a hyperlink to the Dynamic DNS Edit page.

From this page, you can update any of the parameters, delete the domain name, or reset all parameters.

Dynamic DNS Edit

Provider : 2MyDNS - Dynamic DNS Service Provider
Domain Name : people . onlinepeople.net
WAN IP : ☑ Auto Detect
Username : tester
Password : ●●●●●
Wildcard : ⊙ YES ○ NO
Mail Exchanger : ann_tay@powermatic.com.sg
Backup Mail Exchanger : ⊙ YES ○ NO

Save   Reset   Delete   Back

To select **DtDNS as** DDNS Service Provider

1

Under the **Choice** column in the **Choice DDNS Provider** check the radio button for **DtDNS**.
Click **Next**.

Choice DDNS Provider

Choice	Provider Name	Register Now
○	2MyDNS - Dynamic DNS Service Provider	Register Online
◉	DtDNS	Register Online

Next Back

2

At the Dynamic DNS Add page:

1. Enter your **Domain Name**.

2. Select **Auto Detect** to detect your current WAN IP address. Enter your DtDNS account **Username** and **Password**.

3. Click Add.

Dynamic DNS Add

Provider : **DtDNS**
Domain Name : [   ] . [3d-game.com ▼]
WAN IP : [   ] ☑ Auto Detect
Password : [   ]

Add Reset Back

3

Example: While the new domain name, **cool.3d-game.com** is being added to the list, the message 'Waiting in queue…" displays under the **Update Status** column of the **Dynamic DNS List** table.

Dynamic DNS List

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

Add Refresh

Chapter 9: Security Configuration

The **Security Configuration** chapter covers:
- ❑ Firewall Configuration
- ❑ Firewall Logs
- ❑ Packet Filtering
- ❑ URL Filtering
- ❑ Multicast Filtering

The router makes use of Packet Filtering and Stateful Packet Inspection (SPI) to examine each message entering or leaving your LAN and block those that do not satisfy your specified security criteria. Packet Filtering allows you to define security filter rules such that packets that make it through the filter rules are processed as per normal, while those that do not are discarded.

SPI compares the packet content to a database of trusted information instead of only checking the packet header, before letting it through.

Security Level

Depending on the amount of protection you require, you can determine the level of security to implement: Low, Medium, and High.

Log Information

The router allows you to keep a record of data packets that have been allowed and/or that have been refused through the firewall.

By customising the data traffic to record and reviewing the log files at regular intervals, you can monitor the system's performance and identify irregularities.

The following lists the usual types of data packets encountered.
- **TCP** (**Transmission Control Protocol**) packets are exchanged between hosts to establish a connection and exchange data.
- **UDP** (**User Datagram Protocol**) packets are primarily used for broadcasting messages and in streaming audio/video information.
- **ICMP** (**Internet Control Message Protocol**) packets pertaining to error or control information are exchanged between access points.
- **IGMP** (**Internet Group Management Protocol**) packets are sent to establish host memberships such as multicast groups on the LAN.

Firewall Configuration

Follow these steps to configure the firewall.

Firewall Configuration

1 Click **Firewall Configuration** from the **Security Configuration** menu.

2

1. Enable the firewall. You can choose the **Default Low**, **Default Medium**, or **Default High** security options for convenient setup.

2. Choose the type of network activity information to log for reference. Data activity arising from different types of protocol can be recorded.

3. The packet types selected in the **Accepted** section will display in the firewall log if they are detected by the firewall. This also applies to the **Denied** section.

111

Add a new Firewall rule

Rule Name :
Disposition Policy : Accept
Protocols : Tcp

ICMP Types
☐ All Types   ☐ Echo Reply
☐ Destination Unreachable   ☐ Source Quench
☐ Redirect   ☐ Echo Request
☐ Time Exceeded   ☐ Parameter Problem
☐ Timestamp Request   ☐ Timestamp Reply
☐ Information Request   ☐ Information Reply
☐ Address Mask Request   ☐ Address Mask Reply

Source IP Address : Any
(From) :
(To) :
Destination IP Address : Any
(From) :
(To) :
Source Port : Any
(From) :
(To) :
Destination Port : Any
(From) :
(To) :
Check Options :
Check TTL :
TTL value :

[Add] [Cancel]

More firewall rules can be added for specific security purposes.

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

ICMP Packet Type	Description
Echo request	Determines whether an IP node (a host or a router) is available on the network.
Echo reply	Replies to an ICMP echo request.
Destination unreachable	Informs the host that a datagram cannot be delivered.
Source quench	Informs the host to lower the rate at which it sends datagrams because of

		congestion.
	Redirect	Informs the host of a preferred route.
	Time exceeded	Indicates that the Time-to-Live (TTL) of an IP datagram has expired.
	Parameter Problem	Informs that host that there is a problem in one the ICMP parameter.
	Timestamp Request	Information that is from the ICMP data packet.
	Information Request	Information that is from the ICMP data packet.
	Information Reply	Information that is from the ICMP data packet.

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

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

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

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

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

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

Check Options : This parameter refers to the options in the packet header. The

available selection options are abbreviated as follows:

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

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

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

3 1. **Rule Number** ranges from 1 to 40.
Precedence is determined in ascending order such that rule 1 takes precedence over rule 2.

2. Select whether to **Deny** or to **Accept** packets for the **Disposition Policy**.

3. Pick the relevant **Protocol**.

4. For **ICMP Types**, select the checkboxes according to the ICMP information for the gateway to discard/collect.

5. Similarly, the **IGMP Types** section lets you choose which IGMP packets to discard/ record.

6. From **Source IP Address** dropdown list, select whether to apply the rule to:

▪ A **Range** of IP addresses.
Define **(From)** which IP address **(To)** which IP address, the rule applies.

▪ A **Single** IP address.
You need only specify the source IP address in **(From)**.

▪ **Any** IP address
Both **(From)** and **(To)** may be left blank.

7. Similarly, determine the **Destination IP Address**.

8. At the **Source Port** dropdown list, select either:

▪ A **Range** of TCP ports
Define **(From)** which port **(To)** which port, the rule applies.

▪ A **Single** TCP port
You need only specify the source port in the **(From)**.

▪ **Any** IP port
Both **(From)** and **(To)** may be left blank.

Firewall Rule Configuration
Edit a rule

Field	Value
Rule Number	1
Disposition Policy	Deny
Protocols	Icmp

ICMP Types

☐ All Types   ☐ Echo Reply
☐ Destination Unreachable   ☑ Source Quench
☑ Redirect   ☑ Echo Request
☐ Time Exceeded   ☑ Parameter Problem
☑ Timestamp Request ☑ Timestamp Reply
☑ Information Request ☑ Information Reply
☑ Address Mask Request ☑ Address Mask Reply

IGMP Types

☐ All Types   ☐ Host Membership Query
☐ Host Membership Report ☐ Host Leave Message

Source IP Address Any
(From)
(To)
Destination IP Address Any
(From)
(To)
Source Port Any
(From)
(To)
Destination Port Any
(From)
(To)
Check Options
Check TTL
TTL value 0

Apply Cancel

9. Similarly, determine the **Destination Port**.

10. Select from **Check Options**.

11. Select whether to log packets of **TTL Values Equal**, **Less**, **Greater**, or **Not Equal** to the defined TTL value.

12. Enter **TTL value**.

13. Click **Apply** to apply settings.
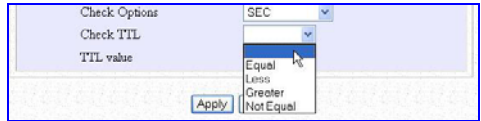
NOTE: Up to 40 firewall rules can be defined, with precedence determined by the rule number.

For example: If Rule 5 blocks all ICMP packets in your LAN, but Rule 6 authorises ICMP-Redirect packets in the LAN, the ICMP Redirect packets will still be blocked.

Firewall Logs

As described previously, from the **Firewall Configuration** page the data traffic to be logged by the router can be defined.

The Firewall Log also records any UDP flooding or SYN flooding attacks on your network.

Firewall Logs

1 Click **Firewall Logs** from the **Security Configuration** menu.

Firewall Log

Time	Action	Protocol	Source Address	Destination Address	Source Port	Destination Port	Information

Refresh

2 1. A firewall log entry consists of:
   - **Time** at which the packet was detected by the firewall.
   - **Action**, which states whether the packet was accepted or denied.
   - **Protocol** type of the packet.
   - **Source Address** from which the packet originated
   - **Destination Address** to which the packet was intended.
   - **Source Port** from which the packet was initiated.
   - **Destination Port** to which the packet was meant for.
   - Any **Information**.

   2. Click **Refresh**, to refresh the log records.

Packet Filtering

With Packet Filtering enabled, the router examines all outgoing packets before deciding - according to predefined rules - whether to block them or to let them pass.   The setting of rules to control the network user access should be done by the system administrators.

This is equivalent to Time-based Access Management and Internet Application Filtering features as packet-filtering rules based on these 3 factors can be defined:

- *Source IP Address*

Restrict Internet activity originating from a specific PC or group of PCs.

- *TCP Port*

Prevent certain applications such as FTP from passing through your access point.

- *Time Frame*

Restrict Internet access to certain times.

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

The router thus provides a wide range of options in monitoring the traffic in your LAN.

As example, for the rule TCP Port **23** from **any** IP on **any** day at **any** time (Port 23 is usually used by TELNET):

If **sent** is selected, all outgoing packets will be sent, except those belonging to TELNET sessions.

If **discarded** is selected, all outgoing packets will be blocked, except for those belonging to TELNET sessions.

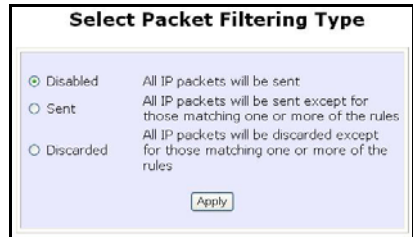Follow these steps to setup packet filtering.

Packet Filtering

1 Click **Packet Filtering** from the **Security Configuration** menu.

Packet Filter Configuration

Packet Filter Type : Disabled   [Change]

2 Clicking **Change** select **Packet Filter Type**.

3 Select from three choices: **Disabled**, **Sent**, **Discarded**, then click **Apply**.
The default is **Disabled**, allowing all packets to be sent.
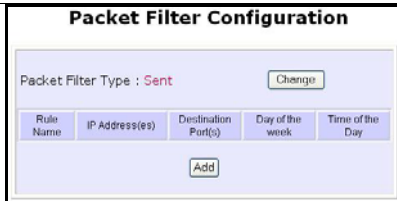
Select Packet Filtering Type

⊙ Disabled   All IP packets will be sent
○ Sent   All IP packets will be sent except for those matching one or more of the rules
○ Discarded   All IP packets will be discarded except for those matching one or more of the rules

[Apply]

Packet Filter Configuration

Packet Filter Type : Sent   [Change]

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

[Add]

4 Click **Add**.

Add a new Packet Filter rule

Rule Name : [____]
IP Address : [Any ▼]
From : 192.168.168. [__]
To : 192.168.168. [__]
Destination Port : [Any ▼]
From : [__]
To : [__]
Day of the Week : [Any ▼]
From : [Mon ▼]
To : [Fri ▼]
Time of the Day : [Any ▼] (hh: 00-23, mm: 00-59)
From : [__] (hh:mm)
To : [__] (hh:mm)

[Add] [Cancel] [Help]

Rule Name : [_____]

The following steps guide you through the packet filter rules that can be defined on this page.

4a). Enter **Rule Name** of the new packet filtering rule. For example: *BlockCS*

119

4b). From the **IP Address** dropdown list, select whether to apply the rule to:

- A **Range** of IP addresses.
  Define **(From)** which IP address **(To)** which IP address, the rule applies.
- A **Single** IP address.
  You need only specify the source IP address in **(From)**.
- **Any** IP address
  Both **(From)** and **(To)** may be left blank.

4c). From the **Destination Port** dropdown list, select whether to apply the rules to:

- A **Range** of IP addresses.
  Define **(From)** which IP address **(To)** which IP address, the rule applies.
- A **Single** IP address.
  You need only specify the source IP address in **(From)**.
- **Any** IP address
  Both **(From)** and **(To)** may be left blank.

4d). From **Day of the Week** dropdown list, select whether the rule should apply to:
  - A **Range** of days
  Define **(From)** which day **(To)** which day, the rule applies.
  - **Any** day
  Both **(From)** and **(To)** may be left blank.

4e). From **Time of the Day** dropdown list, select whether to apply the rule to:
  - A **Range** of time
  Define **(From)** what time **(To)** what time; the rule applies.
  The format is **HH:MM -** where **HH** can take any value from 00 to 23, and

120

MM can take any value from 00 to 59.

▪ **Any** time
Both **(From)** and **(To)** may be left blank.

Click **Apply**, to apply the new rule.
The **Filtering Configuration** table updates.

In this example, the rule BlockCS blocks any IP address (any PCs within the network) from an application using port 27015 from Monday to Friday, 7am to 6pm.

Add a new Packet Filter rule

Rule Name : BlockCS
IP Address : Any
From : 192.168.168.
To : 192.168.168.
Destination Port : Single
From : 27015
To : 27015
Day of the Week : Range
From : Mon
To : Fri
Time of the Day : Range (hh: 00-23, mm: 00-59)
From : 07.00 (hh:mm)
To : 18.00 (hh:mm)

Add   Cancel   Help

URL Filtering

The URL Filtering feature of the router makes it easy to block certain websites from LAN users.

URL Filtering

1 Click **URL Filtering** from the **Security Configuration** menu.

URL Filter Configuration

URL Filter Type :   Disabled   [Change]

2

The **URL Filter Type** can be defined by clicking **Change**.

Selecting **Block**

Select URL Filtering Type

○ Disabled   No Internet access restriction

◉ Block   Block user – specified websites only; allow all other websites

○ Allow   Allow user – specified websites only; block all other websites

[Apply]

Select **Block** or **Allow**, then click **Apply**.
The default is **Disabled**, allowing all websites to be accessed.

URL Filter Configuration

URL Filter Type :   Block   [Change]

Host Name	IP Address

[Add]

Click **Add**.

Selecting **Allow**

Select URL Filtering Type

- ○ Disabled   No Internet access restriction
- ○ Block   Block user – specified websites only; allow all other websites
- ◉ Allow   Allow user – specified websites only; block all other websites

[Apply]

URL Filter Configuration

URL Filter Type :   Allow   [Change]

Host Name	IP Address

[Add]

Add a new URL Filter

Host Name :   [_____]

[Add] [Cancel]

3

In **Host Name**, enter the web site address to be blocked.

Add a new URL Filter

Host Name :   www.objectablewebsites.com

[Add] [Cancel]

For example:
www.objectionablewebsites.com

Click **Add** to complete setup.

Multicast Filtering

This feature lets you allow or disallow streaming over the Internet, if you have registered to ISP services providing videos and TV channel streaming.

1 Click **Multicast** from the **Security Configuration** menu.

Enable/Disable Multicast Filter

Status :   ⊙ Enable ○ Disable

[Apply]

2 Enabling the filter disallows video streaming over the Internet whereas disabling the filter would allow it.
Click **Apply** to complete setup.

Note: This feature is enabled by default.
If such services have been subscribed to, set this feature to **Disable**.

Chapter 10: Web Interface Utilities

This chapter describes the use of:
- The **System Tools** menu
- The **Help** menu

Using the SYSTEM TOOLS Menu

Ping Utility

The Ping Utility works like the commonly used Ping.exe program in Command Prompt.
It allows pinging of IP addresses or domain names.

Follow these steps to use the Ping Utility.

Ping Utility

1

Click **Ping Utility** from the **System Tools** menu.

Ping Utility

Target Host IP Address or Domain Name   `192.168.168.1`

Start

2

Enter the Target Host IP Address or Domain Name and click Start to begin pinging.

If an inavalid IP address or domain name is entered, the field will be reset to the default IP of 192.168.168.1

3

The Ping Utility pings the target with 10 packets of 56 bytes data and displays the results and statistics at the end.

Click Back to return to the previous Ping Utility page.

Ping Return Message

```
Pinging 192.168.168.1 with 56 bytes data:
Reply from 192.168.168.1: bytes=56 icmp_seq=0 ttl=64 time=0.782 ms
Reply from 192.168.168.1: bytes=56 icmp_seq=1 ttl=64 time=0.500 ms
Reply from 192.168.168.1: bytes=56 icmp_seq=2 ttl=64 time=0.491 ms
Reply from 192.168.168.1: bytes=56 icmp_seq=3 ttl=64 time=0.492 ms
Reply from 192.168.168.1: bytes=56 icmp_seq=4 ttl=64 time=0.463 ms
Reply from 192.168.168.1: bytes=56 icmp_seq=5 ttl=64 time=0.491 ms
Reply from 192.168.168.1: bytes=56 icmp_seq=6 ttl=64 time=0.491 ms
Reply from 192.168.168.1: bytes=56 icmp_seq=7 ttl=64 time=0.492 ms
Reply from 192.168.168.1: bytes=56 icmp_seq=8 ttl=64 time=0.489 ms
Reply from 192.168.168.1: bytes=56 icmp_seq=9 ttl=64 time=0.492 ms

--------------------Ping statistics--------------------
10 packets transmitted, 10 received , 0 lost
```

Back

<u>Syslog</u>

Syslog allows remote system logging.
You can setup **Syslog** with the following steps.

Step 1:

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

Step 2:

Select to **Enable Syslog**.

Step 3:

Enter the **Remote IP Address or Domain Name**

Step 4:

Enter the **Remote Port**

Step 5:

Click **Apply** to make the changes.

System Log Setup

Status	⊙ Enable ○ Disable
Remote IP Address or Domain Name	192.168.168.1
Remote Port	514

Apply

To Identify Your System

If your network operates with several of the access points, a means of identifying each individual access point would be useful.
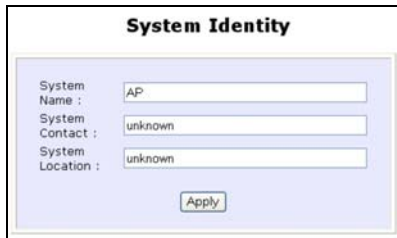
In certain cases your ISP might request identification before dynamically allocating an IP address. The **System Name** of the router can then serve as a **DHCP Client ID** during negotiations with the DHCP Server of your ISP.

You can define the **System Identity** to be utilised as **System Name,** or as **DHCP Client ID**.

Follow these steps to define a **System Identity** for your router.

System Identity

1 Click **System Identity** from the **System Tools** menu.

System Identity

System Name :	AP
System Contact :	unknown
System Location :	unknown

[Apply]

2
1. In **System Name**, enter the DHCP Client ID assigned by your ISP.

2. In **System Contact**, fill in the name of a contact person.

3. Enter **System Location**.
   This entry can help in identification if there are multiple devices in your network or building.

4. Click **Apply** to effect the changes.

<u>Setting the Time of Your System</u>

Synchronising the clocks of the router and your workstation enables effective management and operation of the provided time-based functions.

> **NOTE:** The clock setting will be enabled if the unit is set to operate as a router.

Follow these steps to set your system's clock.

System Clock Setup

1 Click **System Clock Setup** from the **System Tools** menu.

System Time Setting

Current Router Time: 12/31/1969 17:00:45
and Time Zone: GMT-07:00

Proposed Router Time: 11/21/2005 01:57:49
Select your Time Zone:
GMT-07:00 (Mountain Time (US & Canada), ...)

Auto Time Setting (SNTP) ⊙ Enable ○ Disable
Enter a time server(e.g.
time.nist.gov)   time.nist.gov
Or
Select one from the list of cesium.mtk.nao.ac.jp
time servers

Status: Unknown host!

Apply

2 Choose the correct time zone and **Enable** the **Auto Time Setting (SNTP)** using a timeserver such as **time.nist.gov**

Click **Apply.**

<u>To Upgrade the Firmware Version</u>

The products are designed for upgradability.
Click **About System** from the **HELP** menu to check your current firmware version.

Firmware Upgrade

1 Click **Firmware Upgrade** from the **System Tools** menu.

Firmware Upgrade

Notice:
Firmware upgrading will shutdown some services
To proceed, click OK.

[OK]

Firmware Upgrade

Upgrade Firmware (path and file name)

[   ] [Browse...]

[Upgrade]

2 Ensure that the latest firmware has been downloaded onto your local hard disk drive.

1. Enter the path and file name of the downloaded file in **Upgrade Firmware (path and file name)**.

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

2. Click **Upgrade**.

3. Follow the instructions given during the upgrading process.

The router will prompt for reboot when process completes.

NOTE: The device might become unstable if firmware upgrade process is interrupted.

130

<u>Settings Profile</u>

A profile is the set of parameters with which the router is configured.

You may choose to:

- Save your customised profile
- Make a backup of a profile onto your hard disk
- Restore a profile saved on file earlier
- Return the access point to its default settings

Follow these steps to proceed.

Save or Reset Settings

1 Click **Backup or Reset Settings** from the **System Tools** menu.

Backup or Reset Settings

Erase current configuration and restore factory default settings ===> [Reset]

Make a backup copy of current configuration to disk ===> [Backup]

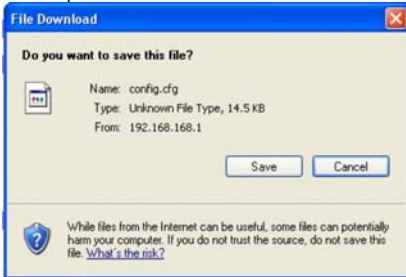Restore backup configuration from disk
[ ] [Browse...] [Restore]

2 To save current profile:

1. Click **Save**.

2. Restart system to ensure the right profile is being used.

To backup current settings onto hard disk drive:

Click **Backup**.

Backup

Browse
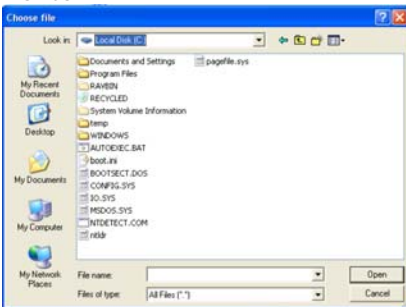
To return system to earlier configuration using backup file:

1. Click **Browse** to search for backup file.

   Or enter file path name in **Restore the Machine's configuration (path and file name)**.

2. Click **Restore**.

To discard <u>ALL</u> configurations made and restore the router to factory settings:

1. Click **Clear and Reset**.

2. Click **yes** when confirmation menu displays.

3. The router will restart and reload default profile.

   Note: Login password will revert to default.

<u>To Reboot</u>

Most changes in system settings require rebooting to take effect.

Follow these steps to reboot the router.

Reboot System

1 Click **Reboot AP** from the **System Tools** menu.

Reboot System

Reboot now?
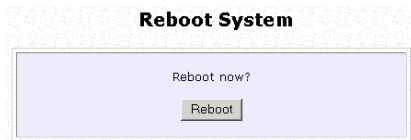
[Reboot]

2 You will be prompted to confirm reboot.

Click **yes** to reboot the router.

NOTE: Reboot AP or **Reboot Router** is displayed under **System Tools** depending on whether the unit is set as access point or router.
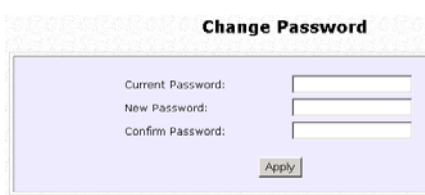
Change Your Login Password

The login password is required to access the web configuration interface, through which the router's settings can be monitored

Follow these steps to change password.

Change Password

1 Click **Change Password** from the **System Tools** menu.

Change Password

Current Password: [   ]
New Password: [   ]
Confirm Password: [   ]

[Apply]

2 Note: Password is case-sensitive.

1. Enter **Current Password**. The default is **password**

2. Enter the new password in **New Password** and **Confirm Password**.

3. Click **Apply**.

<u>To Logout</u>

Follow these steps to logout.

Logout

 Click **Logout** from the **System Tools** menu.

 A login prompt displays.

To access the configuration interface again, click **LOGIN!**

Management

Please enter your password:

●●●●●●● [Log On !]

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

Using the HELP Menu

To Get Technical Support

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

Follow these steps to access the page:

Get Technical Support

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

Support Information

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

Regional Technical Support Centers
U.S.A., Canada, Latin America and South America :

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

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

Compex Systems Pte. Ltd.
135, Joo Seng Road, #08-01,
PM Industrial Building
Singapore 368363
HotLine : (65) 6-286-1805
Fax : (65) 6-283-8337

2 If further information is required, please contact a Technical Support Centre by email, mail, phone, or fax.

<u>About Your System</u>

The **About System** page displays a summary of system configuration information that might be required by support technicians during troubleshooting.

Follow these steps to view the settings.

About System

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

2 The **System Information** page displays a summary of the router's setup parameters.

System Information

Device:	
System Up Time :	0 Days 00:10:07
BIOS/Loader Version :	2.0 (build 0032)
Firmware Version :	1.22 (build E1021)
Network Address Translation :	Enabled
Wireless (A/B/G card):	
Hardware Address :	00-80-48-21-f8-d3
WLAN name (ESSID):	compex-wp18a
Operating frequency :	5210MHz
Operating Channel :	42
Security mode :	None
Wireless (B/G card):	
Hardware Address :	00-80-48-21-f8-d4
WLAN name (ESSID):	compex-wp18bg
Operating frequency :	2457MHz
Operating Channel :	10
Security mode :	None
LAN Port:	
Hardware Address :	00-80-48-12-34-56
IP Address :	192.168.168.1
Network Mask :	255.255.255.0
DHCP Server :	Enabled

Chapter 11: Printer Server Setup

(For NP18 1A, 2B)

The router can also act as a network print server that is easy to operate. When its print server functionality is enabled, you can print from any wired or wireless computer on the network to the USB printer(s) connected to the router.

> ⚠ **NOTE:** You need to install the printer driver software (provided by the printer manufacturer) onto all the PCs in the network that will share the USB printer.
> In this chapter, the step-by-step procedures on using LPR printer are described individually for Windows XP, 2000, 98, and ME users.

After connecting your USB printer to one of the USB ports of the router, turn on the printer. The corresponding USB LED will light up, indicating that the router has detected your printer. Ensure that the printer driver is already installed on your PC and open the web interface of the router:

Adding A Shared Printer Via LPR in Windows XP

For Windows XP Users

Under the **HOME USER FEATURES** command menu, click on **Printer Server Setup.**

Enable/Disable Printer Server

Status :   ⦿ Enable ○ Disable
Apply

Printers List

EPSON Stylus C43
http://192.168.168.1:631/printers/usb0
Remove

refresh

1. Simply choose Enable or Disable for the **Status** of **Printer Server**.

2. Click on the **Apply** button.

3. When you connect the printer to the USB port of the router, the printer will be automatically displayed in the Printer List.

Next to add the printer to your PC:

1. Go to the Windows **Start** Menu; select **Settings**, then followed by **Control Panel**.

2. Then double-click **Printers and Faxes**. Select the **Add a printer** and the **Add Printer Wizard** appears.

3. Click **Next>** to proceed.

4. Check the radio button next to the **Local printer attached to this computer** and click **Next>** to proceed.

Please note that you should not select **Automatically detect and install my Plug and Play printer.**
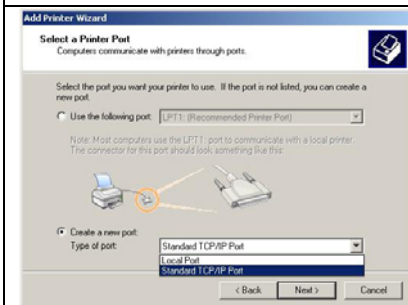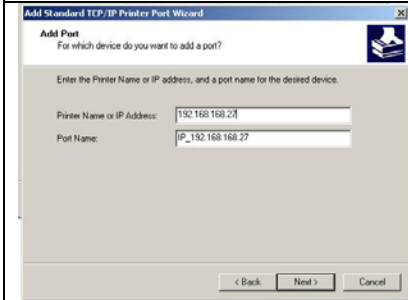

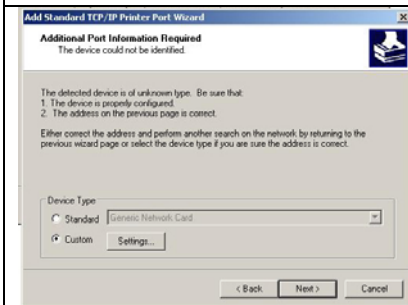Next to select the printer port for your PC:

1. Check the radio button next to **Create a new port**.

2. Then select **Standard TCP/IP Port** for the type of port you will be using.

3. Click on the **Next>** button to proceed.

4. When the **Add Standard TCP/IP Printer Port Wizard** appears, click on the **Next>** button to proceed.

5. Enter your router's IP address in the **Printer Name or IP Address** field. Then the corresponding **Port Name** will be automatically entered.

6. Click on the **Next>** button to proceed.

7. Go to the **Device Type** section and select **Custom**. Next to the Custom radio button, click on the **Settings** button. This brings out **the Configure Standard TCP/IP Port Monitor** window.

8. Go to the **Protocol** section and select **LPR**.

9. Next proceed to the **LPR Settings** section. In the **Queue Name** field, key in '**usb0**'. Please take note that '**usb0**' is an example. The appropriate queue name should be derived from the URL of the printer that connects to the router.
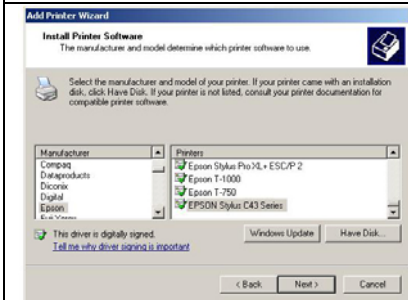
10. Click on the **Next>** button to proceed.

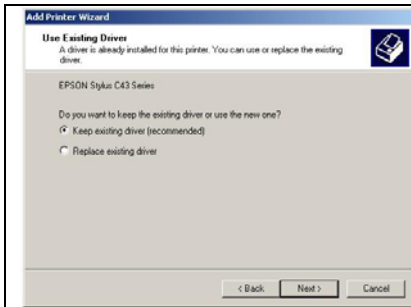
11. After you have successfully configured the selected port, you will see the information display in this window. Click **Finish** to complete the port configuration.

Next to install the printer's driver to your PC:

1. If you cannot find the printer's name in the list, click **Have Disk...** Then you need to install the driver manually.

2. Click on the **Next>** button to proceed.

141

3. Then you will be prompted to choose whether to keep the existing driver or install a new driver. However, it is recommended that you should choose to keep the existing driver.

4. Click on the **Next>** button to proceed.

5. Key in the printer's name.

6. Click on the **Next>** button to proceed.

7. If you want to share the printer with other PC users, click the radio button next to **Share name**. Then key in the share name so that the users will find this name to access the shared printer. Otherwise if you choose not to share the printer, select **do not share this printer**.

8. Click on the **Next>** button to proceed.

9. It is recommended to test the printer. To print the test page, click **Yes**. When you get the test print out, it means that the printer is successfully installed.

10. Click on the **Next>** button to proceed.

11. This window displays a summary of the settings of the printer that is successfully installed.

12. To exit the window, click **Finish**.

Adding A Shared Printer Via LPR in Windows 2000

Under the **HOME USER FEATURES** command menu, click on **Printer Server Setup.**

Enable/Disable Printer Server

1. Simply choose **Enable** or **Disable** for the **Status** of **Printer Server**.

2. Click on the **Apply** button.

3. When you connect the printer the USB port of the router, printer will be automatically displayed in the Printer List.

Next to add the printer to your PC:

1. Go to the Windows **Start** Menu; select **Settings**, then followed by **Control Panel**.

2. Then double-click **Printers and Faxes**. Select the **Add a printer** and the **Add Printer Wizard** appears.

3. Click **Next>** to proceed.

144
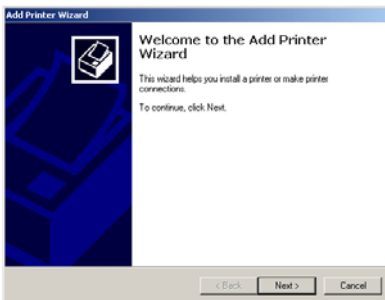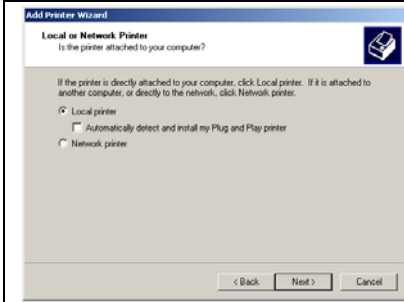
5. Check the radio button next to the **Local printer attached to this computer** and click **Next>** to proceed.

Please note that you should not select **the Automatically detect and install my Plug and Play printer.**
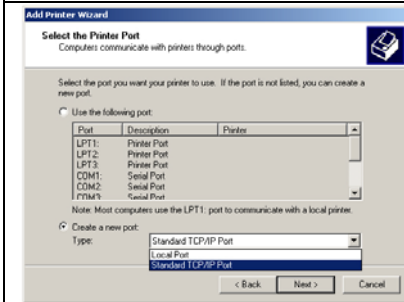
Next to select the printer port for your PC:

1. Check the radio button next to the **Create a new port**.

2. Then select **Standard TCP/IP Port** for the type of port you will be using.

3. Click on the **Next>** button to proceed.

4. When the **Add Standard TCP/IP Printer Port Wizard** appears, click on the **Next>** button to proceed.

145

5. Enter your router's IP address in the **Printer Name or IP Address** field. Then the corresponding **Port Name** will be automatically entered.

6. Click on the **Next>** button to proceed.

7. Go to the **Device Type** section and select **Custom**. Next to the Custom radio button, click on the **Settings** button. This brings out **the Configure Standard TCP/IP Port Monitor** window.

8. Go to the **Protocol** section and select **LPR**.

9. Next proceed to the **LPR Settings** section. In the **Queue Name** field, key in '**usb0**' Please take note that '**usb0**' is an example. The appropriate queue name should be derived from the URL of the printer that connects to the router.

10. Click on the **Next>** button to proceed.

11. After you have successfully configured the selected port, you will see the information display in this window. Click **Finish** to complete the port configuration.

Next to install the printer's driver to your PC:

1. If you cannot find the printer's name in the list, click **Have Disk…**. Then you need to install the driver manually.

2. Click on the **Next>** button to proceed.

3. Then you will be prompted to choose whether to keep the existing driver or install a new driver. However, it is recommended that you should choose to keep the existing driver.

4. Click on the **Next>** button to proceed.
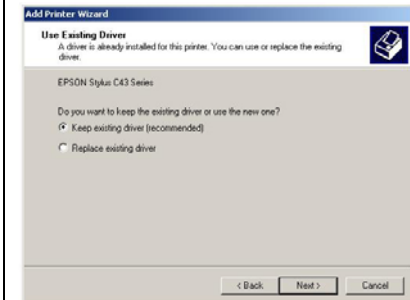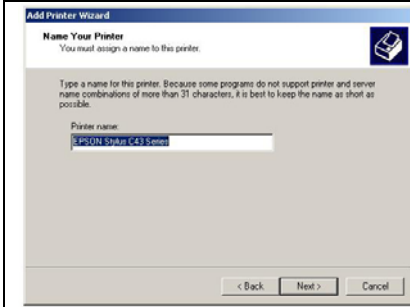
5. Key in the printer's name, you can make it as the default name.

6. Click on the **Next>** button to proceed.

7. If you want to share the printer with other PC users, click the radio button next to **Share name**. Then key in the share name so that the users will find this name to access the shared printer. Otherwise if you choose not to share the printer, select **Do not share this printer**.

8. Click on the **Next>** button to proceed.

9. It is recommended to test the printer. To print the test page, click **Yes**. When you get the test print out, it means that the printer is successfully installed.

10. Click on the **Next>** button to proceed.

11. This window displays a summary of the settings of the printer that is successfully installed.

12. To exit the window, click **Finish**.
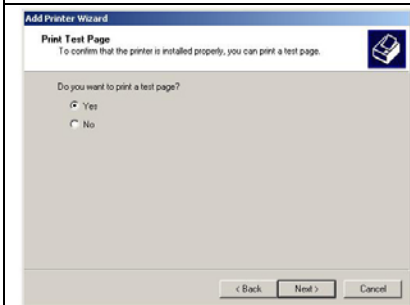
Adding A Shared Printer Via LPR in Windows 98/ME

Before setting up the LPR printer server, you have to download the software of the LPR printer client from the website:
http://www.columbia.edu/acis/access/printing/winME_files/instlpr.exe

Please note that the version of the downloaded software should be V3.4f. Once the download is complete, you can install it to your PC before proceeding with the step-by-step instructions below:

For Windows 98 / ME Users

Under the **HOME USER FEATURES** command menu, click on **Printer Server Setup.**

Simply choose **Enable** or **Disable** for the **Status** of **Printer Server**.

Click on the **Apply** button.

When you connect the printer to the USB port of the router, the printer will be automatically displayed in the Printer List.

Next to add the printer to your PC:

1. Go to the Windows **Start** Menu; select **Settings**, then followed by **Control Panel**. Double-click **Printers**.
2. Double-click **Add Printer.**
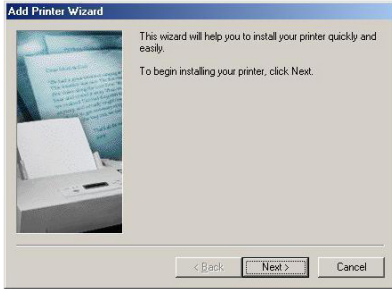
3. The **Add Printer Wizard** (shown on the left) appears.

4. Click **Next>** to proceed.
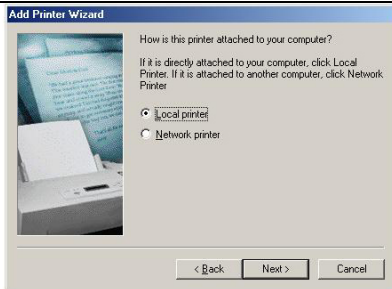
5. Click the radio button next to **Local Printer**. Then click **Next>** to proceed.
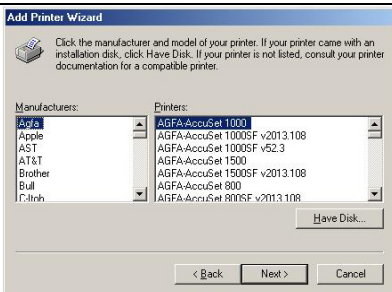
Next to Install the printer's driver to your PC:

1. Select the printer's name available in the **Manufacturers:** and **Printers:** listboxes.

2. But if you cannot find the printer's name in the list, click **Have Disk…**.

3. Click **Next>** to proceed.

4. At the **Install From Disk** screen, click **Browse...** to search for your printer's driver and install it.
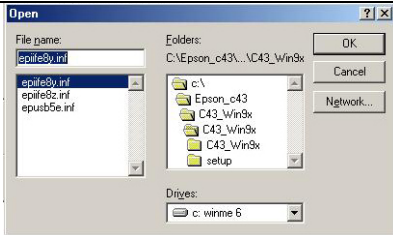
5. The **Open** screen prompts you to select the file name of your printer's driver. Then click **OK** to proceed.
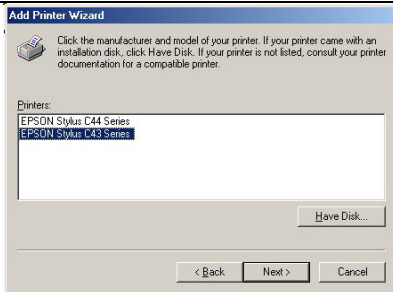
When your printer's driver is added to the **Printers** list, click **Next>** to proceed.
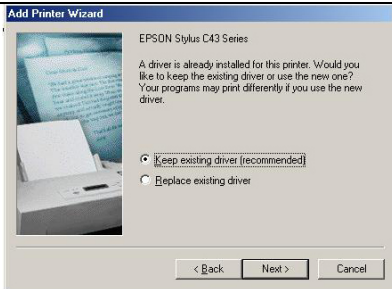
6. Then you will be prompted to choose whether to keep the existing driver or install a new one. But you are advised to keep the existing driver.

7. Click **Next>** to proceed.
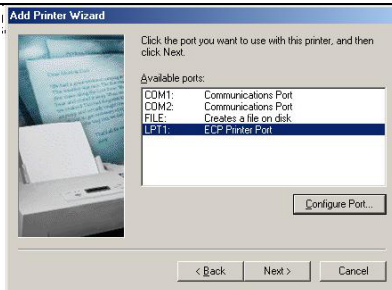
8. Select **LPT1** from the **Available ports:** list box that you want to use for your printer.

9. Click **Next>** to proceed.
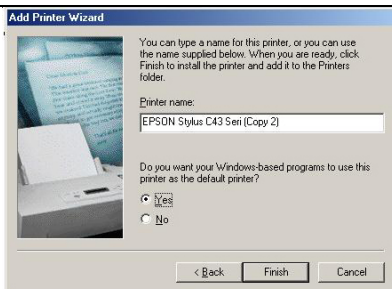
10. Just leave the supplied fields intact as they are. Click **Finish** without editing anything unless required.

11. Wait for a while until the message "Setup is complete" is prompted.

12. Right-click on the icon of the printer you have just installed to select **Properties**.
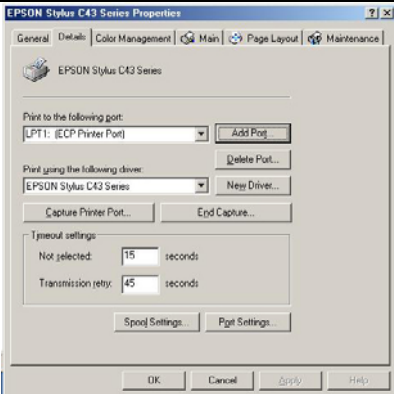
13. At the Details tab of the printer's properties screen, click **Add Port**.
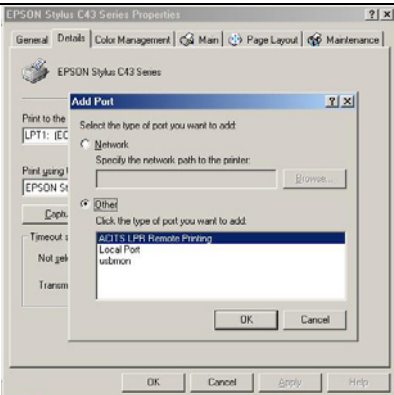
14. The **Add Port** screen is displayed to let you select **Others**.

15. Below the **Others** radio button, highlight and select **ACITS LPR Remote Printing** for the type of port. To confirm the addition, click **OK.**

16. Then the **ACITS LPR Remote Printing** screen pops up.

154
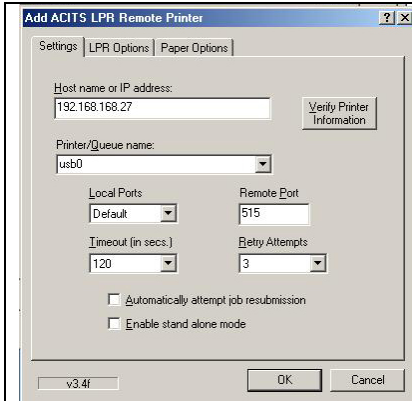
17. At the **Settings tab** of the **ACITS LPR Remote Printing** screen, key in the router's IP address. Proceed to key in the printer/queue name. For example, 'usb0' is the name derived from the URL of the printer connected to the router. For example,http://192.168.168.27:631/printers/usb0.

18. To check if the selected printer is connected to the router or not, click **Verify Printer Information**.
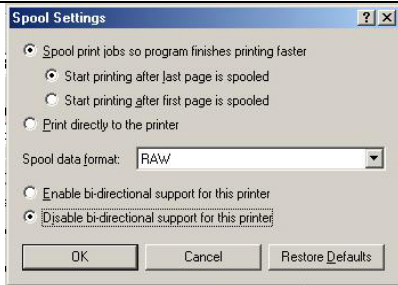
19. At the **Spool Settings** screen, click the radio button next to Start printing after last page is spooled.

20. Then click the radio button next to Disable bi-directional support for this printer.

21. Lastly, click **OK** to complete the printer setup.

Removing the Shared Printer from the Router

To physically remove the network printer from the router safely,

Remove USB Printer

The USB Device
will be removed, continue?

Yes No

Click on the **Remove** button and the system will prompt whether you really want to remove the USB device from the router.

Click **Yes** to confirm. You will then be able to safely disconnect your printer from the USB port of the router.

Chapter 12: USB Storage Disk Sharing

(For NP18 1A, 2B)
The router connects to your USB hard disk/flash disk to allow easy storage sharing in the network and across the Internet. Once your USB hard disk/flash disk is connected to your router, you can access the shared disk via FTP or Windows networking.

> ⚠️ **Note**: The router lets you share entire drives instead of individual folders.

Enable FTP or Windows networking

Under the **HOME USER FEATURES** command menu, click on **USB Storage Disk Sharing.**

There are two ways you can choose to let the users access your USB storage disk: via FTP or Windows networking. If you wish to transfer data via FTP, enable the **FTP Server** option.

A. To enable FTP Server
Using your Web browser or FTP software, you can remotely access the USB disk connected to the router and upload/download files to and from it.

Allow Anonymous: Selecting **Yes** indicates that you allow users to access to your USB storage disk to upload and/or download files without having to key in a username and password. Otherwise, you can create an FTP account to allow only users with authorized username and password to FTP to your storage disk.

Allow Internet: Selecting **Yes** indicates that you allow FTP users to access your storage disk via the Internet. **No** indicates that only LAN access is allowed. **FTP Port:** This is the default TCP port for FTP connection. You may choose another port number if port 21 is being used by another FTP server in the network.

B. To enable Windows File Server
You can easily access the USB storage disk by browsing for the router from a PC in the same Windows workgroup.

You are allowed to define three kinds of user access rights to your USB storage disk: **read and write**, **read** or **disable**.

Read and write access let users view, create and delete files in the USB storage disk. For **Read** access, users are not allowed to modify the disk contents. However, they still can see and open files. Selecting **Disable** prohibits users from accessing to your USB storage disk.

Allow Anonymous: Selecting **Yes** indicates that you allow users to access to your USB storage disk to upload and/or download files without having to key in a username and password. Otherwise, you can create a file server account to allow only users with authorized username and password to use the file server to access your storage disk.

Refer to page 88 for instructions on how to access your storage disk from Windows networking.

USB Storage Disk Sharing

FTP Server:

FTP Server:	⊙ Enable	○ Disable
Allow Anonymous User:	○ Yes	⊙ No
Allow access from the Internet:	○ Yes	⊙ No
FTP Port :	21	

File Server:

Windows File Server:	⊙ Read and Write	
	○ Read Only	
	○ Disable	
Allow Anonymous User:	○ Yes	⊙ No
Allow Internet Access Samba:	○ Yes	⊙ No

Apply

Advanced USB Disk Sharing Functions

Under the **Advanced USB Disk Sharing Functions**, click on **Show connections to USB storage disk**.

Show Connections of Server

This screen displays the number of users connected to the storage disks.

Available connections: It is the maximum number of connections that the router can handle.

Current: This column allows you to monitor the number of active connections established using FTP and Windows networking.

Advanced USB Disk Sharing Functions

Under the **Advanced USB Disk Sharing Functions**, click on **Manage FTP user account**.

FTP Account Configuration

This screen will display the list of FTP user accounts.

Add a new FTP Account

After clicking on **Add**, the **Add a new FTP Account** screen appears. This screen allows you to create FTP user accounts so that when you set **Allow Anonymous** to 'No', only authorized users who login with the correct username and password will be able to FTP to the USB disk connected to your router.

User name: You can create a username to log into the FTP server. For example, *user1*

New Password: You need this password to access to the FTP server.

Confirm Password: Re-type your password for confirmation. Click on the **Add** button to create the new FTP user account.

FTP Account Configuration

User Name	Password
user1	....

Add Back

If you wish to delete an existing or current FTP user account, go to the **FTP Account Configuration** page. Then click on the hyperlink next to its corresponding user name you have selected.

Edit FTP Account

User Name : user1
Password : ••••
Confirm Password : ••••

Save Delete Cancel

This screen below lets you click on the **Delete** button to delete the user account.

Advanced USB Disk Sharing Functions

Storage Disk List

Show connections to USB storage disk

Manage FTP user account

Manage file server user account

Under the **Advanced USB Disk Sharing Functions**, click on **Manage file server user account**.

Advanced USB Disk Sharing Functions

Storage Disk List

Show connections to USB storage disk

Manage FTP user account

Manage file server user account

The **File Server Account Configuration** screen will display the list of users who are using the file server.

Add a new File Server Account

User Name :
New Password :
Confirm Password :

Add   Cancel

After clicking on **Add**, the **Add a new File Server Account** screen appears. This screen allows you to create file server user accounts so that when you set **Allow Anonymous** to 'No', only authorized users who login with the correct username and password will be able to use the file server to access the USB disk connected to your router.

User name: You can create a username to log into the file server. For example, *templar*

New Password: You need this password to access to the file server.

Confirm Password: Re-type your password for confirmation. Click on the **Add** button to create the new file server user account.

162

File Server Account Configuration

User Name
Templar

[Add] [Back]

If you wish to edit an account password or delete a user account, go to the **File Server Account Configuration** page. Then click on the corresponding user name.

Edit File Server Account

User Name :   Templar
Password :
Confirm Password :

[Save] [Delete] [Cancel]

Modify the account password and press **Save** or click on the **Delete** button to delete the user account.

Accessing Your USB Hard Disk Via FTP Server
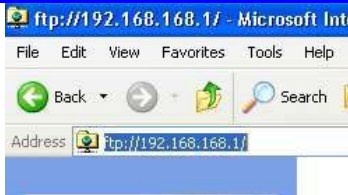
From your Internet Explorer address bar, type in ftp://192.168.168.1, where 192.168.168.1 is the LAN IP address of your router (if you access locally) or its WAN IP address (if you access through Internet).

Click on **File**, followed by **Login As....** In the pop-up window that appears, key in your FTP username and password.

Alternatively,

You may also type in the following format: ftp://username:password@192.168.168.1:21 whereby 'username' and 'password' refer to your FTP account username and password; '192.168.168.1' refers to the LAN IP address (for local access) or the WAN IP address (for Internet access) of your router; '21' refers to the
FTP Port number in the FTP setup.

Accessing Your USB Hard Disk Via Windows File Server

Access via Windows File Server	
	Right-click the **My Network Places** icon on your desktop and select **Search for Computers....**
	Enter the **NETBIOS** name you have set up in the **Computer Name:** field and click on **Search Now** button. Once found, the system will display the device name, Workgroup name and also the server name in their respective fields.
	Double click on the device name, *router*. If you have selected **Allow Anonymous**, the contents of the USB storage disk will appear. Otherwise, you will need to enter your username and password to access the disk contents.
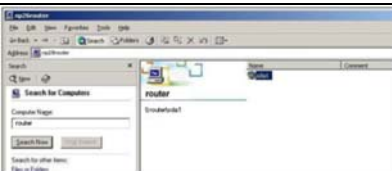
> ⚠ **Note**: The Workgroup Name of both the router and the PC must be the same.

Using Windows File Server to Map to Network Drive

This section explains how to connect to the shared USB storage disk attached to the router and assign a drive letter to this connection so that you can directly access the disk using the **My Computer** icon.

Map Network Drive via Windows File Server	
	From your Windows Explorer, go to **Tools** and select **Map Network Drive...**.
	Alternatively, you may also right-click on the **My Computer** from your desktop and select **Map Network Drive...**.
	Next, enter \\192.168.88.22\sda1, where 192.168.88.22 is the IP address of your router; sda1 is the share name assigned to your USB disk by the router.
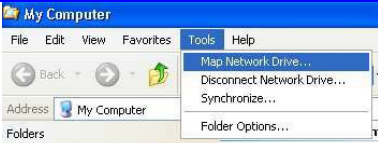
USB HDD List

Device Name	Share Name	Remove
Storage Media	sda	Remove

refresh Back

To check your USB device share name, refer to USB Devices List as shown below. Notice that the router will define the Share Name as sda or sdb, etc according to the order in which you have connected the disks to its USB ports. To map the network drive to your local drive, you need to add a '1' behind the share name, such as 'sda1'.

Click the **Finish** button to map the network drive.

Chapter 13: Webcam Setup and View

(For NP18 1A, 2B)
This chapter describes how you may configure the router to set up your webcam so that authorized users can view your webcam.

Configuring Internet Explorer Security

To be able to view the video stream from your webcam, you need to change the settings of your web browser to accept ActiveX controls.

Internet Explorer Security Settings	
	Open your Internet Explorer, go to **Tools** menu and select **Internet Options…**. From the **Security** Tab, select **Custom Level….** button.
	Under **ActiveX controls and plug-ins**, ensure that all the sub-settings are configured to either **Enable** or **Prompt**. Then click on **OK** and close all the dialog boxes before proceeding.
	Once these steps are completed, you are ready to view the webcam video! Once all security features have been activated, you will be able to view video from your webcam successfully. Remember to choose **Yes** if you are prompted to allow the Active-X interaction.
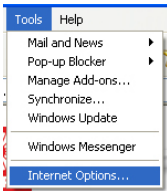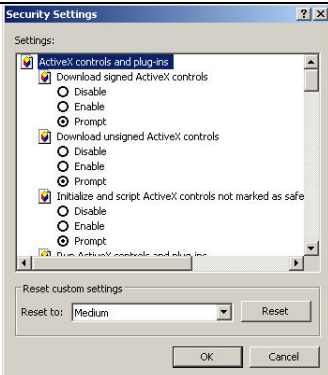
Configuring the Webcam Setup

To be able to configure the webcam setup, you have to enable it first.

Webcam User Setup	
	Under the **HOME USER FEATURES** command menu, click on **Webcam Setup.**
Webcam User Setup Status : ○ Enable ⊙ Disable Webcam Port: 8888 Active User Name No. of visits Time of last visit Group Apply Add **Webcam List** refresh	**Status:** To enable the **Webcam Setup**, check the radio button next to **Enable**. Please note that the **Webcam Setup** is disabled by default. **Webcam Port:** This is the port where you connect your webcam to your router. **Active:** Put a tick to allow user to view the webcam. **User Name:** This is the name that you had created to access to view the webcam. **No of visits:** This is the number of times the user has logged in to view the webcam. **Time of last visit:** The time recorded your last visit to view the webcam.
Webcam User Setup Status : ○ Enable ⊙ Disable Webcam Port: 8888 Active User Name No. of visits Time of last visit Group Apply Add	Click on **Add** button to create new user. The **Add New User** window appears.

Add New User

User Name :	
Password :	

[Add] [Cancel]

Enter your **Username**. For example, 'demo'. Next enter the **Password**.

Webcam User Setup

Status :   ⊙ Enable ○ Disable

Webcam Port: 8888

Active	User Name	No. of visits	Time of last visit	Group
☑	demo	0	unknown	WEBCAM

[Apply] [Add]

Click **Add**. Then the new user is added in the list.

Please note that 'WEBCAM' under **Group** is automatically entered after a new user has been successfully created.

Webcam List

Webcam List `refresh`	Under the **HOME USER FEATURES** command menu, click on **Webcam Setup**. Then go to Camera List.

Camera List
 	
Logitech QuickCam Orbit/Sphere
`Remove`
 	
`refresh`
	If you have just connected your webcam to the router, and you see the empty **Camera List**, click **refresh**.
	Then you will see that this list shows the webcam(s) connected to the router.
	
	To remove the webcam, simply click on the **Remove** button.

Viewing the Webcam

If you see the message read: "Please change its status in Webcam Setup", it shows that you have not enabled the webcam setup. To enable it, refer to the previous section in configuring the webcam setup.

Webcam View	
	Under the **HOME USER FEATURES** command menu, click on **Webcam View.** **Property** Button Click this button to adjust size, display parameters and filters of your screen.
	Capture Button Click this button to capture a still picture from the video feed. Right-click on the still picture and select **"Save Picture As…"** from the menu. Clicking the **Capture** button again will allow you to refresh the still picture to a new instant.
	Left/Up/Center/Down/Right Button These buttons allow you to adjust the position of your webcam if you are using a tracker pod. **Webcam Pan/Tilt** Button This button allows you to adjust the position of your Quickcam Sphere/Orbit webcam.

172

Appendix A: Configuring your PC for network access

This section illustrates how to configure the TCP/IP settings of your computer so that it can communicate with the router or with other computers across your network.

We will consider:

- ❑ Adding TCP/IP protocol for Windows 98/98SE/ME/2000
- ❑ Configuring Dynamic IP Address Allocation for Windows 98/98SE/ME/2000
- ❑ Configuring Static IP Address Allocation for Windows 98/98SE/ME/2000
- ❑ Configuring Wireless Network Settings for Windows XP

Adding TCP/IP protocol for Microsoft Windows 98/98SE/ME/2000

By default, the TCP/IP protocol is installed and set to obtain an IP address automatically in Windows 98, 2K & XP.

However, if your PC does not have TCP/IP installed, the following will guide you through the TCP/IP installation procedure.

Adding TCP/IP protocol in Windows 98/98SE/ME/2000:

1
1. Click on **Start**.
2. Select **Settings**.
3. Click on **Control Panel**.
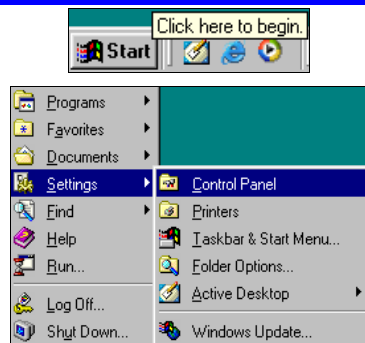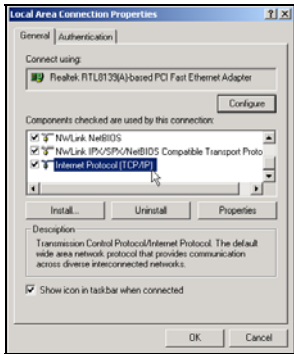
2 Double-click on the **Network** icon.

The **Network** Configuration screen shown on the left will appear.

3 Check your list of **Network Components** in the Network window's **Configuration** tab.

If TCP/IP is not installed:

1. Click on the **Add** button.

   This will bring you to the screen shown on the right.

2. Select **Protocol**.

3. Click on the **Add** button.
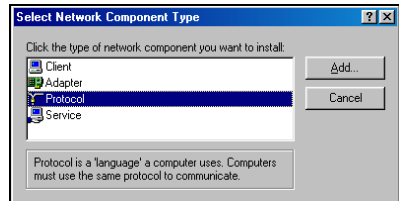
On the next screen that appears:

4. Select **Microsoft** from the **Manufacturers** column.

5. Choose **TCP/IP** from the **Network Protocols** column.

6. Click on the **OK** button.
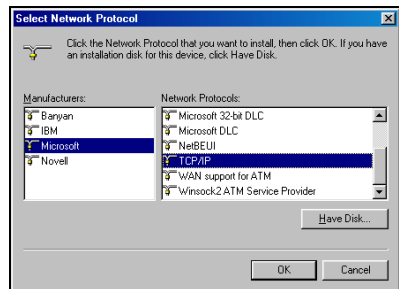
NOTE: Windows may ask you for the original Windows installation disk or for additional files. Check for the files at `C:\windows\options\cabs`, or insert the Windows CDROM disc into the CDROM drive to search for the appropriate files.

174

Configuring Dynamic IP address allocation

<u>Microsoft Windows 98/98SE/ME/2000</u>

Follow these steps to configure your PC for dynamic IP address allocation.

Dynamic IP address allocation in Windows 98/98SE/ME/2000:

1

1. Click on **Start**.
2. Select **Settings**.
3. Click on **Control Panel**.
4. Double-click on the **Network** icon.
5. The **Network** configuration screen will appear as illustrated on the right.
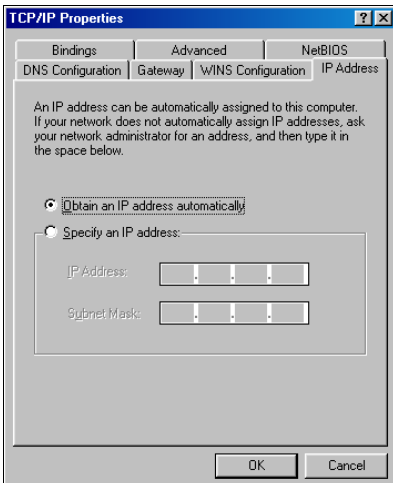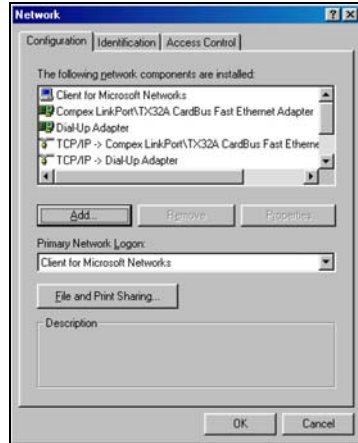
2

1. In the Network window's **Configuration** tab, select the TCP/IP component corresponding to your Ethernet adapter.
2. Click on the **Properties** button.

    This will bring you to the screen shown on the left.

3

1. Click on the **IP Address** tab.

2. Enable the **Obtain an IP address automatically** radio button.

3. Click on the **Gateway** tab.

4. Verify that the **Installed Gateways** list is blank.

5. Click on the **OK** button.

   This will return you to the **Network** dialog page.

6. Click on the **OK** button to close all windows and reboot your computer.
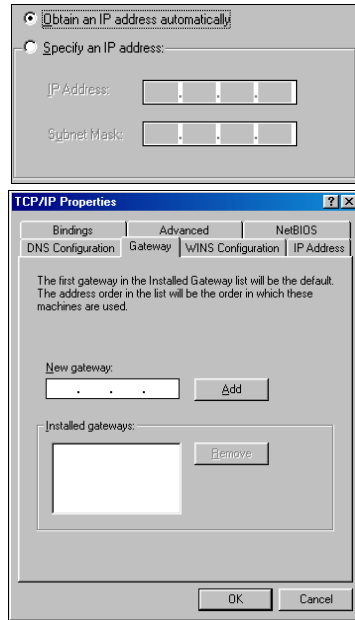
Configuring Static IP address allocation

Microsoft Windows 98/98SE/ME/2000

The following will help you configure your PC with static IP address allocation.

Static IP address allocation in Windows 98/98SE/ME/2000:

1

1. Click on **Start**.
2. Select **Settings**.
3. Click on **Control Panel**.
4. Double-click on the **Network** icon.
5. The **Network** Configuration screen shown on the right will appear.
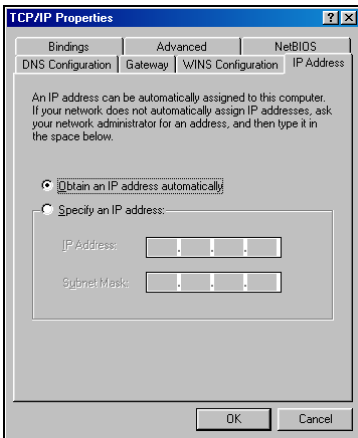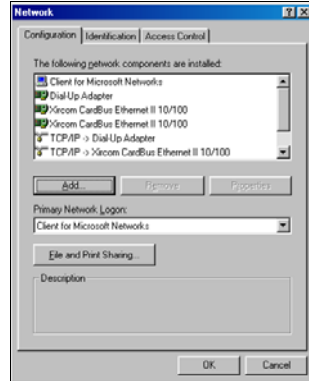
2

1. In the Network window's **Configuration** tab, select the TCP/IP component corresponding to your Ethernet adapter.
2. Click on the **Properties** button.

   This will bring you to the screen shown on the left.

3

1. Click on the **IP Address** tab.

2. Enable the **Specify an IP address** radio button.

3. Fill in the **IP Address** field as **192.168.168.X**, where **X** can take any value from 2 to 254.

   For illustration, we keyed in **192.168.168.45** as IP address.

4. Key in **255.255.255.0** as the **Subnet Mask**.

○ Obtain an IP address automatically

● Specify an IP address:

IP Address: `192.168.168. 45`

Subnet Mask: `255.255.255. 0`
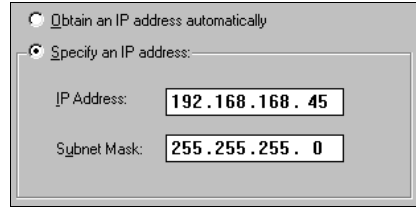
4

1. Click on the **Gateway** tab.

2. Key in the IP address of the router in the **New Gateway** field.

   The default IP address of the router is 192.168.168.1 as we illustrate on the left.

3. Click on the **Add** button.

TCP/IP Properties

Bindings | Advanced | NetBIOS
DNS Configuration | Gateway | WINS Configuration | IP Address

The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

New gateway:
`192.168.168. 1`   Add

Installed gateways:

Remove

OK   Cancel
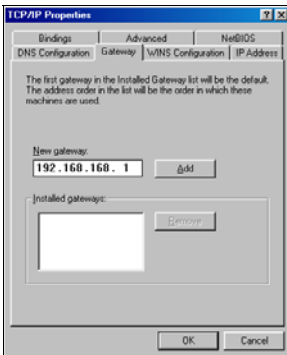
5

1. Click on the **DNS Configuration** tab.

2. Select the **Enable DNS** radio button.

3. Type in a unique identifying name in the **Host** field.

4. We illustrate on the left with **Serv_01**.

5. Key in the IP address of your DNS server, as specified by your Internet Service Provider in the **DNS Server Search Order** field.

6. Click on the **Add** button.

TCP/IP Properties

Bindings | Advanced | NetBIOS
DNS Configuration | Gateway | WINS Configuration | IP Address

○ Disable DNS

● Enable DNS

Host: Serv_01   Domain: Accounts

DNS Server Search Order

`165. 21 .100. 88`   Add

Remove

Domain Suffix Search Order

Add

Remove

OK   Cancel
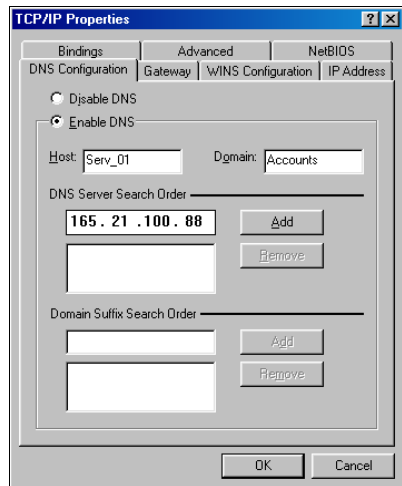
Configuring Wireless Network Settings for Windows XP

It is usually recommended to configure the wireless client PC or notebook with automatic IP addressing.

These steps will guide you in configuring your wireless network settings.

1

1. Right-click on **Wireless Network Connection** corresponding to the wireless Ethernet adapter that you wish to connect to the router.

2. Click on **Properties**.

Wireless Network Connection
Wireless connection unavailable
Intersil PRISM Wireless LAN 8...
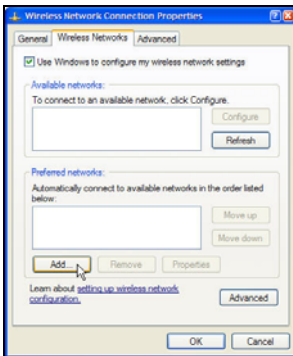
2

1. Click on the **Wireless Network** tab.

2. Click on the **Add** button.

3

1. Key in the SSID of the wireless network in the **Network name** field.

   Ensure that the ESSID entered is the same as that entered for the router as well as all other clients within the same wireless network.

2. Click on the **OK** button.
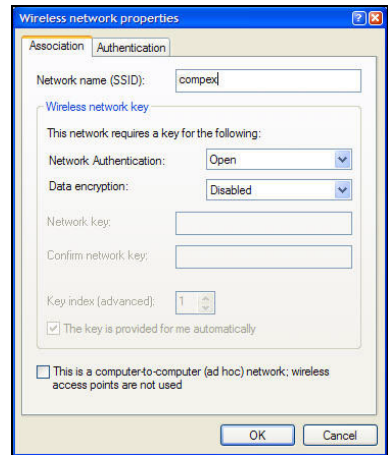
Appendix B: Troubleshooting

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 router.

1. **I want to know whether my PC is connected to the router and 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.
       - If you get a reply, the computer is communicating with the router.

       - If you do <u>NOT</u> get a reply, please check the cables and ensure that the settings are correct before trying again.

    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.

2. **I 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 router, and verify whether the router has a valid IP address from the **About System** page. Then refer to suggested steps A, B & C to Problem 1 as described above, to verify the connectivity of the gateway.

    B. Ensure that the WAN settings suit 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 router and the Cable/ADSL modem. Turn on the Cable/ADSL modem then wait for 1 minute before turning on the router. Lastly, turn on your computer. Verify whether you have been allocated an IP address and are able to surf the web.

3. **I am a PPPoE and am not able to access Internet**

    A. Refer to Problem 1 follow the suggested steps described to verify your connectivity to the router.

    B. If you are a PPPoE user, you will need to remove the proxy settings or the dial-up pop-up window.

    C. Open 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.

        ▪ 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.

4.   I want to reset the default login password of the router.

A. Power up the router

B. Depress the **Reset** button situated at the back of the device and hold it for 5 seconds before releasing it.

5.   I want to set the router to its factory default settings.

A. Power up the router.

B. Depress the **Reset** button situated at the back of the device and hold it for 8 seconds before releasing it.

6.   My laptop is not able to access the router.

A. 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 router.
    - If you do <u>NOT</u> get a reply, please go through the following steps.

B. 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.

C. Verify whether your router 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.

D. Check whether your router and your laptop are using the same frequency band.

  ♦ If you have set up the router in the 2.4GHz frequency band, your laptop should be able to support either IEEE 802.11b or IEEE 802.11g wireless standards.

  ♦ If you have set up the router in the 5GHz frequency band, your laptop should be able to support IEEE 802.11a wireless standards.

7. My network contains several routers but they are unable to connect to each other.

If you are running the **Parallel Broadband** feature:
Although they may belong to different SSIDs, the routers <u>MUST</u> operate in the same frequency band.

Appendix C CLI Commands

Get Operation List

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

Set Operation List

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

Save Configuration

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

Long Range
Check for recommended values from long distant option setup page.

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

TX Power

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

TX Rate

SYNTAX	DESCRIPTION
Set txrate <string>	Values are: (default auto) (802.11a)-- 6, 9, 12, 18, 24, 36, 48, 54, auto (802.11b/g mixed)-- 1, 2, 5,5, 11, 6, 9, 12, 18, 24, 36, 48, 54, auto (802.11b-only)-- 1, 2, 5.5, 11, auto

Wireless Mode

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

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

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

Add or Delete User

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

Country Code

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

185

```
{CTRY_FRANCE,        "FR" },
{CTRY_FRANCE2,       "F2" },
{CTRY_GEORGIA,       "GE" },
{CTRY_GERMANY,       "DE" },
{CTRY_GREECE,        "GR" },
{CTRY_GUATEMALA,     "GT" },
{CTRY_HONDURAS,      "HN" },
{CTRY_HONG_KONG,     "HK" },
{CTRY_HUNGARY,       "HU" },
{CTRY_ICELAND,       "IS" },
{CTRY_INDIA,         "IN" },
{CTRY_INDONESIA,     "ID" },
{CTRY_IRAN,          "IR" },
{CTRY_IRELAND,       "IE" },
{CTRY_ISRAEL,        "IL" },
{CTRY_ITALY,         "IT" },
{CTRY_JAPAN,         "JP" },
{CTRY_JAPAN1,        "J1" },
{CTRY_JAPAN2,        "J2" },
{CTRY_JAPAN3,        "J3" },
{CTRY_JAPAN4,        "J4" },
{CTRY_JAPAN5,        "J5" },
{CTRY_JAPAN6,        "J6" },
{CTRY_JORDAN,        "JO" },
{CTRY_KAZAKHSTAN,    "KZ" },
{CTRY_KOREA_NORTH,   "KP" },
{CTRY_KOREA_ROC,     "KR" },
{CTRY_KOREA_ROC2,    "K2" },
{CTRY_KOREA_ROC3,    "K3" },
{CTRY_KUWAIT,        "KW" },
{CTRY_LATVIA,        "LV" },
{CTRY_LEBANON,       "LB" },
{CTRY_LIECHTENSTEIN, "LI" },
{CTRY_LITHUANIA,     "LT" },
{CTRY_LUXEMBOURG,    "LU" },
{CTRY_MACAU,         "MO" },
{CTRY_MACEDONIA,     "MK" },
{CTRY_MALAYSIA,      "MY" },
{CTRY_MALTA,         "MT" },
{CTRY_MEXICO,        "MX" },
{CTRY_MONACO,        "MC" },
{CTRY_MOROCCO,       "MA" },
{CTRY_NETHERLANDS,   "NL" },
{CTRY_NEW_ZEALAND,   "NZ" },
{CTRY_NORWAY,        "NO" },
{CTRY_OMAN,          "OM" },
{CTRY_PAKISTAN,      "PK" },
{CTRY_PANAMA,        "PA" },
{CTRY_PERU,          "PE" },
{CTRY_PHILIPPINES,   "PH" },
{CTRY_POLAND,        "PL" },
{CTRY_PORTUGAL,      "PT" },
{CTRY_PUERTO_RICO,   "PR" },
{CTRY_QATAR,         "QA" },
{CTRY_ROMANIA,       "RO" },
{CTRY_RUSSIA,        "RU" },
{CTRY_SAUDI_ARABIA,  "SA" },
{CTRY_SINGAPORE,     "SG" },
{CTRY_SLOVAKIA,      "SK" },
{CTRY_SLOVENIA,      "SI" },
{CTRY_SOUTH_AFRICA,  "ZA" },
{CTRY_SPAIN,         "ES" },
{CTRY_SWEDEN,        "SE" },
{CTRY_SWITZERLAND,   "CH" },
{CTRY_SYRIA,         "SY" },
{CTRY_TAIWAN,        "TW" },
{CTRY_THAILAND,      "TH" },
{CTRY_TRINIDAD_Y_TOBAGO, "TT" },
```

	{CTRY_TUNISIA, "TN" }, {CTRY_TURKEY, "TR" }, {CTRY_UKRAINE, "UA" }, {CTRY_UAE, "AE" }, {CTRY_UNITED_KINGDOM, "GB" }, {CTRY_UNITED_STATES, "US" }, {CTRY_URUGUAY, "UY" }, {CTRY_UZBEKISTAN, "UZ" }, {CTRY_VENEZUELA, "VE" }, {CTRY_VIET_NAM, "VN" }, {CTRY_YEMEN, "YE" }, {CTRY_ZIMBABWE, "ZW" },

Channel

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

SSID

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

Closed System

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

Per Node

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

RTS, Fragment, and Beacon Interval

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

WLAN State

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

Reset Button

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

Appendix D: Glossary of Terms

List of commonly used terms

10Base-T	An IEEE Ethernet standard for 10Mbps data transmission using unshielded twisted pair wires.
100Base-Tx	An IEEE Ethernet standard for 100Mbps data transmission using two pairs of Category 5 UTP wire.
802.11b	An IEEE standard for wireless networking standard specifying a maximum data transmission rate of 11Mbps using DSSS modulation and an operating frequency of 2.4GHz.
802.11g	An IEEE standard for wireless networking standard specifying a data transfer rate of 54Mbps using ODFM modulation and an operating frequency of 2.4GHz, as well as backward compatibility with the 802.11b devices.
Bit	Short for "Binary Digit." It uses 0 and 1 as the value for the binary numbering system. It is also the smallest form of data.
Broadcasting	To simultaneously send the same message to all network members.
Browser	The browser is a general name given to applications designed to view and interact with HTML pages on the World Wide Web.
CAT 5	It is a standard developed by the Electronics Industries Association that specifies network cabling which consists for twisted pairs of copper wire with a sustainable data rate of 100Mbps.
Database	A database is a collection of information that is organized so that the contents may be easily accessed/managed.
Data Packet	In an IP network, packet switching is the method employed to transmit data and the smallest chunk of data is called a packet (packet size can vary).
DHCP	Dynamic Host Configuration Protocol. It is a protocol that allows the network administrator to centrally manage and assign IP addresses to devices in the network.
DMZ	De-Militarized Zone hosting allows the administrator to expose a private IP address onto the Internet. It is used for a PC/Server assigned with a Static IP address and requiring multiple TCP/IP ports to be opened.
DNS	Domain Name System translates Internet domain names to IP addresses, giving meaningful and easy-to-remember names to otherwise arcane IP addresses.
Driver	A piece of software developed to interface a piece of hardware with its immediate upper-layer software (i.e. operating system) so that it can be recognized and operated.

DSSS	Direct Sequence Spread Spectrum is a modulation scheme employed by the 802.11b standard that uses a chipping code (redundant bit) during its transmission to reject interference.
Dynamic IP Address	It is an IP address that is dynamically allocated or assigned to a client device within a TCP/IP network, typically by a DHCP server.
Encryption	Encryption is a security method applying specific algorithms to make sure that all the data from one computer is encoded into a form that only the other intended party will be able to decode and view the information.
Ethernet	An IEEE standard network protocol that specifies how data is transmitted over a common medium. It uses CSMA/CD, which stands for Carrier Sense Multiple Access with Collision Detection. It has a defined data rate of 10Mbps.
Fast Ethernet	An IEEE standard extended from 10Base-T Ethernet to support 100Mbps data rate.
Firewall	It is a software layer that controls network access from within and without so that any undesired activity by malicious or snooping parties may be prevented.
Firmware	It is a software code written and saved within the read-only memory (ROM) or programmable read-only memory (PROM). The firmware that is written on the ROM/PROM is retained even when the device is powered off.
FTP	File Transfer Protocol. It is a protocol designed to transfer files over a TCP/IP network.
Full Duplex	It defines the ability of a device to transmit data simultaneously in both upstream and downstream directions over a single line.
Gateway	A gateway is a device that interconnects networks.
Half Duplex	It defines the ability of a device to transmit in one direction at a time over a single line.
HTTP	HyperText Transport Protocol is a common protocol used to connect servers on the World Wide Web, with its primary function being to establish a connection with a web server and transmit HTML pages to the client's browser.
ICMP	Internet Control Message Protocol is a message control and error reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.
IGMP	Internet Group Management Protocol is the standard for IP multicasting on the Internet. It is used to establish host memberships in particular multicast groups on a single network. The mechanisms of the protocol allow a host to inform its local router, using Host Membership Reports, that it wants to receive messages addressed to a specific

		multicast group. All hosts conforming to level 2 of the IP multicasting specification require IGMP.
IEEE		It is the Institute of Electrical and Electronic Engineers. The IEEE is a professional technical body promoting the development and application of technology.
IP Address		At the moment, IP address is a 32-bit binary digit that defines each sender or receiver of information across an IP network.
IPSec		Internet Protocol Security. It is a suite of protocols used to implement secure exchange of packets at the IP layer.
ISP		Internet Service Provider. It is a company that provides individuals or corporations with Internet access and other related services.
LAN		Local Area Network is a group of computers and devices sharing a common communication medium within a small geographical area.
Latency		Latency is a time-delay.
MAC Address		MAC is the abbreviation for Media Access Control. The MAC address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter or router. It allows a network to identify the hardware. Unlike IP addresses, this number is permanent and is therefore a valuable identifier.
Mbps		Mega bits per second. It is a unit of measurement for data transmission indicating a million bits per second.
Multicasting		To transmit a single message to a select group of network recipients.
NAT		Network Address Translations multiplexes multiple private IP addresses for the LAN to a single public IP address on the Internet.
OFDM		Orthogonal Frequency Division Multiplexing. It is a modulation scheme employed by the IEEE 802.11g standard, which combines numerous signals of different frequencies to form a single signal for transmission over a medium.
Packet Filtering		This is a means of discarding unwanted network traffic based on its originating IP addresses or the type of packet/data transmitted.
Parallel Broadband		This exclusive feature enables the connection of multiple broadband routers to a single network.
Ping		Packet Internet Groper is a utility used to determine whether a particular IP address is available online. It works by sending out a packet and waiting for a response from the recipient.
PPPoE		Point-to-Point Protocol over Ethernet is a method for the encapsulation of PPP packets over Ethernet frames.

PPTP		Point-to-Point Tunneling Protocol supports the creation of Virtual Private Networks by ensuring that messages transmitted from one VPN node to another are secure. Users can use PPTP to dial in to their corporate network via the Internet.
Preamble		A preamble is a signal used in network communications to synchronize the transmission timing between two or more systems. Proper timing ensures that all systems are interpreting the start of the information transfer correctly. While a short preamble improves throughput, a long preamble ensures compatibility.
RJ-45		A connector used for Ethernet devices that holds up to eight wires.
Short Slot Time		A reduced short slot time decreases backoff, or the length of waiting time before sending a packet on the LAN, thus improving throughput.
SNMP		Simple Network Management Protocol is a monitoring and controlling protocol. SNMP devices/applications report network activity within to a workstation console so that it may be monitored and controlled.
Subnet Mask		Subnet masking is a method of splitting IP networks into subgroups.
TCP		Transmission Control Protocol enables two hosts to establish a connection and exchange streams of data, guaranteeing delivery of data and that packets will be delivered in the same order in which they were sent.
Throughput		It is the measurable amount of data moved from one place to another within a given time period.
UConfig		The **uConfig** is a unique feature that provides the ability to directly access web-configurable Ethernet devices without the need to know absolute IP addresses. This feature is standard on all the devices that feature web-based configuration.
UDP		User Datagram Protocol is a connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP provides a direct way to send and receive datagrams over an IP network and is used primarily for broadcasting messages over a network.
Unicasting		Communication that takes place over a network between a single sender and a single receiver.
URL		Uniform Resource Locator is the address that defines the location of a file on the World Wide Web.
UTP		Unshielded Twisted Pair is the most common kind of copper wiring designed to reduce crosstalk between copper wires.
VPN		Virtual Private Network is a secure means to join remote networks using comprehensive authentication and encryption. They may be "virtually" joined even across a public network like the Internet by using secure protocols like IPSec amongst others.
WAN		Wide Area Network. It is a communication network that extends over a large geographical area.

WEP		Wired Equivalent Privacy is a wireless data privacy encryption protocol based on a 64-bit or 128-bit shared key algorithm.
WLAN		Wireless Local Area Network is a group of computers and associated devices that communicate with each other wirelessly.

Appendix E: Technical Specifications

Technical Specification	
Industrial Standards	*Wired:* • IEEE 802.3 10Base-T • IEEE 802.3u 100Base-Tx • IEEE 802.3x Flow Control *Wireless:* • IEEE 802.11a • IEEE 802.11b • IEEE 802.11g
WAN Interface	1x Auto MDI/MDI-X RJ45 Ethernet Port for external Cable/ADSL modem
WAN Type	• Static IP • Dynamic IP • PPP over Ethernet (PPPoE) • PPTP • L2TP
LAN Interface	Integrated 4-port 10/100Mbps Switch
Wireless Security	• WPA Personal • WPA Enterprise • WPA2-Personal • WPA2-Enterprise • WPA-Auto-Personal • WPA-Auto-Enterprise • 64/128-bit WEP • 802.1 x Authentication
IP Protocol Set	Dynamic IP Addressing, Static IP Addressing, DHCP server, PPPoE, NAT, TCP, UDP, IP, IPCP, PPTP, PAP, CHAP, SNTP, SNMP, L2TP
VPN Tunneling	Site-to-Site VPN Tunneling
IP Addressing	All Classful/Classless subnets
Built-in-DHCP Server	Yes
DHCP Reservation	Yes
NAT Firewall	Yes

Stateful Packet Inspection (SP I) Firewall	Yes
Universal Plug and Play	Yes
Dynamic DNS Service (Subscribe service)	Yes
Time-based Access Control	Yes
Broadband Internet Sharing	Yes
Support for Watchdog Timer	Yes
Load-Balancing/Fail-Over Internet Connectivity	Parallel Broadband
Virtual Server	IP and Port Forwarding, De-Militarized Zone hosting
IP Packet Filtering	Time-based, TCP Port, Source IP Filtering
URL Filtering	Yes
IP Routing	Static and Dynamic Routing Entry
VPN Client Pass-Through	PPTP, IPSec
Management and Monitoring	SNMP, Web-based Configuration Interface, uConfig
Profile Backup and Restore	Yes
Firmware Upgradeable	Yes
Power Requirements	• Voltage: 5VDC • Current Rating: 3A
Physical and Environment	Temperature: • Operating: 0°C to 55°C • Storage: -20°C to 75°C Humidity: • Operating: 10% to 80% RH • Storage: 5% to 90% rh
Physical Dimension	31mm x 160mm x 170mm (H x W x D)