

Wireless-G Broadband Multimedia Router



networks@work

USER'S MANUAL



NetPassage NP27G

NetPassage NP27G

NetPassage NP27G

NetPassage NP27G

NetPassage NP27G

Manual Number: U-0512-V1.4C

© 2006 Compex Systems Pte Ltd

All Rights Reserved

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

Trademark Information

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

Notice: Copyrights © 2006 by Compex, Inc. All rights reserved. Reproduction, adaptation, or translation without prior permission of Compex, Inc. is prohibited, except as allowed under the copyright laws.

Manual Revision by Daniel

Manual Number: U-0512-V1.4C Version 1.4, September 2006

Disclaimer

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

Your Feedback

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

Fax: (65) 62809947

Email: feedback@compex.com.sg

FCC NOTICE

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

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

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

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

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

Declaration of Conformity

Compex, Inc. declares that the product:

Product Name: **Compex Wireless-G Broadband Multimedia Router**

Model No.: **NetPassage 27G** conforms to the following Product Standards:

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

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

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

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

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

Compex, Inc. also declares that:

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

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

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

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

About This Document

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

The product described in this document, Compex Wireless-G Broadband Multimedia Router Series, NetPassage 27G, is a licensed product of Compex Systems Pte Ltd. This document contains instructions for installing, configuring and using Compex NetPassage 27G. It also gives an overview of the key applications and the networking concepts with respect to the product.

This documentation is for both network administrators and end-users that possess some basic knowledge of networking structures and protocols.

It makes the assumption that the host computer has already been installed with TCP/IP and is ready to access Internet. Procedures for Microsoft Windows 98SE/ME/2000/XP operating systems are included in this document. However, for other operating systems, you may need to refer to your operating system's documentation for networking instructions.

Firmware

Please take note that this User's Manual is written based on NetPassage 27G Firmware Release Version 2.2

Table of Contents

Chapter 1: Introduction.....	1
Chapter 2: Getting to Know Your Product	3
KEY FEATURES BRIEFING.....	3
<i>Basic features</i>	3
<i>Security Features</i>	4
<i>Security Features</i>	5
Chapter 3: Let's Get Going-Hardware Setup.....	7
POWER UP IN 4 STEPS:.....	7
NETWORK APPLICATION EXAMPLES.....	8
Chapter 4: Let's Get Going-Software Setup.....	11
PREPARING THE PCs + ROUTER	11
PART 1 - CONFIGURING THE PCs.....	11
PART 2 - BASIC ROUTER SETUP.....	18
Chapter 5: Advanced Configuration	26
DETAILED CONFIGURATION OF THE ROUTER.....	26
<i>CONFIGURATION : Wireless Setup</i>	27
<i>CONFIGURATION : Wireless Setup : Security Mode</i>	29
<i>CONFIGURATION : Wireless Setup : WDS Configuration</i>	33
<i>Steps to set up WDS in the router</i>	34
<i>CONFIGURATION : Wireless Setup : Wireless Pseudo VLAN</i>	37
<i>Wireless Pseudo VLAN Per Node</i>	37
<i>Steps to set up Wireless Pseudo VLAN Per Node on the router</i>	38
<i>Wireless Pseudo VLAN Per Group</i>	39
<i>Steps to set up Wireless Pseudo VLAN Per Group on the router</i>	39
<i>CONFIGURATION : LAN Setup : Advanced DHCP Server Options</i>	42
<i>Steps to configure Advanced DHCP Server Options in the router</i>	45
<i>CONFIGURATION : WAN Setup</i>	47
<i>CONFIGURATION : Routing</i>	54
<i>Steps to configure Static Routing the router</i>	55
<i>CONFIGURATION : NAT</i>	56
<i>Steps to configure Virtual Servers based on DMZ Host</i>	57
<i>Steps to configure Virtual Servers based on Port Forwarding</i>	58
<i>Steps to configure Virtual Servers based on IP Forwarding</i>	61
<i>CONFIGURATION : Remote Management</i>	62
<i>Steps to set up Remote Management</i>	62
<i>CONFIGURATION : Parallel Broadband</i>	62
<i>CONFIGURATION : Parallel Broadband</i>	63
<i>2 Steps to enable Parallel Broadband on the router</i>	64
<i>HOME USER FEATURES : SMTP Redirection</i>	67

<i>Steps to enable/disable SMTP Redirection.....</i>	<i>67</i>
<i>HOME USER FEATURES : Static Address Translation (SAT).....</i>	<i>68</i>
<i>Steps to enable/disable Static Address Translation.....</i>	<i>68</i>
<i>HOME USER FEATURES : DNS Redirection.....</i>	<i>69</i>
<i>Steps to enable/disable DNS Redirection.....</i>	<i>70</i>
<i>HOME USER FEATURES : Dynamic DNS Setup.....</i>	<i>70</i>
<i>Steps to enable/disable Dynamic DNS Setup.....</i>	<i>71</i>
<i>Steps to manage Dynamic DNS List (DDNS).....</i>	<i>71</i>
<i>HOME USER FEATURES : UPnP Configuration.....</i>	<i>74</i>
<i>HOME USER FEATURES : NETBIOS Name Setup.....</i>	<i>76</i>
<i>HOME USER FEATURES : USB Storage Disk Sharing.....</i>	<i>77</i>
<i>Advanced USB Disk Sharing Functions.....</i>	<i>78</i>
<i>Accessing your USB Hard disk via FTP Server.....</i>	<i>84</i>
<i>Accessing your USB Hard disk via Windows File Server.....</i>	<i>85</i>
<i>Using Windows File Server to map to Network drive.....</i>	<i>86</i>
<i>SECURITY CONFIGURATION : Packet Filtering.....</i>	<i>88</i>
<i>Steps to configure Packet Filtering.....</i>	<i>88</i>
<i>SECURITY CONFIGURATION : URL Filtering.....</i>	<i>92</i>
<i>Steps to configure URL Filtering.....</i>	<i>92</i>
<i>SECURITY CONFIGURATION : Multicast Filtering.....</i>	<i>93</i>
<i>SECURITY CONFIGURATION : Firewall.....</i>	<i>94</i>
<i>Steps to configure SPI Firewall.....</i>	<i>94</i>
<i>SECURITY CONFIGURATION : Firewall Logs.....</i>	<i>98</i>
<i>Steps to view Firewall Logs.....</i>	<i>98</i>
<i>SYSTEM TOOLS : Ping Utility.....</i>	<i>99</i>
<i>SYSTEM TOOLS : System Identity.....</i>	<i>99</i>
<i>SYSTEM TOOLS : Set Router's Clock.....</i>	<i>100</i>
<i>Steps to synchronize the router's Clock.....</i>	<i>100</i>
<i>SYSTEM TOOLS : Firmware Upgrade.....</i>	<i>101</i>
<i>Steps to Upgrade the router's firmware.....</i>	<i>101</i>
<i>SYSTEM TOOLS : Save or Reset Settings.....</i>	<i>102</i>
<i>Steps to Save or Reset Settings on the router.....</i>	<i>102</i>
<i>SYSTEM TOOLS : Reboot Router.....</i>	<i>103</i>
<i>Steps to Reboot the Router.....</i>	<i>103</i>
<i>SYSTEM TOOLS : Change Password.....</i>	<i>103</i>
<i>Steps to change the password.....</i>	<i>103</i>
<i>HELP : About System.....</i>	<i>104</i>
<i>Steps to access the About System page on the Router.....</i>	<i>104</i>
Chapter 6: Printer Server Setup Configuration.....	105
<i>Adding a shared printer via LPR in Windows XP.....</i>	<i>105</i>
<i>Adding a shared printer via LPR in Windows 2000.....</i>	<i>111</i>
<i>Adding a shared printer via LPR in Windows 98/ME.....</i>	<i>117</i>
<i>Removing the shared printer from the router.....</i>	<i>123</i>

Chapter 7: Setting Up Special Printers	124
<i>Manual upload of printer firmware and driver</i>	124
<i>Automatic upload of printer file</i>	127
Chapter 8: Configuring Network Applications	130
<i>Scenario: Accessing USB hard disk & printer via the router</i>	130
I. CONFIGURE YOUR ROUTER #1	130
Appendix A: Troubleshooting	133
SOLUTIONS TO COMMON PROBLEMS	133
Appendix B: Frequently Asked Questions.....	137
ANSWERS TO FREQUENTLY ASKED QUESTIONS	137
Appendix C: NETBIOS Protocol Installation.....	138
Appendix D: Glossary of Terms.....	140
Appendix E: Technical Specifications.....	144
Appendix F: Technical Support Information	147

Chapter 1: Introduction

Thank you for purchasing the Wireless-G Broadband Multimedia router! We are committed to deliver, meet and even exceed your expectations of a high-performance, feature-rich, user-friendly and cost-effective network router. We are excited that you will soon be discovering more about a product that we have proudly developed.

Advanced Features

- *Keep snoopers away with WPA-PSK and 64/128-bits WEP Encryption!*
- *Extend your wireless network infrastructure with WDS (Wireless Distribution System)!*
- *Integrated USB Print Server and Storage Server for network printing and network storage.*

Read on to find out more about these features!

The high-performance Wireless-G Broadband Multimedia router supports an external Cable/ADSL modem for broadband Internet sharing among your wired and wireless network users at the workplace or at home. To simplify your wired network setup, the router supports Auto MDI/MDI-X and will accommodate either type of Ethernet cable to make the right connection. Then on top of its integrated 4-port 10/100Mbps Fast Ethernet switch, the router adopts the 802.11g standard for its wireless operation, employing OFDM technology to deliver data rates of up to 54Mbps within the 2.4GHz band!

Also, because the 802.11g standard is backwards compatible with 802.11b, your existing 802.11b devices can still operate at speeds of up to 11Mbps in the same frequency range with the router.

You will also be pleased to know that the router comes with 2 integrated USB1.1 ports that support USB printers and hard disks. This effectively extends the functional capabilities of the router to include remote network printing and network storage.

To protect your data and privacy, the router supports 64/128-bits WEP (Wired Equivalent Privacy) to encrypt all your wireless transmissions. To ensure better security and data encryption, the router also supports WPA-PSK (Wi Fi Protected Access Pre Shared Key)

Additionally with the support of WDS (Wireless Distribution System), you can noticeably extend the range of your network simply by connecting several routers wirelessly.

The router also ships with the exclusive features like Wireless Pseudo VLAN to ensure data privacy between clients, and Parallel Broadband support to provide scalable bandwidth, load balancing and fail-over redundancy capabilities.

By incorporating VPN client pass-through, built-in DHCP server, URL and Packet Filtering with time-based management, Virtual Servers (IP and Port Forwarding), NAT firewall and SPI firewall, the router lets you do more within your home or office network.

You can share a high-speed Internet connection, speedily exchange files, and play multi-player games with greater flexibility, speed and security you ever thought possible before!

Exclusive!

- *Enhance your wireless network privacy with **Wireless Pseudo VLAN!***
- *Boost network performance and reliability with **Parallel Broadband!***
- *Quickly access your network device's administration setup with **uConfig!***

Read on to find out more about these features!

Chapter 2: Getting to Know Your Product

Key Features Briefing

Your router is endowed with a high-performance design and a rich feature set. To maximize the potential of your purchase, we have highlighted a list of features:

Basic features

Compatible with IEEE 802.11g and IEEE 802.11b standards

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

Static IP, Dynamic IP, PPP over Ethernet, PPTP, and L2TP WAN types

Whether you are going to use your router for broadband Cable or ADSL modem connection sharing, you will be up and running in no time using our fuss-free web-based configuration menu.

Auto MDI/MDI-X crossover support on all Ports

Forget the confusing past! We no longer need to use crossover cables for uplinking! The router supports Auto MDI/MDI-X on all its ports, auto-detecting the inserted cable type.

Wireless Distribution System (WDS) Support

Using WDS, it is possible to wirelessly connect several routers, and in doing so, extend your network to locations where cabling is not possible or is inefficient to implement.

Virtual Servers based on Port-forwarding, IP-forwarding

The router allows you to set up application servers such as FTP file servers and HTTP web servers based on IP-forwarding and Port-forwarding.

Domain Name System (DNS) Redirection

To avoid repetitive setup of DNS addresses for every PC in your network, the router supports DNS redirection, which enables all DNS connection requests from your PCs to be automatically redirected by the router.

Static Routing

By defining a Static Routing entry, you define a specific Router IP address to which data packets will be re-directed to reach a specific IP address or subnet.

Dynamic DNS

The router supports Dynamic DNS. By automatically maintaining the relationship between the fixed URL name and the changing IP, it makes webhosting feasible, with easier implementation, control and flexibility.

De-Militarized Zone (DMZ) hosting

The router supports a form of Virtual Server hosting known as DMZ so that you can operate specific applications that require the opening of multiple TCP/IP ports.

Virtual Private Network (VPN) pass-through

The router is an advanced device that will recognize tunneled packets (IPSec, PPTP) for VPN connections and allow them to pass through.

Universal Plug and Play (UPnP)

UPnP allows you enjoy the benefits of NAT without elaborate configuration procedures. Working alongside an UPnP-aware operating system like Windows XP, other UPnP-enabled devices and applications can negotiate to open certain ports to traverse the NAT device.

Security Features

Understanding the need to protect your data and privacy, we have put in place several security elements to give you a peace of mind.

WPA-PSK and 64/128-bit WEP encryption support for wireless security

The router uses a private key encryption known as Wired Equivalent Privacy protocol with key lengths of either 64-bit or 128-bit, so that data communication in your wireless network can be protected. Additionally, with WPA-PSK, the router provides home and SOHO users with the highest-level security.

Built-in "NAT" firewall

As the router handles the incoming and outgoing traffic of data packets between the internal and external network, it checks whether incoming WAN packets are legitimate replies to requests from LAN users before allowing them to pass into the LAN. This checking provides effective firewall protection because rogue Internet packets will be automatically discarded.

Stateful Packet Inspection (SPI) firewall

More than just a "NAT" firewall, there is a powerful Stateful Packet Inspection (SPI) firewall in the router. Stateful inspection compares certain key parts of the packet to a database of trusted information. SPI Firewall is unlike the normal firewall that only checks the headers of the packets, it also scrutinizes the contents of the packets, ensuring the integrity of the packets.

Internet Access Policies: Time-based Management, URL filtering, Packet filtering

To complement the powerful firewall technologies incorporated into the router product, you can use the comprehensive set of security management features to regulate the types of Internet access permitted. You may set up time-based access policies and block objectionable websites from children, or even set up packet filtering rules to control the transmission of TCP, UDP packets for different ports.

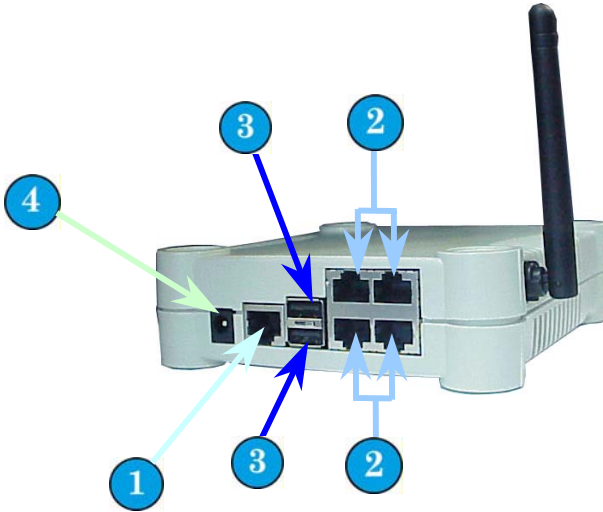
Wireless Pseudo VLAN

The exclusive Wireless Pseudo VLAN feature extends the security advantages of the Ethernet based VLAN to wireless networks. This feature adds another layer of data privacy and protection to the wireless network by isolating individual users/groups of users so that they may not access another user's/group's PC. This is especially useful in a public hotspot or in other public access deployments.

Chapter 3: Let's Get Going-Hardware Setup

Power Up in 4 Steps:

In 4 simple steps, you shall have your router running and functional. After which, you may proceed to the software configuration to get ready to surf the Internet at high-speed!



- 1 Connect the Ethernet cable from your Cable/ADSL modem on one end, and then connect the cable to the socket labeled WAN on the router.
- 2 Connect one of the LAN ports to a PC with a straight Ethernet cable.
- 3 Connect the USB devices (such as USB storage disk or USB printer) to the USB ports of the router.
- 4 Next, plug in the power adapter that is supplied to the main electrical supply, and connect the power plug to the socket on the router.

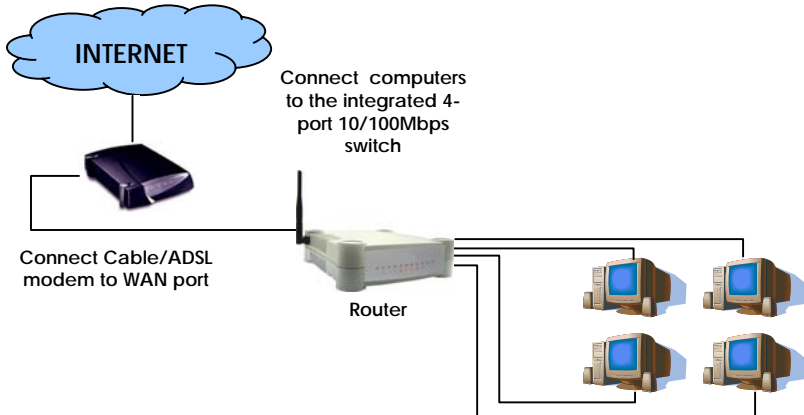
Network Application Examples

Using its web-based configuration interface, you can easily set up your feature-rich router for different network configuration and applications.

We have illustrated three application examples for the router below:

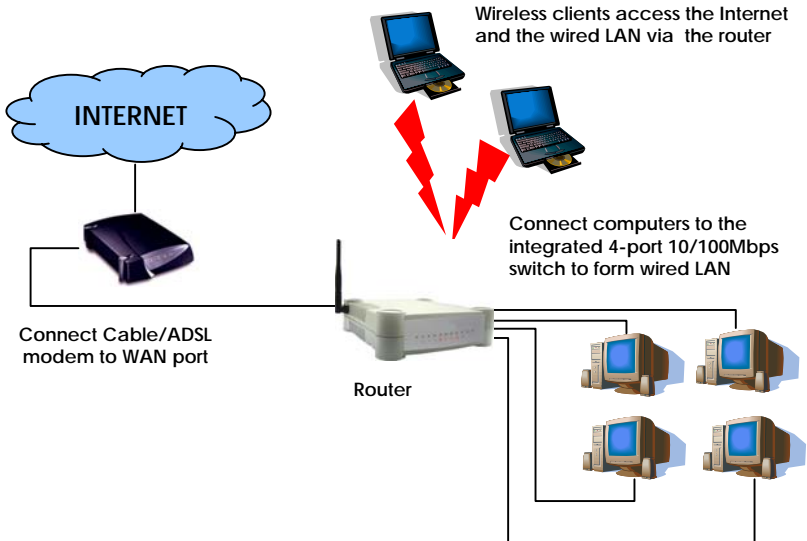
1. **Broadband Internet Access Distribution to Fast Ethernet Network**
2. **Broadband Internet Access Distribution to Fast Ethernet & Wireless Network**
3. **Broadband Internet Access Distribution to Fast Ethernet & Wireless Network using WDS**

1 Broadband Internet Access Distribution to Fast Ethernet Network



In this example, four computers are connected to the integrated 4-port 10/100Mbps Fast Ethernet switch of the router. These computers are able to share a single broadband Internet connection as well as their resources amongst themselves.

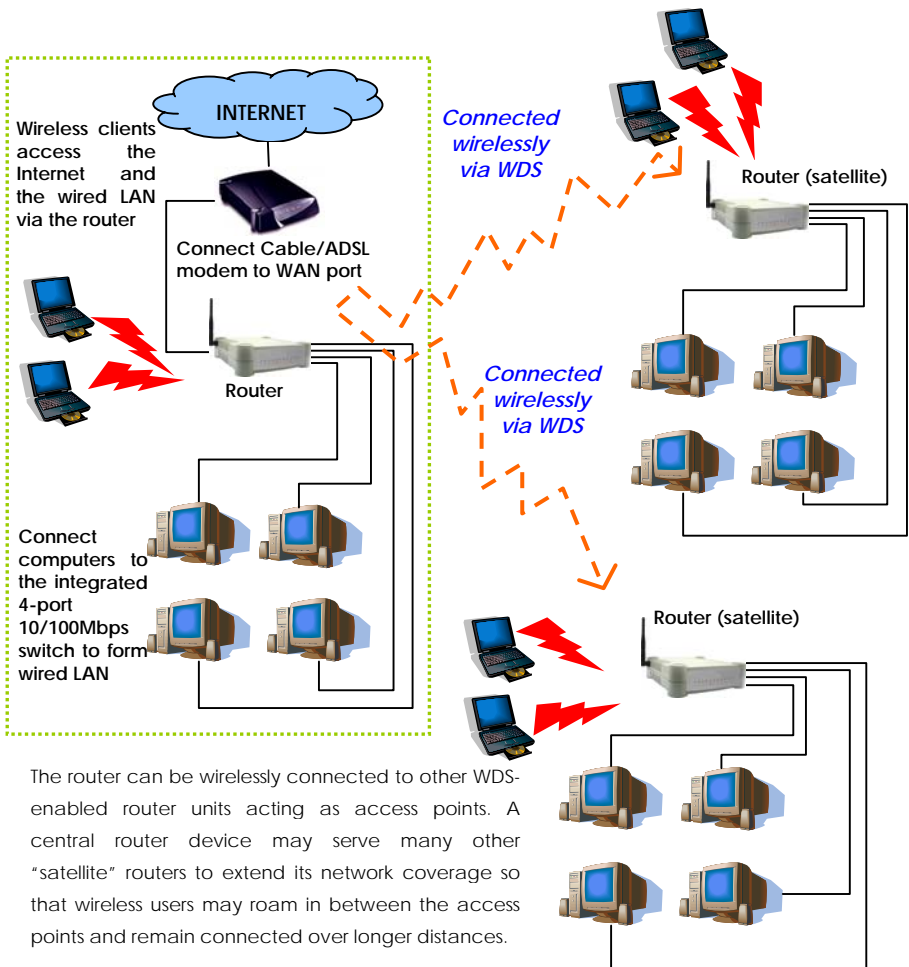
2 Broadband Internet Access Distribution To Fast Ethernet Network & Wireless Network



This example is similar to the previous with the exception of the two additional notebooks set up as wireless clients as illustrated above. Here, the router acts as an access point allowing the wireless clients to access the wired network resources as well as to share Internet access. Your wired network can thus be easily expanded to include wireless clients, enabling them to share network resources and broadband Internet access.

The next example involves using the Wireless Distribution Systems (WDS) feature to wirelessly connect several router units, thus enabling the extension of your network to locations where cabling is not possible or not cost-effective to implement.

3 Broadband Internet Access Distribution to Fast Ethernet Wireless Network using WDS



Chapter 4: Let's Get Going-Software Setup

Preparing the PCs + Router

The router comes with a powerful array of features that can be administered via a web-based configuration interface. This section of software setup will be presented in two essential portions:

Part 1. Configuring the PCs - Concerns the preparation of PCs for network access

Part 2. Basic Router Setup - Covers steps for online access & Internet sharing

Part 1 - Configuring the PCs

The instructions found here will help you to configure each of your computers to communicate with the router.

> For Computers that will be wired to the router:

The first step is to make sure the PC gets an IP address that it will use to communicate with the router and with other PCs across the network. You can begin by setting up your PC to function as a DHCP client, which will obtain an IP address automatically from router. Alternatively, you may want to give your PC a static IP address if you are an expert user.

Whether you choose to allocate static or dynamic IP settings, the next few pages will walk you through the TCP/IP configuration in a step-by-step process. You may skip to Part 1(a), (b), (c) or (d) according to the Microsoft Windows operating system you use. Please ensure that you have an Ethernet or wireless adapter successfully installed in each PC you are configuring.



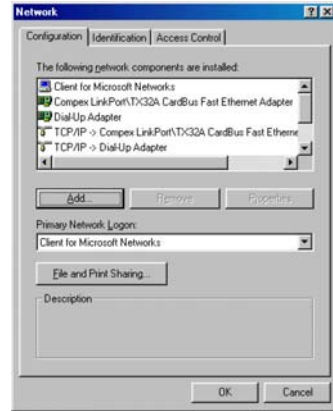
Important: By default, Windows 98SE, ME, 2000 and XP have the TCP/IP protocol installed and set to obtain an IP address automatically.

Part 1(a): Configuring your PC to Dynamically obtain an IP address...

a

If you are using Microsoft Windows 98SE or Windows Millennium

1. Click the **Start** button. Select **Settings** and click the **Control Panel** icon. Then double-click the **Network** icon. You will see the Network dialog on the right.
2. On the **Configuration** tab, highlight the **TCP/IP** line corresponding to your Ethernet adapter and click on the **Properties** button. You will be brought to the **TCP/IP Properties** page below.



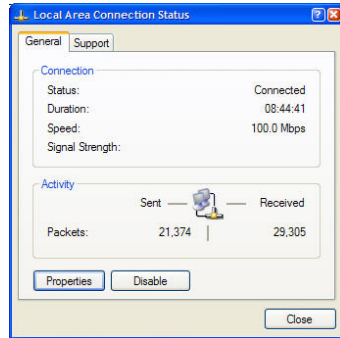
3. Click on the **IP Address** tab, and select **Obtain an IP address automatically**.
4. Next, click the **Gateway** tab, and verify that the **Installed Gateway** field is blank. Now, click the **OK** button.
5. On the Network dialog page, click on the **OK** button.
6. Windows may ask you to restart the PC, if so, click the **Yes** button and allow the PC to restart in order to complete the configuration.

Part 1(b): Configuring your PC to Dynamically obtain an IP address...

b

If you are using Microsoft Windows 2000 or Windows XP

1. Click the **Start** button. Select **Settings** and click the **Control Panel** icon. Then double-click the **Network and Dial-up Connection** (Windows 2000) or **Network Connection** (Windows XP) icon.
2. Double-click the **Local Area Connection** icon for the network adapter applicable to your Internet connection, and click the **Properties** button. You will be brought to the dialog page below.

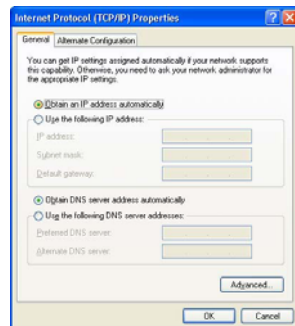


3. On the **General** tab, make sure the box next to **Internet Protocol (TCP/IP)** is checked. Then highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button.



4. Select **Obtain an IP address automatically**.

Then click the **OK** button on this page, and the **OK** button on the previous page it returns you to.



eXpert

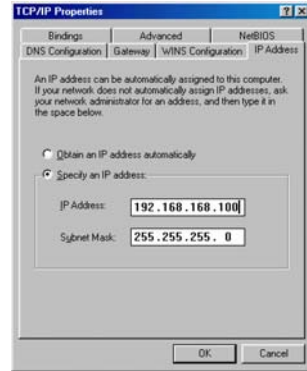
Part 1(c): Configuring your PC with a Static IP address...



If you are using Microsoft Windows 98SE or Windows Millennium

1. To begin the Static IP address configuration, follow steps 1 & 2 of Part 1(a) to get to the page on the right.
2. Click on the **IP Address** tab. Then type in an **IP address** and **Subnet Mask** as 192.168.168.X and 255.255.255.0 respectively, where X is any number from 2 to 254.

(Note that the default IP address of the router is 192.168.168.1)



3. Next, click the **Gateway** tab to see the dialog page on the left.
4. Under the **New Gateway** field, key in the IP address of the router (which is 192.168.168.1 by default). Follow by clicking the **Add** button.



5. Now, select the **DNS Configuration** tab and on the page you see, select **Enable DNS**. Type in a preferred name as the **Host**. Then, follow that up by keying in the IP address of your DNS Server in the **DNS Server Search Order** field and press the **Add** button.
6. You complete by clicking the **OK** button, and then restarting the computer.



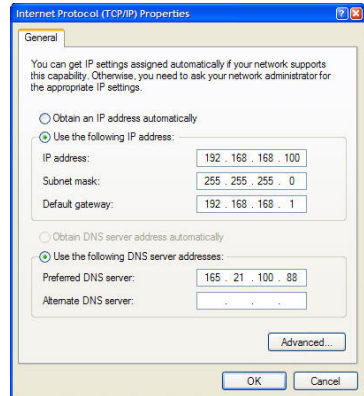
eXpert

Part 1(d): Configuring your PC with a Static IP address...



If you are using Microsoft Windows 2000 or Windows XP

1. To begin the Static IP address configuration, follow steps 1, 2 & 3 of Part 1(b) to get to the page on the right.
2. Select **Use the following IP address**, and then key in 192.168.168.X for the **IP address** field, where X is any number from 2 to 254. Following that, enter 255.255.255.0 for the **Subnet mask**, and key in the IP address of the router as the **Default gateway**.



(Note that the default IP address of the router is 192.168.168.1)

3. Now select **Use the following DNS server addresses**, and then key in the IP address of your DNS server in the **Preferred DNS server field**. Finally, click the **OK** button to complete.



Important: You should not configure more than one computer with the same IP address or the same host name within a network. This will result in a conflict.

Your Internet Service Provider (ISP) should provide the DNS Server's IP address. If you are unsure about it, please contact your ISP.

For Computers that will be connected as Wireless clients:

The first step is similar to that of wired PCs connected to the Fast Ethernet. We have to ensure that the wireless client gets an IP address that it will use to communicate with the router and other PCs across the network.

Hence, refer to Part 1(a) or (b) for the TCP/IP setup instructions, while noting that in Windows XP, you will need to select **Wireless Network Connection** corresponding to the wireless adapter you use.

Once you have completed the IP configuration for the wireless client, you may proceed to set up your wireless client's SSID (Network name) so that it will connect with the router.

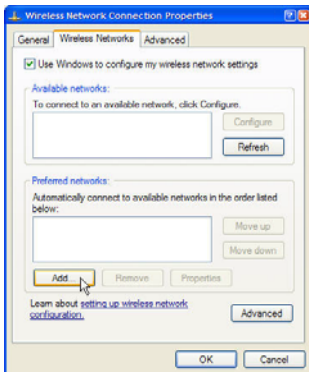
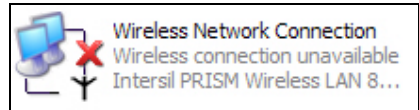


Note for Windows 98SE/ME/2000 users: the following configuration steps for wireless client setup may differ for different wireless Ethernet adapters with vendor specific driver and utilities. Please refer to your adapter's manual for more information.

Part 1(e): Configuring your Wireless Client...

If you are using Microsoft Windows XP

1. Right-click on **Wireless Network Connection** corresponding to the wireless adapter you wish to connect with the router, and click on **Properties**.

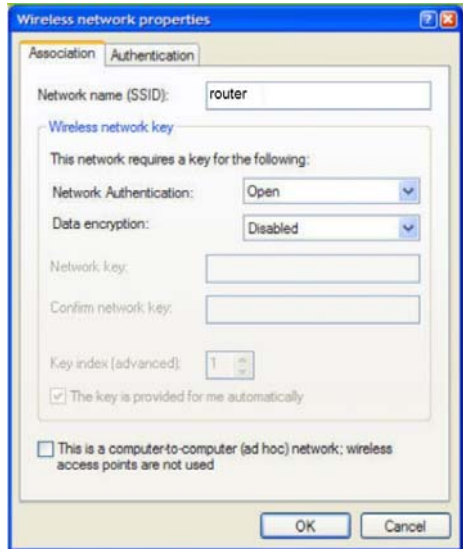


2. On the dialog box presented, click the **Wireless Networks** tab, and click on the **Add** button.

3. Next, key in the **Network name (SSID)** of the wireless network. It must be the same as the SSID of the router in Part 2. For illustration purpose, we typed **router**, which is the default SSID for the router (Take note that the SSID is case-sensitive).

Ensure that the **Network name (SSID)** value is the same for all the wireless clients in the same wireless network.

For now, you may leave the other information as default (**Network Authentication** -> Open; **Data encryption** -> Disabled).



Completing Part 1, we have set up our PCs & wireless clients' IP addressing properties. We are now ready to discuss both the Basic and Advanced setup of the router to go online!

Part 2 - Basic Router Setup

In this basic setup, you will find information on how you may configure the router to function in your network, to access the Internet and begin sharing Internet access and USB devices with your wired and wireless clients.

Part 2(a) : Getting Ready to go Online!

a

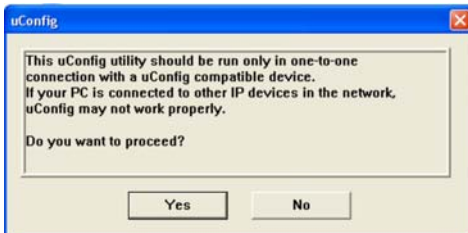
Using uConfig

uConfig: Bringing You to the Web-Based Configuration Without Fail **Exclusive!**

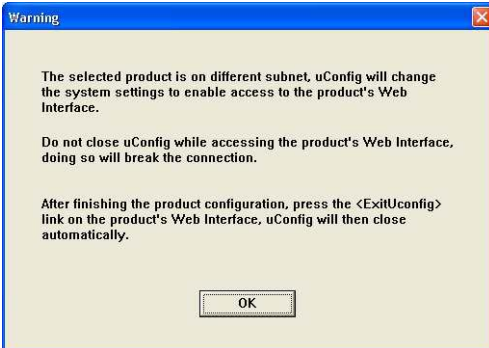
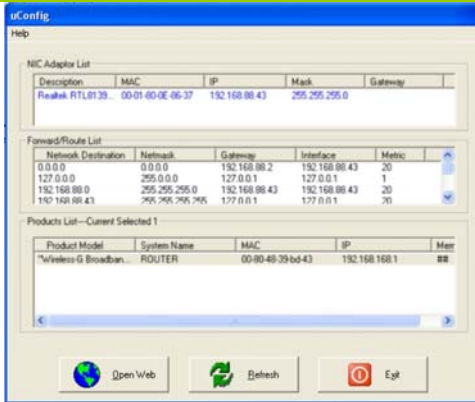
The powerful uConfig utility has been developed to provide you hassle-free access to the router's web-based configuration page. If you do not wish to modify the TCP/IP settings of your PC, or you have changed but forgotten the router's management IP address, uConfig will bring you to the router's setup – every time! It is simple. Ensure that your PC is connected to one of the LAN ports of the router. Follow the 3 simple steps below.

Step 1: Insert the Product CD into your CD-ROM drive. The CD will autorun to the Welcome Page.

Step 2: Click on **Utilities** and then click on **uConfig** to run it. You will see the following screen:



Step 3: When the uConfig window is prompted, click **Yes** to proceed. With the router selected under **Products List**, click on **Open Web**. Click on **OK** and you are done!



Part 2(b): Getting Ready to go Online!

Accessing the Basic Web-based Configuration Interface

1. Open your web browser. At the **Address** bar, enter the IP address of the router, as `http://192.168.168.1` and hit the **Enter** key.



Note: If your PC has a TCP/IP setting differing from the steps described in Part 1, or if you have changed but forgotten the management IP of the router, you may be unable to access the web-configuration page with step 1. The powerful uConfig utility has been developed to bring you directly to the router setup. Please refer to following section on uConfig .

2. The default password is pre-entered in the field provided. Just click on the **LOGIN!** button to access the main page of the router. The default password is 'password'



3. Once you have successfully logged in to access the interface of the router, you are prompted to select the type of setup, Basic or Advanced.

Below is the router Setup Status that provides a summary of the current settings.



4. Click on the radio button next to the **Basic Setup**. Then click on the **Next** button to proceed.

The Setup Wizard page appears, asking you to follow the instructions.

- **Internet Connection**

This functionality lets you specify the type of Internet Connection you want to use.

- **Wireless Setup**

This functionality lets you configure the settings of the router to suit your wireless network.

- **Settings**

This functionality lets you identify the router and create a workgroup for the router. It also lets you set up your local time zone.

From this page, click on the **Next** button to proceed.

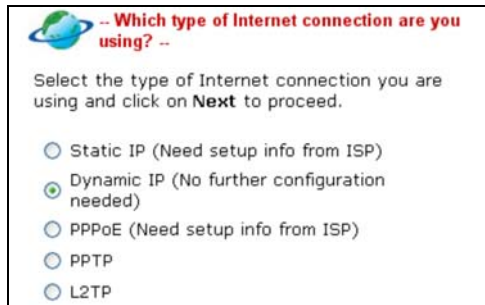


Note: For a clearer understanding of these functionalities, you can refer to the **Help** on the right side of the main page .

5. To set up the WAN connection, select the type of Internet Connection you are using. Click on the **Next** button to proceed.

- **Static IP**

For configuring **Static IP**, you need to click on the **Change** button and enter the IP Address, Network Mask and Gateway IP Address that are provided by your ISP.



- **Dynamic IP**

For **Dynamic IP**, no further configuration is required.

- **PPPoE**

For configuring **PPPoE**, you have to click on the **Change** button and enter the account Username and Password that are provided by your ISP.

- **PPTP**

For configuring **PPTP**, you have to click on the **Change** button and enter the account Username, Password, Network Mask and VPN Server that are provided by your ISP. Take note that VPN Server refers to the IP address of your ISP's PPTP server. The default DHCP server is enabled.

- **L2TP**


For configuring **L2TP**, you have to click on the **Change** button and enter the account Username, Password, Network Mask and VPN Server that are provided by your ISP. Take note that VPN Server refers to the IP address of your ISP's L2TP server.

6. The **WLAN Setup** section lets you configure the following basic wireless parameters :

- **SSID**

The default SSID is 'router'.


For configuring Static IP

IP Address	<input type="text" value="203.120.12.240"/>	
Network Mask	<input type="text" value="255.255.255.0"/>	
Gateway IP Address	<input type="text" value="203.120.12.2"/>	


For configuring PPPoE

Username	<input type="text" value="guest"/>	
Password	<input type="text"/>	

For configuring PPTP

Username	<input type="text"/>		
Password	<input type="text"/>		
IP Address	<input type="text"/>		<input checked="" type="checkbox"/> DHCP
Network Mask	<input type="text"/>		
VPN Server	<input type="text"/>		

For configuring L2TP

Username	<input type="text"/>	
Password	<input type="text"/>	
IP Address	<input type="text"/>	
Network Mask	<input type="text"/>	
VPN Server	<input type="text"/>	

Click on the **Change** button to enter your preferred SSID.

- **Channel**

Click on the down-arrow button next to **Channel**. From the list, select your preferred wireless network channel.

- **Security Mode**

You may choose to enable **WEP** or **WPA-PSK** to secure the wireless connection.

If **WEP** is enabled, select **Hex** or **ASCII** for the key string type to be used. Select **64Bit** or **128Bit** for the transmission key. Then key in the WEP transmission key.

Use the **Reset** button to clear the transmission key.

If **WPA-PSK** is enabled, select **Hex** or **ASCII** for the key string type. Change the default WPA-PSK key that is set to '11111111'. The default **GTK update** is '600' (recommended value).

To proceed, click on the **Next** button.

Please ensure that your router and wireless client settings match.

-- Customising WLAN Setup --

Select the type of wlan connection and click on **Next** to proceed.

SSID: **Change**

Channel:

Security Mode:

Back **Next** **Exit**

Security Mode:

Back **Next** **Exit**

-- WEP key --

Input key and click on **Next** to proceed.

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

Transmission key:

-- WPA-PSK key --

Input key and click on **Next** to proceed.

Key String Type:

Hex (0~9, a~f, A~F) Length 64

Ascii (0~9, a~z, A~Z) Length 8~63

WPA-PSK:

GTK update(seconds): (60~9999)

7. The Wizard will automatically detect if any USB printer or USB storage disk is connected to the router.

If you want to allow access to your storage disk via Internet, click **Yes**. Click **Next** to proceed. Then you will be prompted to enter the following data :

- **System Name**

The default name is 'ROUTER'. You may change it to a better name that will identify your router.

- **NetBios Name**

This is the name under which the router will appear when you browse the MS Windows Network Neighbourhood. You can change it to another name that will help you to identify the router better.

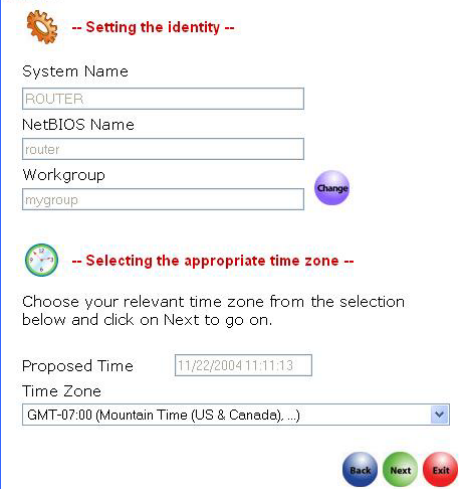
- **Workgroup**

The default name is 'mygroup'. Create an appropriate name for the workgroup of your router and its wireless clients.

- **Time Zone**

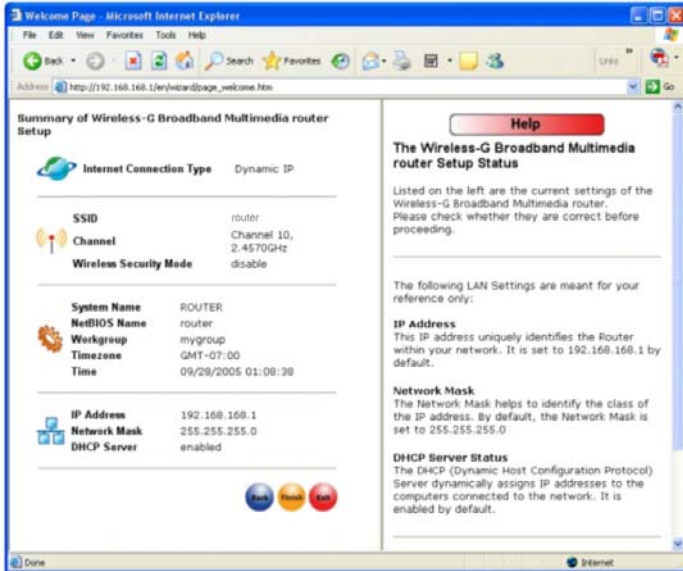
Choose your local time zone from the dropdown list.

To proceed, click on the **Next** button.



The screenshot shows a two-step wizard interface. The first step, titled "-- Setting the identity --", contains three text input fields: "System Name" (with "ROUTER" entered), "NetBIOS Name" (with "router" entered), and "Workgroup" (with "mygroup" entered). A "Change" button is located to the right of the Workgroup field. The second step, titled "-- Selecting the appropriate time zone --", instructs the user to "Choose your relevant time zone from the selection below and click on Next to go on." It features a "Proposed Time" field showing "11/22/2004 11:11:13" and a "Time Zone" dropdown menu currently set to "GMT-07:00 (Mountain Time (US & Canada), ...)". At the bottom right of the wizard are three buttons: "Back" (blue), "Next" (green), and "Exit" (red).

8. You will see the summary of the router setup appear. Check if the settings are correct.



9. Click on the **Back** button to go back to the previous pages and amend your settings or click on the **Finish** button to save the settings and reboot the router.



10. You will be returned to the Login page after 30 seconds.



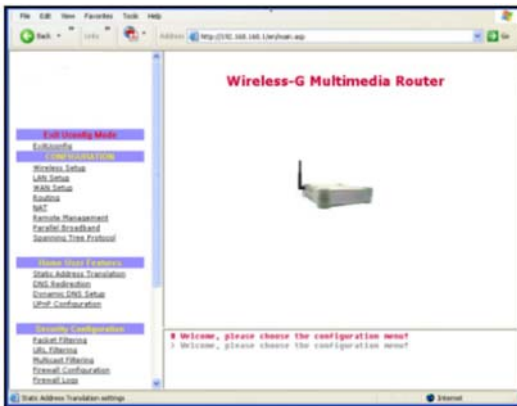
Note: The factory default password to access the web-based interface is <password>. It is recommended that you change to another stronger password by following the steps described in section **System Tools : Change Password**.

Chapter 5: Advanced Configuration *expert*

Detailed Configuration of the Router

This part of the setup for the router is meant for the advanced user who requires more than the essential information to set up a wired/wireless network infrastructure. Adopting a top-down approach to explain the features found on the router, what follows is a detailed walkthrough of the configurable settings available within the web-based administration menu:

Once you have successfully logged in to access the interface of the router, check the radio button next to **Advanced Setup**.



Then click on the Next button to proceed. You shall find a comprehensive list of configurable features as shown on the left.

CONFIGURATION : Wireless Setup

The router supports wireless LAN connectivity that is fully compliant with the IEEE 802.11g and IEEE 802.11b standards. It also employs WPA-PSK or WEP to secure data transmissions of the wireless clients within your network.

- Operation Mode** : The router can operate as an access point.
- Status** : The wireless operation is enabled by default. You can choose to enable or disable the wireless operation. If the wireless operation is disabled, you will not access the wireless setup to edit any configuration.
- WLAN name (ESSID)** : Enter a preferred name for the wireless network. Your wireless clients must be configured with the same ESSID (or sometimes simply referred to as SSID).
- Wireless mode** : Select from the list of wireless modes available:
 - **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 1Mbps, 2 Mbps, 5.5 Mbps, 11Mbps, 6 Mbps, 12 Mbps and 24 Mbps.
- Country Code** : This is where you are located during the connection.
- Channel** : This option allows you to select a frequency channel for the wireless communication.

Transmit Power	: This option allows you to select a specific transmit power for the wireless communication. The Transmit Power controls the signal strength transmitted by the antenna. If the antenna has a weak RF coverage, increase the Transmit Power. If the antenna has a strong RF coverage, decrease the Transmit Power.
Security mode	: The router supports two types of security modes : WPA-PSK and WEP . Two types of WEP private encryption are provided: 64-bit WEP and 128-bit WEP . Click on the Change button to select your security mode.
Closed system	: The router will not broadcast its WLAN name (ESSID) when Closed system is enabled. By default Closed system is disabled.



Note: The ESSID, channel and security mode of the wireless clients attempting to connect to the router must match those of the router.

CONFIGURATION : Wireless Setup : Security Mode

Security plays a vital role in securing wireless 802.11 networks to prevent unauthorised users from accessing and using the network resources. WPA is one of the strongest standards for wireless security.

Having learnt the significance of implementing a security-based network infrastructure, listed here are the steps to configure your router:

The Security mode comes in two types: **WPA-PSK** and **WEP**.

WPA-Pre Shared Key (WPA-PSK) provides strong encryption protection for home users without authentication server.

To set the Security mode to WPA-PSK, follow these instructions:



Select Security Mode

WPA-PSK
 WEP
 Disable

Apply Cancel

1. Under the **CONFIGURATION** command menu, you will find the **Wireless Setup** page. Click on the **Change** button next to the **Security mode**. Then check the radio button next to **WPA-PSK**, followed by the **Apply** button.



Wireless Setup

Operation Mode: **Access Point**

Status: [Click to Disable Wireless](#)

WLAN name (ESSID): router

Wireless Profile: 802.11b/g mixed

Country Code: UNITED STATES-US

Channel: Channel 2. 2.4170GHz

Transmit Power: 20 dBm

Security Mode: **WPA-PSK** [Change](#)

Key String Type:

Hex (0-9, a-f, A-F) Length 64
 ASCII (0-9, a-z, A-Z) Length 8=63

WPA-PSK Passphrase: 11111111

Cipher Type: TKIP

GTK Update: 600 (60-9999 seconds)

Closed System: Enable Disable

Apply

2. You will see the page of the **Wireless Setup** enabled with **WPA-PSK**.
3. Choose whether to use **Hex** or **ASCII** characters to enter your WPA-PSK secret passphrase. You must enter 64 Hex characters or at least 8 ASCII characters respectively.
4. Select an appropriate Cipher Type. AES is the strongest cipher type and is required by the latest WPA2 security standard. **TKIP** is used by the WPA protocol. **Auto** will let the router automatically detect the encryption type used in the network.
5. The GTK (Group Transient Key) update lets you control the frequency at which the group key used to secure multicast/broadcast

traffic among the router and the clients connected to it, will be changed.

6. **Closed System** is disabled by default. If you do not want the router to broadcast its SSID, set **Closed System** to **Enable**.
7. Click on **Apply** to let your settings take effect.

Wired Equivalent Privacy is implemented in the network. It is a security protocol in a wireless local area network.

To set the Security mode to WEP, follow these instructions:

1. Under the **CONFIGURATION** command menu, you will find the **Wireless Setup** page. Click on the **Change** button next to the **Security mode**. Then check the radio button next to **WEP**, followed by the **Apply** button.
2. You will see the page of the **Wireless Setup** enabled with **WEP**, displaying the following parameters:

Transmission key:

This option allows you to select from a list of user-defined encryption keys (1-4).

Key 1-4:

You may enter up to 4 encryption keys. If you selected 64-bit WEP, you will need to enter 10 hexadecimal characters. For 128-bit WEP, it requires 26 hexadecimal characters.

(See the table below).

The table below describes the key length required for 64-bit and 128-bit encryption.

WEP encryption	Hexadecimal	ASCII
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters

3. **Closed System** is disabled by default. If you do not want the router to broadcast its SSID, set **Closed System** to **Enable**.
4. Click on the **Apply** button.

To disable the Security mode (not recommended), follow these instructions:



Select Security Mode

WPA-PSK
 WEP
 Disable

1. Under the **CONFIGURATION** command menu, you will find the **Wireless Setup** page. Click on the **Change** button next to the **Security mode**. Then check the radio button next to **Disable**, followed by the **Apply** button.



Wireless Setup

Operation Mode: **Access Point**

Status :

ESSID:

Wireless Profile:

Country Code:

Channel:

Transmit Power:

Security Mode: **Disabled**

Closed System: Enable Disable

2. You will see the page of the **Wireless Setup** set to **Disable**.
3. Click the **Apply** button.

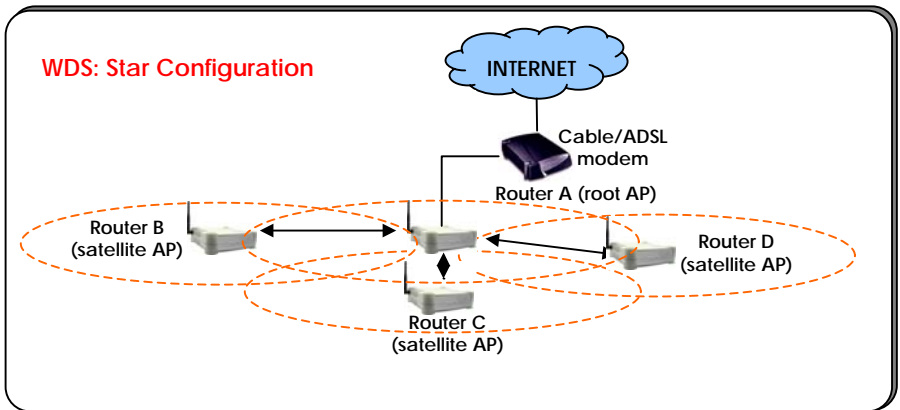
CONFIGURATION : Wireless Setup : WDS Configuration

As described in the network application example 3 in Chapter 3, when WDS (Wireless Distribution System) is enabled, the router can be connected wirelessly with other router units acting as APs (access points) to extend the coverage of the wireless network.

We shall list two popular network configurations the router may be set up to achieve when using WDS:

Star Configuration Infrastructure Network

In a star configuration WDS, the links are established between one root (central) router and several other satellite router APs as depicted below. The satellite routers are positioned to cover an area larger than can be covered by the single root device.

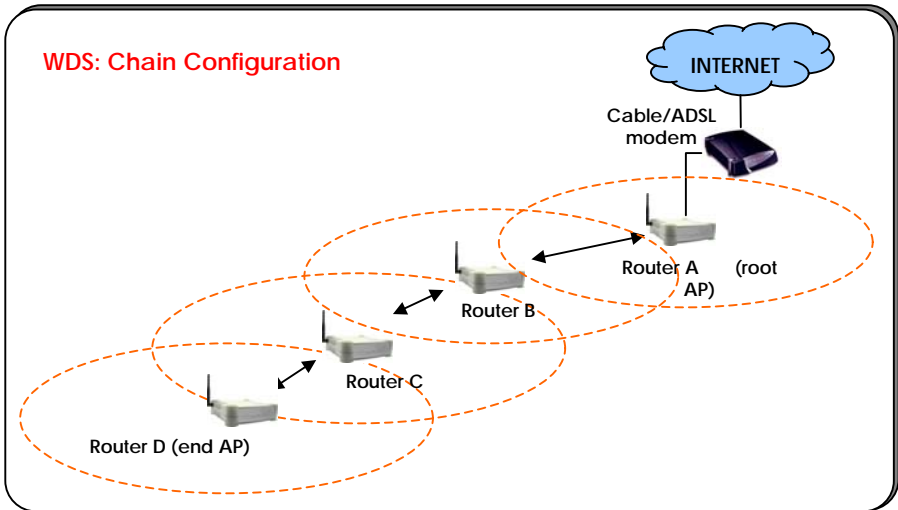


In addition to the expanded area, every router can service its own wired and wireless clients.

In this setup, the root access point has three WDS links enabled to connect with three satellites while each of the satellites has one WDS link enabled to communicate with the root.

Chain Configuration Infrastructure Network

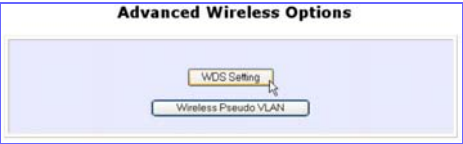

A chain configuration WDS allows the coverage of a long shaped area (a long corridor for instance). The satellite access points are chained together starting from a root access point as illustrated below.



In this setup, the routers at either end of the chain will have one WDS link enabled, while the access points in the middle of the chain will have two WDS links configured to associate with their neighbouring routers upward and downward in the chain.

Steps to set up WDS in the router

Having learnt the flexibility of implementing a WDS-based network infrastructure, listed here are the steps to configure your router for WDS:

- Under the **CONFIGURATION** command menu, you will find the **Advanced Wireless Options** within the **Wireless Setup** page. Click on the **WDS Configuration** button.
 
- By default, you will note that the **WDS Mode** is disabled. Click the **Change** button.
 

3. Make the selection to **Enable** WDS, followed by clicking the **Apply** button.

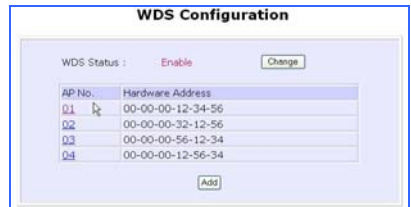


4. In the following page, the non-editable MAC address refers to that of the router. Click on the **Add** button.



5. On the following screen, in the **Hardware address** field, enter the wireless MAC address of the wireless access point (AP) you wish the router to associate with. Then hit the **Add** button.

6. The AP added will be reflected in a table as shown on the right. You may add more access points to be associated to your router.



The table below explains how we have configured the different routers illustration in the configuration examples above:

<p>WDS: Star Configuration</p> <p>Router A has the MAC address of Router B, C and D. Router B, C or D has the MAC address of Router A only.</p>
<p>WDS: Chain Configuration</p> <p>Router A has the MAC address of Router B. Router B has the MAC address of Router A and C. Router C has the MAC address of Router B and D. Router D has the MAC address of Router C.</p>

**Important considerations:**

If the WDS setup contains several access points and each individual access point is required to support several wireless clients, end-to-end throughput may be noticeably lower.

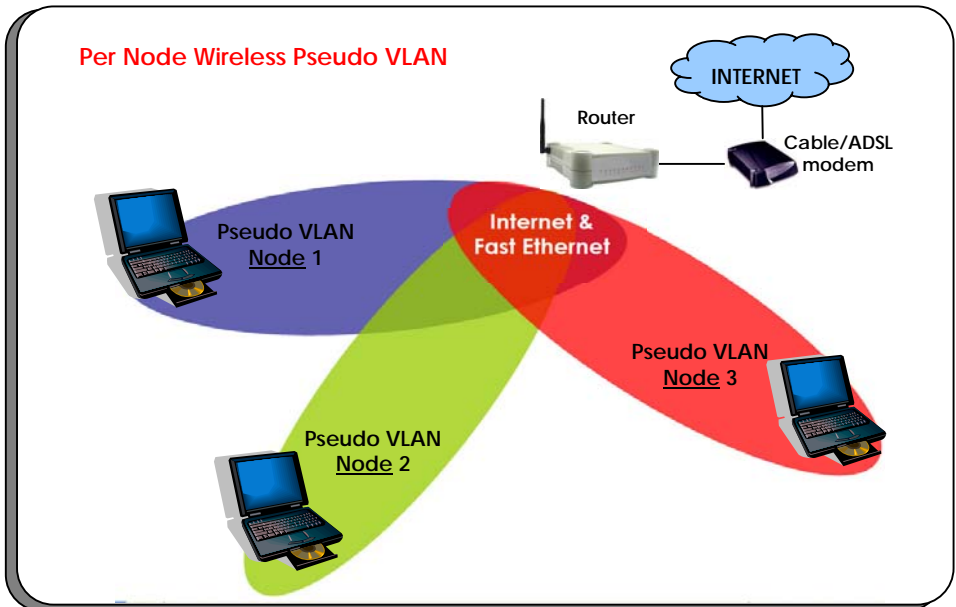
Currently, WDS can only be encrypted using WEP as security mode.

CONFIGURATION : Wireless Setup : Wireless Pseudo VLAN

The Wireless Pseudo VLAN feature on the router has been exclusively created to provide enhanced inter-client security. It is a natural extension of the Ethernet-based VLAN into the wireless network and is especially useful for corporate WLANs or even in a public 'hotspot' establishment.

Wireless Pseudo VLAN segregates a single wireless LAN into multiple virtual LANs. Communication is only possible between wireless nodes of the same VLAN. The router allows you to create virtual LANs containing either a single wireless user, or a group of users. We call this Wireless Pseudo VLAN Per Node and Wireless Pseudo VLAN Per Group respectively.

Wireless Pseudo VLAN Per Node


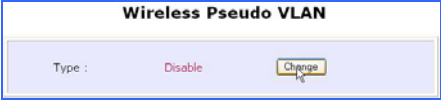
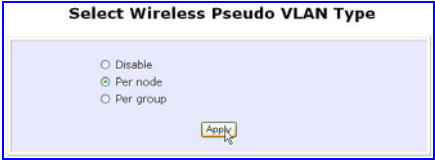


Wireless Pseudo VLAN Per Node, if implemented, segregates every wireless user, or node, in its own Pseudo VLAN. As illustrated in the figure below, while access to the Internet and to the printer connected to the router is unrestricted, wireless clients may not communicate with one another. This implementation of Wireless Pseudo VLAN is most suitable for public premises such as Wi-Fi 'hotspots' at coffee joints or the airport. Users

who log onto such wireless networks can be certain that files on their laptops will not be subjected to prying eyes from other wireless user.

Steps to set up Wireless Pseudo VLAN Per Node on the router

Setting up Wireless Pseudo VLAN Per Node on the router is merely a 3 steps affair:

1. Under the **CONFIGURATION** command menu, you will find the **Advanced Wireless Options** at the bottom of the **Wireless Setup** page. Click on the **Wireless Pseudo VLAN** button.
2. By default, you will note that **Wireless Pseudo VLAN** is disabled. Click the **Change** button.
3. On the next screen, click the **Per node** radio button and hit **Apply** to complete the selection.

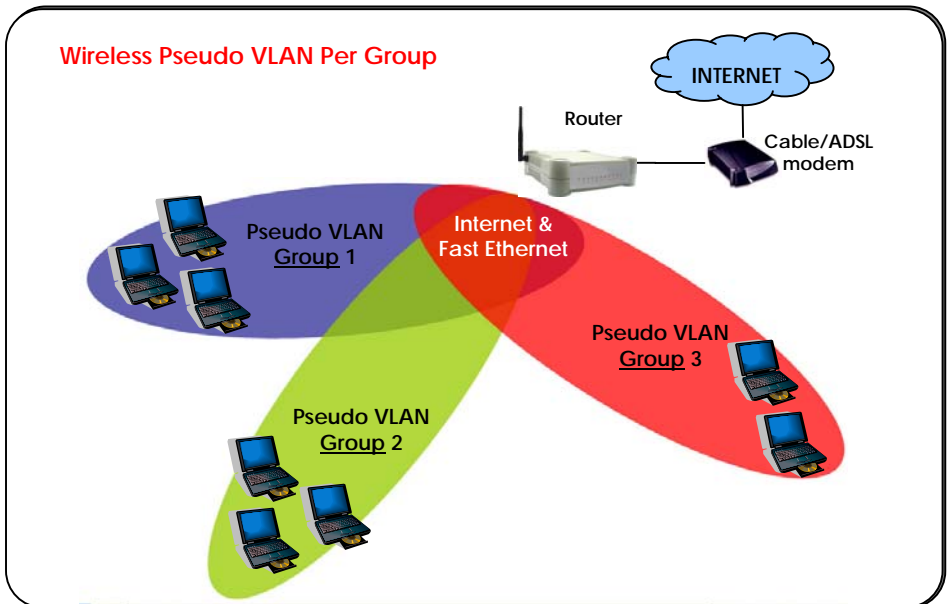
With this, you have successfully set up a Wireless Pseudo VLAN Per Node whereby each wireless user is isolated from the other.

Wireless Pseudo VLAN Per Group

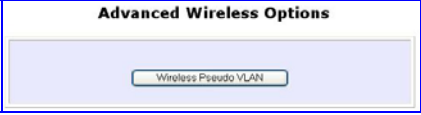
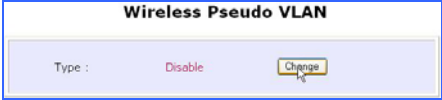
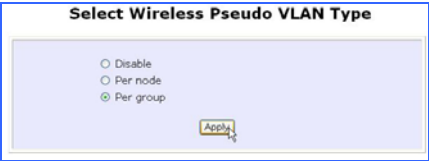
In contrast to single user segregation, Wireless Pseudo VLAN Per Group supports multiple wireless nodes per VLAN. Users grouped in the same Wireless Pseudo VLAN may access files from each other, but are prevented from accessing users from other groups. The router supports four Pseudo VLAN groups.

This implementation of Wireless Pseudo VLAN is useful for corporate workgroups of departmental wireless clients.


Steps to set up Wireless Pseudo VLAN Per Group on the router



Wireless Pseudo VLAN Per Group gives you great flexibility in your wireless network setup, and with the steps below, you may configure private virtual LANs quickly and easily between workgroups:

- Under the **CONFIGURATION** command menu, you will find the **Advanced Wireless Options** at the bottom of the **Wireless Setup** page. Click on the **Wireless Pseudo VLAN** button.
 
- By default, you will note that **Wireless Pseudo VLAN** is disabled. Click the **Change** button.
 
- On the next screen, click the **Per group** radio button and hit **Apply** to complete the selection of your **Pseudo VLAN Type**.
 
- You will be brought to the following screen.

Click on the **Add** button.


- From the **Add Group** drop-down list, choose a group number and then key in the **Hardware Address** (wireless MAC address) of the client before clicking the **Add** button.
 

- You may continue to create more groups or to assign more wireless clients to existing groups by repeating steps 1 to 5 described above.

In the example shown on the right, 3 wireless clients are divided into two Wireless Pseudo VLAN Per Group 01 and 02. Two clients are assigned to Group 01 while the third one is put into Group 02.

Wireless Pseudo VLAN

Type : Per group

Group	Hardware Address
01	aa-11-bb-22-cc-33
01	aa-bb-cc-dd-ee-ff
02	11-22-33-44-55-66



Note: A client can also be a member of more than one Wireless Pseudo VLAN group, For example, if a client is a member of Wireless Pseudo VLAN groups 01 and 03, it will be able to communicate with the other clients in both groups.

CONFIGURATION : LAN Setup : Advanced DHCP Server Options

Please note that **192.168.168.1** is the default IP address assigned to the router, with a **Network Mask** of 255.255.255.0. You may leave them as they are.

LAN Setup: Completing your general LAN Setup

1. Click on **LAN Setup** under **CONFIGURATION**.
2. If you need to change the LAN settings, please remember to click **Reboot Router** under **SYSTEM TOOLS** and hit the **Reboot** button to let the settings take effect.

Learn more from our [DHCP Technology Primer](#)

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 is set by default to 192.168.168.1 . When the DHCP server of the router is enabled (unless you set a different <DHCP Gateway IP address>), this LAN <IP address> would be allocated as the Default Gateway of the DHCP client.
Network Mask	The Network Mask serves to identify the subnet in which your router resides. The default network mask is 255.255.255.0 .
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.	

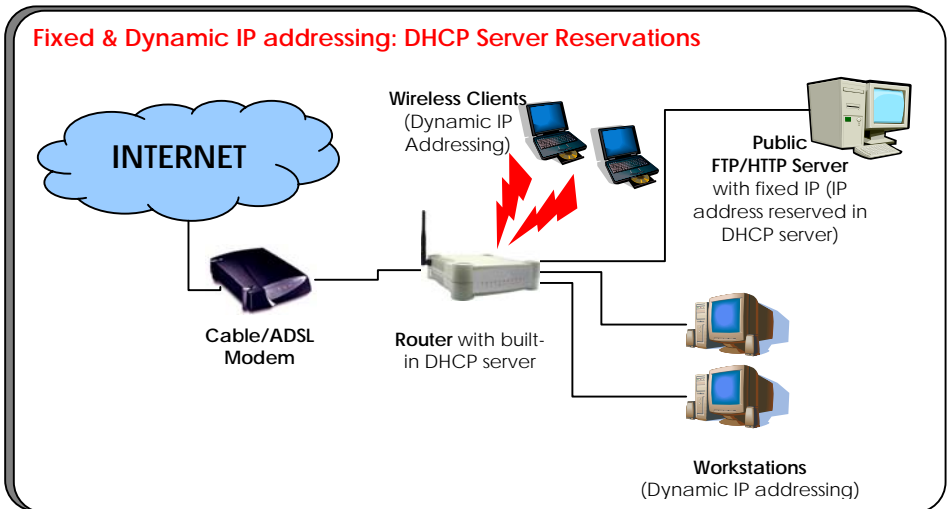
DHCP Start IP Address	This is the first IP address that the DHCP server will assign. The value that you input here should belong to the same subnet as your router. For example, if the IP address and network mask of your router are 192.168.168.1 and 255.255.255.0 respectively, the DHCP Start IP Address should be 192.168.168.X, where X can take any value from 2 to 254. It is pre-set to 192.168.168.100 .
DHCP End IP Address	This is the last IP address that the DHCP server can assign. It should also belong to the same subnet as your router. For instance, 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 can take any value from 2 to 254. It is pre-set as 192.168.168.254 .
DHCP Gateway IP Address	<p>Insert the IP address of the gateway to Internet or of the router if this router is the one connecting to the Internet.</p> <p>If your network uses multiple gateways/routers, you may wish the router to act as DHCP server to a LAN segment while another router/AP connects to the Internet or to another LAN.</p> <p>Though usually, the DHCP server also acts as the Default Gateway of the DHCP Client, the router gives you the option to define a different <DHCP Gateway IP address>, which will be allocated as the Default Gateway of the DHCP client.</p> <p>The DHCP client will thus receive its dynamic IP address from the Router but will access to the Internet or to the other LAN through the Default Gateway defined by the <DHCP Gateway IP address>.</p>
Always use these DNS servers	Leave the Always use these DNS servers unchecked, unless you wish to use the DNS server you have specified below.
Primary DNS IP Address	If you have enabled the Always use these DNS servers option, please enter the IP address of the DNS server to use here.
Secondary DNS IP Address	This optional field is reserved for the IP address of a secondary DNS server.
DHCP Server	If you disable the DHCP server, you will need to manually configure the TCP/IP parameters of each computer in your LAN.

In this section, we shall examine the Advanced DHCP Server Options available to the network administrator.

You can easily manage your network's IP address allocation with the built-in DHCP server found on the router. Once set up as described in Chapter 4, it will automatically and dynamically allocate addresses from a pool, to devices or computers connected to the network. To learn more about DHCP, please turn to the DHCP Technology Primer found on the Product CD.

Under the Advanced DHCP Server Options, we will discuss making DHCP Server reservations for specific IP and MAC addresses. As illustrated below, this feature is useful in situations when you have to set up a publicly accessible FTP/HTTP server that resides within a private LAN. It will require a fixed IP address, but at the same time, your private LAN comprises a group of PCs whose IP address allocation you want the DHCP Server to manage dynamically.

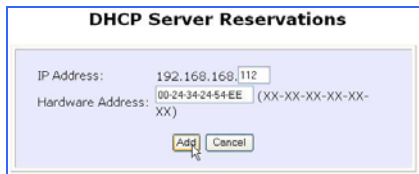
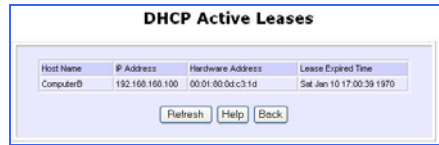
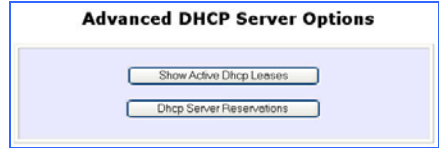
Hence, with the ability to make IP reservations, you can assign a fixed IP to your FTP/HTTP server and then inform the DHCP Server not to assign this IP in its dynamic allocation.



Steps to configure Advanced DHCP Server Options in the router

Listed here are the steps to configure the Advanced DHCP Server options available on the router:

1. Under the **CONFIGURATION** command menu, you will find the **Advanced DHCP Server Options** within the **LAN Setup** page.
2. You may click on **Show Active DHCP Leases** to view the current IP leases managed by the DHCP server. Otherwise, you can click on **DHCP Server Reservations** to reserve a specific IP Address for a device (indicated by its hardware MAC address).



3. To add a **DHCP Server Reservation**, click on the **Add** button.
4. On the following screen, enter the **IP Address** you wish to reserve and the **Hardware Address** (MAC address) of that PC's Ethernet card. Finish up by clicking on the **Add** button.

5. You will see the entered **IP address** and **Hardware Address** tabled as shown on the right. To add more reservations, repeat steps 3 through 4 above or click on the **Back** button to return to the previous page.





Note: The reserved IP address must not be within the range of the DHCP Start and End IP addresses in the Router's LAN Setup configuration page.

An invalid date and time shown under the Expires column in the Show Active DHCP Leases table indicates that the router's clock has not been set. Refer to Chapter 5, section on SYSTEM TOOLS – Set Router's Clock.

CONFIGURATION : WAN Setup

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

- i. **Cable Internet where your ISP dynamically assigns a WAN IP address** to you, refer to WAN Setup - Cable Internet with Dynamic IP Assignment.
- ii. **Cable Internet where your ISP provides you with a fixed WAN IP address** (or a range of fixed IP addresses), refer to WAN Setup - Cable Internet with Static IP Assignment.
- iii. **ADSL Internet that requires standard PPP over Ethernet (PPPoE)** for authentication, refer to WAN Setup - ADSL Internet using PPP over Ethernet (PPPoE).
- iv. **ADSL Internet that requires standard Point-to-Point Tunneling Protocol (PPTP)** for authentication, refer to WAN Setup – ADSL Internet using Point-to-Point Tunneling Protocol (PPTP).
- v. **ADSL Internet that requires standard Layer 2 Tunneling Protocol (L2TP)** for authentication, refer to WAN Setup – ADSL Internet using Layer 2 Tunneling Protocol (L2TP). L2TP is an extension to the PPP protocol that enables ISPs to operate VPNs. It is the best combination of PPTP (from Microsoft) and L2F (from Cisco Systems). It has the most similar parameters of the PPTP except it does not support the DHCP server.

WAN Setup - Cable Internet with Dynamic IP Assignment



Selecting the Correct WAN Type

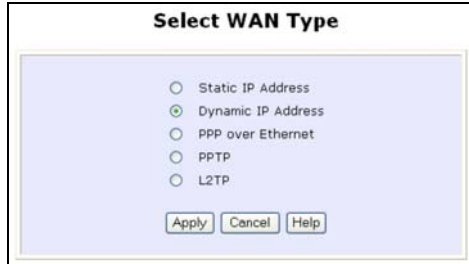
The router is pre-configured to support a WAN type that dynamically obtains an IP address from the ISP. However, you may verify the WAN settings with the following steps:

1. Under the **CONFIGURATION** on the command menu, click on **WAN Setup**.
2. On the **WAN Dynamic Setup** screen that follows, verify that

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

the **WAN Type** reads **Dynamic (DHCP)** in red colour. Otherwise, click on the **Change** button.

3. Simply select **Dynamic IP Address** and hit the **Apply** button.
4. Please remember to click **Reboot Router** under **SYSTEM TOOLS** and hit the **Reboot** button to let the settings take effect.



Important: Please note the exceptional cases described below for certain Cable Internet Service Providers.

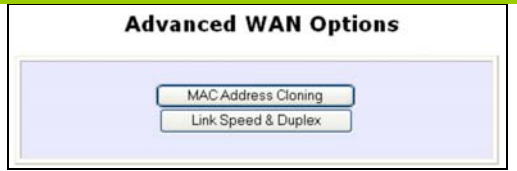
Note: There are exceptional cases where additional configuration is required before your ISP allocates an IP address to the router.

- b. Certain ISPs log the MAC address of the first device used to connect to the broadband channel and will not release a WAN IP address unless the MAC address matches the one in their log. Therefore, if yours is not a new Cable Internet subscription (i.e. your PC was formerly connected directly to your cable modem), refer to **steps 5 - 7** to clone the “approved” MAC address onto the router.
- c. Certain ISPs require authentication through a DHCP Client ID before releasing a public IP address to you. The router uses the System Name in the System Identity as the DHCP Client ID.

Therefore, if this is the case, refer to your ISP for the correct DHCP Client ID to be set and follow **steps 8 - 10** to accomplish the setup.

5. Steps 5 - 7 are for those who need to clone their Ethernet adapter’s MAC address.

In the **WAN Setup** found under the **CONFIGURATION** command menu, you will see the **Advanced WAN Options**. Click **MAC Address Cloning** to continue.



6. Simply click on the **Clone** button so that your router clones the ISP-recognized MAC address of your Ethernet adapter.



Take note: (If required, you may reset the router's MAC address to its factory default by clicking **Reset** on that same page)

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

8. Steps 8 - 10 are for those who need to set up the **System Name** in **System Identity** so that your ISP can authenticate it as a valid DHCP Client ID.

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



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

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

WAN Setup - Cable Internet with Static IP Assignment

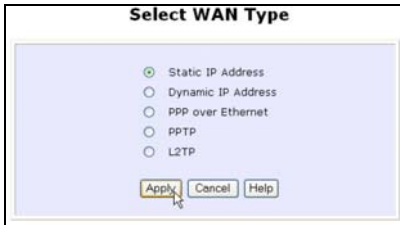


Selecting the Correct WAN Type

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

IP Address : 203.120.12.47
 Network Mask : 255.255.255.0
 Gateway IP Address : 203.120.12.15

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



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

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



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

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



Selecting the Correct WAN Type

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

1. Under the **CONFIGURATION** on the command menu, click on **WAN Setup**.
2. Access the **Select WAN Type** page and choose **PPP over Ethernet** before clicking the **Apply** button. You will then be brought to the following page requiring your inputs.
3. For **Username**, key in your ISP assigned account name (e.g. guest for this example), followed by your account **Password**.
4. Select **Always-On** if you want your router to always maintain a connection with the ISP. Otherwise, you may select **On-Demand**. The router will then connect to the ISP automatically when it receives Internet requests from the PCs in your network.

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

WAN Setup – ADSL Internet using PPTP



Selecting the Correct WAN Type

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

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

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

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

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

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

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

WAN Setup – ADSL Internet using L2TP



Selecting the Correct WAN Type

If you subscribe to an ADSL service using Layer 2 Tunneling Protocol (L2TP) authentication, you can set up your router's WAN type from the steps that follow. For example, if the ISP provided you with the following set up information, you can set up your WAN as described below:

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

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

2. Access the **Select WAN Type** page and choose **L2TP** before clicking the **Apply** button. You will then be brought to the following page requiring your inputs.

3. Fill in the information provided by your ISP in the **IP Address**, **Network Mask** and **VPN Server** fields, followed by clicking the **Apply** button.
4. Please remember to click **Reboot Router** under **SYSTEM TOOLS** and hit the **Reboot** button to let the settings take effect.

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

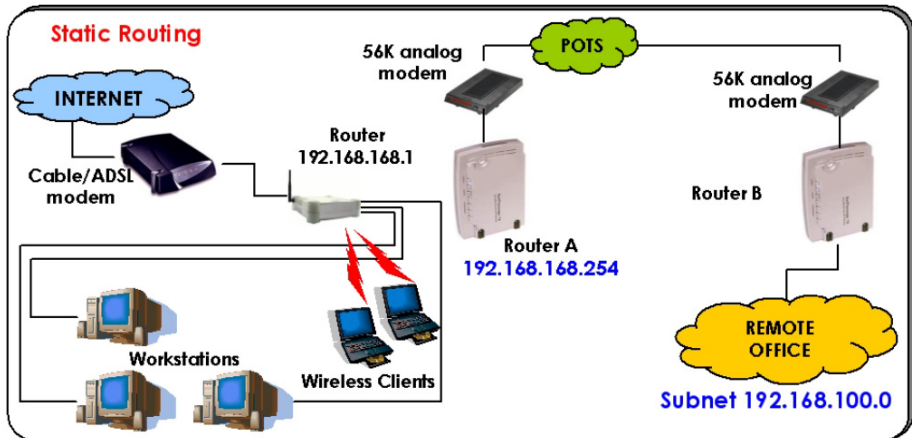
CONFIGURATION : Routing

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



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

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



In this network, the main office of subnet 192.168.168.0 contains two routers: the office is connected to the Internet via the router (192.168.168.1) and to the remote office via Router A (192.168.168.254). The remote office resides on a subnet 192.168.100.0.

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

Steps to configure Static Routing the router

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

- Under the **CONFIGURATION** command menu, click on **Routing** to be brought to the **System Routing Table** shown (on the right).

Initially, the table will contain the default routing entries built into the router.

System Routing Table

Destination	Network Mask	Gateway
192.168.168.43	255.255.255.255	*
127.0.0.0	255.255.255.0	*
192.168.168.0	255.255.255.0	*

Static Routing Table

Destination	Network Mask	Gateway

- Click on the **Static Routing Table** button above.
- On this page, click the **Add** button.

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

Static Routing Table

Destination IP Address :

Destination Net Mask :

Gateway IP Address :

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

Static Routing Table

Destination	Network Mask	Gateway
192.168.100.0	255.255.255.0	192.168.168.254

CONFIGURATION : NAT

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

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

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

Learn more from our [NAT Technology Primer](#)

Under the **CONFIGURATION** command menu, click on **NAT**. NAT is enabled by default. To disable it, click **Disable**. Click **Apply** to effect the setting.



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

Steps to configure Virtual Servers based on DMZ Host


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

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

When using DMZ on a PC, any reply not recognized by the router 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.


Here are the steps to set it up:



- Under the **CONFIGURATION** command menu, click on **NAT**. You will find the **Advanced NAT Options** available near the bottom of the page.
- Click the **DMZ** button to configure Virtual Servers based on De-Militarized Zone host.

- On the **NAT DMZ IP Address** page, you have to define the **Private IP Address** of the DMZ host. In this example, we keyed in the private IP address for the PC we wish to place within the DMZ : 192.168.168.55

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



- Remember to click the **Apply** button.

**NOTE:**

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

Steps to configure Virtual Servers based on Port Forwarding

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

Here are the steps to set it up:



1. Under the **CONFIGURATION** command menu, click on **NAT**. You will find the **Advanced NAT Options** available near the bottom of the page.
2. Click the **Port Forwarding** button to configure Virtual Servers based on Port Forwarding.

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



Add Port Forward Entry

Known Server

Server Type : HTTP

Private IP Address :

Add Help Cancel

Custom Server

Server Type :

Protocol : TCP

Public Port : Single

From :

To :

Private IP Address :

Private Port From :

Add Cancel

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

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

Known Server

- Server Type** : Select from the drop-down list of known server types: (HTTP, FTP, POP3 or Netmeeting).
- Private IP Address** : Specify the LAN IP address of your server PC running within the private network.

Custom Server

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

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


Port Forward Entries

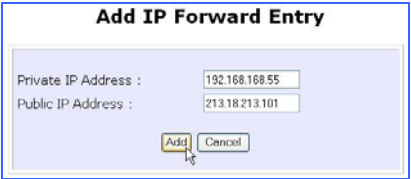
Server Type	Protocol	Public Port	Private IP	Private Port
HTTP	TCP	80	192.168.168.55	80


Steps to configure Virtual Servers based on IP Forwarding

When you have subscribed for more than one IP address from your ISP, you may define Virtual Servers based on IP Forwarding for which all Internet requests, regardless of ports, are forwarded to defined computers in the private network.

If you require more information of its function, please refer to the NAT Technology Primer on the Product CD. Here are the steps to set it up:

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

The screenshot shows a window titled "Advanced NAT Options" with three buttons: "DMZ", "Port Forwarding", and "IP Forwarding". The "IP Forwarding" button is highlighted with a mouse cursor.
- Click the **IP Forwarding** button to configure Virtual Servers based on IP Forwarding.
- At the next screen **Add IP Forward Entry**, you have to specify a **Private IP Address** and a **Public IP Address**. In this example, we would like all requests for 213.18.213.101 to be forwarded to a PC with **Private IP Address** 192.168.168.55. Click the **Add** button to continue.
 

The screenshot shows a form titled "Add IP Forward Entry". It has two input fields: "Private IP Address" with the value "192.168.168.55" and "Public IP Address" with the value "213.18.213.101". Below the fields are "Add" and "Cancel" buttons. A mouse cursor is pointing at the "Add" button.
- The **IP Forward Entries** page will reflect your new addition.
 

The screenshot shows a table titled "IP Forward Entries". The table has two columns: "Private IP" and "Public IP". The first row contains the values "192.168.168.55" and "213.18.213.101". Below the table are "Add" and "Back" buttons. A mouse cursor is pointing at the "192.168.168.55" value.



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

CONFIGURATION : Remote Management

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

Steps to set up Remote Management

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

Remote Management

Remote Http Port : (disable:0 default:80)

1. Under the **CONFIGURATION** command menu, click on **Remote Management**, and you will be brought to the following screen.
2. By default, **Remote Management** is disabled. (To disable Remote Management, just enter 0 for **Remote Http Port**).
3. To enable **Remote Management**, enter a port number that is not being used by other applications in the network. Please take note that it is recommended to use a different port number other than port 80 because some ISP block port number 80.



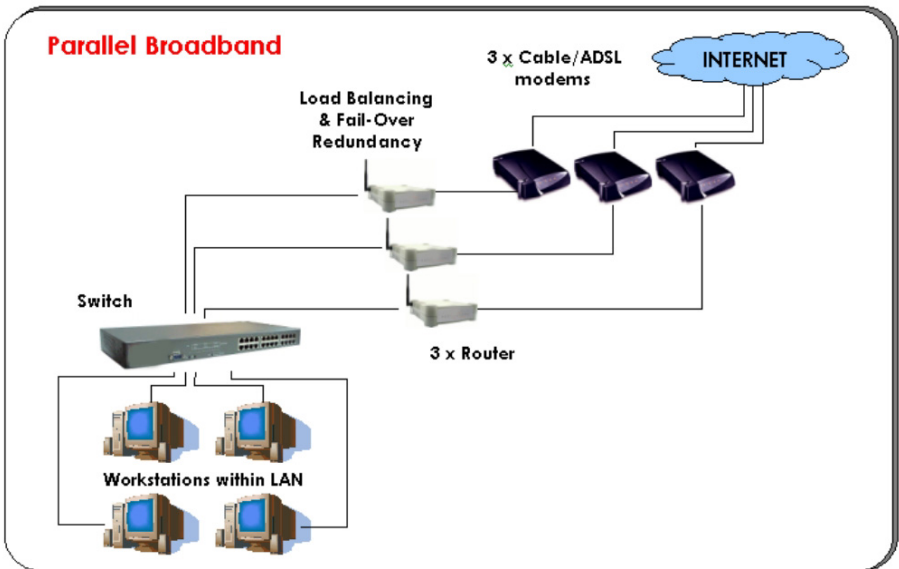
In view of preventing unauthorized management from a remote location, please remember to replace the default password with a new one.

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

CONFIGURATION : Parallel Broadband **Exclusive!**

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

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



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

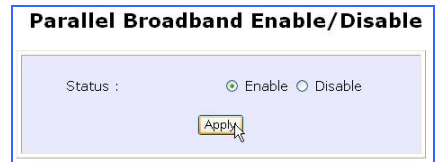
2 Steps to enable Parallel Broadband on the router

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

- each of the routers is connected to an Ethernet port in the network as illustrated above or
- the routers are interconnected by WDS or
- the routers are wired to each other.

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

1. Under the **CONFIGURATION** command menu, click on **Parallel Broadband**.
2. Next simply select **Enable** and click the **Apply** button to make the changes effective.
3. Repeat this for the other routers in your network and they will communicate with each other and assign each new user to the router that has the smallest load, so that there is approximately the same number of users on each router.



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

CONFIGURATION : Email Notification

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

WAN PPPoE Setup

WAN Type : **PPPoE**

Username :

Password :

On-Demand Always-On

Idle Timeout (0:disabled) seconds

Reconnect Time Factor seconds

Status : **Connecting**

IP Address
Network Mask
Default Gateway
Primary DNS
Secondary DNS

Email Notification

Email Notification: Enable Disable

Email address of Receiver:

IP address of Mail Server : Needs

Authentication

User Name :

Password :

Email address of Sender:

Status :

1. Under the **CONFIGURATION** command menu, click on **WAN PPPoE Setup** or **WAN PPTP Setup**, and you will be brought to the following screen.
2. Click on the **Email Notification** button.
3. Click on the **Enable** button and key in the following fields as described below:

Email address of Receiver:

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

IP address of Email Server:

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

User Name:

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

Password:

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

Email address of Sender:

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

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

4. Then click on the **Apply** button.

HOME USER FEATURES : SMTP Redirection

Using this feature, it accepts mails from anyone whose ISP blocks incoming connections on the SMTP port and relays the mails to an alternate port that is not blocked.

Steps to enable/disable SMTP Redirection

Here are two simple steps to activate or deactivate this feature:

1. Under the **HOME USER FEATURES** command menu, click on **SMTP Redirection**.

2. Select **Enable** next to **SMTP Redirection**. This will help the subscriber automatically redirect to the correct email server. The **Need Auth** checkbox is ticked by default.

3. Key in the **Email Server** and **Password**. These mandatory fields are the subscriber's ISP server account for receiving and sending emails.

Status	Explanation
Can Use!	This message tells you that you can use this function after a maximum of 4 subscribers have sent emails at the same time.
Cannot Use!	This message tells you that you cannot use this function.
Can Use but it will be slowly!	This message tells you that you can use this function only after each time a subscriber sends an email.
Down!	This message tells you that your router fails to connect to the server.

The **Message** field will display error messages if the SMTP server faces some problems.

4. Click **Add**.

HOME USER FEATURES : Static Address Translation (SAT)

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 router 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 router 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 router 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 (the router).

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



Note: For SAT to function properly:

1. The IP address of the notebook should belong to a different subnet from the LAN IP address of the router.
2. The <Default Gateway> in the TCP/IP settings of your notebook should NOT be left blank.

Steps to enable/disable Static Address Translation

Here are two simple steps to activate or deactivate the Static Address Translation feature:

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)



HOME USER FEATURES : DNS Redirection

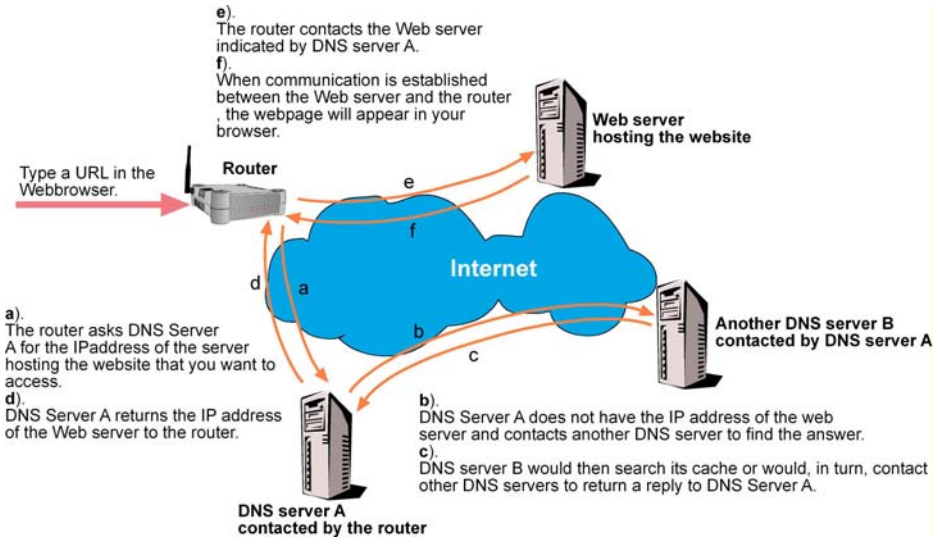
When you enter a URL in your Internet browser, the browser requests for a name-to-IP address translation from the Domain Name System (DNS) servers to be able to locate the web server hosting the website you want to access.

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

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

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

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



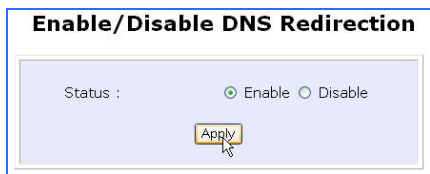


Note: For Internet access, please do NOT leave the DNS Server field of the PC's TCP/IP Properties blank. Simply key in any legal IP address for it (e.g. 10.10.10.10) even though you do not have the exact DNS IP address.

Steps to enable/disable DNS Redirection

Here are two simple steps to activate or deactivate the DNS Redirection feature:

1. Under the **HOME USER FEATURES** command menu, click on **DNS Redirection**.



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

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

HOME USER FEATURES : 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.

Steps to enable/disable Dynamic DNS Setup

Here are two simple steps to activate or deactivate the Dynamic DNS Setup feature:

1. Under the **HOME USER FEATURES** command menu, click on **Dynamic DNS Setup**.
2. You may then choose to **Enable** or **Disable** Dynamic DNS here, followed by clicking the **Apply** button. (Note: Dynamic DNS is disabled by default)



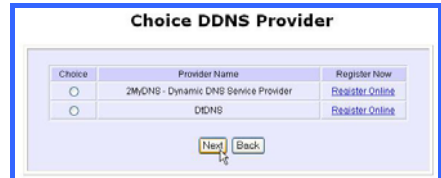
Steps to manage Dynamic DNS List (DDNS)

Here are simple steps to manage the Dynamic DNS List feature:

1. Under the **HOME USER FEATURES** command menu, click on **Dynamic DNS Setup**.
2. If you have already created a list earlier, click on the **Refresh** button to update the list.



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



Choice :

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

Provider Name :

This is the name of your preferred DDNS provider.

Register Now :

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

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

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

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

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

Next Back

Enter your **Domain Name**.

Select **Auto Detect** to let the DDNS server learn your current WAN IP address. Enter your DDNS account **Username** and **Password**.

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

2. (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 on the Add button to save the new addition.

Provider : 2MyDNS - Dynamic DNS Service Provider

Domain Name : ▼

WAN IP :

Username :

Password :

Wildcard : YES NO

Mail Exchanger :

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

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

Domain Name	Update Status
MyCoding.mycoding.com	
people.onlinepeople.net	

Add Refresh

Provider : 2MyDNS - Dynamic DNS Service Provider
 Domain Name : people . onlinepeople.net
 WAN IP : Auto Detect
 Username : lester
 Password : *****
 Wildcard : YES NO
 Mail Exchanger : mxn_tay@powemetic.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 table of **Choice DDNS Provider** check the radio button next to the **DtDNS**. Then click on the **Next** button to proceed.

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

Next Back

Enter your **Domain Name**.

Select **Auto Detect** to let the DtDNS server learn your current WAN IP address. Enter your DtDNS account **Username** and **Password**.

Provider : DtDNS
 Domain Name : . 20-qdms.com
 WAN IP : Auto Detect
 Password :

Add Reset Back

2. Then click on the Add button.

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



HOME USER FEATURES : UPnP Configuration

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 router 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

1. Under the **HOME USER FEATURES** command menu, click on **UPnP Configuration**



2. Simply choose **Enable** or **Disable** for the **Status** of UPnP.

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

HOME USER FEATURES : NETBIOS Name Setup

Under the **HOME USER FEATURES** command menu, click on **NETBIOS Name Setup**.



NETBIOS Name: This is the name used to identify your router when browsing the Microsoft network.

Workgroup: Computers within the same workgroup that are connected to a network are allowed to share data. Therefore,

setting your PCs in the same workgroup as the router allows you to see the router when browsing your **Windows Neighbourhood/My Network Places**, and to access the storage disk(s) connected to the router.

NETBIOS is a protocol that allows applications on the different computers in a LAN to communicate. It is installed by default on the Microsoft Windows Operating System. Refer to Appendix C "NETBIOS Protocol Installation" on page 117 for details.



Note: Please note that to be able to search for the USB disk attached to your router, you need to:

1. Set a NETBIOS name and workgroup for the Router.
2. Set your PCs to be within the same workgroup as the router.
3. Set your access rights to **Read** or to **Read and Write**.

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

HOME USER FEATURES : USB Storage Disk Sharing

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: Router lets you share the whole storage disk instead of individual folders.

1. 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.

2. If you wish to transfer data via FTP, enable the **FTP Server** option.

A. To enable FTP Server

using your Web browser or an 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 (refer to page 78) 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 networking

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 (refer to page 80) to allow only users with authorized username and password to use the file server to access your storage disk.

Refer to page 85 for instructions on how to access your storage disk from Windows networking.

Advanced USB Disk Sharing Functions

In this **Advanced USB Disk Sharing Functions** section, you can:

- View the list of USB storage devices connected to the router.
- View the number of users connected via FTP and via Windows.
- Create and delete FTP user accounts.
- Create and delete file server user accounts for accessing the storage disk from Windows networking.



USB HDD List

Under the **Advanced USB Disk Sharing Functions**, click on **Storage Disk List**. This screen displays the list of USB storage disks connected to the router.



Device Name: This is the name of your USB device.

Share Name: This is the name generated by the router to identify the USB devices.

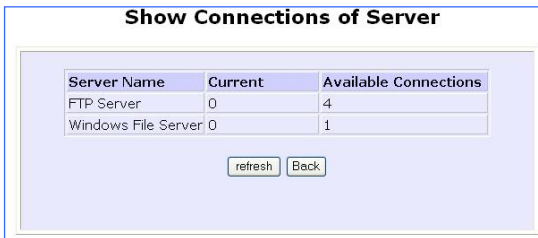
Remove: Click on this button to remove the corresponding storage disk from the router.



Note: To physically remove your USB storage disk, click on the **Remove** button first before unplugging your device.

Show Connections of Server

Under the **Advanced USB Disk Sharing Functions**, click on **Show connections to USB storage disk**. 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.

FTP User Account List

Under the **Advanced USB Disk Sharing Functions**, click on **Manage FTP user account**. This screen displays the list of FTP user accounts.



The screenshot shows a window titled "FTP Account Configuration". Inside the window, there are two text input fields: "User Name" and "Password". Below these fields are two buttons: "Add" and "Back".

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.



The screenshot shows a window titled "Add a new FTP Account". Inside the window, there are three text input fields: "User Name", "New Password", and "Confirm Password". Below these fields are two buttons: "Add" and "Cancel".

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.

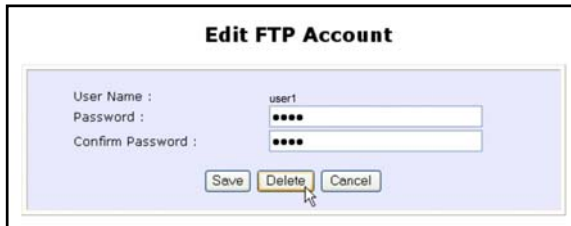
Confirm Password: Re-type your password for confirmation. Click on the **Add** button to create the new FTP user account.

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.



The screenshot shows a web interface titled "FTP Account Configuration". It features two input fields: "User Name" with the value "user1" and "Password" with a masked password of ten asterisks. Below the fields are two buttons: "Add" and "Back".

This screen below lets you click on the **Delete** button to delete the user account.



The screenshot shows a web interface titled "Edit FTP Account". It features three input fields: "User Name" with the value "user1", "Password" with a masked password of four asterisks, and "Confirm Password" with a masked password of four asterisks. Below the fields are three buttons: "Save", "Delete", and "Cancel". A mouse cursor is pointing at the "Delete" button.

File Server User Account List

Under the **Advanced USB Disk Sharing Functions**, click on **Manage file server user account**. The **File Server Account Configuration** screen displays the list of users who are using the file server.



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.

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.



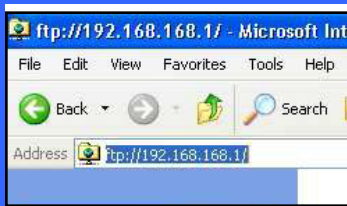
The screenshot shows a web interface titled "File Server Account Configuration". It features a table with a single row containing the text "User Name" and "Templar". A mouse cursor is pointing at the "Templar" text. Below the table are two buttons: "Add" and "Back".

Modify the account password and press **Save** or click on the **Delete** button to delete the user account.



The screenshot shows a web interface titled "Edit File Server Account". It contains three labeled input fields: "User Name" (with the value "Templar"), "Password", and "Confirm Password". Below these fields are three buttons: "Save", "Delete", and "Cancel". A mouse cursor is pointing at the "Delete" button.

Accessing your USB Hard disk via FTP Server



1. 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



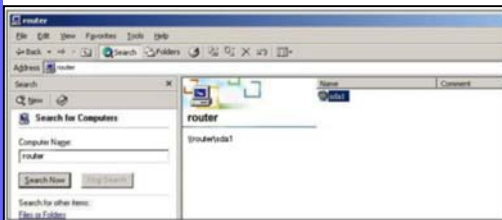
1. Right-click the **My Network Places** icon on your desktop and select **Search for Computers...**



Note: The Workgroup Name of both the router and the PC must be the same.

2. Enter the **NETBIOS** name you have set up on page 71 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.



3. 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.

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.

1. 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.



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.

SECURITY CONFIGURATION : Packet Filtering

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

Steps to configure Packet Filtering

Here are the steps to set up the Packet Filtering feature in your router:

1. Under the **SECURITY CONFIGURATION** command menu, click on **Packet Filtering**.

Packet Filter Configuration

Packet Filter Type : Disabled

Example: **Packet Filtering Type** set to Disabled.

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

Default **Packet Filter Type** is Disabled.

Packet Filter Configuration

Packet Filter Type : Block

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

Example: **Packet Filtering Type** set to Block.

Packet Filter Configuration

Packet Filter Type : Allow

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

Example: **Packet Filtering Type** set to Allow.

3. Select from three choices: **Disabled**, **Sent**, **Discarded**, and then click on the **Apply** button. The default is **Disabled**, which allows all packets to be sent.

Packet Filter Configuration

Packet Filter Type : **Sent** Change

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

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

- 4a). Enter **Rule Name** for this new packet filtering rule. For example, *BlockCS*
- 4b). Enter **MAC Address** for this new packet filtering rule.
- 4c). From the **IP Address** drop down list, select whether to apply the rule to:
- A **Range** of IP addresses
In this case, you will have to define the **(From)** which IP address (**To**) which IP address, your range extends.

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

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

Add a new Packet Filter rule

Rule Name :

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

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 :

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

IP Address : **Range** ▼

From : 192.168.168.

To : 192.168.168.

IP Address : **Single** ▼

From : 192.168.168.

To : 192.168.168.

- **Any** IP address

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

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

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

- A **Range** of TCP ports

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

Destination Port :	Range
From :	21
To :	81

- A **Single** TCP port

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

Destination Port :	Single
From :	25
To :	

- **Any** IP port

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

Destination Port :	Any
From :	
To :	

- 4e). From the **Day of the Week** drop down list, select whether the rule should apply to:

- A **Range** of days

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

Day of the Week :	Range
From :	Wed
To :	Fri

- **Any** day

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

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

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

- A **Range** of time

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

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

- **Any** time

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

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

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

Add a new Packet Filter rule

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

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

6. Packet Filter Configuration page displays the packet filter rule.

Packet Filter Configuration

Rule Name	Mac Address	IP Address(es)	Destination Port(s)	Day of the week	Time of the Day
BlockCS	00-80-45-e5-0d-07	Any	27017	Mon-Fri	07:00-18:00

SECURITY CONFIGURATION : URL Filtering

The router supports URL Filtering that allows you to easily set up rules to block objectionable web sites from your LAN users.

Steps to configure URL Filtering

Here are the configuration steps:

1. Under the **SECURITY CONFIGURATION** command menu, click on **URL Filtering**.



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

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



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



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

SECURITY CONFIGURATION : 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. Under the **SECURITY CONFIGURATION** command menu, click on **Multicast Filtering**



2. If you enable this filter, it means that the router will disallow video streaming over the Internet. Disabling this feature will allow users to stream video from the Internet.

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

Take note that this feature is enabled by default. You are recommended to **disable** it if you have subscribed to such a service.

SECURITY CONFIGURATION : Firewall

More than just a "NAT" firewall, there is a powerful Stateful Packet Inspection (SPI) firewall option that can be activated on the router. Stateful inspection compares certain key parts of the packet to a database of trusted information before allowing it through.

Common hacker attacks like IP Spoofing, Port Scanning, Ping of Death and SynFlood can be easily thwarted with the router's SPI firewall.

Steps to configure SPI Firewall

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

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

Firewall Configuration

Warning: Incorrect configuration may cause undesirable behavior.

Firewall Status: Enable Disable

Log Information

Accepted TCP Packets UDP Packets
 ICMP Packets IGMP Packets

Denied TCP Packets UDP Packets
 ICMP Packets IGMP Packets

No.	Active	Name	Disposition Policy	Protocol	Source Address (es)	Destination Addresses	Source Ports	Destination Ports
<input type="button" value="Add"/> <input type="button" value="Apply"/>								
<input type="button" value="Default Low"/> <input type="button" value="Default Medium"/> <input type="button" value="Default High"/>								

2. First, enable the firewall. You can choose among the **Default Low**, **Default Medium** or **Default High** security options for convenient setup.
3. Then you may choose the type of network activity information you wish to log for reference. Data activity arising from different types of protocol can be recorded.

The packet types that you have selected in the **Accepted** section will be displayed in the firewall log if they are detected by the firewall. This also applies to the **Denied** section.

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

- Rule Name** : Enter a unique name to identify this firewall rule.
- Disposition Policy** : This parameter determines whether the packets obeying the rule should be accepted or denied by the firewall. Choose between Accept and Deny.
- Protocols** : Users are allowed to select the type of data packet from: TCP, UDP, ICMP, IGMP or ALL.
- Note: If users select either ICMP or IGMP, they are required to make further selection in the ICMP Types or IGMP Types respectively.
- ICMP Types** : This IP protocol is used to report errors in IP packet routing. ICMP serves as a form of flow control, although ICMP messages are neither guaranteed to be received or transmitted.

ICMP Packet Type	Description
Echo request	Determines whether an IP node (a host or
Echo reply	Replies to an ICMP echo request.
Destination	Informs the host that a datagram cannot
Source quench	Informs the host to lower the rate at which
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

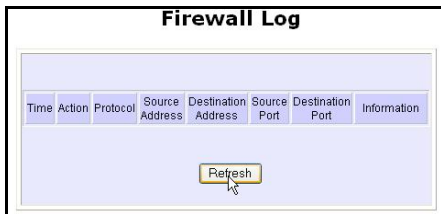
SECURITY CONFIGURATION : Firewall Logs

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

Steps to view Firewall Logs

Here is how you may view the Firewall Logs:

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

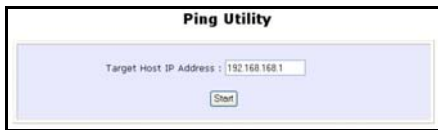


2. Click the **Refresh** button to see new information captured in the log.

SYSTEM TOOLS : Ping Utility

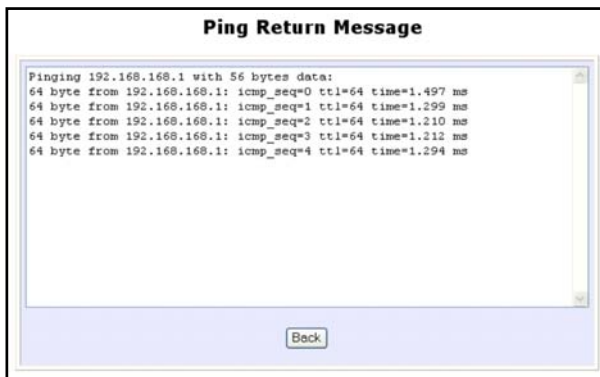
This feature lets you determine whether your router can communicate (ping) with another network host.

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



2. Enter the IP address of the target host where the target host you want the router to ping to.

3. To ping the router, click **Start**.



4. The Ping messages will be displayed.

SYSTEM TOOLS : System Identity

As described before in Chapter 4, Part 2(d)I, Steps 8-10, you may define a name for your router, System Contact person and the System Location of the router. This name will also be used as the DHCP Client ID when the router negotiates with your ISP for IP release.

Please refer to the earlier chapter for reference on this setup.

SYSTEM TOOLS : Set Router's Clock

The router is specially designed with Simple Network Time Protocol (SNTP) compatibility so that the router's clock can be synchronized with that of the managing computer. The router's clock is an important feature that affects all the time-based functions.

Steps to synchronize the router's Clock

It is a simple 2 steps process to ensure that the router's clock is synchronized. However, please ensure that the router is connected to the Internet:

1. Select **Set Router's Clock** under the **SYSTEM TOOLS** command menu.



The screenshot shows the 'System Time Setting' configuration page. At the top, it displays the 'Current Router Time' as 07/05/2005 22:51:03 and the 'Time Zone' as GMT-07:00. Below this, the 'Proposed Router Time' is also 07/05/2005 22:51:03. The 'Select your Time Zone' dropdown menu is set to 'GMT-07:00 (Mountain Time (US & Canada) ...)'. Under 'Auto Time Setting (SNTP)', the 'Enable' radio button is selected. There are two input fields for time servers: 'time.nist.gov' and 'cesium.mk.nao.ac.jp'. The 'Status' is currently 'Unknown host!'. An 'Apply' button is located at the bottom of the form.

2. From a drop-down selection, choose the correct Time Zone and simply **Enable** the **Auto Time Setting (SNTP)** using a **Time Server** such as **time.nist.gov**. Finish by clicking the **Apply** button.

SYSTEM TOOLS : Firmware Upgrade

Significantly, the router is built with upgradability in mind. You can keep your router updated with the latest capabilities by means of a simple firmware upgrade obtainable from your vendor.

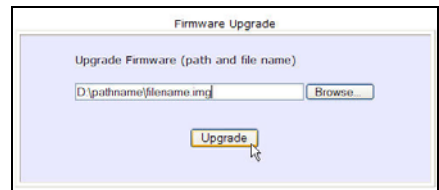
Steps to Upgrade the router's firmware

Here is how you go about upgrading your router's firmware with the latest update:

1. Select **Firmware Upgrade** under the **SYSTEM TOOLS** command menu. The screen displays a notice to inform you that the services being used will be terminated. Click **OK** to continue.



2. Ensure that you have downloaded the latest firmware into a location on your hard disk drive.
3. Click on the **Browse** button to search your hard drive for the new firmware file.
4. Press the **Upgrade** button to begin the firmware upgrade.



5. Once the firmware upgrade process is completed, your router will automatically restart.



Important: It is critical that the firmware upgrade process is NOT interrupted. Ensure that the router is not turned off and that power is not cut off from the router, or it will render the device unusable.

SYSTEM TOOLS : Save or Reset Settings

A useful feature is built into the router allowing you to save configuration profiles, especially the painstakingly crafted firewall security rules, and the intricate IP and Port settings of your Virtual Servers that effect a host of network applications.

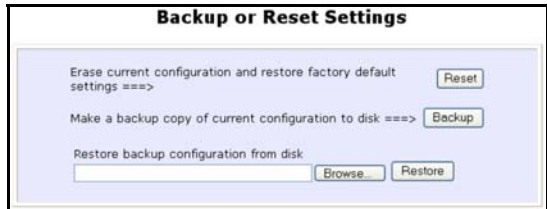
You may choose to save the configuration profile onto the router as a backup onto your hard disk drive. If needed, you may also restore an earlier profile, or reset the router to its factory default.

Refer to **Troubleshooting** section for the usage of the Reset button.

Steps to Save or Reset Settings on the router

The configuration screen is clearly labeled and simple to use:

1. From the **SYSTEMS TOOLS** command menu, click on the **Save or Reset Settings** option to arrive at the following screen below.
2. Press the **Reset** button to return the router to factory default (Note that this will discard all the configuration you have done).
3. Press the **Backup** button if you wish to save the configuration profile as a file on your PC's hard disk drive.
4. If you wish to return the router to an earlier saved file from the hard disk drive, click **Browse** to search for the filename and click on **Restore**.



Important: Pressing the **Reset** button will discard all your configuration information you may have set in the router.

SYSTEM TOOLS : Reboot Router

This feature serves an important function so that the router settings will become effective.

Steps to Reboot the Router

Rebooting the router is as easy as a few mouse-clicks:

1. Select **Reboot Router** under the **SYSTEM TOOLS** command menu.



2. The router will prompt you to confirm your decision before executing a reboot. Hit the **Reboot** button again when you are ready.

SYSTEM TOOLS : Change Password

This feature serves an important security so that the router will not be misused or abused by unauthorized users.

Steps to change the password

Changing the password is as easy as a few mouse-clicks:

1. Select **Change Password** under the **SYSTEM TOOLS** command menu.



2. Type in the **Current Password**, the **New Password** and allow verification by keying your new password in the **Confirm Password** field. Then click **Apply**.

HELP : About System

The About System page gives the administrator an overview of the router customizations/settings. This is a useful summary of the operating parameters you have put in place.

Steps to access the About System page on the Router

In a single mouse click, you will be able to glance at the settings applied to your router:

1. Click **About System** under the **HELP** command menu, and you will be brought to the following **System Information** page.

System Information	
Device:	
System Up Time :	0 Days 02:54:20
BIOS/Loader Version :	2.0 (build 0027)
Firmware Version :	1.4 (build 0704)
Network Address Translation :	Enabled
Wireless:	
Hardware Address :	00-80-40-35-67-9f
WLAN name (ESSID):	router
Operating frequency :	2.4570G
Operating Channel :	10
Security mode :	None
LAN Port:	
Hardware Address :	00-00-00-12-34-56
IP Address :	192.168.168.1
Network Mask :	255.255.255.0
DHCP Server :	Enabled
WAN Port:	
Hardware Address :	00-00-00-12-34-78
WAN Type :	PPPoE

2. The **System Information** page reveals the router's settings that you have executed.

Chapter 6: Printer Server Setup Configuration

The router can also act as a network's 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.

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

1

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



2

- (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.

3

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** (shown on the right) appears.

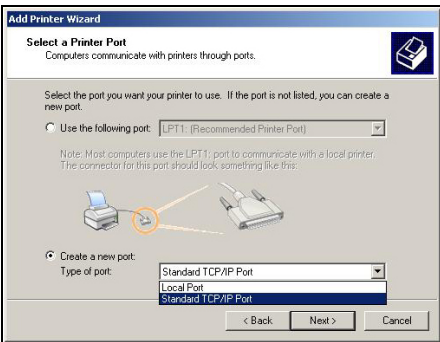


- (3). Click **Next>** to proceed.



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

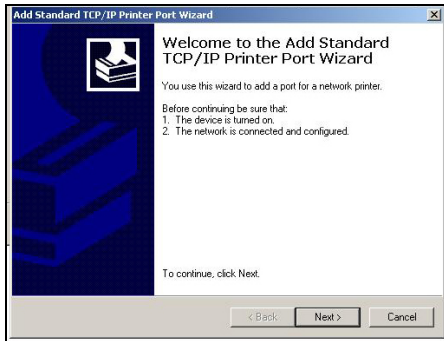
Please note that you should not select the **Automatically detect and install my Plug and Play printer**.



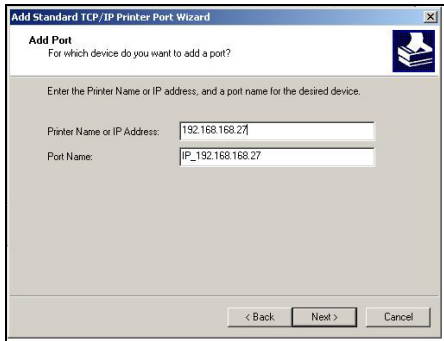
4

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.

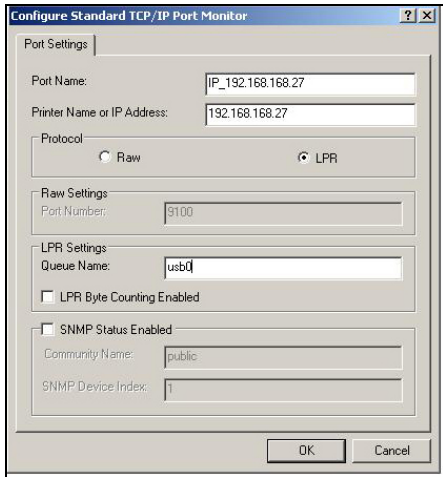


- (5). Enter your router's IP address in the **Printer Name or IP Address** field. Then the corresponding **Port Name** will be automatically entered.

- (6). Click on the **Next>** button to proceed.



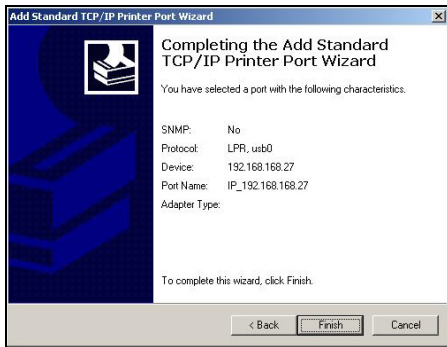
- (7). Go to the **Device Type** section and select **Custom**. Next to the Custom radio button, click on the **Settings** button. This brings out the **Configure Standard TCP/IP Port Monitor** window.



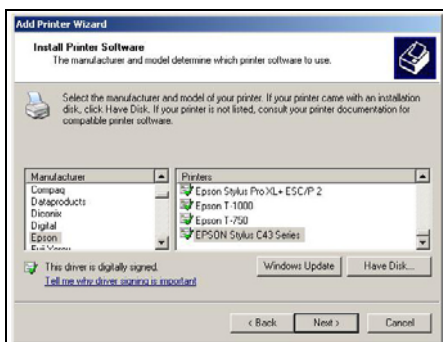
(8). Go to the **Protocol** section and select **LPR**.

(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.

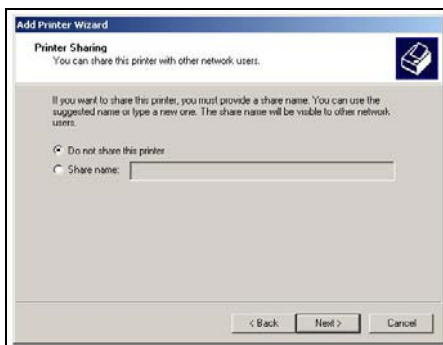
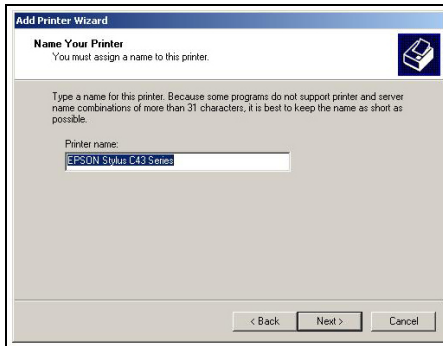
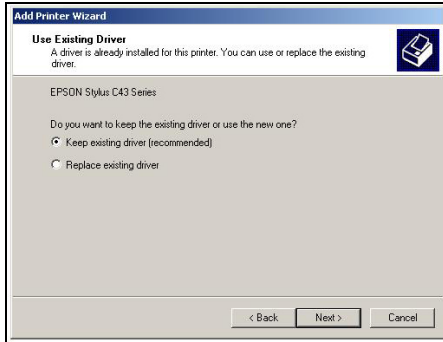


5

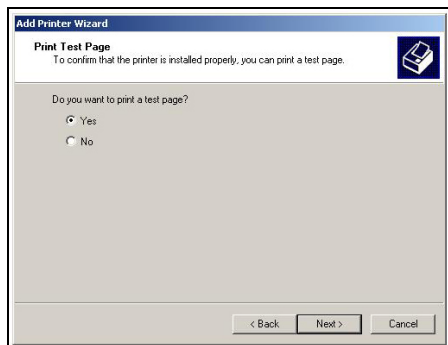
Next to install the printer's driver to your PC:

(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, which 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 2000

1

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



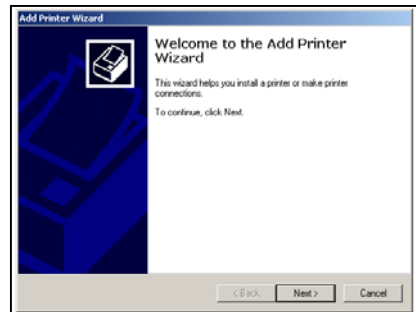
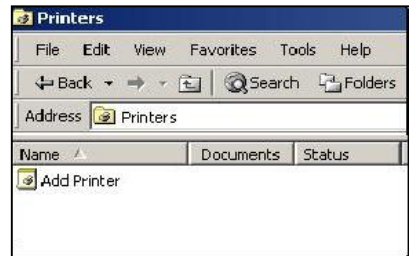
2

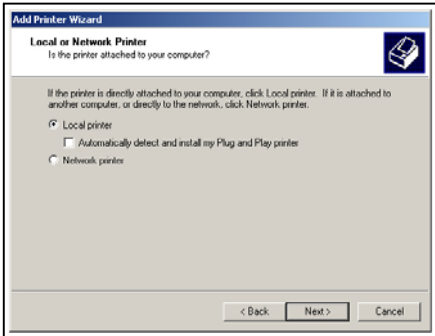
- (1). Simply choose **Enable** or **Disable** for the **Status** of **Printer Server**.
- (2). Click on the **Apply** button.
- (3). When you connect the printer to the USB port of the router, the printer will be automatically displayed in the Printer List.

3

Next to add the printer to your PC:

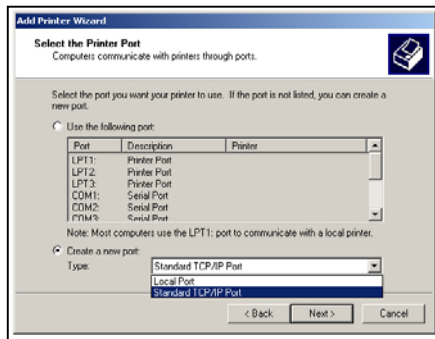
- (1). Go to the Windows **Start** Menu, select **Settings**, then followed by **Control Panel**.
- (2). Then double-click **Printers and Faxes**. Select the **Add a printer** and the **Add Printer Wizard** (shown on the right) appears.
- (3). Click **Next>** to proceed.





- (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**.



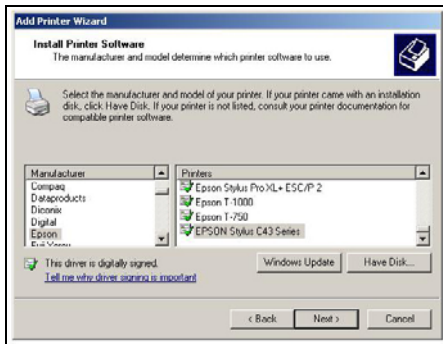
4

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.



- (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.

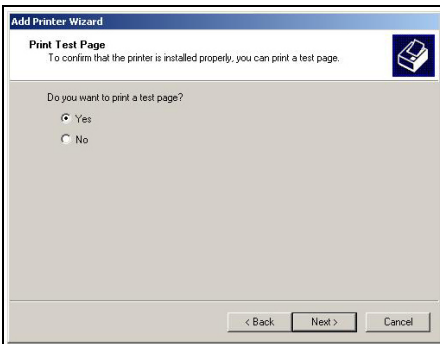
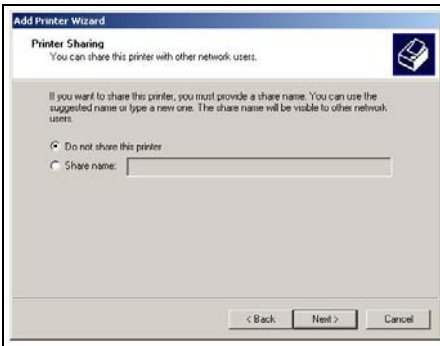
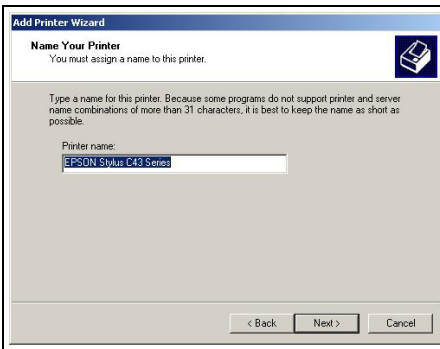


- (11). After you have successfully configured the selected port, you will see the information display in this window. Click **Finish** to complete the port configuration.

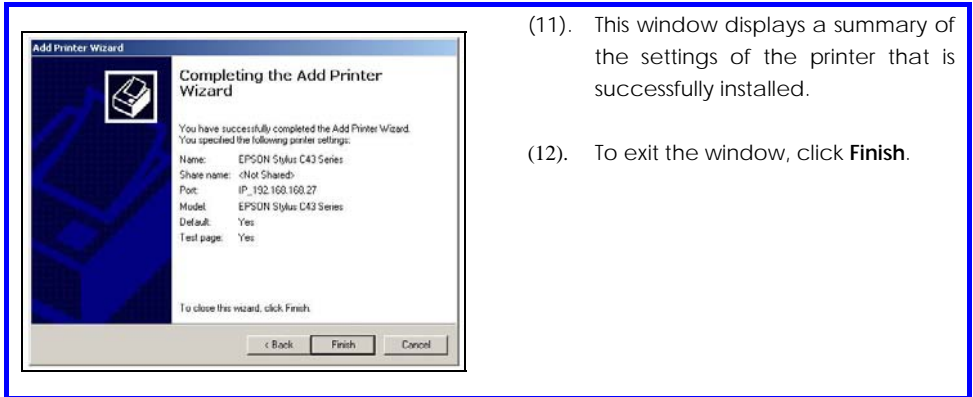
5

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, which 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:

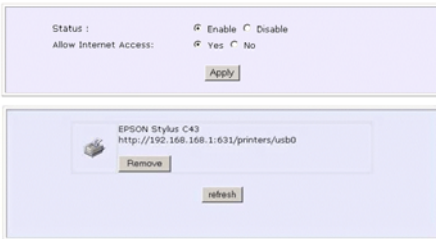
http://www.columbia.edu/acis/access/printing/winME_files/instlpr.exe

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:

1

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

Enable/Disable Printer Server



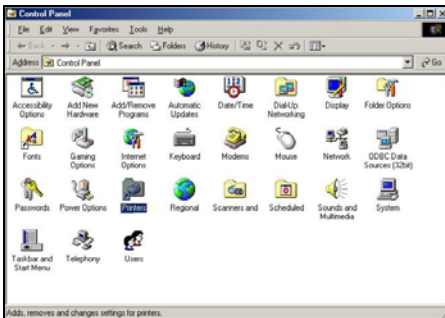
2

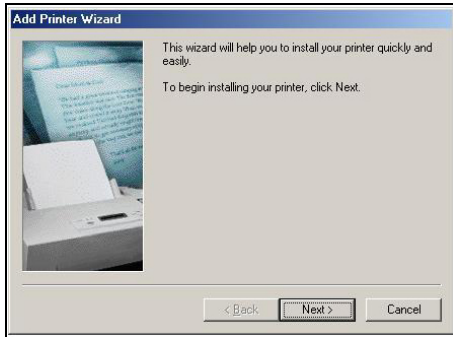
- (1). Simply choose **Enable** or **Disable** for the **Status** of **Printer Server**.
- (2). Click on the **Apply** button.
- (3). When you connect the printer to the USB port of the router, the printer will be automatically displayed in the Printer List.

3

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**.



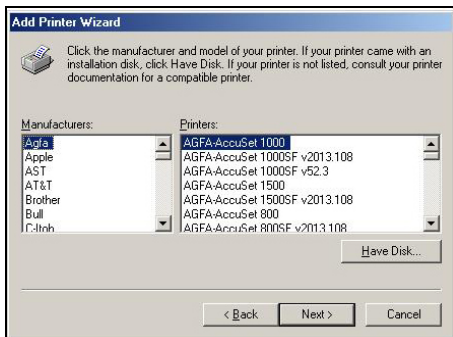


(3). The **Add Printer Wizard** (shown on the left) appears.

(4). Click **Next>** to proceed.



(5). Click the radio button next to **Local Printer**. Then click **Next>** to proceed.



4

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

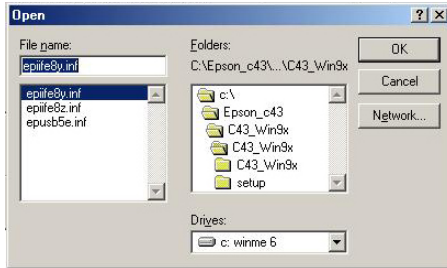
(1). Select the printer's name available in the **Manufacturers:** and **Printers:** listboxes.

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

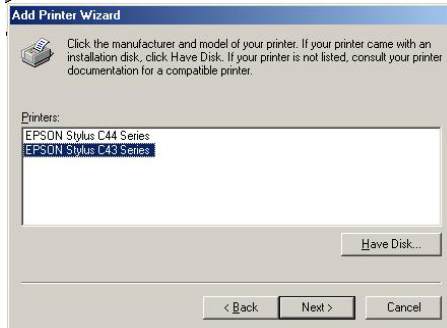
(3). Click **Next>** to proceed.



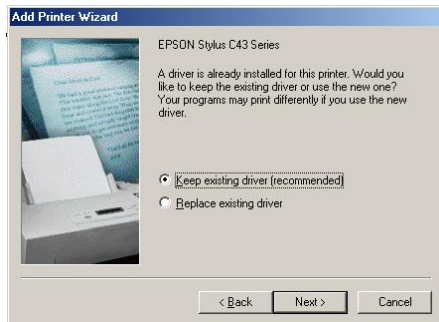
- (4). At the **Install From Disk** screen, click **Browse...** to search for your printer's driver and install it.



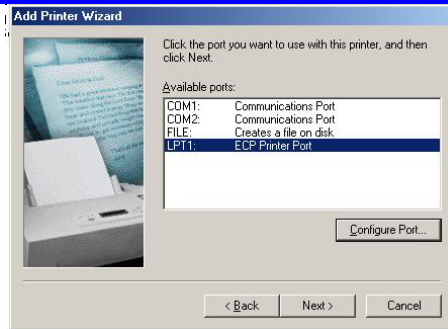
- (5). The **Open** screen prompts you to select the file name of your printer's driver. Then click **OK** to proceed.



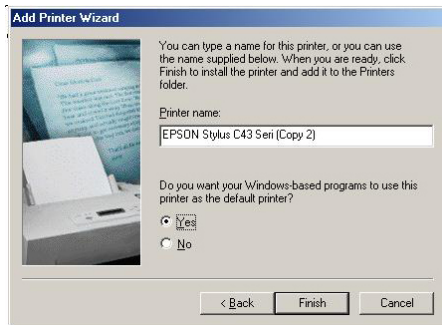
- When your printer's driver is added to the **Printers** list, click **Next>** to proceed.



- (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.



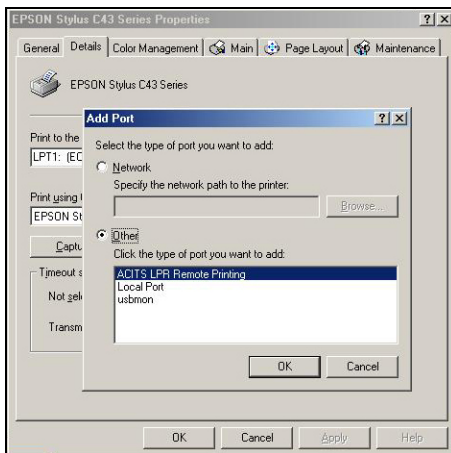
- (10). Just leave the supplied fields intact as they are. Click **Finish** without editing anything unless required.
- (11). Wait for a while until the message "Setup is complete" is prompted.



- (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.

- (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,

1

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



2

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

Chapter 7: Setting Up Special Printers

This chapter explains how to setup and upload the printer file manually and automatically from router for special printers of different design from standard USB printers.

Most USB printers have the printer firmware in their flash ROM. However, special printers like the HP LJ1020 require the computer to load the printer firmware through the printer driver installation instead, so as to be ready for printing after powering up.

The router supports both manual and automatic uploading of printer file to the printer.

Manual upload of printer firmware and driver

The user can setup support for such printers immediately by uploading the printer file manually.

Follow these steps to upload printer driver manually:

1. Beforehand, copy the printer file from the router product CD to your local hard drive.
2. Start the uConfig utility.
3. Under the **HOME USER FEATURES** command menu, click on **Printer Server Setup**.



2

Printer Server Setup page displays.

1. Ensure that printer server **Status** is set to **Enable**.
2. Click **Set firmware**.
If Printers List is not refreshed with your printer, click **Refresh** to update the list.

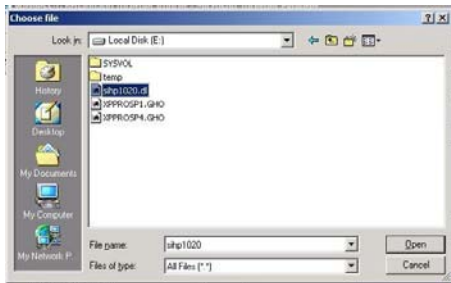


Please note: The absence of a URL link below the printer model name (Example: <http://192.168.168.113:631/prn/usb0>) indicates that the printer has NOT been initialized and is NOT ready to print.

Printer Driver Setup

Printer Driver File:

Printer Driver Upload



Printer Driver Setup

Printer Driver File:

Printer Driver Upload

3

- (1). Click **Browse**.
Choose file window displays.
- (2). Select the printer driver file and click **Open**.
Printer Driver Upload displays the selected printer driver file.
- (3). Click **Upload**.

4

Printer Server Setup page displays.

If page is not updated:

Click **Refresh** button to refresh the page.

Enable/Disable Printer Server

Status : Enable Disable
Allow Internet Access: Yes No

Printers List

HP LaserJet 1020
<http://192.168.168.113:631/pn/usb0>



Please note: The printer URL link
(Example: <http://192.168.168.113:631/pn/usb0>)
indicates that the printer has been properly initialized
and is ready to print.

Note: With manual upload of printer file: When the printer is powered up and down again, the printer firmware uploaded will be lost and the printer file needs to be uploaded again before the printer can start to receive print jobs.

For automatic upload of printer file, please refer to the following section.

Automatic upload of printer file

When the printer is powered up, the router can automatically upload the printer file stored in a thumb drive or USB hard drive that is plugged to the router USB port.

Follow these steps to setup the uploading of printer file automatically:

1

- (1). Beforehand, copy the printer driver file to a thumb drive or USB external hard drive.
- (2). Start the uConfig utility.
- (3). Under the **HOME USER FEATURES** command menu, click on **Printer Server Setup**.



Printers List



Please note: The absence of a URL link below the printer model name (Example: <http://192.168.168.113:631/prn/usb0>) indicates that the printer has NOT been initialized and is NOT ready to print.

2

Printer Server Setup page displays.

- (1). Ensure that printer server **Status** is set to **Enable**.
- (2). Click **Set firmware**.
If Printers List is not refreshed with your printer, click **Refresh** to update the list.

3

Printer Driver Setup



Printer Driver File:

Apply

- (1). Plug the thumb drive or USB external hard drive containing the printer file to the router USB port.
- (2). If it is the only storage device plugged in, the router will add the device with the name "sda_drive01"

Printer Driver Setup



Printer Driver File:

Apply

You should have the printer file already copied into this storage device.

Path/Filename Example:

LJ1020/sihp1020.dl

- (3). Enter the printer driver path and filename in **Printer Driver File** text field.
Example:
sda_drive01/LJ1020/sihp1020.dl
- (4). Click **Apply** to load printer file to the printer.


4

Enable/Disable Printer Server

Status : Enable Disable
Allow Internet Access: Yes No

Printers List

HP LaserJet 1020
<http://192.168.168.113:631/pnm/usb0>

 Please note: The printer URL link (Example: <http://192.168.168.113:631/pnm/usb0>) indicates that the printer has been properly initialized and is ready to print.

Updated Printer Server Setup page displays.

The router will load the printer file automatically from the designated thumb drive or USB external hard drive location that is plugged to the router whenever it powers up or reboots.

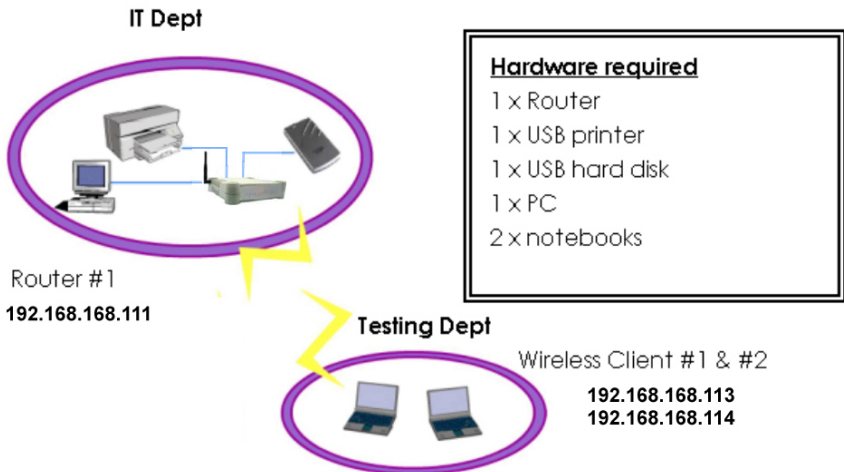
Chapter 8: Configuring Network Applications

In this chapter, we shall illustrate some examples in configuring the router with USB devices, such as USB printers and storage disks.

Scenario: Accessing USB hard disk & printer via the router

In the IT department, Router #1 acts as a router cum printer server. It is connected to a USB hard disk to allow authorized users to access shared data files. One wired user and two wireless clients are allowed to use the printer and share the data files in the USB file server in the IT department.

The below illustration is an example on how to use the router to share the USB hard disk and the USB printer wirelessly.



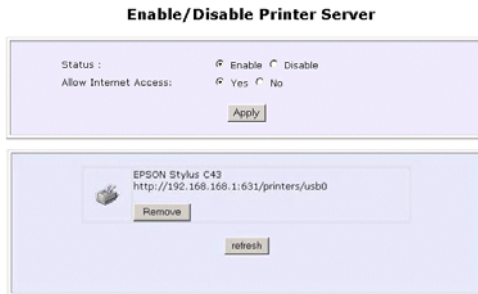
I. Configure your Router #1

1. After the hardware, TCP/IP and wireless configuration have been set up, install the printer driver to your PC and notebooks.
2. Next, insert the Product CD to your CD-ROM drive, go to **Utilities** section and activate the **uConfig** program, select **Wireless-G Broadband Internet Router** and click on **OpenWeb** button.
3. Click on **LOGIN!** button to access to the main page of Router #1.



Access to the network printer via Router #1

4. Select **Printer Server Setup** from your **Configuration** Command menu.
5. Before enabling the printer server, ensure that your printer is well connected to any USB port of your Router #1.
6. Select **Enable** and Click on the **Apply** button to update the changes.



Now wireless clients can also print via Router #1. Do bear in mind that printer drivers need to be installed onto all computers that will use the printer.

Access to your USB hard disk via Router #1

7. From Configuration Menu, select NETBIOS setup to ensure that the router is assigned to the same workgroup as the rest of the computers.
8. Select **USB Storage Disk Sharing** from your **Configuration** Command menu.

USB Storage Disk Sharing

FTP Server:

FTP Server: Enable Disable

Allow Anonymous User: Yes No

Allow access from the Internet: Yes No

FTP Port :

File Server:

Windows File Server: Read and Write
 Read Only
 Disable

Allow Anonymous User: Yes No

9. Choose the access rights to the disk (**Read and Write** or **Read Only**). Select Yes for **Allow Anonymous User** to allow direct access to the disk.
10. Click on **Apply** button to update the changes.
11. Now, you can simply go to **My Computer**, right click and select **Search for Computers....**
12. Type in the **NETBIOS** name you have assigned to the router and **click Search Now**.
13. Refer to **HOME USER FEATURES: USB HDD Share** for details on how to allow only authorized users to access the disk.

Appendix A: Troubleshooting

Solutions to Common Problems

In the section, we attempt to address common problems that may arise during the installation and operation of the router. Listed here are suggested steps you may follow to rectify a possible problem that you encounter.

1. I am unable to surf the Internet.

- A. Make sure that your Ethernet cable is properly connected from your Cable/ADSL modem to the router's WAN port, and verify from the **About System** page if a valid IP address (from the ISP) is shown under the WAN port section.
- B. If not, ensure that your WAN settings correspond to the type of broadband Internet connection you have subscribed to. You may contact your ISP to see if your Internet connection type: is Dynamic IP, Static IP addressing, PPPoE (commonly used for ADSL subscriptions) or PPTP. Please refer to Part 2 of Chapter 4 for WAN Setup. Remember to reboot the router after changing your WAN settings.
- C. If you are able to surf the Internet when your Cable/ADSL modem is connected directly to your PC, but after setting up the router and verifying the settings in steps A & B above, your router is still unable to get an IP address from the ISP, then you may need to refer to Chapter 4 Part 2(d) steps 5-7 to clone the MAC address of your Ethernet adapter onto the router.
- D. If all configurations from the above points A to C have been followed, power off the computer, the router and the Cable/ADSL modem. Turn on the Cable/ADSL modem, then wait for a period 1 minute before turning on the router. Lastly, turn on your computer. Verify again if you received an IP address and attempt to surf the web.
- E. If you are a PPPoE user, you will need to remove the proxy settings or the dial-up pop-up window.
 - For Microsoft Internet Explorer 5.0 or higher, start Internet Explorer, from the **Tools** menu bar, select **Internet Options** and then click on the **Connections** tab.
 - From the **Connection** 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 higher, start Netscape Navigator. From the **Edit** menu bar, select **Preferences**, then **Advanced**, and finally **Proxies**.

- o Make sure that the **Direct connection to the Internet** option is selected.
- o Close all windows to finish.

2. I wish to start all over. I want to set the router to its factory default settings.

- F. In the event that you wish to return the router to its original factory default settings, you may depress the Reset button (at the back of the router) when the router is powered up and hold the button for 8 to 10 seconds before releasing it.

3. I have forgotten my password and therefore cannot access the router's web-configuration page.

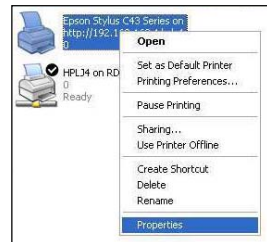
- G. If you have forgotten your password, hold the Reset button (at the back of the router) for 5 seconds (when the router is powered up). The password will be reset to its default, which is 'password'.

4. The firmware is corrupted and I can't access the router's "Firmware Upgrade" page anymore.

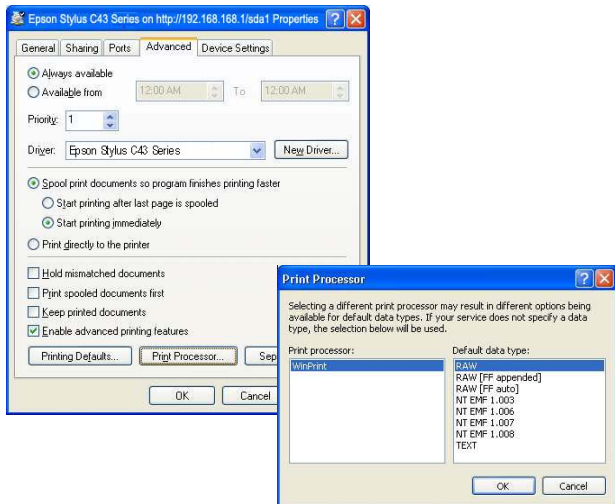
- H. Verify the Diagnostic LED. If it keeps blinking rapidly, you will have to perform a manual firmware recovery procedure. First, power OFF your router. Except for your PC, disconnect all other networked devices from the router.
- I. You MUST give your PC a static IP address of 192.168.168.100 with a subnet mask of 255.255.255.0.
 - If you are using Windows 98SE or Windows Millennium, follow Part 1(c) on page 14 of the manual to set the static IP address.
 - If you are using Windows 2000 or Windows XP, follow Part 1(d) on page 15 of the manual to set the static IP address
- J. Insert the Product CD into the CD-ROM drive of your PC, where the CD-ROM drive is X:\, double-click "27grcv.bat" to begin the firmware recovery process.
- K. It takes about 1 minute to complete the whole process. Slower blinking of the Diagnostic LED will indicate this. Power OFF and then power ON the router to continue with normal operation.

5. I have installed my printer driver but still cannot print.

- L. You need to check your print processor status. Go to your **Printers & Faxes**, select your printer and right click to choose **Properties**.



- M. Go to your **Advanced** tab and click on **Print Processor** button. Ensure that your **default data type** is set to *RAW* as shown in the figure below:



Appendix B: Frequently Asked Questions

Answers to Frequently Asked Questions

In the section, we have compiled a short list of answers to some frequently asked questions about this product.

Question	Answer
1. Does the router support IPSec pass-through?	Yes. It is an automatically enabled feature supported by the router.
2. Does the router support other operating systems other than Windows 98SE, ME, 2000 and XP?	Yes. However, technical support is not provided for the setup, configuration or troubleshooting for non-Windows operating systems.
3. What is the maximum number of IP addresses that the router supports?	The router will support up to 253 IP addresses.
4. Does the WAN connection of the router support 100Mbps Ethernet?	Yes. 100Mbps Ethernet is supported on its WAN port. However, your Internet connection speed will vary depending on the speed/type of broadband subscription.
5. What printers does the router support?	The router supports most USB printers. You can also verify a non-exhaustive list of compatible printers at http://www.linuxprinting.org . Please note that only sharing of printer function is supported for multifunction printers.

Appendix C: NETBIOS Protocol Installation

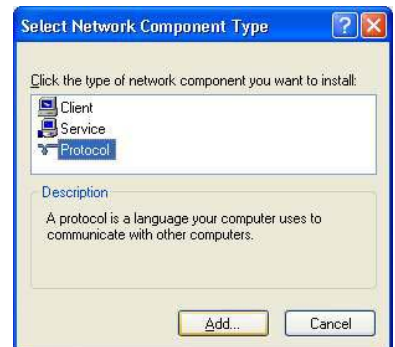
To check if the NETBIOS protocol is installed on your PC:

1. Right-click on **My Network Place** and select **Properties**.
From your **Local Area Connection** icon, right click and select **Properties**.

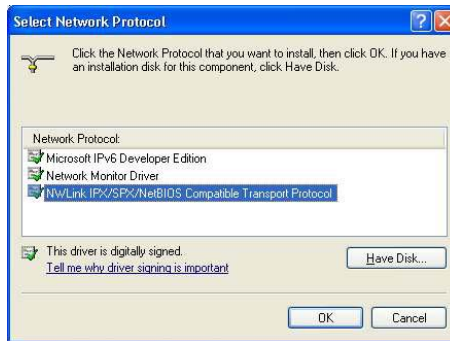


2. Next, from the **General** tab, scroll down to look for *NwLink IPX/SPX/NetBIOS Compatible Transport Protocol*. If you have found this protocol, make sure that the checkbox next to it is enabled. This means that NETBIOS protocol is being used by your system. If not, click on **Install...** button to install this protocol.

3. Select the network component as *Protocol* and click on the **Add...** button.



- Next, select *NwLink IPX/SPX/NetBIOS Compatible Transport Protocol* and click **OK** button.



Now, NETBIOS Protocol has been installed to your system successfully!

Appendix D: Glossary of 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 that specifies a data transfer rate of 54Mbps using OFDM modulation and an operating frequency of 2.4GHz, as well as backward compatibility with the 802.11b devices.
Auto MDI/MDI-X	An Auto MDI/MDI-X port automatically senses the inserted cable type for transmission, and thus eliminates the need for crossover cables.
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.
Browser	The browser is a general name given to applications designed to view and interact with HTML pages on the World Wide Web, eg. Internet Explorer, Netscape Navigator.
CAT 5	It is a standard developed by the Electronics Industries Association that specifies network cabling which consists of 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, the smallest chunk of data is called a packet (packet sizes 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. For more information on DHCP, please refer to the DHCP Technology Primer found on the Product CD.
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 that has to run specialized applications requiring multiple TCP/IP ports to be opened.
DNS	Domain Name System is transparent to the user and translates Internet domain names to IP addresses, so that the user only needs to remember meaningful and easy-to-remember names rather than 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 intended party will be able to decode to 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 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) of the device so that it 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.
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 router 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 that 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.
MDI	Medium Dependent Interface. On a network hub/switch, a MDI port (uplink port) connects to another hub/switch using a straight cable. To connect a MDI port to a computer, a crossover cable is used.
MDI-X	Medium Dependent Interface Crossed. On a network hub/switch, a MDI-X port connects to a computer using a straight cable. To connect a MDI-X port to another hub/switch, use a crossover cable.
Multicast	A multicast is a packet that is sent to a subset of end stations in a LAN, or VLAN that belong to a <i>multicast group</i> . If the network is set up correctly, a multicast can only be sent to an end station if it has joined the relevant group.
NAT	Network Address Translations multiplexes multiple private IP addresses on the LAN to a single public IP address on the Internet. For more information on NAT, please refer to the NAT Technology Primer on the Product CD.
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 addresses or the type of data transmitted.
Ping	Packet Internet Groper is a utility used to determine whether a particular network device (IP address) is available online. It works by sending out a packet to the device and waiting for its response.
PPPoE	Point-to-Point Protocol over Ethernet is a method for the encapsulation of PPP packets over Ethernet frames.
PPTP	PPTP stands for Point-to-Point Tunneling Protocol. It is a protocol that allows authorized users to extend their own networks through private "tunnels" over the ISP or online service. This kind of interconnection is known as VPN (Virtual Private Network)
RJ-45	A connector used for Ethernet devices that holds up to eight wires.
Router	A router is a device that interconnects networks.

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.
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.
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 means of employing IPsec amongst others.
WAN	Wide Area Network. It is a communication network that extends over a large geographical area. For example, the Internet.
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.
WPA-PSK	WPA-PSK stands for Wi Fi Protected Access Pre Shared Key . WPA-PSK is a special mode for home users without authentication server and yet provides the same strong encryption protection.

Appendix E: Technical Specifications

Industry Standards	<p>Wired:</p> <ul style="list-style-type: none"> - IEEE 802.3 10Base-T - IEEE 802.3u 100Base-Tx - IEEE 802.3x Flow Control <p>Wireless:</p> <ul style="list-style-type: none"> - IEEE 802.11b - IEEE 802.11g
WAN Interface	<ul style="list-style-type: none"> - 1x Auto MDI/MDI-X RJ45 Ethernet Port for external Cable/ADSL modem
WAN Type	<ul style="list-style-type: none"> - Static IP - Dynamic IP - PPP over Ethernet (PPPoE) - Point to Point Tunneling Protocol (PPTP) - Layer 2 Tunneling Protocol (L2TP)
LAN/WLAN Interface	<p>Wired:</p> <ul style="list-style-type: none"> - Integrated 4x Auto MDI/MDI-X 10/100Mbps Switch <p>Wireless:</p> <ul style="list-style-type: none"> - Operating channels, frequency of: 11 Channels 2.400~2.4835, US, Canada 13 Channels, 2.400~2.4970, Europe 4 Channels 2.400~2.4835, France - Direct Sequence Spread Spectrum modulation, Orthogonal Frequency Division Multiplexing modulation - Data rates: 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 11Mbps, 9Mbps, 6Mbps, 5.5Mbps, 2Mbps, 1Mbps - Security: 64-bit/128-bit WEP Wireless Pseudo VLAN WPA-PSK

USB Ports	2X integrated USB1.1 ports supporting: <ul style="list-style-type: none"> - USB Printer - USB Hard Drive/ Flash Drive (based on FAT/FAT 32 file system)
External Antenna Type	2 dBi (non-detachable)
IP Addressing	All Classful/Classless subnets
Built-in DHCP Server	Yes
DHCP Reservation	Yes
NAT Firewall	Yes
Stateful Packet Inspection (SPI) Firewall	Yes
Load-Balancing/ Fail-Over Redundancy	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 Routing Entry
VPN Client Pass-Through	PPTP, IPSec
Multicast Filtering	Yes
Configuration Interface	Web-based Configuration Menu
Profile Backup and Restore	Yes
Firmware Upgradeable	Yes
Environment Requirement	Temperature: <ul style="list-style-type: none"> - Operating : 0°C to 40°C - Storage : -20°C to 70°C Humidity: <ul style="list-style-type: none"> - Operating : 10% to 80% RH - Storage : 5% to 90% RH

Physical Dimension	174mm x 104mm x 40mm (L x W x H)
Weight	~ 0.8 Kg (including power adapter)

Appendix F: 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 Centers:

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