Wireless Super-G BroadBand Multimedia Router

Wireless Super-G BroadBand Multimedia Router

networks@work

USER'S MANUAL

COMPEX **NETPASSAGE** SERIES

NetPassage 28G HotSpot

NetPassage 28G HotSpot
NetPassage 28G HotSpot
NetPassage 28G Hotspot
NetPassage 28G Hotspot

Manual Number: U-0481-V1.2C

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.

Manual Revision by Ann
Manual Number: U-0481-V1.2C Version 1.2, January 2006

Disclaimer

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

Your Feedback

We value your feedback. If you find any errors in this user's manual, or if you have suggestions 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 the following:
Product Name: **Wireless Super-G Broadband Multimedia Router** Model No.: **Router** conforms to the following Product Standards: Radiated Emission Standards: EN55022A, FCC Part 15 Class B; Conducted Emission Standards: EN60555Pt2 conducted emission; EN55022A conducted emission, FCC Part 15 Class B; Immunity Standards: IEC 801-2; IEC 801-3; IEC 801-4. **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 Super-G Broadband Multimedia Router Series, Router, is a licensed product of Compex Systems Pte Ltd. This document contains instructions for installing, configuring and using Router. It also gives an overview of the key applications and the networking concepts with respect to the product.

This documentation is for both Network Administrators and the end-users who possess some basic knowledge in the networking structure and protocols.

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

Firmware

Please take note that this User's Manual is written based on Firmware Release 1.39 Build 0117.

Conventions

In this document, special conventions are used to help present the information clearly. The Compex Wireless Super-G Broadband Multimedia NetPassage 28G is often referred to as NetPassage 28G or Router in this document. Here is a list of conventions used within the manual:

⚠	This symbol signifies an important notice to be heeded. The user is advised to read the instructions carefully before proceeding further.
eXpert	This symbol represents a section meant for advanced users, or specific features meant for exceptional non-standard applications. The user is assumed to have relevant network knowledge to carry out the necessary configuration or understand the information given.
Technology Primer	This symbol signifies that the user may find additional networking information from our unique Technology Primer documents found within the Product CD. The documents explain particular network concepts, Compex-exclusive features and provide illustrated walkthroughs for common networking scenarios.
exclusive!	This symbol signifies an exclusive feature found on this Compex product, or Compex's family of products.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION 1

CHAPTER 2: GETTING TO KNOW YOUR PRODUCT 3

KEY FEATURES BRIEFING 3
Basic features 3
Security Features 5
PACKAGE CONTENTS 6
PACKAGE CONTENTS 7
SCHEMATIC OVERVIEW OF THE ROUTER 7

CHAPTER 3: LET'S GET GOING-HARDWARE SETUP 9

POWER UP IN 4 STEPS: 9
NETWORK APPLICATION EXAMPLES 10

CHAPTER 4: LET'S GET GOING-SOFTWARE SETUP 12

PREPARING THE PCS + ROUTER 12
PART 1 - CONFIGURING THE PCS 12
PART 2 - BASIC SETUP 18
CONFIGURATION: WAN SETUP 25

CHAPTER 5: ADVANCED CONFIGURATION 31

DETAILED CONFIGURATION OF THE ROUTER 31
CONFIGURATION : Wireless Setup 31
HARDWARE SETUP OF THE ROUTER 33
CONFIGURING YOUR PC 34
CONFIGURATION FOR THE ROUTER AS ACCESS POINT 34
CONFIGURATION FOR THE ROUTER AS ACCESS POINT CLIENT 36
CONFIGURATION: Wireless Setup: Security Mode 37
CONFIGURATION : Wireless Setup: Wireless Pseudo VLAN 40
CONFIGURATION : LAN Setup : Advanced DHCP Server Options ... 44
CONFIGURATION : WAN Setup 46
CONFIGURATION : Routing 46
CONFIGURATION: NAT 48
CONFIGURATION : Remote Management 53
CONFIGURATION : Parallel Broadband 55
CONFIGURATION : Email Notification 57

ADVANCED FEATURES : Transparent Proxy 59

ADVANCED FEATURES : Static Address Translation (SAT) *60*
ADVANCED : SMTP Redirection *61*
ADVANCED FEATURES : DNS Redirection.. *62*
ADVANCED FEATURES : Dynamic DNS Setup....................................... *63*
ADVANCED FEATURES : UPnP Configuration...................................... *67*

SECURITY CONFIGURATION: Packet Filtering....................................... *69*
SECURITY CONFIGURATION : Multicast Filtering *72*
SECURITY CONFIGURATION: URL Filtering... *73*
SECURITY CONFIGURATION: Firewall *74*
SECURITY CONFIGURATION : Firewall Logs *78*
SECURITY CONFIGURATION: Log of IPs visited...*79*
SECURITY CONFIGURATION: Web Model... *80*

SYSTEM TOOLS : System Identity.. *81*
SYSTEM TOOLS : Set Router's Clock *81*
SYSTEM TOOLS : Firmware Upgrade *82*
SYSTEM TOOLS : Save or Reset Settings.. *82*
SYSTEM TOOLS : Reboot Router... *83*

HELP : Get Technical Support *85*
HELP : Memory Information *85*
HELP : About System.. *86*

CHAPTER 6: USING HOTSPOT CAPABILITIES 87

HOTSPOT : HotSpot Authentication *89*
HOTSPOT : Bandwidth *95*
HOTSPOT : Walled Garden *96*
HOTSPOT : Keypad or Printer Status..*98*
HOTSPOT : Radius Configuration...*100*
HOTSPOT : Accounts *102*

APPENDIX A: TROUBLESHOOTING... 111

SOLUTIONS TO COMMON PROBLEMS 111

APPENDIX B: FREQUENTLY ASKED QUESTIONS 115

ANSWERS TO FREQUENTLY ASKED QUESTIONS... 115

APPENDIX C: NETBIOS PROTOCOL INSTALLATION 116

APPENDIX D: GLOSSARY OF TERMS 118

APPENDIX E: TECHNICAL SPECIFICATIONS 122

APPENDIX F: TECHNICAL SUPPORT INFORMATION 124

Chapter 1: Introduction

Thank you for purchasing the Wireless Super-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 device. We are excited that you will soon be discovering more about a product which we have proudly developed.

Advanced Features

- *New **108Mbps** Wireless Super-G 802.11g **10X faster** than 802.11b!*
- *Keep snoopers away with **WPA, WPA-PSK** and **64/128-bits WEP Encryption**!*
- *Integrated USB **Print Server** and **Storage Server** for network printing, network storage and remote wireless surveillance.*

Read on to find out more about these features!

This high-performance Wireless Super-G Broadband Multimedia Router supports external Cable/ADSL modem for broadband Internet sharing to your wired and wireless networks at the workplace or at home. To simplify your wired network setup, the router supports Auto MDI/MDI-X to eliminate the requirement for crossover cables. Then on top of its integrated 3-port 10/100Mbps Fast Ethernet switching capability, the router adopts the new 802.11g standard for its wireless operation, employing OFDM technology to transmit data at up to 108Mbps within the 2.4GHz band!

This means that within the specified range of this device, you will be able to transfer large files up to ten times faster than the widely deployed 802.11b products! You can now sit back and watch an MPEG movie played over the network without noticeable delays. Also, because the 802.11g standard is backwards compatible with 802.11b devices, your existing devices can still operate at speeds of up to 11Mbps in the same frequency range.

You will also be pleased to know that the router comes with 4 integrated USB ports to provide for print server support, USB HDD and USB Flash Disk. This effectively extends the functional capabilities of the router to include remote network printing, network storage and remote video surveillance.

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

The router also ships with Compex-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, play multi-player games with greater flexibility, speed and security you never thought possible before!

Compex 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

The router is endowed with a high-performance design and a rich feature set you should familiarize yourself with. To maximize the potential of your purchase, we have highlighted a list of features to help you be familiarized with it:

Basic features

Compatible with IEEE 802.11g and IEEE 802.11b standards hot

Adopting the industry standard 802.11g standard, the router provides you 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 and PPTP WAN types

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

Auto MDI/MDI-X crossover support on all Ports hot

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

Built-in Dynamic Host Configuration Protocol (DHCP) Server

As a 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, it will automatically and dynamically allocate addresses from a pool, to devices or computers connected to the network.

*Learn more from our **DHCP*** **Technology Primer**

Virtual Servers based on Port-forwarding, IP-forwarding hot

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

*Learn more from our **NAT*** **Technology Primer**

Domain Name System (DNS) Redirection

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

Static Routing

The router supports Static Routing. By defining a Static Routing configuration, you set in place a definite Router IP address whereby a packet could reach a specific IP address or subnet.

Dynamic DNS

The router supports Dynamic DNS. By automatically maintaining the relationship between the fixed 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.

*Learn more from our **NAT*** ***Technology Primer***

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) hot

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, you will be glad to learn about the security elements put in place to give you a peace of mind.

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.

WPA-PSK

With WPA-PSK, the router provides home and SOHO users with the highest level of security.

Built-in "NAT" firewall

As the router handles the incoming and outgoing data packets transacting between the internal and external network, it looks and validates individual packet information before passing it onto a client in the network. This checking provides effective firewall protection because rogue packets will be automatically discarded.

Learn more from our ***NAT*** **Technology Primer**

Stateful Packet Inspection (SPI) firewall hot

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

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 hot

Compex's exclusive Wireless Pseudo VLAN feature extends the security advantages of the Ethernet based VLAN to wireless networks. This feature offers data privacy and protection between individual clients on a wireless network, especially useful in a corporate network or in a public 'hotspot'. To learn more about Pseudo VLAN, read our white paper at www.compex.com.sg.

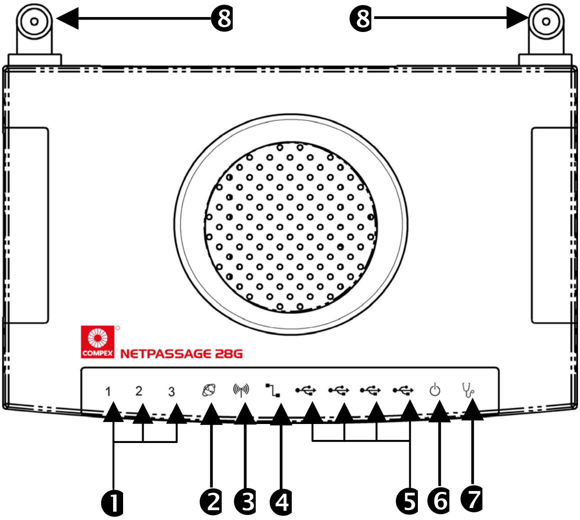
Package Contents

The router's retail package contains the following items to start you off:

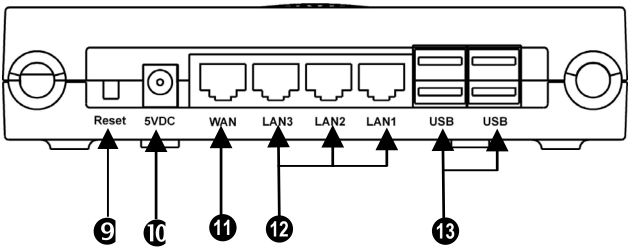
- 1x Router
- 1x External Power Adapter
- 1x Read-me-first Note
- 1x Product CD (consists Quick Install Guide, User's Manual, Firmware Recovery Tool & Utilities)
- 1x Wall-Mounting Template
- 1x UTP RJ45 Ethernet straight cable

Schematic Overview of the Router

Top View



Back View

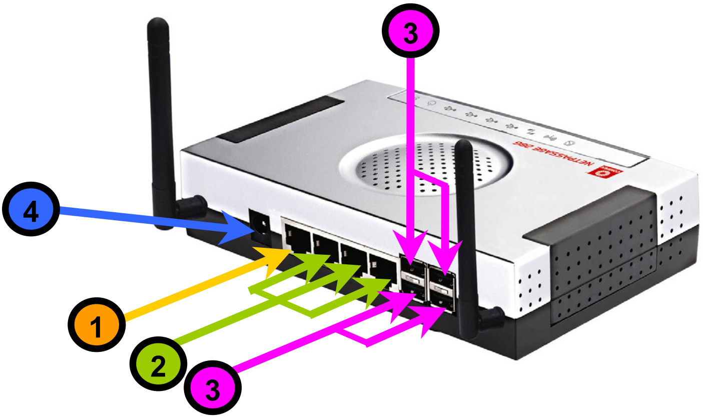


Label	Name	Description	
❶	LAN Link/Act LEDs 1, 2,3	Steady GREEN	LAN connection is on.
		Flashing GREEN	Data transmission at LAN connection.
❷	WAN LED	Steady GREEN	WAN connection is on
❸	Wireless LAN Link/Act LED	Steady GREEN	At least one wireless client is present.
		Flashing GREEN	Activity is detected in the wireless network.
❹	WAN Link/Act LED	Flashing GREEN	Data transmission at WAN connection.
❺	USB LEDs 1,2,3,4	Steady GREEN	USB device is detected.
		Flashing GREEN	Data transmission at respective USB ports.
❻	Power LED	Steady BLUE	The device has powered up.
❼	Diagnostic LED	Flashing GREEN	It indicates that the firmware is corrupted.
❽	External Antennas	SMA detachable antennas	
❾	Reset	Push button	To reboot, press once. To reset password, press and hold the button for 5 seconds before releasing it. To restore factory default settings, press and hold the button for more than 8 seconds before releasing it.
❿	5 VDC	Power Input	
⓫	WAN (RJ45 Port)	WAN port connects to Cable/ADSL modem	
⓬	LAN RJ45 Ports 1,2,3	Integrated LAN Switch Ports	
⓭	USB Ports 1, 2,3,4	Integrated USB2.0 Ports	

Chapter 3: Let's Get Going-Hardware Setup

Power Up in 4 Steps:

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



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 If you have a computer with an Ethernet connection you wish to join to the wired network, connect an Ethernet cable from that PC to any LAN ports on the router (labeled 1-3).

3 Connect the USB devices (such as 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.

You may power on the device now. You are done with the hardware setup!

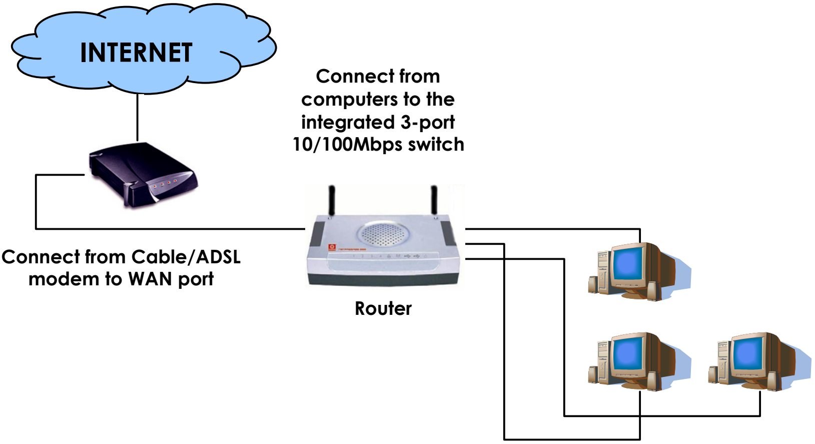
Network Application Examples

The router is suited to accomplish different network configurations you may have in mind. Combined with a web-based configuration interface, you can easily set up your feature-rich router for these applications.

Here, before proceeding to the next chapter on software setup, you may like to reference the following three application examples for the router:

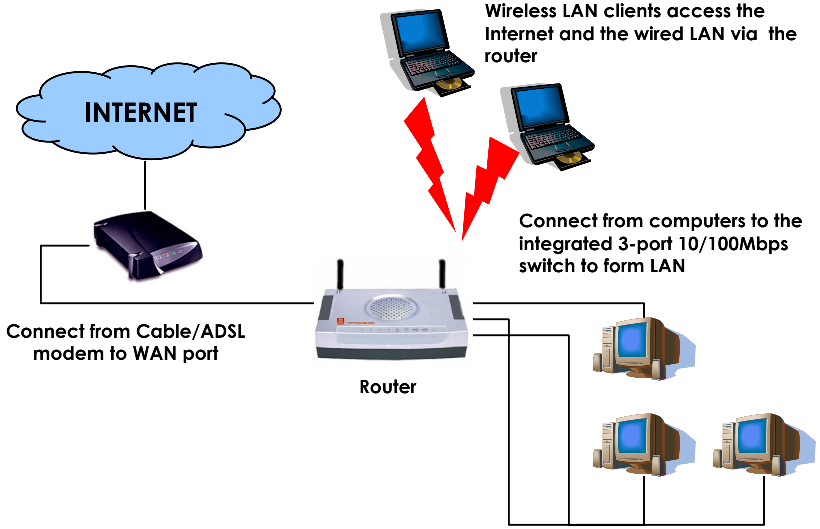
1. **Broadband Internet Access Distribution to Fast Ethernet Network**
2. **Broadband Internet Access Distribution to Fast Ethernet & Wireless Network**

1 Broadband Internet Access Distribution to a Fast Ethernet Network


INTERNET
Connect from computers to the integrated 3-port 10/100Mbps switch
Connect from Cable/ADSL modem to WAN port
Router

In this set up example, three computers are connected to the integrated 3-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 a Fast Ethernet Network & Wireless Network


Wireless LAN clients access the Internet and the wired LAN via the router
INTERNET
Connect from computers to the integrated 3-port 10/100Mbps switch to form LAN
Connect from Cable/ADSL modem to WAN port
Router

This set up example is similar to the previous with the exception of the two notebooks set up as wireless clients as illustrated above. They are connected to the Internet as well as the wired LAN via the 802.11g/801.11b-compatible router. Your wired network can thus be easily expanded to include wireless clients, enabling them to share network resources and a broadband Internet access.

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 aimed to quickly enable effective use of the product:

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 configure each of your computers to communicate with the router.

> For Computers that will be connected to the Fast Ethernet via cables:

The first step is to make sure the PC gets an IP address for which it will use to communicate with the router and each other across the network. You can begin by setting up your PC to function as a DHCP client, configuring its network settings to obtain an IP address automatically. 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 performance of this 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 (also known as a network 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.

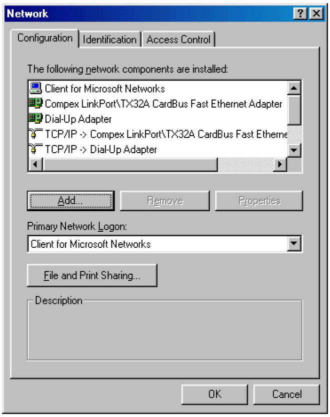
If your PC does not have TCP/IP installed, click the **Start** button and then click on **Help**. Search for the keyword TCP/IP and then follow the instructions to install the protocol.

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

If you are using Microsoft Windows 98SE or Windows Millennium

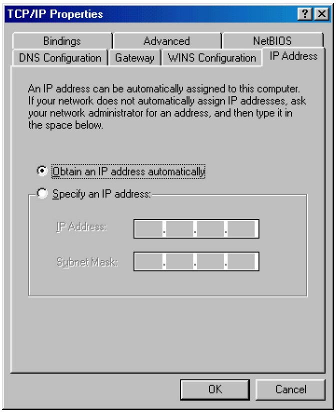
1. Click the **Start** button. Select **Settings** and click the **Control Panel** icon. Then double-click the **Network** icon. You will see the Network dialog on the right.

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.



The following network components are installed:
- Client for Microsoft Networks
- Compex LinkPort\TX32A CardBus Fast Ethernet Adapter
- Dial-Up Adapter
- TCP/IP -> Compex LinkPort\TX32A CardBus Fast Etherne
- TCP/IP -> Dial-Up Adapter

Primary Network Logon: Client for Microsoft Networks



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

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.

Windows may ask you for the original Windows installation disk or additional files. Check for the files at c:\windows\options\cabs, or insert the Windows CDROM disc into the CDROM drive and check the correct file and drive location.

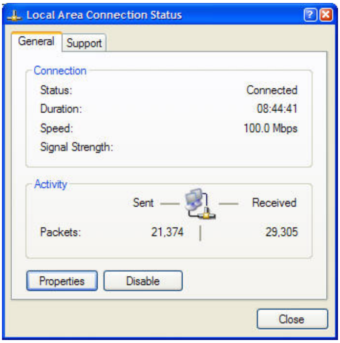
6. Windows may ask you to restart the PC, if so, click the **Yes** button and allow the PC to restart. If not, restart the PC to complete the configuration.

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.



Local Area Connection Status

Connection

Status: Connected

Duration: 08:44:41

Speed: 100.0 Mbps

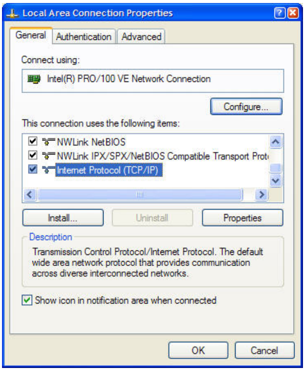
Signal Strength:

Activity

Sent — Received

Packets: 21,374 | 29,305

2. Double-click the **Local Area Connection** icon for the Ethernet adapter applicable to your Internet connection, and click the **Properties** button. You will be brought to the dialog page below.



Local Area Connection Properties

Connect using:

Intel(R) PRO/100 VE Network Connection

This connection uses the following items:

☑ NWLink NetBIOS

☑ NWLink IPX/SPX/NetBIOS Compatible Transport Prot

☑ Internet Protocol (TCP/IP)

Description

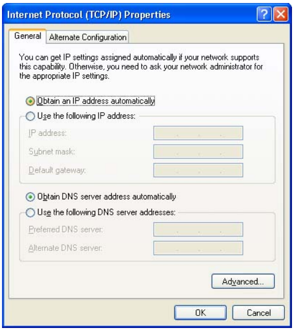
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

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.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

5. Restart your computer to complete the PC configuration.

eXpert

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

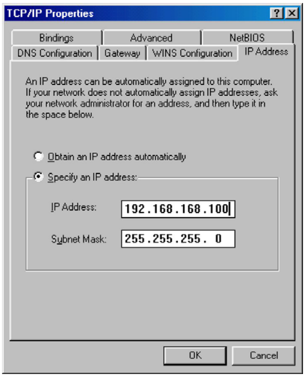
If you are using Microsoft Windows 98SE or Windows Millennium

c

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 the **IP address** and **Subnet Mask** of 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)

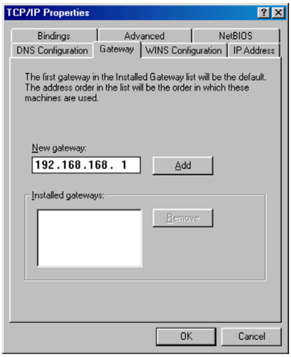


TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically
● Specify an IP address:

IP Address: 192.168.168.100
Subnet Mask: 255.255.255. 0



TCP/IP Properties

The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

New gateway: 192.168.168. 1

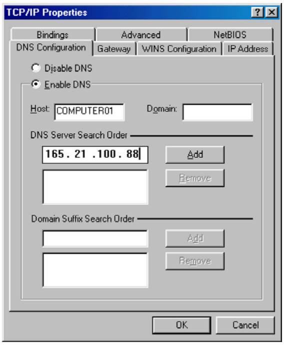
Installed gateways:

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 where its default is 192.168.168.1. Follow up 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 can complete the set up by clicking the **OK** button, and then restarting the computer.



TCP/IP Properties

○ Disable DNS
● Enable DNS

Host: COMPUTER01 Domain:

DNS Server Search Order
165. 21 .100. 88

Domain Suffix Search Order

Important: For step 5 above, you should not configure more than one computer with the same host name within a network. This will result in a conflict.

The DNS Server's IP address required in step 5 should be provided by your Internet Service Provider (ISP). If you are unsure about it, please contact your ISP.

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

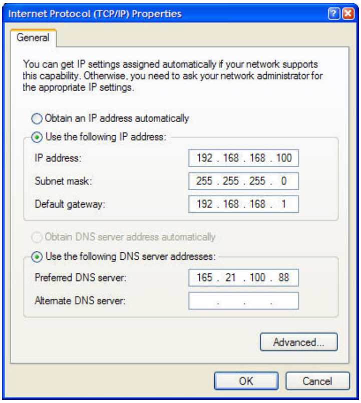
If you are using Microsoft Windows 2000 or Windows XP

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.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 168 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 168 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 165 . 21 . 100 . 88

Alternate DNS server: . . .

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 for which it will use to communicate with the router and each other across the network.

Hence, refer to Part 1(a) and (b) for the setup instructions, while noting that the likely network connection name you will encounter in Windows XP is **Wireless Network Connection** corresponding to the wireless Ethernet adapter you use.

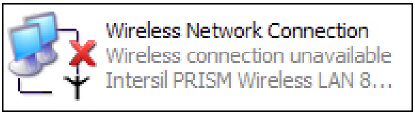
Once you have completed the IP configuration for the wireless client, you may proceed to set up your wireless client's SSID (Network name) so that it will connect with the router.

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

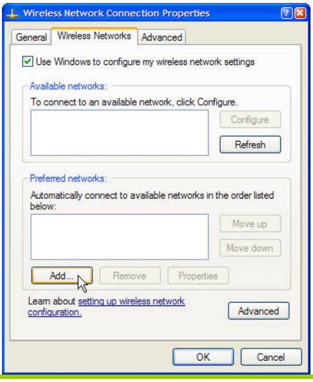
Part 1(e) : Configuring your Wireless Client…

If you are using Microsoft Windows XP

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



Wireless Network Connection
Wireless connection unavailable
Intersil PRISM Wireless LAN 8…



Wireless Network Connection Properties

General | Wireless Networks | Advanced

☑ Use Windows to configure my wireless network settings

Available networks:
To connect to an available network, click Configure.

Preferred networks:
Automatically connect to available networks in the order listed below:

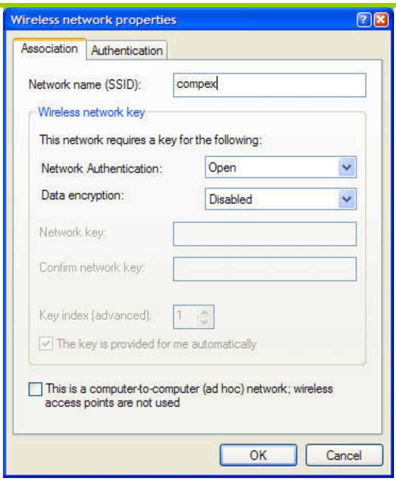
Learn about setting up wireless network configuration.

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

3. Next, key in a **Network name** with the SSID of the wireless network. It must be the same as the **WLAN name (ESSID)** in Part 2. For illustration purpose, we typed **compex**. (Take note that 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).



Network name (SSID): compex

This network requires a key for the following:

Network Authentication: Open

Data encryption: Disabled

Network key:

Confirm network key:

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Completing Part 1, we have set up our PCs & wireless clients' IP addressing properties. We will now be ready to discuss the software setup of the router configurations to go online!

Part 2 - Basic Setup

In this portion on the basic set up, you will find information on how you may configure the NetPassage 28G to function in your network, to access the Internet and begin sharing the connection with your wired and wireless clients. Please note that the NetPassage 28G, by factory default, is loaded with router firmware.

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

exclusive!

Compex has developed a powerful uConfig utility which will provide you hassle-free access to the router's web-based configuration page. Whether you have non-standard TCP/IP settings on the PC, or you have changed but forgotten the router's default management IP, uConfig will bring you to the router's set up – every time!

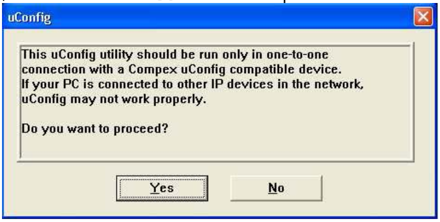
It is simple. Ensure that the router is switched on, and the PC is connected to a LAN port, then you will be brought to the web-based configuration page by following the 3 simple steps below.

Part 2 : Getting Ready to go Online!

Accessing the Web Page Interface through uConfig

1. Insert the Product CD into your CD-ROM drive. The CD will run automatically. From the **Utilities** section, select to install the **uConfig** utility to your hard disk.

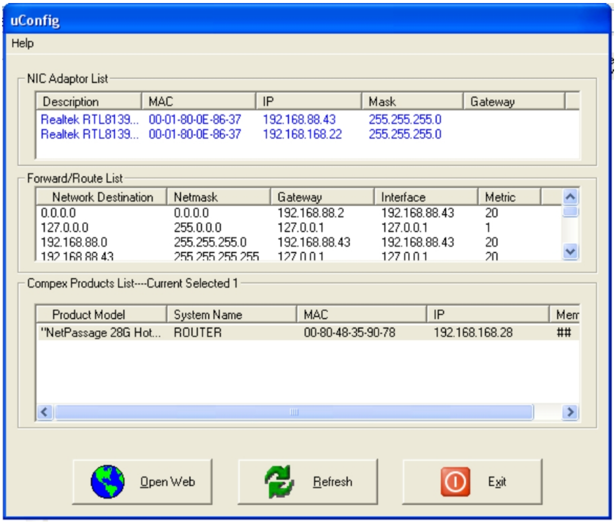
2. When the utility has been installed, double-click on the **uConfig** icon. The following screen will appear, click on the **Yes** button to proceed.



This uConfig utility should be run only in one-to-one connection with a Compex uConfig compatible device.
If your PC is connected to other IP devices in the network, uConfig may not work properly.

Do you want to proceed?

3. Select ***NetPassage 28G Hotspot*** in the **Compex Products List** section and click on the **Open Web** button. To retrieve and display the latest device(s) in the list, click on the **Refresh** button.



NIC Adaptor List

Description	MAC	IP	Mask	Gateway
Realtek RTL8139...	00-01-80-0E-86-37	192.168.88.43	255.255.255.0	
Realtek RTL8139...	00-01-80-0E-86-37	192.168.168.22	255.255.255.0	

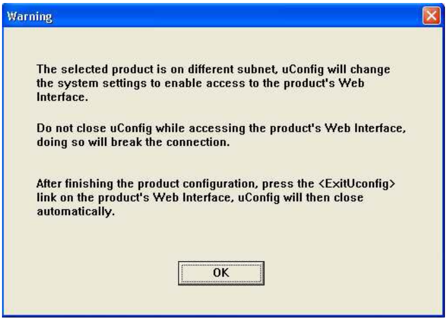
Forward/Route List

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.88.2	192.168.88.43	20
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.88.0	255.255.255.0	192.168.88.43	192.168.88.43	20
192.168.88.43	255.255.255.255	127.0.0.1	127.0.0.1	20

Compex Products List---Current Selected 1

Product Model	System Name	MAC	IP	Mem
"NetPassage 28G Hot...	ROUTER	00-80-48-35-90-78	192.168.168.28	##

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

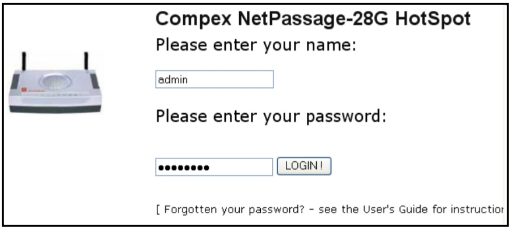


The selected product is on different subnet, uConfig will change the system settings to enable access to the product's Web Interface.

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

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

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



Compex NetPassage-28G HotSpot

Please enter your name:

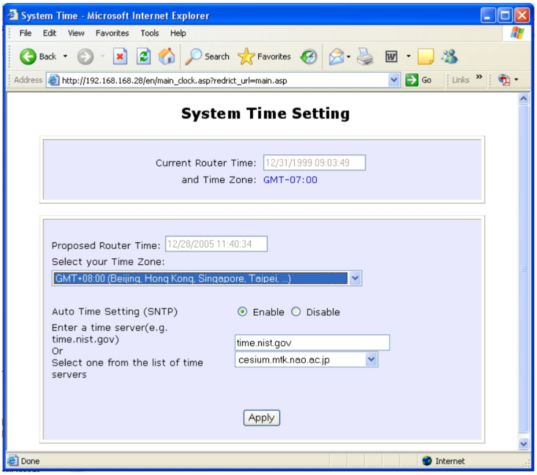
admin

Please enter your password:

•••••••••

[Forgotten your password? - see the User's Guide for instructior

6. For the first time login, you will be prompted to select your time zone setting first before accessing the router's main web page. Take note that during the next and subsequent logins, you will not see the **System Time Setting** page again.



System Time - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go
Links
Done
Internet

http://192.168.168.28/en/main_clock.asp?redrict_url=main.asp

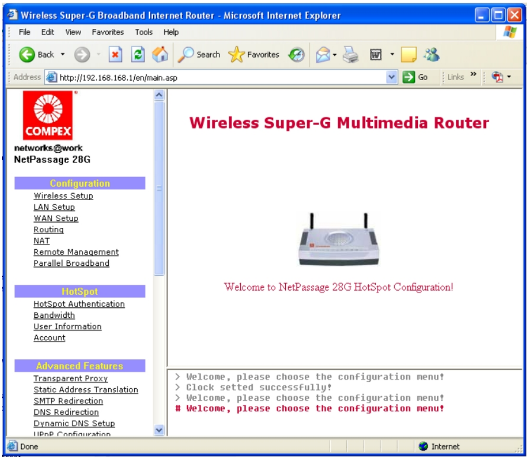
System Time Setting

Current Router Time: 12/31/1999 09:03:49
and Time Zone: GMT-07:00

Proposed Router Time: 12/28/2005 11:40:34
Select your Time Zone:
GMT+08:00 (Beijing, Hong Kong, Singapore, Taipei, ...)

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

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



http://192.168.168.1/en/main.asp

Wireless Super-G Multimedia Router

Welcome to NetPassage 28G HotSpot Configuration!

```
> Welcome, please choose the configuration menu!
> Clock setted successfully!
> Welcome, please choose the configuration menu!
# Welcome, please choose the configuration menu!
```

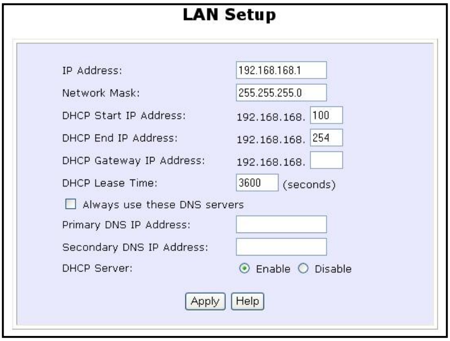
Part 3 (a) : Getting Ready to go Online!

Completing your general LAN Setup

1. The **DHCP Start IP Address** and the **DHCP End IP Address** has been pre-configured from 192.168.168.100 to 192.168.168.254 (You may select any number from 2 to 254).

2. Next, we shall move on to configure the router to handle IP addressing. Click on **LAN Setup** under **CONFIGURATION**.

You will 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. (The router's subnet is 192.168.168.0)



LAN Setup

IP Address: 192.168.168.1

Network Mask: 255.255.255.0

DHCP Start IP Address: 192.168.168. 100

DHCP End IP Address: 192.168.168. 254

DHCP Gateway IP Address: 192.168.168.

DHCP Lease Time: 3600 (seconds)

□ Always use these DNS servers

Primary DNS IP Address:

Secondary DNS IP Address:

DHCP Server: ● Enable ○ Disable

3. For **DHCP Gateway IP address**, set it as 192.168.168.1 unless you have another device you like to use as the router for your clients.

4. Leave the **Always use these DNS servers** unchecked, unless you wish to access certain specific DNS servers only. You may leave the **Primary DNS IP Address** and **Secondary DNS IP Address** as blank. If the **Always use these DNS servers** is set to be enabled, the user has to input the **Primary DNS IP Address**.

5. 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	Insert the IP address of the gateway to Internet or of the router if this router is the one connecting to the Internet. 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. 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. 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>.
Always use these DNS servers	Enable this checkbox if you want the router to only use the DNS server you have specified below.

Primary DNS IP Address	The IP address of the DNS server is usually provided by your ISP.
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.

You can now proceed to Part 3(b) which pertains to the set up of the router's wireless feature.

Part 3(b) : Getting Ready to go Online!

b

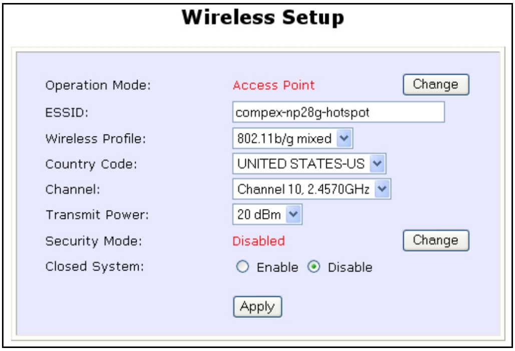
Completing your Wireless Setup

1. Quickly we move on to the router settings for your wireless users. Click on **Wireless Setup** under **CONFIGURATION** and you will see the settings screen.

2. It is important here you key in the **WLAN name (ESSID)** to be that which you intend to use for your wireless clients. This is the same as the Network Name (SSID) discussed in Part 1(e).

   Remember to change your wireless clients' settings after the router has rebooted and the new SSID has taken effect.

3. Now choose a **Wireless mode** suitable for the types of devices you have in your network. Modes such as pure 802.11g or mixed network, etc, are supported, and you may also define your preferred **Operating frequency.**



Wireless Setup

Operation Mode: Access Point
ESSID: compex-np28g-hotspot
Wireless Profile: 802.11b/g mixed
Country Code: UNITED STATES-US
Channel: Channel 10, 2.4570GHz
Transmit Power: 20 dBm
Security Mode: Disabled
Closed System: ○ Enable ● Disable

4. Leave **Security mode** as **None** for now and the other remaining settings empty. Click the **Apply** button to complete your wireless setup.

   Take note that **Security Mode** will be discussed in the next chapter.

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

CONFIGURATION: WAN SETUP

The **WAN Setup** in Part 3(c) is a critical section on broadband setup. A successful configuration requires you to identify the type of broadband Internet access you subscribed to:

i. ***Cable Internet where your ISP dynamically assigns an IP address*** to you, refer to Part 3(c)i titled WAN Setup - Cable Internet with Dynamic IP Assignment.

ii. ***Cable Internet where your ISP provides you with an IP*** (or a range of IP addresses), refer to Part 3(c)ii titled WAN Setup - Cable Internet with Static IP Assignment.

iii. ***ADSL Internet that requires standard PPP over Ethernet (PPPoE)*** for authentication, refer to Part 3(c)iii titled 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 Part 3(c)iv titled WAN Setup – ADSL Internet using Point to Point Tunneling Protocol (PPTP).

Part 3(c)i : WAN Setup - Cable Internet with Dynamic IP Assignment

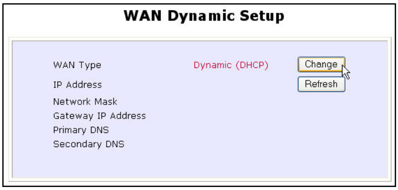
Selecting the Correct WAN Type

The router is pre-configured to support a WAN type that dynamically obtains an IP address from the ISP. However, you may verify that the settings are correct 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 the **WAN Type** reads **Dynamic (DHCP)** in red colour. Otherwise, click on the **Change** button.

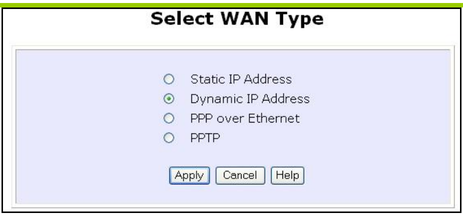
3. Simply select **Dynamic IP Address**, hit the **Apply** button and you are done!



WAN Dynamic Setup

WAN Type Dynamic (DHCP)
IP Address
Network Mask
Gateway IP Address
Primary DNS
Secondary DNS

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



Select WAN Type

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

Important: Please note the exceptional cases described on the following page for certain Cable Internet Service Providers.

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

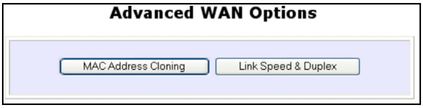
a. Certain ISPs log the MAC address of the first device connected to the broadband channel and refuse to release an IP address unless the MAC address matches the one in their log. Therefore, if yours is not a new Cable Internet subscription (i.e. you have an adapter formerly connected directly to your cable modem), refer to **steps 5 - 7** to clone the "approved" MAC address to the router.

b. Certain ISPs require the authentication of a DHCP Client ID before releasing an IP address to you. The router uses the System Name set 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 set up.

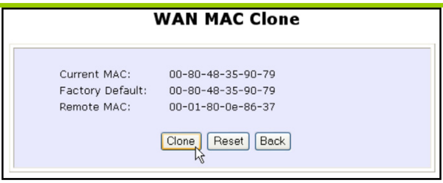
5. Steps 5 - 7 are for those who need to clone their Ethernet adapter's MAC address.

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



Advanced WAN Options

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



WAN MAC Clone

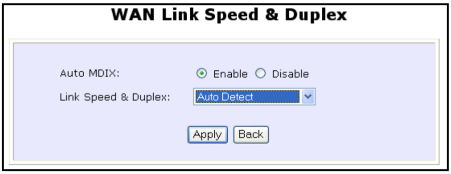
Current MAC: 00-80-48-35-90-79
Factory Default: 00-80-48-35-90-79
Remote MAC: 00-01-80-0e-86-37

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

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

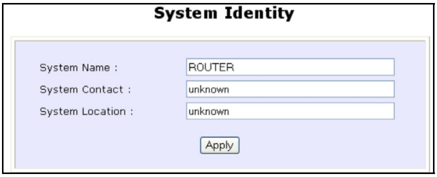
8. Steps 8 - 10 are for those who need to set up the **System Name** in **System Identity** so that your ISP can authenticate it as a valid DHCP Client ID.

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



WAN Link Speed & Duplex

Auto MDIX: ● Enable ○ Disable
Link Speed & Duplex: Auto Detect



System Identity

System Name : ROUTER
System Contact : unknown
System Location : unknown

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.

Part 3(c)ii : WAN Setup - Cable Internet with Static IP Assignment

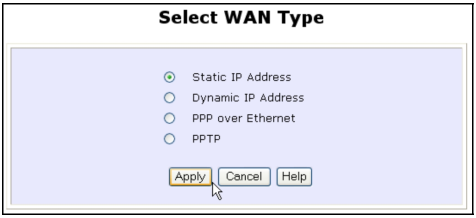
c

Selecting the Correct WAN Type

If you have an ISP that leases a static 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 set up 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

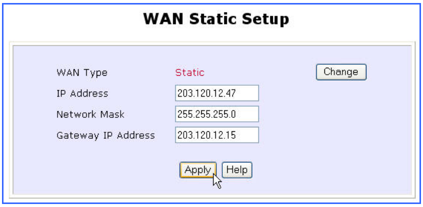
1. Under the **CONFIGURATION** on the command menu, click on **WAN Setup**.



Select WAN Type

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

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.



WAN Static Setup

WAN Type	Static	Change
IP Address	203.120.12.47	
Network Mask	255.255.255.0	
Gateway IP Address	203.120.12.15	

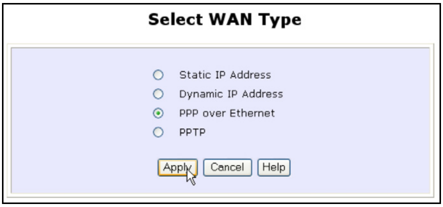
3. Fill in the information provided by your ISP in the **IP Address**, **Network Mask** and **Gateway IP Address** fields, followed by clicking the **Apply** button.

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

Part 3(c)iii : 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 in these steps that follow. For example, you may configure an account whose username is 'guest' as described below:



Select WAN Type

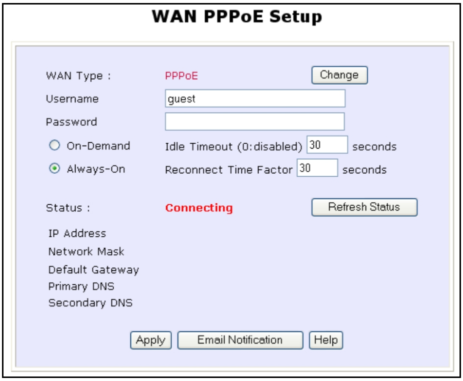
○ Static IP Address
○ Dynamic IP Address
● PPP over Ethernet
○ PPTP

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 wish that your router will always maintain an established connection with the ISP. Otherwise, you may select **On-Demand**. The router will connect to the ISP automatically when it receives Internet requests from your PCs.



WAN PPPoE Setup

WAN Type : PPPoE
Username: guest
Password:
○ On-Demand — Idle Timeout (0:disabled) 30 seconds
● Always-On — Reconnect Time Factor 30 seconds

Status : Connecting

IP Address
Network Mask
Default Gateway
Primary DNS
Secondary DNS

The **Idle Timeout** setting is associated with the **On-Demand** option, allowing you to specify the value (in seconds) for 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** 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.

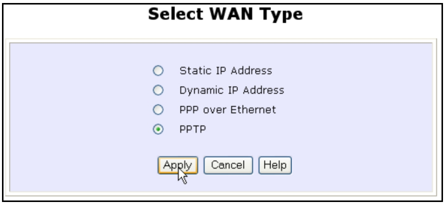
Part 3(c)iv : WAN Setup – ADSL Internet using PPTP

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 in these 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**.

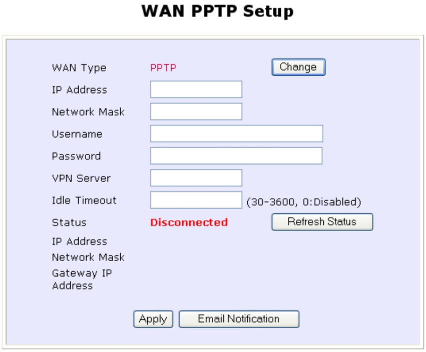

Select WAN Type

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

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.


WAN PPTP Setup

WAN Type	PPTP
IP Address	
Network Mask	
Username	
Password	
VPN Server	
Idle Timeout	(30-3600, 0:Disabled)
Status	Disconnected
IP Address	
Network Mask	
Gateway IP Address	

The **Idle Timeout** setting is associated with the **On-Demand** option, allowing you to specify the value (in seconds) for which the router will disconnect from the ISP after the last Internet activity. A value of "0" will disable idle timeout.

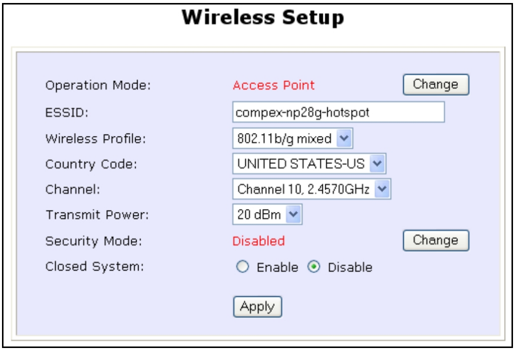
Chapter 5: Advanced Configuration

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 menus:

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 a WPA-PSK or WEP to secure data transmissions within your wireless clients and the network.



Wireless Setup

Operation Mode:	Access Point	Change
ESSID:	compex-np28g-hotspot	
Wireless Profile:	802.11b/g mixed	
Country Code:	UNITED STATES-US	
Channel:	Channel 10, 2.4570GHz	
Transmit Power:	20 dBm	
Security Mode:	Disabled	Change
Closed System:	○ Enable ● Disable	

Operation Mode : The router can choose to operate as an access point or a access point client. The Access Point operation mode is set by default. If you want to change the operation mode, just click on the **Change** button.

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 a list of wireless modes available:

- **802.11b only**

This mode supports wireless B clients with bandwidth up to 11Mbps in the distance range of 2.4Hz.

- **802.11g only**

This mode supports wireless G clients that offer transmission over relatively short distances at up to 54Mbps.

- **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.

- **Super-G**

This mode supports wireless super-G clients that offer transmission rates of up to 108Mbps in the 2.4GHz frequency band.

Operating frequency : This option allows you to select a frequency channel for the wireless communication.

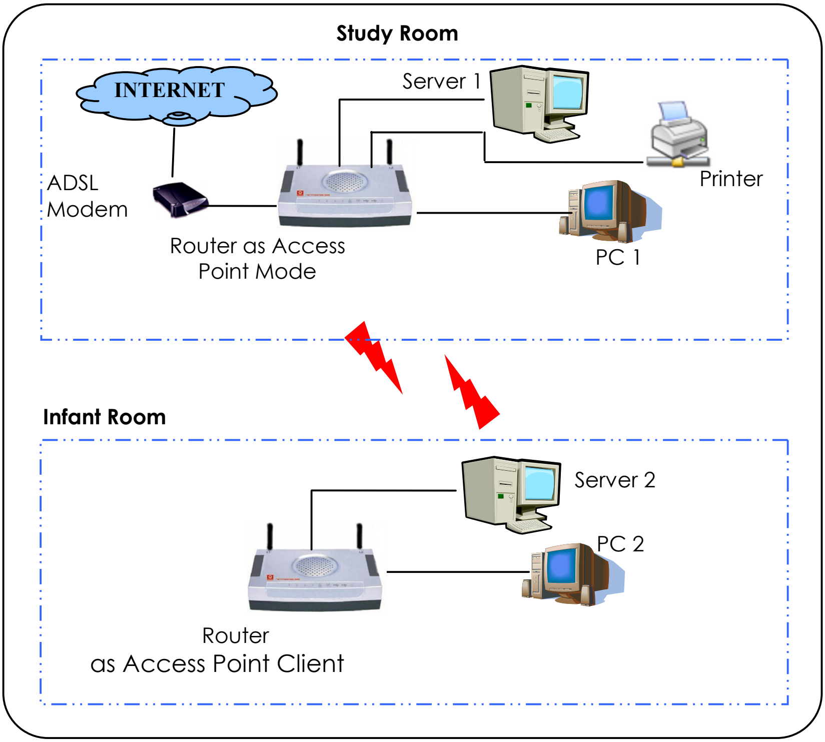
Transmit Power : This option allows you to select a specific transmit power for the wireless communication. The Transmit Power controls the signal strength transmitted by the antenna. If the antenna has a weak RF coverage, increase the Transmit Power. If the antenna has a strong RF coverage, decrease the Transmit Power.

Security mode : The router supports three types of authentication : **WPA-PSK** and **WEP**. Two types of WEP private encryption are 64-bit WEP and 128-bit WEP. You may also opt to disable wireless security by setting **Security mode** to **Disable**. (Not recommended).

Close system : The router will not broadcast its **WLAN name (ESSID)** when **Close system** is enabled. By default, **Close system** is disabled.

Hardware setup of the Router

The router can also operate in two modes such as Access Point and Access Point Client. With its built-in USB ports functionality that is easy to operate, you can print from any PC on the network to any printer connected to the router via its USB port.



The above illustration is an example on how to use the two routers as Access Point Mode and Access Point Client respectively to print wirelessly in two separate rooms.

1. Connect an Ethernet cable to your Cable/ADSL modem and then to the socket labeled **WAN** on your router.

2. Connect one end of the RJ45 Ethernet cable to your network adaptor in your PC and the other end to the LAN port of your router.

3. Next, plug in the power adapter that is supplied in the package to the main electrical supply, and connect the power plug to the socket on the router. You may power on the device now. You are done with the hardware setup!

Configuring your PC

Configure your PC to obtain its IP address automatically. Alternatively, you may want to give your PC a static IP address if you are an expert user. For the details in configuring your PC to obtain dynamic IP address, kindly refer to the User's Manual on.

Configuration for the Router as Access Point

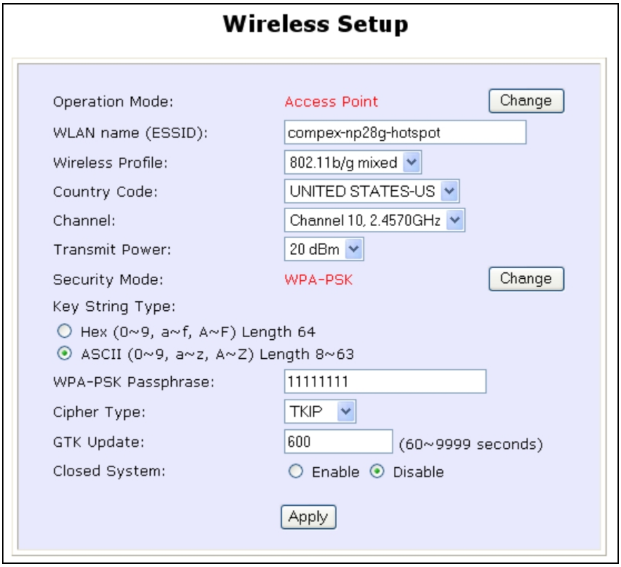
1. When all hardware installation and PC configuration have done, insert the Product CD to your CD-ROM drive, go to **Utilities** section and activate the **uConfig** program, select **Router** and click on **OpenWeb** button.

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

3. From your **Configuration** Command menu, select **Wireless Setup**. You may leave the ESSID as the default setting.

4. Next, you can select the channel at **Channel 10, 2.4570GHz**, for your operating frequency unless you have problem operating at this frequency.

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



Wireless Setup

Operation Mode:	Access Point	Change
WLAN name (ESSID):	compex-np28g-hotspot	
Wireless Profile:	802.11b/g mixed	
Country Code:	UNITED STATES-US	
Channel:	Channel 10, 2.4570GHz	
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

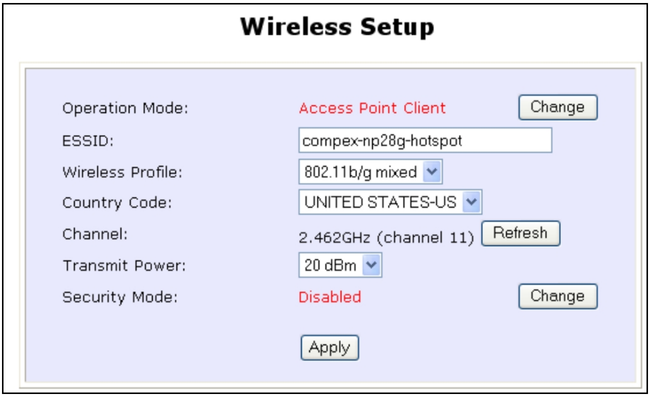
6. Next, proceed to the **WAN Setup** from the **Configuration** Command menu. From here, choose the correct **WAN** type depending on your ISP. For example, if you are using the cable modem, use **Dynamic** WAN type. (For more details, refer to the section on **WAN Setup**).

7. Reboot the router.

Configuration for the Router as Access Point Client

1. As shown in this screen, when the operation mode is defaulted to Access Point, click **Change** to edit the operation mode. Select **Access Point Client**.

2. Update the required changes.



Wireless Setup

Operation Mode:	Access Point Client
ESSID:	compex-np28g-hotspot
Wireless Profile:	802.11b/g mixed
Country Code:	UNITED STATES-US
Channel:	2.462GHz (channel 11)
Transmit Power:	20 dBm
Security Mode:	Disabled

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

4. Next, proceed to the **WAN Setup** from the **Configuration** Command menu. Set your WAN Type to **PPPoP Setup** and click **Apply** to make the changes. Ensure that your modem is connected to your router's WAN port.

5. Enter the **Username** and **password** that are provided by your ISP. Click **Apply** to update the changes. When done, logout from your router's main page.

CONFIGURATION: Wireless Setup: Security Mode

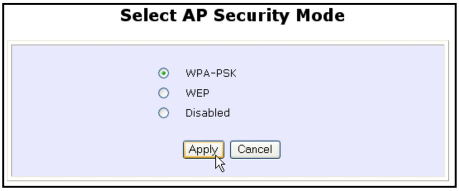
Security plays a vital role of securing wireless (802.11) networks to prevent unauthorised users from accessing sensitive data in the networks. WPA is one of the strongest standards for wireless security.

Having learnt the significance of implementing a security-based network infrastructure, listed here are the steps to configure your router: (Take note that the router is operating as an access point. We use it as an example here).

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

WPA-**P**re **S**hared **K**ey (WPA-PSK) is a special mode for home users without authentication server.

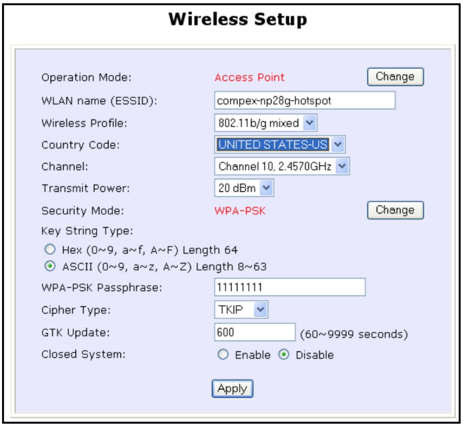
To set the Security mode to WPA-PSK, follow these instructions:



Select AP Security Mode

● WPA-PSK
○ WEP
○ Disabled

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
WLAN name (ESSID): compex-np28g-hotspot
Wireless Profile: 802.11b/g mixed
Country Code: UNITED STATES-US
Channel: Channel 10, 2.4570GHz
Transmit Power: 20 dBm
Security Mode: WPA-PSK
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

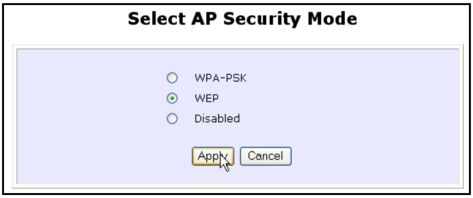
2. You will see the page of the **Wireless Setup** enabled with **WPA-PSK**.

3. Enter the inputs, then followed by the **Apply** button. You must enter at least 8 ASCII characters. Enter the inputs, then followed by the **Apply** button.

Wired **E**quivalent **P**rivacy 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:

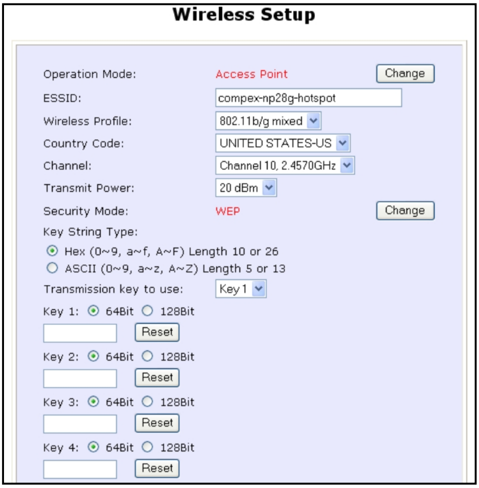
1. Under the **CONFIGURATION** command menu, you will find the **Wireless Setup** page. Click on the **Change** button next to the **Security mode**. Then check the radio button next to **WEP**, followed by the **Apply** button.



Select AP Security Mode

○ WPA-PSK
● WEP
○ Disabled

2. You will see the page of the **Wireless Setup** enabled with **WEP**, displaying the following parameters:



Wireless Setup

Operation Mode: Access Point
ESSID: compex-np28g-hotspot
Wireless Profile: 802.11b/g mixed
Country Code: UNITED STATES-US
Channel: Channel 10, 2.4570GHz
Transmit Power: 20 dBm
Security Mode: WEP
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 to use: Key 1
Key 1: ● 64Bit ○ 128Bit
Key 2: ● 64Bit ○ 128Bit
Key 3: ● 64Bit ○ 128Bit
Key 4: ● 64Bit ○ 128Bit

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

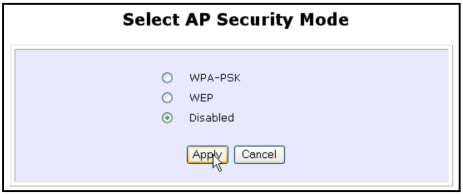
Key 1-4:
You may enter up to 4 encryption keys. If you selected 64-bit WEP, you will need to enter 10 characters. For 128-bit WEP, it requires 26 characters.
(See the table below).

The table below describes the 64-bit and 128-bit encryption.

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

3. Enter the inputs, then followed by the **Apply** button.

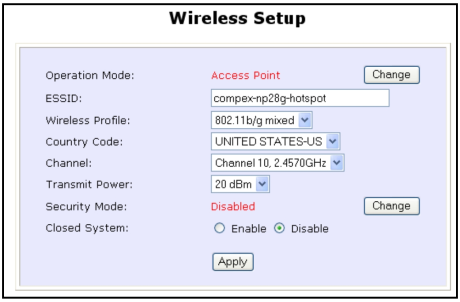
To set the Security mode to **Disabled**, follow these instructions:



Select AP Security Mode

○ WPA-PSK
○ WEP
● Disabled

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 **Disabled**, followed by the **Apply** button.



Wireless Setup

Operation Mode: Access Point
ESSID: compex-np28g-hotspot
Wireless Profile: 802.11b/g mixed
Country Code: UNITED STATES-US
Channel: Channel 10, 2.4570GHz
Transmit Power: 20 dBm
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.

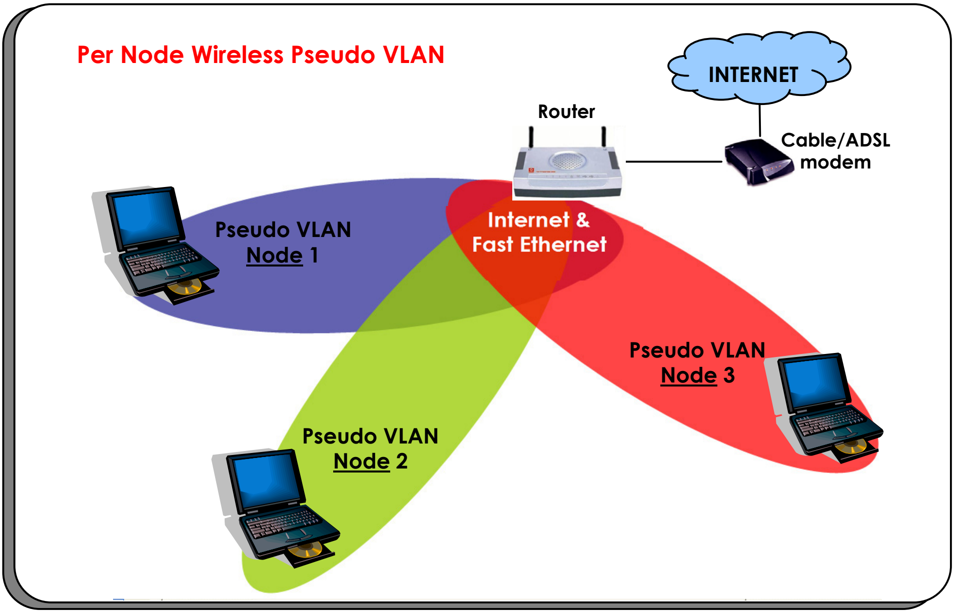
CONFIGURATION : Wireless Setup: Wireless Pseudo VLAN

The Wireless Pseudo VLAN feature on the router is exclusively created to solve the problem of privacy and data protection, to provide multiple levels of inter-client security. It is a natural extension of the Ethernet-based VLAN onto the wireless network in a corporation 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, and the router allows you to create a virtual LAN containing either a single wireless user, or a group of users. We call this Per Node and Per Group Wireless Pseudo VLAN respectively.

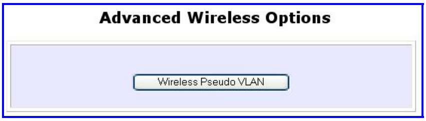
Per Node Wireless Pseudo VLAN

Per Node Wireless Pseudo VLAN, if implemented, segregates every wireless user, or node, in its own Pseudo VLAN. As illustrated in the figure below, while access to the Internet 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 their files will not be subjected to prying eyes.



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

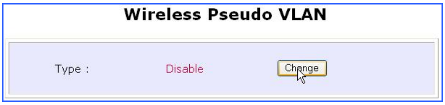
Setting up Per Node Wireless Pseudo VLAN on the router is merely a 3 steps affair:



Advanced Wireless Options

1. Under the **CONFIGURATION** command menu, you will find the **Advanced Wireless Options** within 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.

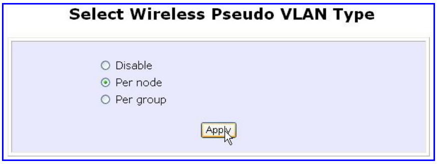


Wireless Pseudo VLAN

Type : Disable

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 Per Node Wireless Pseudo VLAN whereby each wireless user is isolated from one another.



Select Wireless Pseudo VLAN Type

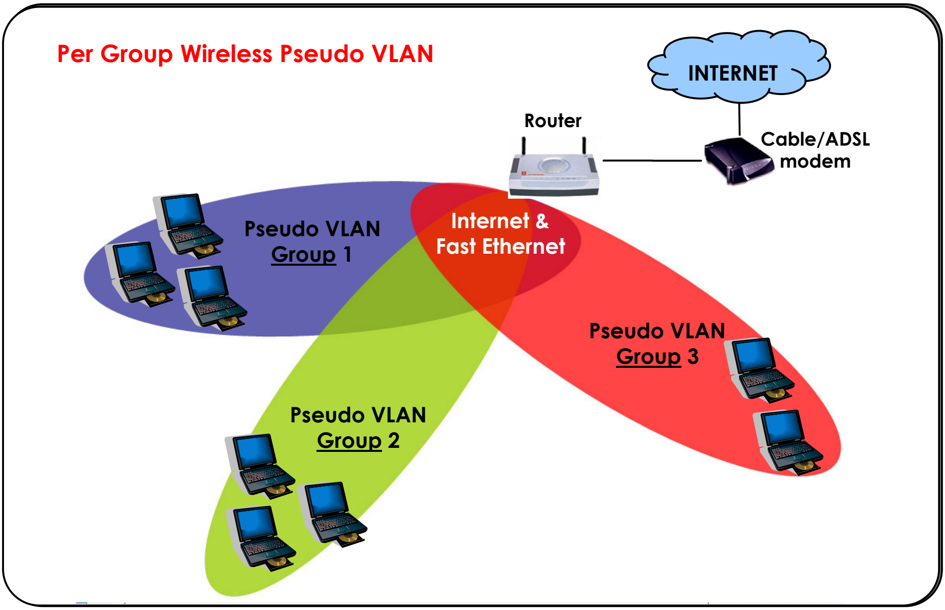
○ Disable
● Per node
○ Per group

Per Group Wireless Pseudo VLAN

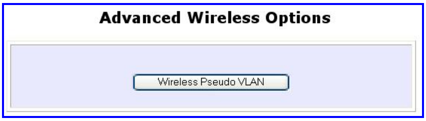
In contrast to single user segregation, Per Group Wireless Pseudo VLAN supports multiple wireless nodes per VLAN. Users grouped in the same Wireless Pseudo VLAN may access files from each other, but users from different groups are prevented from this communication. The router supports four Pseudo VLAN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

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

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

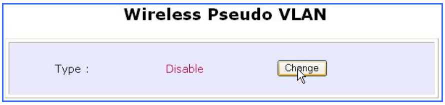


Per Group Wireless Pseudo VLAN gives you great flexibility in your wireless network set up, and with 6 steps, you may configure private virtual LANs quickly and easily between workgroups:



1. Under the **CONFIGURATION** command menu, you will find the **Advanced Wireless Options** within the **Wireless Setup** page. Click on the **Wireless Pseudo VLAN** button.

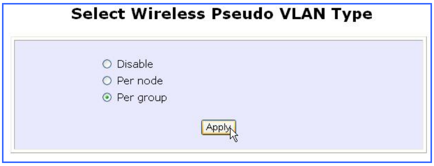
2. By default, you will note that **Wireless Pseudo VLAN** is disabled. Click the **Change** button.



Wireless Pseudo VLAN

Type : Disable

3. On the next screen, click the **Per group** radio button and hit **Apply** to complete the selection of your **Pseudo VLAN Type**.

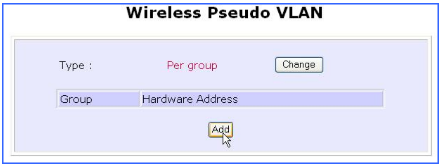


Select Wireless Pseudo VLAN Type

○ Disable
○ Per node
● Per group

4. You will be brought to the following set up screen requiring you to assign the hardware address of your client to a specific group you wish to segregate.

   Click on the **Add** button.

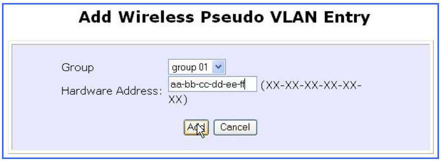


Wireless Pseudo VLAN

Type : Per group

Group	Hardware Address

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



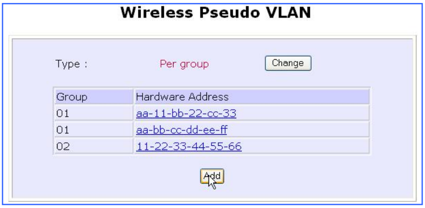
Add Wireless Pseudo VLAN Entry

Group: group 01

Hardware Address: aa-bb-cc-dd-ee-ff (XX-XX-XX-XX-XX-XX)

6. Until now, you may continue to add more groups or assign more wireless clients to groups with steps 1 to 5 described here.

   In the example shown on the right, 3 wireless clients are divided into two Per Group Wireless Pseudo VLANs 01 and 02. Two clients are assigned to Group 01 while the other 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

CONFIGURATION : LAN Setup : Advanced DHCP Server Options

For instructions on basic LAN setup within the router, please refer to Chapter 4, part 2. In this portion, we shall examine the Advanced DHCP Server Options available to the network administrator.

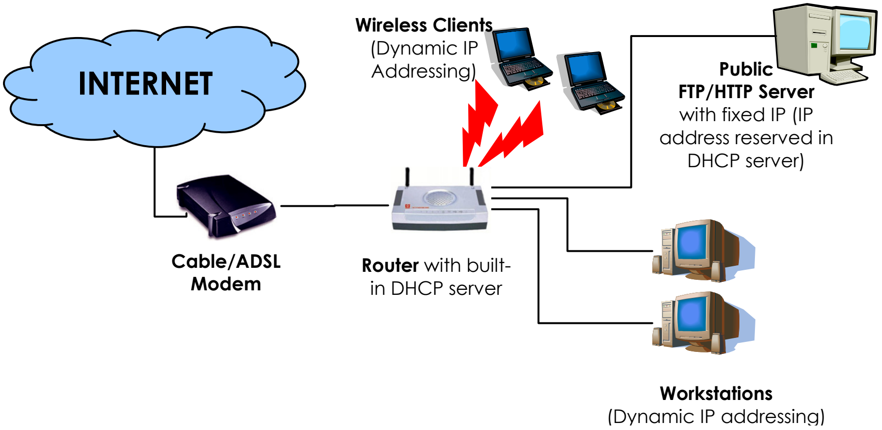
You can easily manage your network's IP address allocation with the built-in DHCP server found on the router. Once set up as described in Chapter 4, it will automatically and dynamically allocate addresses from a pool, to devices or computers connected to the network. To learn more about DHCP, please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

Learn more from our ***DHCP Technology Primer***

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 allocations 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.

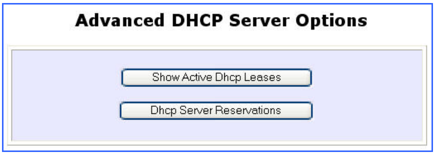
Fixed & Dynamic IP addressing: DHCP Server Reservations



Steps to configure Advanced DHCP Server Options in the router

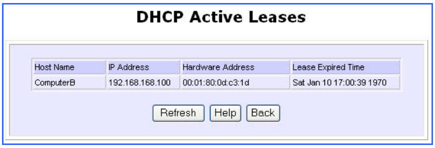
Listed here are the steps to configure the Advanced DHCP Server options available on the router:

1. Under the **CONFIGURATION** command menu, you will find the **Advanced DHCP Server Options** within the **LAN Setup** page.



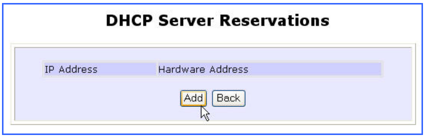
Advanced DHCP Server Options

2. You may click on **Show Active DHCP Leases** to view information of the current IP leases managed by the DHCP server. Otherwise, you can click on **DHCP Server Reservations** to reserve any specific IP Address for a certain network MAC address.



DHCP Active Leases

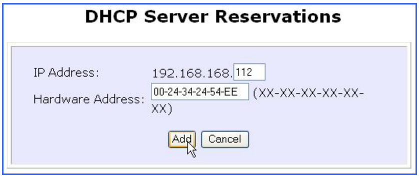
Host Name	IP Address	Hardware Address	Lease Expired Time
ComputerB	192.168.168.100	00:01:80:0d:c3:1d	Sat Jan 10 17:00:39 1970



DHCP Server Reservations

IP Address	Hardware Address

3. To add **DHCP Server Reservations**, click on the **Add** button.



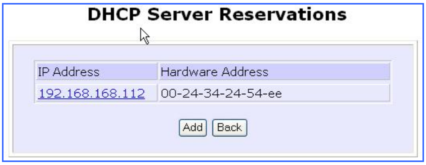
DHCP Server Reservations

IP Address: 192.168.168.112

Hardware Address: 00-24-34-24-54-EE (XX-XX-XX-XX-XX-XX)

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 on the right. After this, you may also add more reservations.



DHCP Server Reservations

IP Address	Hardware Address
192.168.168.112	00-24-34-24-54-ee

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.

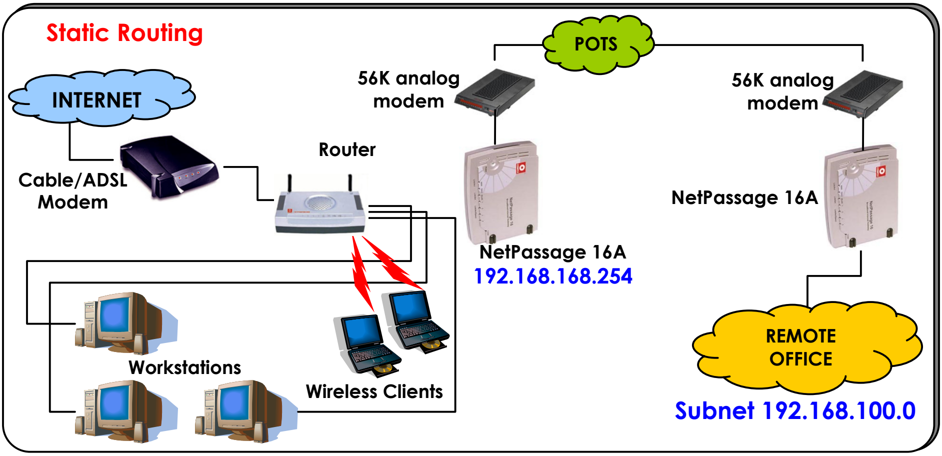
An invalid date and time shown under Expires column in Show Active DHCP Leases indicates that the router's clock has not been set. Refer to Chapter 5, section on SYSTEM TOOLS – Set Router's Clock.

CONFIGURATION : Routing

The router allows the network administrator to add a static routing entry into the routing table. Other than the default Router to the Internet, the router may reroute the IP packets to another network you defined. 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 which you have two routers in the network. One router is used for broadband Internet sharing and 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 NetPassage 16A (192.168.168.1) and to the remote office via NetPassage 16A (192.168.168.254). The remote location resides on a subnet 192.168.100.0.

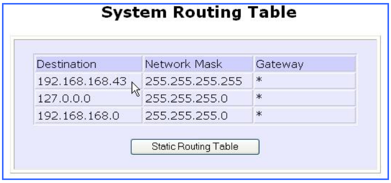
You may add a static routing entry into the router's routing table so that IP packets from the clients in the main office with a destination IP address of 192.168.100.X (where X is any number from 2 to 254) will be re-routed to the NetPassage 16A router with IP address 192.168.168.254.

Steps to configure Static Routing of the router

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

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

   What you see here are the default routing entries built into the router depending on its IP Address and Network Mask.

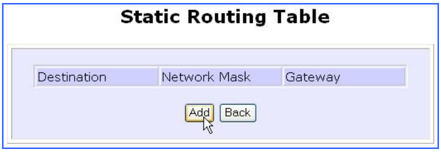


System Routing Table

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	*

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

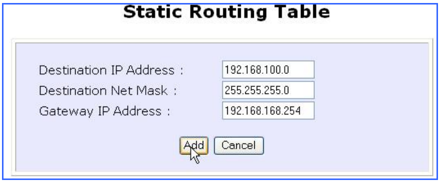
3. On this page, click the **Add** button.



Static Routing Table

Destination	Network Mask	Gateway

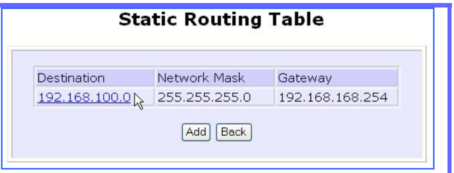
4. You may specify the **Destination IP Address**, **Destination Net Mask** and **Gateway IP Address** here. For this example, they are 192.168.100.0, 255.255.255.0 and 192.168.168.254 respectively. Hit the **Add** button to finish.



Static Routing Table

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

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

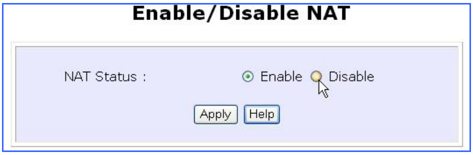


Static Routing Table

Destination	Network Mask	Gateway
192.168.100.0	255.255.255.0	192.168.168.254

CONFIGURATION: NAT

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



Enable/Disable NAT

NAT Status : ● Enable ○ Disable

The basic purpose of NAT is to share a single public IP address with multiple PCs in the private network by using different TCP ports for each PC. NAT is enabled by default.

Due to the NAT, computers behind the router will not be directly accessible from the Internet. Hence, if there is a need to traverse the NAT from without, you will need to employ the use of Virtual Servers. 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 these complementary technologies found on Compex's products please turn to the NAT Technology Primer found on the Product CD.

Learn more from our ***NAT*** ***Technology Primer***

> **Important**: Do NOT disable NAT unless you are certain about what you are doing. Disabling NAT will disable broadband Internet sharing effectively.

Steps to configure Virtual Servers based on De-Militarized Zone (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 NAT-enabled network directly accessible from the Internet.

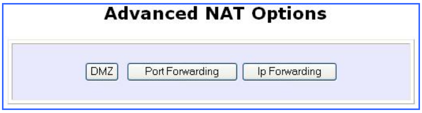
When NAT is enabled, a request from a client within the private network first goes to the router. Upon receiving a request, the router keeps track of which client is using which port number. Since any reply from Internet goes to the router first, the router (from the port number in the reply packet) 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.

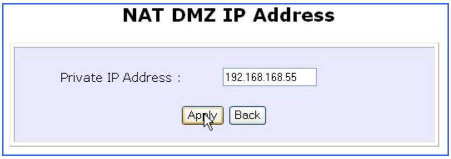
Here are the steps to set it up:



Advanced NAT Options

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



NAT DMZ IP Address

Private IP Address : 192.168.168.55

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

4. Enter **0.0.0.0** as the **Private IP Address** will disable DMZ. Remember to click the **Apply** button.

NOTE:

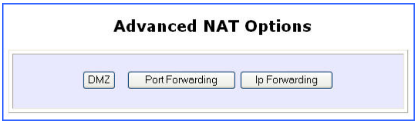
1. When you enable DMZ, the Static IP Address configuration is recommended for the DMZ host. Otherwise, if the address is allocated by DHCP, it may change and DMZ will not function properly.

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 of its function, please refer to the NAT Technology Primer on the Product CD.

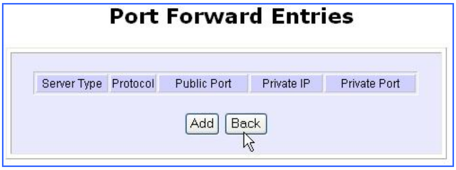
Here are the steps to set it up:

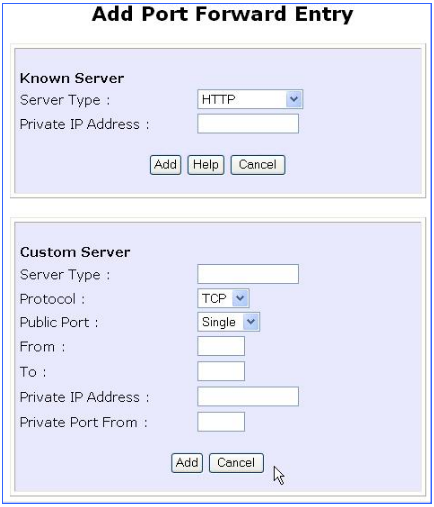


1. Under the **CONFIGURATION** command menu, click on **NAT**. You will find the **Advanced NAT Options** available near the bottom of the page.

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

3. Hit the **Add** button on this screen on **Port Forward Entries**.





Add Port Forward Entry

Known Server

Server Type : HTTP

Private IP Address :

Custom Server

Server Type :

Protocol : TCP

Public Port : Single

From :

To :

Private IP Address :

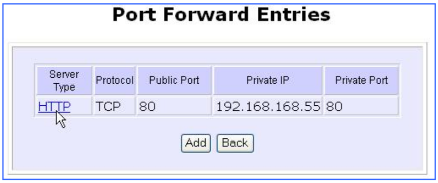
Private Port From :

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

For an elaborated explanation, please refer to the NAT Technology Primer found on the Product CD.

Learn more from our ***NAT*** ***Technology Primer***

5. In this example, for **Known Server**, if you selected **HTTP** for the **Server Type** and entered a **Private IP Address** of 192.168.168.55, followed by clicking 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

Known Server

Server Type : Select from the drop-down list of server types (HTTP, FTP, POP3 or Netmeeting.

Private IP Address : Specify the 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 from the drop-down list of either TCP or UDP protocol type.

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.

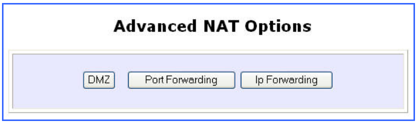
Private IP Address	:	Specify the IP address of your server PC running within the private network.
Private Port From	:	Starting private port number. The ending private port number will be calculated automatically according to the public port range.

Steps to configure Virtual Servers based on IP Forwarding

When you have more than one IP address subscribed 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.

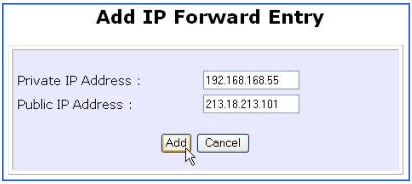
If you require more information of its function, please refer to the NAT Technology Primer on the Product CD. Here are the steps to set it up:

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



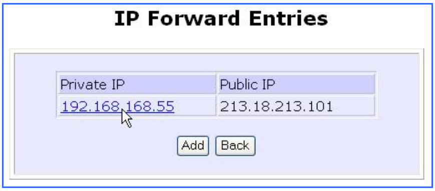
2. Click the **IP Forwarding** button to configure Virtual Servers based on IP Forwarding.

3. At the next screen **Add IP Forward Entry**, you have to specify a **Private IP Address** and a **Public IP Address**. In this example, we would like all requests for 213.18.213.101 to be forwarded to a PC with **Private IP Address** 192.168.168.55. Click the **Add** button to continue.



Private IP Address : 192.168.168.55
Public IP Address : 213.18.213.101

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



Private IP	Public IP
192.168.168.55	213.18.213.101

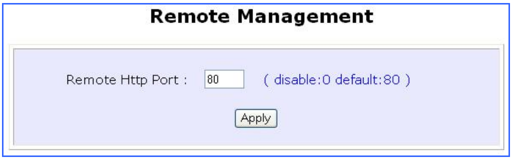
For step 3 above, please ensure that you have subscribed to the Public IP Address you intend to forward from.

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 of you to set up remote management for the router.



Remote Management

Remote Http Port : 80 (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. (In this case, to disable Remote Management, just enter 0 for **Remote Http Port**).

3. To enable **Remote Management**, enter a port number which is not being used by other HTTP Server in the network. Please take note that it is recommended to use a different port number other than port 80 because some ISP block the port number 80.

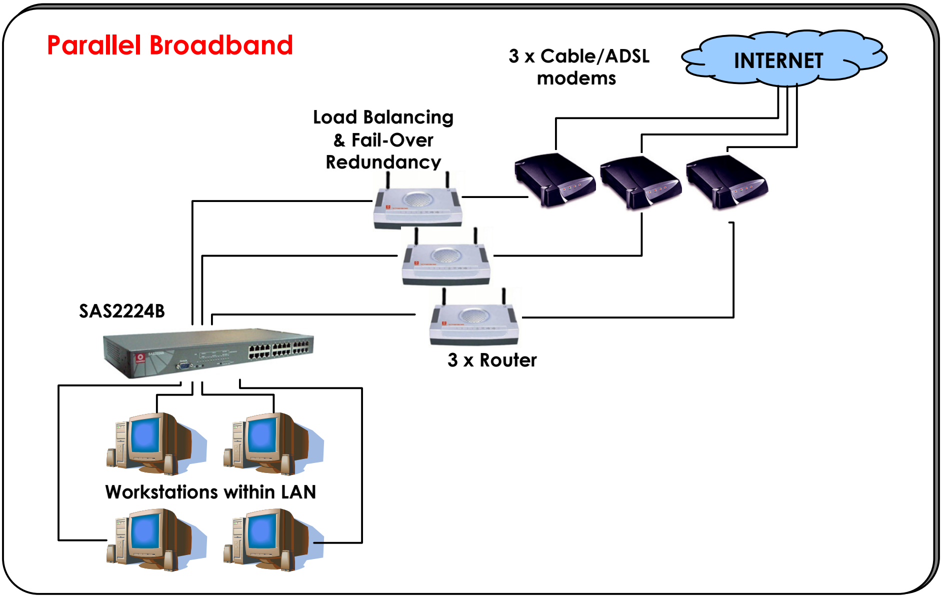
In view of preventing unauthorized management from a remote location, please remember to replace the default password with a new one.

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 you 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 you with aggregated bandwidth! In the event of a particular broadband connection failing, the router in cascade will automatically switch to use the 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, while the other to an ADSL line.

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

2 Steps to enable Parallel Broadband on the Router

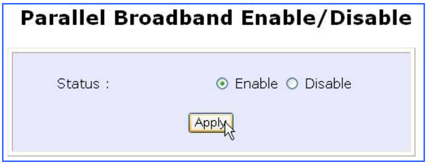
Before you begin, ensure that each of your router within the network is properly configured to connect to its individual broadband Internet account. Then ensure that each of the router is connected to an unused Ethernet port in the network as illustrated above.

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 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.



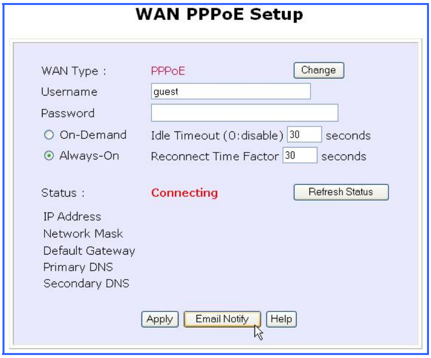
Parallel Broadband Enable/Disable

Status : ● Enable ○ Disable

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 a feature to notify you of the events. For example, you will be notified by email when there is a change in WAN IP that was earlier supplied to you.



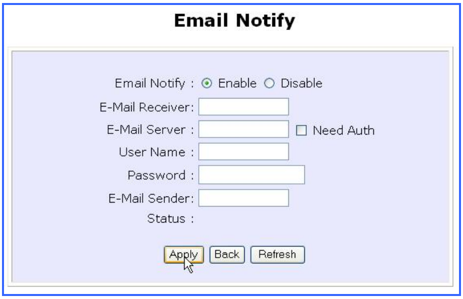
WAN PPPoE Setup

WAN Type : PPPoE
Username guest
Password
○ On-Demand Idle Timeout (0:disable) 30 seconds
● Always-On Reconnect Time Factor 30 seconds
Status : **Connecting**
IP Address
Network Mask
Default Gateway
Primary DNS
Secondary DNS

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 Notify** button to be activated by the router.

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



Email Notify

Email Notify : ● Enable ○ Disable
E-Mail Receiver:
E-Mail Server : □ Need Auth
User Name :
Password :
E-Mail Sender:
Status :

E-Mail Receiver:
This is the email address of the receiver to whom the message would be sent.

E-Mail 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 user's name that should be entered if authentication is required.

Password:

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

E-Mail Sender:
This is the email address of the sender from whom the message will appear to come.

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

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

ADVANCED FEATURES : Transparent Proxy

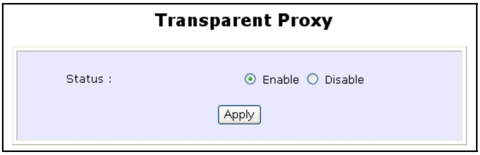
The router can support transparent proxy by redirecting TCP connections to local ports. The transparent proxy is when you grab a certain type of traffic at your router and send it through the proxy without the user's or client's knowledge. It also can be used to transport traffic around at the firewall for certain applications (such as Netmeeting). This way, the router allows the applications using a transparent proxy to avoid the firewall by letting traffic pass through.

Steps to enable/disable Transparent Proxy

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

1. Under the **ADVANCED FEATURES** command menu, click on **Transparent Proxy**.

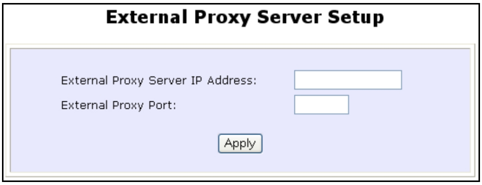
2. Select **Enable**, followed by clicking the **Apply** button. This function redirects you to the proxy.



Transparent Proxy

Status : ● Enable ○ Disable

3. In the **External Proxy Server Setup** section, enter the IP address and port of the external Proxy Server. Then click **Apply**.

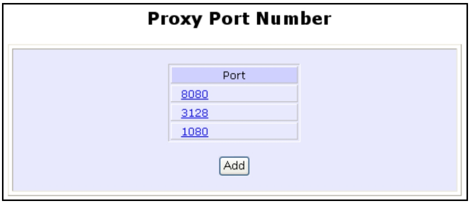


External Proxy Server Setup

External Proxy Server IP Address:

External Proxy Port:

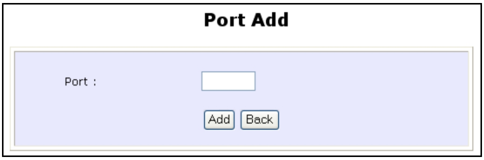
4. In the **Proxy Port Number** section, this table shows a list of available ports added earlier. To add a new proxy port number, click **Add**.



Proxy Port Number

Port
8080
3128
1080

Then the **Port Add** page appears allowing you to key in the new port number. To be listed in the table, click **Add**.



Port Add

Port :

ADVANCED 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 NetPassage 28G which 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 which 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 (router).

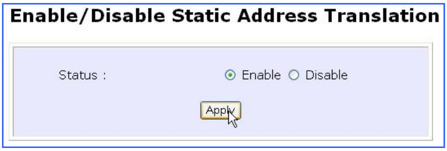
Once the notebook has been informed that the gateway to the Internet is the router, it will contact the latter (router) to access the Internet, without any change to its TCP/IP settings required.

Steps to enable/disable Static Address Translation

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

1. Under the **ADVANCED FEATURES** command menu, click on **Static Address Translation**.

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



Enable/Disable Static Address Translation

Status : ● Enable ○ Disable

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.

ADVANCED : SMTP Redirection

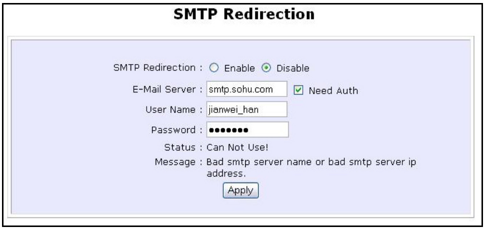
Using this feature, it accepts mails from anyone whose ISP blocks incoming connections on the SMTP port and relays the mails to an alternate port that is not blocked.

Steps to enable/disable SMTP Redirection

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

1. Under the **ADVANCED 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.



SMTP Redirection

SMTP Redirection : ○ Enable ● Disable

E-Mail Server : smtp.sohu.com ☑ Need Auth

User Name : jianwei_han

Password : •••••••

Status : Can Not Use!

Message : Bad smtp server name or bad smtp server ip address.

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**.

ADVANCED FEATURES : DNS Redirection

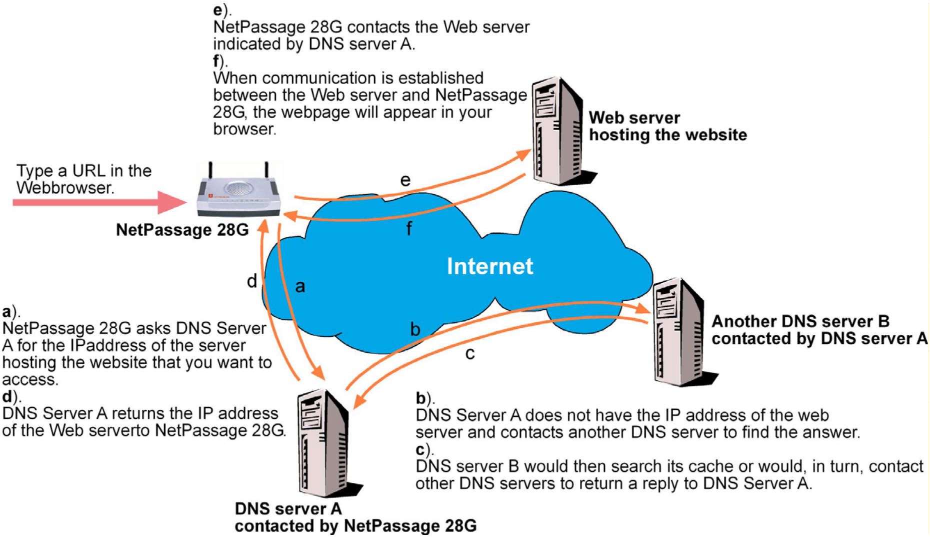
When you enter a URL in your Internet browser, the browser requests for a name-to-IP address translation from the Domain Name System (DNS) servers to be able to locate the web server hosting the website you want to access.

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, DNS requests from the LAN clients will be processed by the router. Unless in the router's **LAN Setup** you have already assigned a specific DNS server which 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.



e).
NetPassage 28G contacts the Web server indicated by DNS server A.

f).
When communication is established between the Web server and NetPassage 28G, the webpage will appear in your browser.

Type a URL in the Webbrowser.

a).
NetPassage 28G asks DNS Server A for the IPaddress of the server hosting the website that you want to access.

d).
DNS Server A returns the IP address of the Web serverto NetPassage 28G.

b).
DNS Server A does not have the IP address of the web server and contacts another DNS server to find the answer.

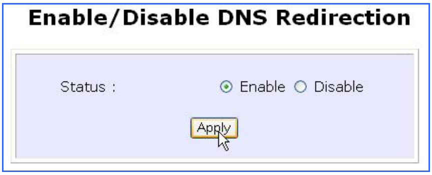
c).
DNS server B would then search its cache or would, in turn, contact other DNS servers to return a reply to DNS Server A.

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 **ADVANCED FEATURES** command menu, click on **DNS Redirection.**



Enable/Disable DNS Redirection

Status : ● Enable ○ Disable

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

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

ADVANCED 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.

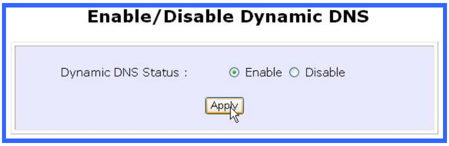
The Dynamic DNS service is ideal for a home website, file server, or just to keep a pointer back to your home PC so you can access those important documents while you are at work

Steps to enable/disable Dynamic DNS Setup

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

1. Under the **ADVANCED 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)



Enable/Disable Dynamic DNS

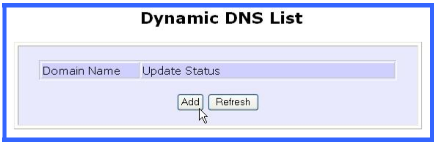
Dynamic DNS Status : ● Enable ○ Disable

Steps to manage Dynamic DNS List (DDNS)

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

1. Under the **ADVANCED FEATURES** command menu, click on **Dynamic DNS Setup**.

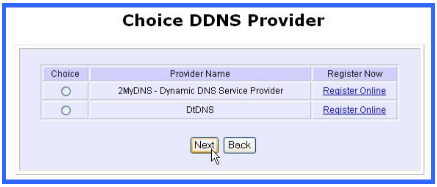
2. You may then choose to **Add** or **Refresh** Dynamic DNS list here. If the list is earlier created, click on the Refresh button to update the list. But for the first record, the list is usually blank.



Dynamic DNS List

Domain Name	Update Status

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 which you can use. The following parameters are explained below:



Choice DDNS Provider

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

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

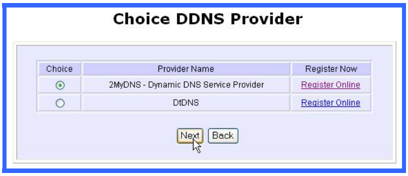
Provider Name :
This is the name of your preferred DDNS provider.

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

There are two types of DDNS providers that are pre-defined for you.

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

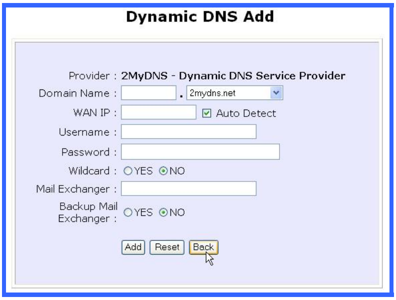
1. Under the **Choice** column in the table of **Choice DDNS Provider** check the radio button next to the **2MyDNS – DNS Service Provider**. Then click on the **Next** button to proceed.



Choice DDNS Provider

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

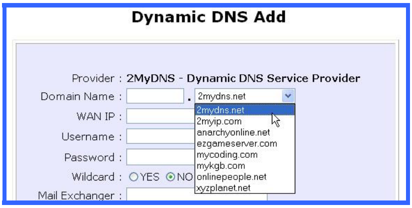
The **2MyDNS – DNS Service Provider** is depicted on the right.



Dynamic DNS Add

Provider :	2MyDNS - Dynamic DNS Service Provider
Domain Name :	. 2mydns.net
WAN IP :	☑ Auto Detect
Username :	
Password :	
Wildcard :	○ YES ● NO
Mail Exchanger :	
Backup Mail Exchanger :	○ YES ● NO

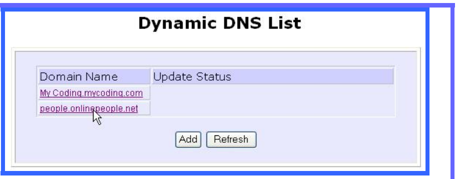
2. Input your settings for a new domain name. Once done, click on the Add button to save the new addition.



Dynamic DNS Add

Provider :	2MyDNS - Dynamic DNS Service Provider
Domain Name :	. 2mydns.net
WAN IP :	
Username :	
Password :	
Wildcard :	○ YES ● NO
Mail Exchanger :	

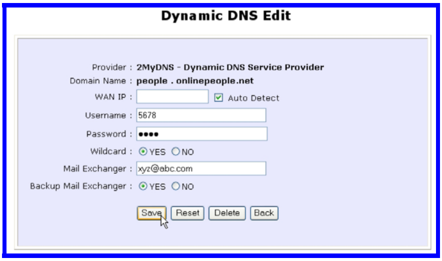
3. The new domain is added to the Dynamic DNS list table.



Dynamic DNS List

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

It becomes a hyperlink which allows you to go back to the Dynamic DNS Edit page. From this page, you can update any of the parameters or delete the domain or reset all parameters to be blank again.



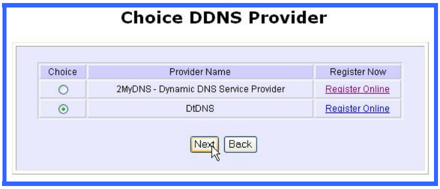
Dynamic DNS Edit

Provider : 2MyDNS - Dynamic DNS Service Provider
Domain Name : people . onlinepeople.net
WAN IP : ☑ Auto Detect
Username : 5678
Password : ●●●●
Wildcard : ● YES ○ NO
Mail Exchanger : xyz@abc.com
Backup Mail Exchanger : ● YES ○ NO

To select **DtDNS as** DDNS Service Provider

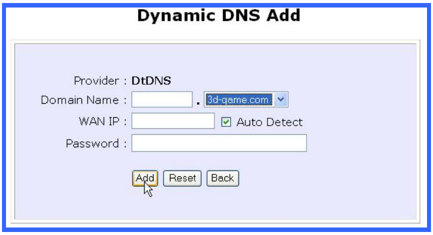
1. Under the **Choice** column in the table of **Choice DDNS Provider** check the radio button next to the **DtDNS**. Then click on the **Next** button to proceed.

   The **DtDNS** is depicted on the right.



Choice DDNS Provider

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

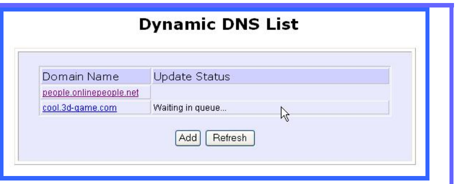


Dynamic DNS Add

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

2. Complete your inputs. Then click on the Add button.

3. The new domain name, **cool.3d-game.com** is added to the list. But if that domain is still waiting in queue, this state, 'Waiting in queue…" will be displayed under the **Update Status** column of the **Dynamic DNS List** table.



Dynamic DNS List

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

ADVANCED FEATURES : UPnP Configuration

The presence of Network Address Translation can complicate the setup of many compelling new home PC networking experiences like multi-player games, real-time communications, and other peer-to-peer services. These applications run into hiccups when they use private address on the public Internet or attempt simultaneous use of the same port number. The router supports Universal Plug and Play (UPnP) so that you may enjoy the benefits of NAT without having to worry about elaborate configuration procedures. Through an UPnP-aware operating system like Windows XP, the router can be recognized through its Ethernet connection so that other UPnP-enabled devices and applications can negotiate to open certain ports to traverse the NAT router device.

The following are issues which 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.

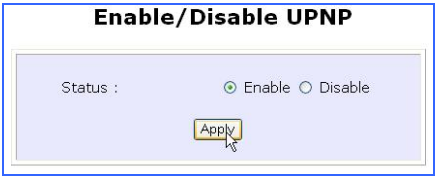
NAT traversal relies on the discovery and control protocols that are part of the Universal Plug and Play (UPnP) architecture. The UPnP specification is based on TCP/IP and Internet protocols that let devices discover the presence and services offered by other UPnP devices in the network. It also supports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



Enable/Disable UPNP

Status : ● Enable ○ Disable

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

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

Learn more from our ***NAT*** ***Technology Primer***

SECURITY CONFIGURATION: Packet Filtering

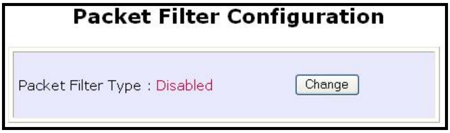
As part of the comprehensive security package found on the router, you may perform IP packet filtering to selectively allow/disallow certain applications from connecting to the Internet.

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.**

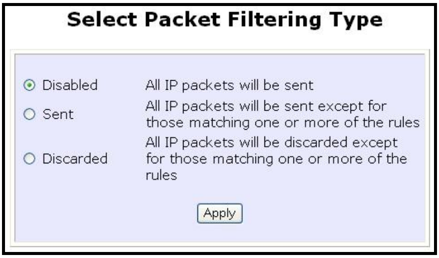
2. You must first choose the **Packet Filter Type** by clicking on the **Change** button.



Packet Filter Configuration

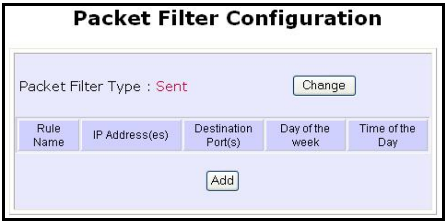
Packet Filter Type : Disabled

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



Select Packet Filtering Type

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

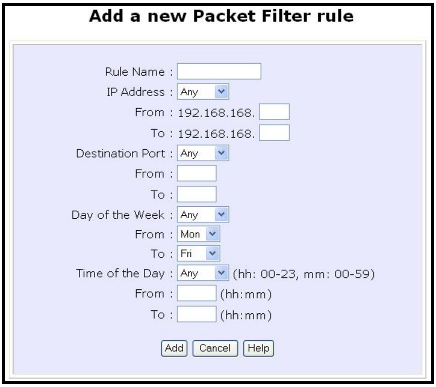


Packet Filter Configuration

Packet Filter Type : Sent

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

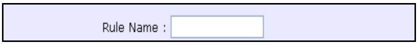
4. Click on the **Add** button and you will be able to define the details of your **Packet Filter Rule** from the screen on the right.



Add a new Packet Filter rule

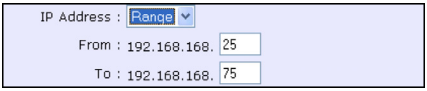
Rule Name :
IP Address : Any
From : 192.168.168.
To : 192.168.168.
Destination Port : Any
From :
To :
Day of the Week : Any
From : Mon
To : Fri
Time of the Day : Any (hh: 00-23, mm: 00-59)
From : (hh:mm)
To : (hh:mm)

4a). Enter **Rule Name** for this new packet filtering rule. For example, *BlockCS*



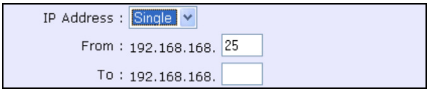
Rule Name :

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



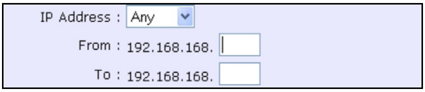
IP Address : Range
From : 192.168.168. 25
To : 192.168.168. 75

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



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

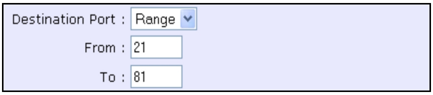
- A **Single** IP address
  Here, you need only specify the source IP address in the **(From)** field.



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

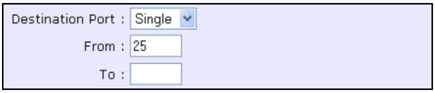
- **Any** IP address
  You may here, leave both, the **(From)** as well as the **(To)** fields, blank.

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



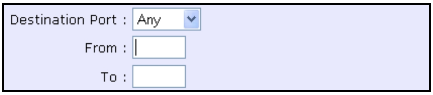
Destination Port : Range
From : 21
To : 81

- A **Range** of TCP ports
  In this case, you will have to define **(From)** which port **(To)** which port, your rule applies.



Destination Port : Single
From : 25
To :

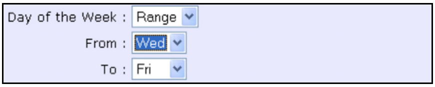
- A **Single** TCP port
  Here, you need only specify the source port in the **(From)** field.



Destination Port : Any
From :
To :

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

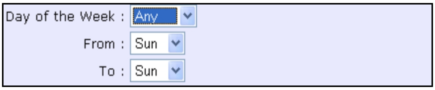
4d). From the **Day of the Week** drop down list, select whether the rule should apply to:



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

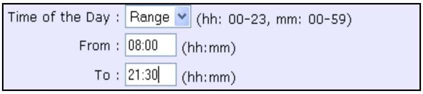
- A **Range** of days
  Here, you will have to select **(From)** which day **(To)** which day

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



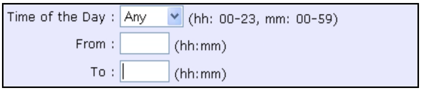
Day of the Week : Any
From : Sun
To : Sun

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



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

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

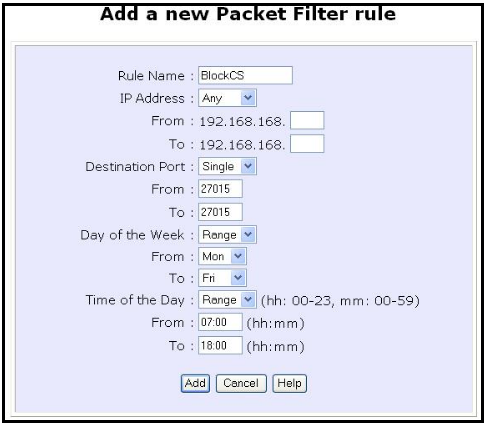


Time of the Day : Any (hh: 00-23, mm: 00-59)
From : (hh:mm)
To : (hh:mm)

- **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

Rule Name : BlockCS
IP Address : Any
From : 192.168.168.
To : 192.168.168.
Destination Port : Single
From : 27015
To : 27015
Day of the Week : Range
From : Mon
To : Fri
Time of the Day : Range (hh: 00-23, mm: 00-59)
From : 07:00 (hh:mm)
To : 18:00 (hh:mm)

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

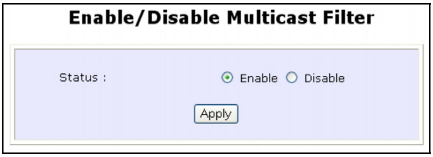
   Therefore, for a rule we name BlockCS, the entries as depicted on the left are entered. Hit the **Add** button to complete the entry.

SECURITY CONFIGURATION : Multicast Filtering

Multicasts are sent by the router to all PCs on a LAN or VLAN. When multicast filtering is disabled, the router allows users to only receive multicast traffic if they register / subscribe to some ISP services which provide video and TV channel streaming.

The purpose of configuring router with this feature is to allow or disallow streaming over the Internet.

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



Enable/Disable Multicast Filter

Status : ● Enable ○ Disable

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.

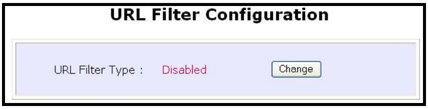
SECURITY CONFIGURATION: URL Filtering

The router supports URL Filtering which allows you to easily set up rules to block objectionable web sites from your users. Blocking only one IP address of that website prevents users from using it. Especially parents can play a role in screening the undesireable content (eg. pornographic, violence or hate-oriented content) which their children have access to from the computer.

Steps to configure URL Filtering

Before you begin the set up of URL Filtering, you have to ensure that your router can access the Internet. Here are the configuration steps:

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

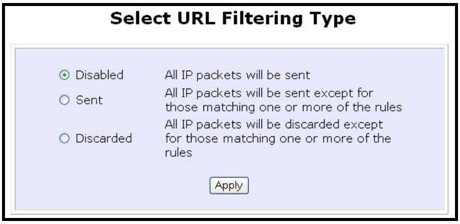


URL Filter Configuration

URL Filter Type : Disabled

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

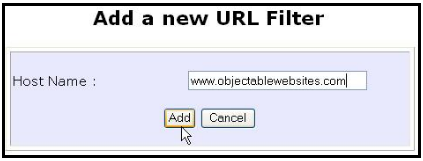
3. Select from three choices: **Disabled**, **Sent**, **Discarded**, then click on the **Apply** button. The default is **Disabled**, which allows all packets to be sent.



Select URL 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

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



Add a new URL Filter

Host Name : www.objectablewebsites.com

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: 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. SPI Firewall is unlike the normal firewall that only checks the headers of the packets, it also rigorously scrutinizes the contents of the packets, ensuring the integrity of the packets.

How the SPI Firewall works is that it examines all incoming data transmission. If a packet is deemed a legitimate reply to a previous request from within the network, the SPI Firewall would permit its passage through. Otherwise, access is denied. Such an approach allows relatively unrestricted transmission from within the network, and selective but flexible access from the outside. The SPI Firewall also uses a monitoring algorithm to track individual connections and it is also enabled to grant open temporary access in the firewall under appropriate conditions. For example, packets are allowed to pass only if associated with a valid session initiated from within the network.

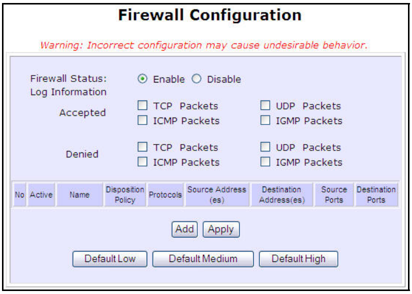
Common hacker attacks like IP Spoofing, Port Scanning, Ping of Death and SynFlood can be easily thwarted with Compex's SPI firewall.

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

Steps to configure SPI Firewall

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

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	Protocols	Source Address (es)	Destination Address(es)	Source Ports	Destination Ports

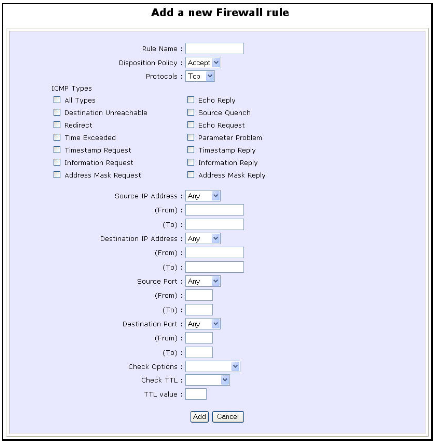
2. First, you can choose to **Enable** or **Disable** the firewall and use the **Default Low**, **Default Medium** or **Default High** security options for convenient setup.

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 **Add** radio button at the screen shown above, followed by **Edit** button and the screen on the left will appear.



Add a new Firewall rule

Rule Name :

Disposition Policy : Accept

Protocols : Tcp

ICMP Types

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

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

Rule Name : This is the identifier for the firewall configuration. Each Firewall setting will be associated with a rule number. Please enter a number in this field.

Disposition Policy : This parameter determines whether the data packets would be accepted or denied by firewall. Choose between Accept or Deny.

Protocols : Users are allowed to select the type of data packet that are allowed into the network. Users are able to choose 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 protocol is actually part of an IP implementation and is used to report errors in IP datagram routing. ICMP serves as a form of flow control, although ICMP messages are neither guaranteed to be received or transmitted. It is merely a way to provide feedback to the sender of IP datagrams.

Echo request	Determines whether an IP node (a host or

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

IGMP Types : This protocol is actually part of an IP implementation and 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 determines the set of workstations that generate the data packets. Users can either set a single IP address or set a range of IP addresses.

Destination IP : This parameter determines 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 : This parameter determines the application from the specified port number from the source. Users can either set a single port number or a range of port numbers. Port numbers are from 0 to 65536. Ports 0 to 1024 are reserved for use by certain privileged services. For example, the port number for Telnet is 23 and the port number for http is 80.

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

Check Options : This parameter would determine the check options. The available selection options are abbreviated as follows:

SEC – Security
LSRR – Loose Source Route
Timestamp – Timestamp
RR – Record Packet Route
SID – Satnet ID
SSRR – Strict Source Route
RA – Router Alert

Check TTL : This parameter would set the checking rule for TTL. It would determine whether the parameter is equal, less then, greater than or not equal to the TTL value. The available selection options are:

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

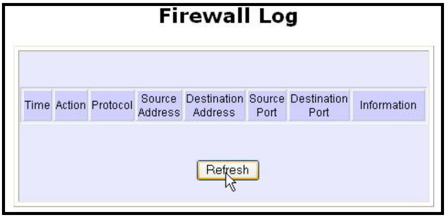
SECURITY CONFIGURATION : Firewall Logs

When the router's SPI firewall is in operation, valuable network data traffic patterns that passes 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 information as well as the action taken by the SPI firewall.

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.**



Firewall Log

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

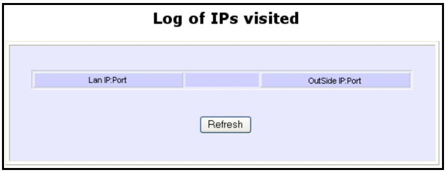
2. Click the **Refresh** button to see any new information captured in the log.

SECURITY CONFIGURATION: Log of IPs visited

This feature allows you to keep track of the IPs that have been visited by LAN users. To ensure better security, the router can check which PC user have accessed which website. Sometimes when a parent needs to control the child's Internet access rights to play games online and surf Internet under the busy parent's little supervision, the parent can block some unsuitable IPs that are inaccessible for the child.

Steps to keep track of the IP log

1. Select **Log of IPs visited** under the **SECURITY CONFIGURATION** command menu.



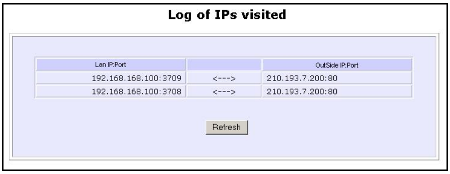
Log of IPs visited

Lan IP:Port		OutSide IP:Port

2. To update and retrieve the IP log, click **Refresh**. Take note of the following fields:

LAN IP: Port
This field displays the LAN IP address and port number of your PC which you are using to surf Internet.

Outside IP: Port
This field displays the IP address and port number of the Internet host/website you have visited.



Log of IPs visited

Lan IP:Port		OutSide IP:Port
192.168.168.100:3709	<--->	210.193.7.200:80
192.168.168.100:3708	<--->	210.193.7.200:80

Take this screen as an example. Let us assume that you have a PC with an IP address, 192.168.168.100 and you intend to visit the yahoo website at www.yahoo.com.sg.

After you have visited the website via this PC, the PC's **LAN IP:Port** and the website's **Outside IP:Port** are displayed in this log.

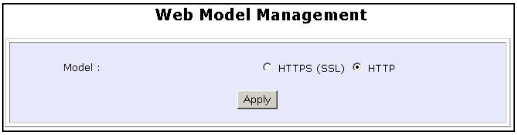
SECURITY CONFIGURATION: Web Model

This feature allows you to change the router's web protocol for a better and secure data communication. For instance, transferring data from the HTTP page to the HTTPs page should be safe because HTTPs includes SSL handshake that will authenticate the server and the data will be sent encrypted.

Steps to change the HTTP protocol of the router

Changing the router's protocol is as easy as a few mouse-clicks:

1. Select **Web Model** under the **SECURITY CONFIGURATION** command menu.



Web Model Management

Model : ○ HTTPS (SSL) ● HTTP

2. The HTTP protocol is displayed by default. If you wish to have your web browser with an adequate degree of encryption, select **HTTPs (SSL)**. By selecting it, the communication will be more secure as data is encrypted before it is being transmitted.

3. Click **Apply** to effect the change.

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.

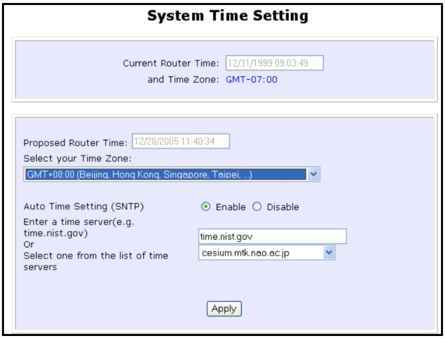
SYSTEM TOOLS : Set Router's Clock

The router is specially designed with Simple Network Time Protocol (SNTP) compatibility so that the router's clock can be synchronized with a 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.



System Time Setting

Current Router Time: 12/31/1999 09:03:49
and Time Zone: GMT-07:00

Proposed Router Time: 12/28/2005 11:40:34
Select your Time Zone:
GMT+08:00 (Beijing, Hong Kong, Singapore, Taipei, ...)

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

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 upgradeability in mind. You can keep your router updated with the latest capabilities by means of a simple firmware upgrade obtainable from Compex's corporate web site at www.compex.com.sg or www.cpx.com.

Steps to Upgrade the Router's firmware

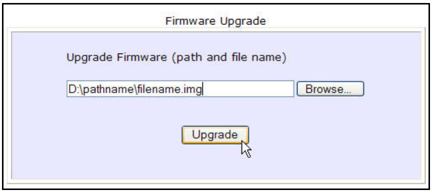
Here is how you go about upgrading your router's firmware with the latest update:

1. Select **Firmware Upgrade** under the **SYSTEM TOOLS** command menu.

2. Ensure that you have the latest firmware downloaded into a location on your hard disk drive.

3. On the next screen, simply fill filename prefixed with the drive letter and the pathname where you have stored the file as illustrated on the right. Alternatively, you may click on the **Browse** button search for the firmware image file.

4. Press the **Upgrade** button to begin the firmware upgrade.



Firmware Upgrade

Upgrade Firmware (path and file name)

D:\pathname\filename.img

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 or the power 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's flash ROM or make a backup of the configuration profile onto your hard disk drive. In times of need, 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.

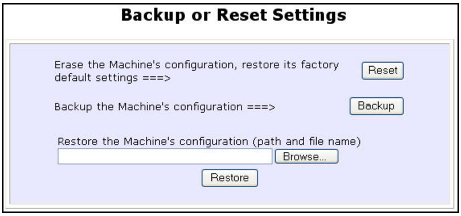
Steps to Save or Reset Settings on the Router

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 defaults (Note that this will discard all the configuration you have done).

3. Press the **Backup** button if you wish to save the configuration profile onto the hard disk drive.



Backup or Reset Settings

Erase the Machine's configuration, restore its factory default settings ===> Reset

Backup the Machine's configuration ===> Backup

Restore the Machine's configuration (path and file name)

Browse...

Restore

4. Click on **Restore** if you wish to return the router to an earlier saved file from the hard disk drive. You may click **Browse** to search or simply type in the drive letter, pathname, followed by the filename.

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

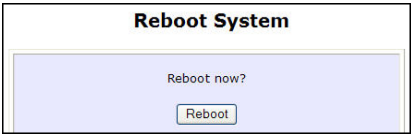
SYSTEM TOOLS : Reboot Router

This feature serves an important function so that the router will make effective the many settings we set up from time-to-time.

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.



Reboot System

Reboot now?

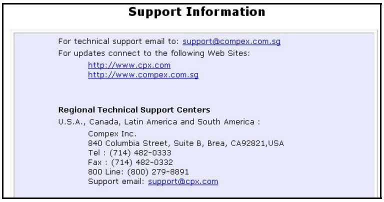
2. The router will prompt you to confirm your decision before executing a reboot. Hit the **Reboot** button again when you are ready.

HELP : Get Technical Support

You may wish to access this page for the relevant email, telephone/fax numbers and our corporate web site addresses so that you may find pertinent information.

Steps to access the Get Technical Support page on the Router

1. Select **Get Technical Support** under the **HELP** command menu.



Support Information

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

Regional Technical Support Centers
U.S.A., Canada, Latin America and South America :
Compex Inc.
840 Columbia Street, Suite B, Brea, CA92821,USA
Tel : (714) 482-0333
Fax : (714) 482-0332
800 Line: (800) 279-8891
Support email: support@cpx.com

2. You have been looking at an extremely feature-packed device! Hence if you require more support information than the manual or datasheet can provide you, feel free to mail/phone the Compex's tech-support found on this page.

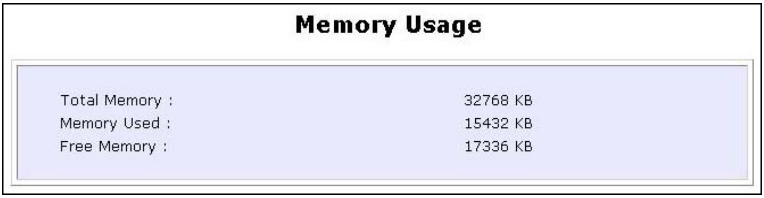
HELP : Memory Information

The **Memory Information** page gives the administrator an overview of the memory status of the router.

Steps to access the Memory Information page on the Router

In a single mouse click on the command window, you will be able to glance at the memory information of the router:

1. Select **Memory Information** under the **HELP** command menu.



Memory Usage

Total Memory :	32768 KB
Memory Used :	15432 KB
Free Memory :	17336 KB

2. From the page, you will be able to keep track of the memory status of your router.

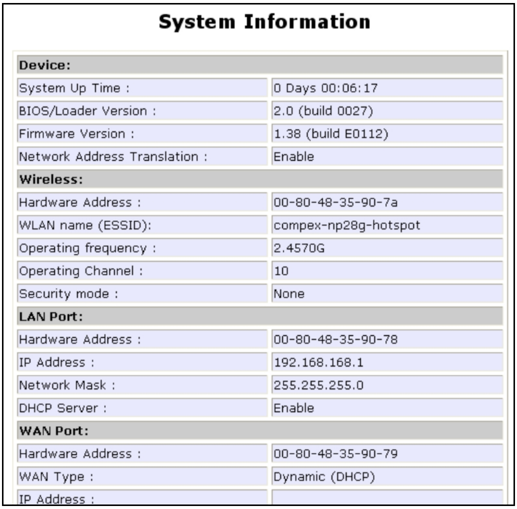
HELP : About System

The About System page gives the administrator an overview of the network 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 on the command window, you will be able to glance at the settings applied to in your functional network:

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 00:06:17
BIOS/Loader Version :	2.0 (build 0027)
Firmware Version :	1.38 (build E0112)
Network Address Translation :	Enable
Wireless:	
Hardware Address :	00-80-48-35-90-7a
WLAN name (ESSID):	compex-np28g-hotspot
Operating frequency :	2.4570G
Operating Channel :	10
Security mode :	None
LAN Port:	
Hardware Address :	00-80-48-35-90-78
IP Address :	192.168.168.1
Network Mask :	255.255.255.0
DHCP Server :	Enable
WAN Port:	
Hardware Address :	00-80-48-35-90-79
WAN Type :	Dynamic (DHCP)
IP Address :	

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

Chapter 6: Using Hotspot Capabilities

This section covers the capabilities of using hotspots in a wireless networking communication.

Public HotSpots integrated with Wi-Fi technology are rapidly becoming common in coffee shops, hotels, convention centers, airports, libraries, and other places where people gather. In these locations, a Wi-Fi network can provide Internet access to subscribers (eg. guests, visitors or customers). These people can connect either by using their own laptop computers equipped with Wi-Fi and portable computing devices, or by using Wi-Fi equipped desktop computers provided at the location. A single networked printer with a built-in print server can also be connected to the access point, to provide printing services to users.

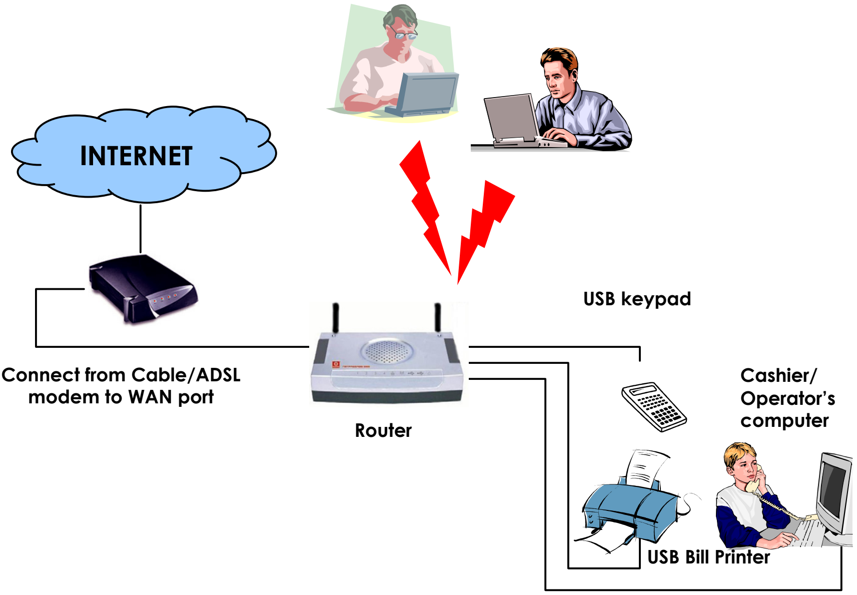
HotSpots operate in various ways. A small public HotSpot may provide free access to its guests, or it may charge a membership, per-time or data-use connection fee. Even if the venue is providing Internet connectivity as a free value added service, it asks users to provide user and registration information before they can connect to the Internet.

This document describes how the router can be used to configure hot spots for subscribers seeking Wi-Fi Internet access. Launching and operating the hot spots via the router, the café cashiers or operators can easily print receipt with billing and password information, and can easily add time increments or credits to the requesting subscribers by just pressing the keypad. During a transaction, the cashier or operator can press the keypad to generate a new access key for the subscriber. When a subscriber launches his own web browser, the built-in captive portal feature (SMTP Redirection) automatically directs the subscriber to the secure login page. After entering the access key, he/she can securely surf the Internet. See **Scenario for Setting up a HotSpot**.

The router is suited to accomplish a simple network configuration you may have in mind. Combined with a web-based configuration interface, you can easily set up your feature-rich router for these hot spot applications.

Scenario :
Internet Access in Public Areas

Subscribers use their wireless LAN laptops to access the Internet via the router


INTERNET
USB keypad
Connect from Cable/ADSL modem to WAN port
Router
Cashier/ Operator's computer
USB Bill Printer

This set up example illustrates the demand for wireless network that is increasing at heavily populated areas such as airports, hotels, restaurants and cafes. Using the the web-based configuration interface, the cashier/operator is able to monitor the status of subscribers while the subscribers are able to log in to access almost any web-browsers.

HOTSPOT : HotSpot Authentication

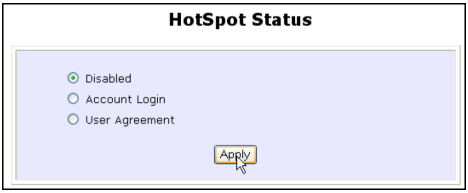
The HotSpot page gives the administrator an overview of the network customizations/settings. This is a useful summary of the operating parameters you have put in place.

Steps to enable or disable Hotspot on the router

In a single mouse click on the command window, you will be able to glance at the settings applied to in your functional network:

Disabling HotSpot function

1. Under **HotSpot** on the command menu, click on **HotSpot Authentication**. You will see that there are three options to select: **Disabled**, **Account Login** or **User Agreement**.



HotSpot Status

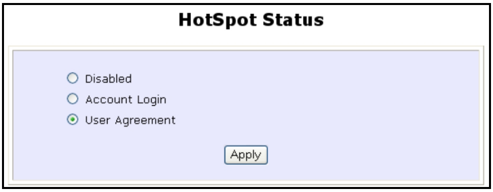
● Disabled
○ Account Login
○ User Agreement

The hotspot function is disabled by default after you have logged into the web-based configuration interface.

Selecting User Agreement

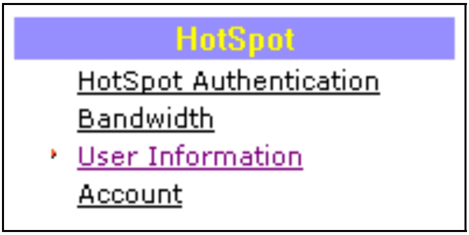
1. Under **HotSpot Status**, tick the radio button next to **User Agreement**. Click **Apply**. The next screen include the following features:

- **Bandwidth**
- **User Information**
- **Account**

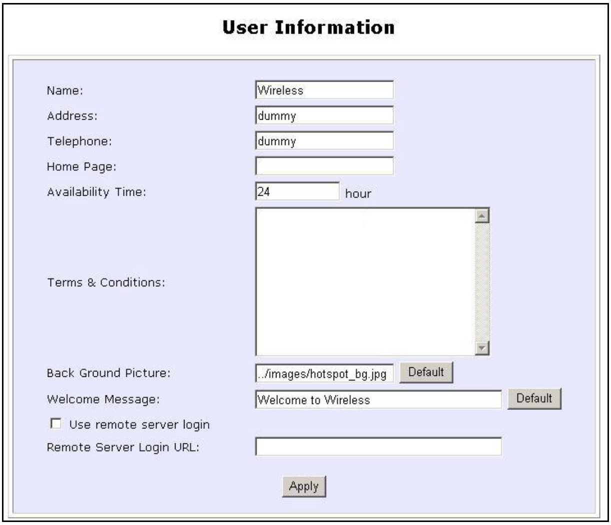


HotSpot Status

○ Disabled
○ Account Login
● User Agreement



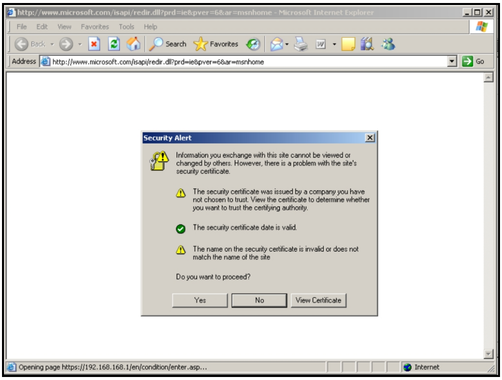
2. Under **Hotspot**, click on **User Information**. The **Terms & Conditions** text box lets you compose the text and then click **Apply**.



User Information

Name:	Wireless
Address:	dummy
Telephone:	dummy
Home Page:	
Availability Time:	24 hour
Terms & Conditions:	
Back Ground Picture:	../images/hotspot_bg.jpg Default
Welcome Message:	Welcome to Wireless Default
☐ Use remote server login	
Remote Server Login URL:	

3. To see if the text in the **Terms & Conditions** has been successfully updated, first open your Internet browser. Wait for a while until you see the **Security Alert** window. Click **Yes**.



http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome Go
Security Alert
Yes
No
View Certificate
Internet

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

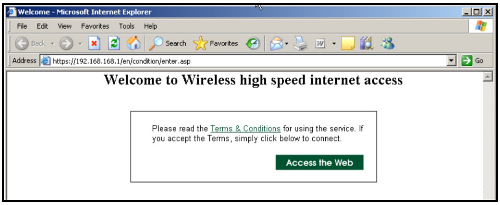
The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Opening page https://192.168.168.1/en/condition/enter.asp...

4. This screen appears showing you the page incorporated with the **Terms & Conditions**. Click on this hyperlink to read the terms and conditions which you are unable to edit here. If you wish to edit it again, follow the steps 3 and 4.

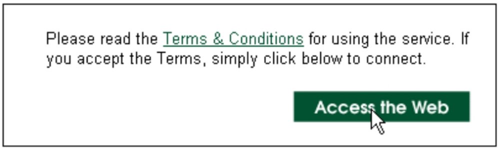


Welcome - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.168.1/en/condition/enter.asp Go
Access the Web

Welcome to Wireless high speed internet access

Please read the Terms & Conditions for using the service. If you accept the Terms, simply click below to connect.

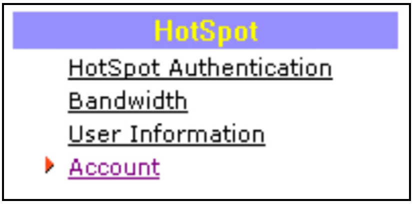
5. The **Access the Web** hyperlink lets you access the Compex website.



Please read the Terms & Conditions for using the service. If you accept the Terms, simply click below to connect.

Selecting Account from User Agreement

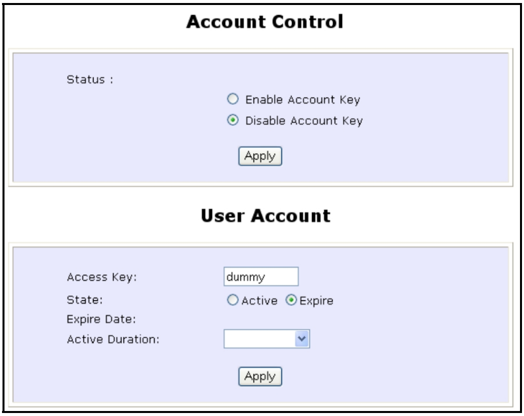
1. In the **User Agreement** hotspot page, click on **Account**.



2. At the **Account Control** section, the **Disable Account Key** is displayed by default. If enabled, the subscriber will be able to key in the access key before using the internet access.

3. At the **User Account** section, input the required data for the subscriber's account key.

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



Account Control

Status : ○ Enable Account Key ● Disable Account Key

Apply

User Account

Access Key: dummy

State: ○ Active ● Expire

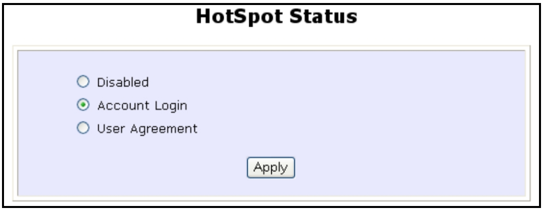
Expire Date:

Active Duration:

Apply

Selecting Account Login

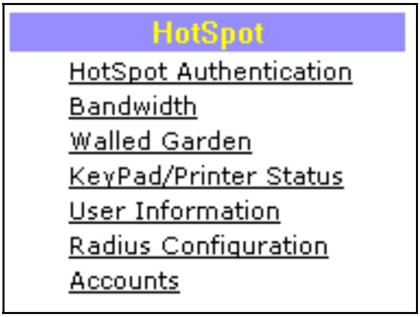
1. Under **HotSpot Status**, tick the radio button next to **Account Login**. Click **Apply**.



HotSpot Status

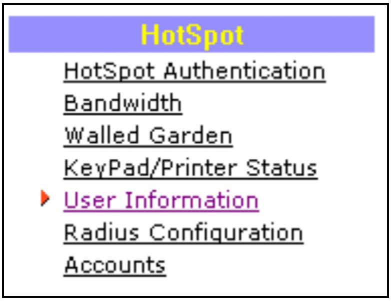
○ Disabled
● Account Login
○ User Agreement

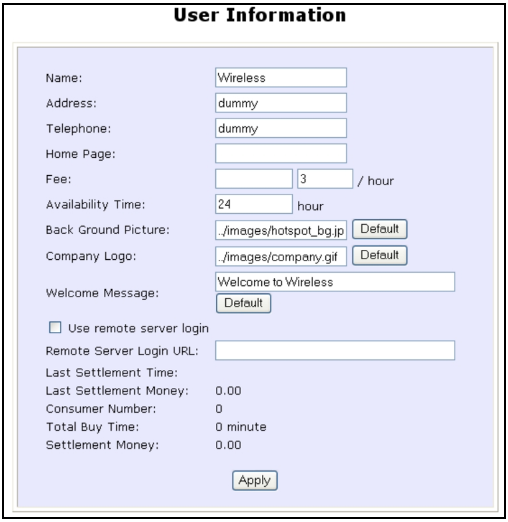
2. You will see the menu list under **Hotspot** on the left of your browser.



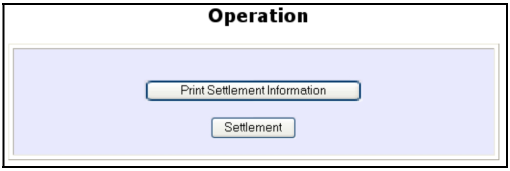
Selecting User Information from Account Login

From the **HotSpot Authentication** menu command, click on **User Information**.




User Information

Name:	Wireless
Address:	dummy
Telephone:	dummy
Home Page:	
Fee:	3 / hour
Availability Time:	24 hour
Back Ground Picture:	../images/hotspot_bg.jp Default
Company Logo:	../images/company.gif Default
Welcome Message:	Welcome to Wireless Default
□ Use remote server login	
Remote Server Login URL:	
Last Settlement Time:	
Last Settlement Money:	0.00
Consumer Number:	0
Total Buy Time:	0 minute
Settlement Money:	0.00


Operation

HOTSPOT : Bandwidth

The Bandwidth Control page gives the administrator the choice to enable or disable the bandwidth control of subscribers in case of massive data transfer which causes slowdown problems when surfing the Internet.

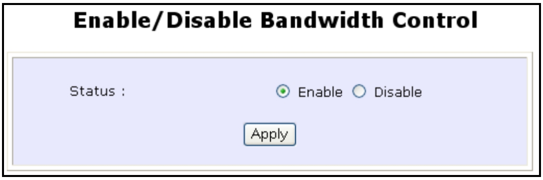
Steps to disable or enable Bandwidth Control on the router

In a single mouse click on the command window, you will be able to control the bandwidths of individual Internet users accessing your router if enabled.

Enabling Bandwidth

1. Under the **HotSpot** on the command menu, click on **Bandwidth**.

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



Enable/Disable Bandwidth Control

Status : ● Enable ○ Disable

HOTSPOT : Walled Garden

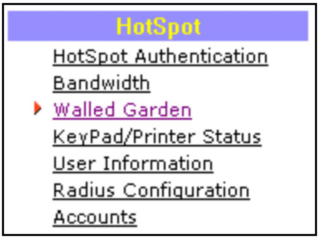
The Walled Garden page gives the administrator an overview of the walled garden list. If enabled, the subscriber can access the websites that you just have added to the Walled Garden list without the need for permission. You can add the websites with domains or IP addresses.

Steps to enable or disable Walled Garden on the router

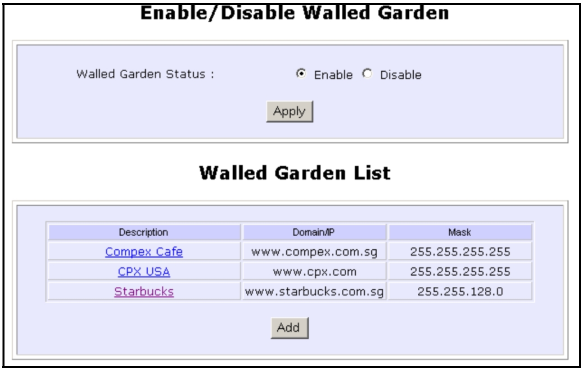
In a single mouse click on the command window, you will be able to glance at the settings applied to in your functional network:

Enabling Walled Garden

1. Under the **HotSpot** on the command menu, click on **Walled Garden**.



2. The **Walled Garden** is enabled by default. You may disable it in order to deny users access to the pages.



Enable/Disable Walled Garden

Walled Garden Status : ● Enable ○ Disable

Apply

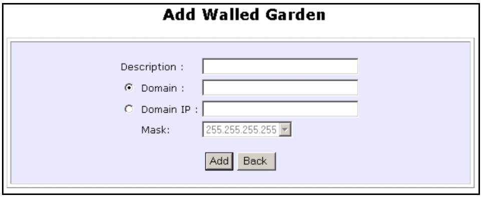
Walled Garden List

Description	Domain/IP	Mask
Compex Cafe	www.compex.com.sg	255.255.255.255
CPX USA	www.cpx.com	255.255.255.255
Starbucks	www.starbucks.com.sg	255.255.128.0

Add

3. To access any of the earlier created websites in the **Walled Garden List**, follow the steps below:

3a. To add the domain of the website you wish to surf, click website you wish to surf, click **Add**.



Add Walled Garden

Description :

● Domain :

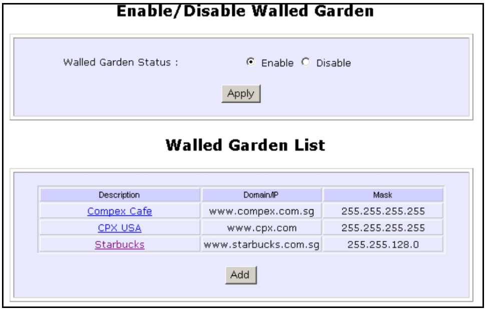
○ Domain IP :

Mask: 255.255.255.255

3b. Enter **Description** for the name of the website.

3c. Select **Domain or Domain IP** to specify the website's URL or IP Address so that you can access that website**.** If you prefer to select **Domain IP**, select the IP address from the **Mask list**.

3d. To confirm the new addition, click **Add**.



Enable/Disable Walled Garden

Walled Garden Status : ● Enable ○ Disable

Walled Garden List

Description	Domain/IP	Mask
Compex Cafe	www.compex.com.sg	255.255.255.255
CPX USA	www.cpx.com	255.255.255.255
Starbucks	www.starbucks.com.sg	255.255.128.0

3e. The new domain you have created is now added to the **Walled Garden List**. To add more domains, click **Add**.

3f. The **Walled Garden List** allows you to directly access the websites that are added in this list as well as to control user's access to the websites contained or barred from the wall garden.

HOTSPOT : Keypad or Printer Status

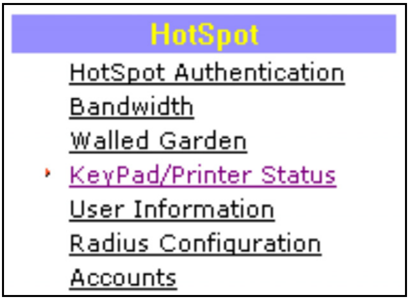
The Keypad/Printer Status page gives the administrator an overview of the keypad and/or printer status when the keypad or printer or both are connected to the USB port of your router.

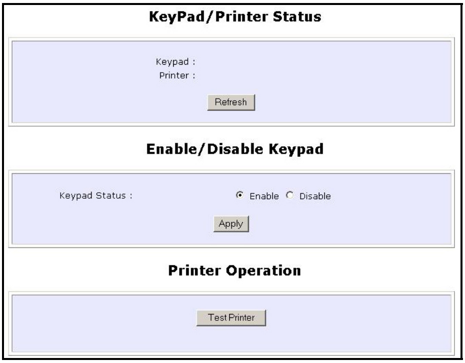
Steps to configure Keypad and Printer on the router

In a single mouse click on the command window, you will be able to glance at their status when the keypad and/or printer are connected to your router.

Configuring Keypad and Printer Status

1. Under the **HotSpot** on the command menu, click on **KeyPad/Printer Status**.




KeyPad/Printer Status

Keypad :
Printer :

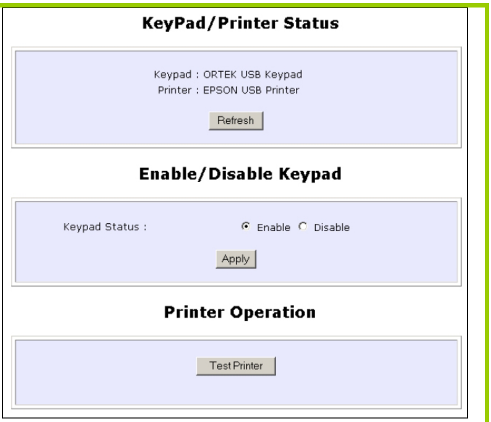
Enable/Disable Keypad

Keypad Status : ● Enable ○ Disable

Printer Operation

2. Before you can use this screen on the left, always ensure that your keypad and/or printer are switched on.

3. In the **KeyPad/Printer Status** section, click **Refresh** to retrieve and display the information on the names of the keypad and/or the printer only after you have connected the keypad and printer to your router.



KeyPad/Printer Status

Keypad : ORTEK USB Keypad
Printer : EPSON USB Printer

Enable/Disable Keypad

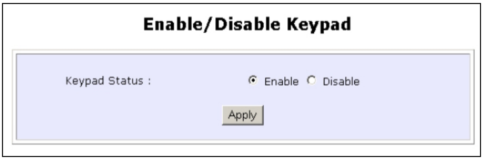
Keypad Status : ● Enable ○ Disable

Printer Operation

3a. To enable or disable the keypad:

After you have plugged the keypad into the USB port of the router, the router will detect it automatically.

In the **Enable/Disable Keypad** section, if you need to activate your keypad, click **Enable** and then **Apply**.



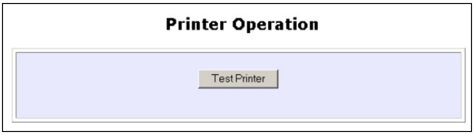
Enable/Disable Keypad

Keypad Status : ● Enable ○ Disable

3b. To test the printer:

After you have plugged the printer into the USB port of the router, the router will detect the printer automatically.

In the **Printer Operation** section, the click the **Test Printer** button to check if the printer is working or not.



Printer Operation

HOTSPOT : Radius Configuration

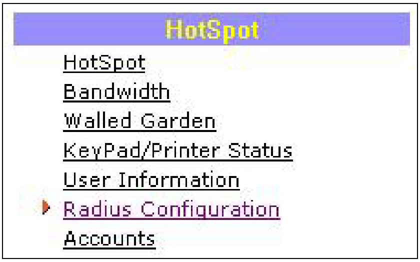
The Radius Configuration page gives the administrator an overview of the Radius Server configured in your router.

Steps to configure the Radius Server on the router

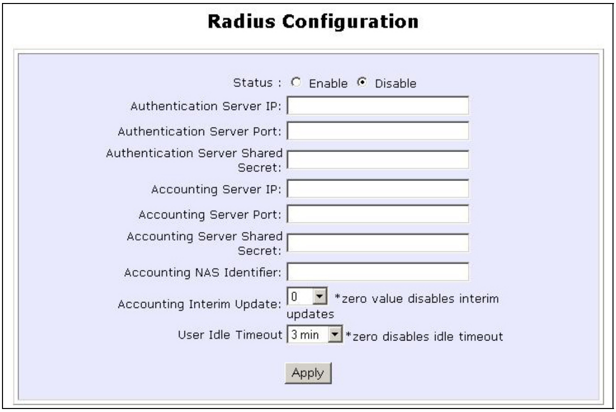
In a single mouse click on the command window, you will be able to glance at the configuration of the Radius Server.

Configuring Radius authentication in the router

1. Under the **HotSpot** on the command menu, click on **Radius Configuration**.



2. In the **Enable/Disable Status** section, if you need to activate your Radius authentication function, click **Enable** and then **Apply**.



Radius Configuration

Status :	○ Enable ● Disable
Authentication Server IP:	
Authentication Server Port:	
Authentication Server Shared Secret:	
Accounting Server IP:	
Accounting Server Port:	
Accounting Server Shared Secret:	
Accounting NAS Identifier:	
Accounting Interim Update:	0 *zero value disables interim updates
User Idle Timeout	3 min *zero disables idle timeout

Apply

The following table describes the fields in the **Radius Configuration** screen:

Field	Description
Authentication Server IP	This field displays the IP address of the authentication server.
Authentication Server Port	This field displays the port number of the authentication server.
Authentication Server Shared Secret	This field displays the encrypted password that is shared with the authentication server and client.
Accounting Server IP	This field displays the IP address of the accounting server.
Accounting Server Shared Secret	This field displays the encrypted password that is shared with the accounting server and client.
Accounting NAS Identifier	This field displays any value of the identifier.
Accounting Interim Update	This field displays the interval time of transmitted accounting packets. If the value is "0", the accounting packets will stop transmitting.
User Idle Timeout	The field displays the selected timeout for when the user is inactive. If the user is inactive, the accounting process will be stopped.

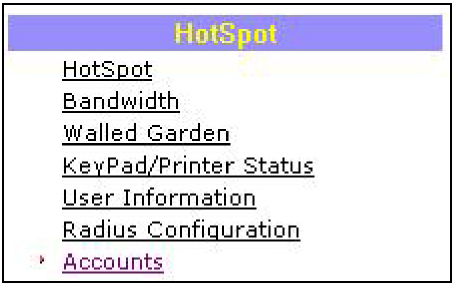
HOTSPOT : Accounts

The Accounts page gives the administrator an overview on the management of user accounts to access the Internet via the router.

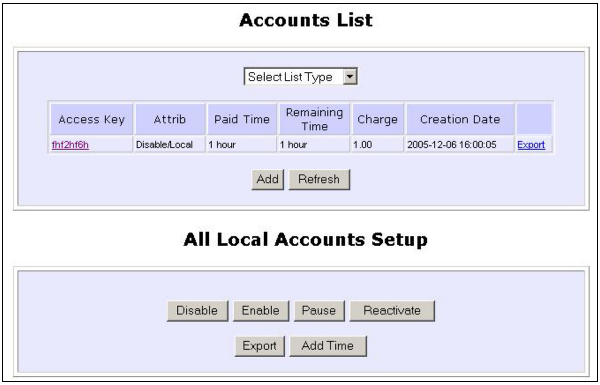
Steps to manage accounts

In a single mouse click on the command window, you will be able to create, edit and delete user accounts on the router.

1. Under **HotSpot** on the command menu, click on **Accounts**. This page shows up with the sections, **Accounts List** and **All Local Accounts Setup**.



2. In the **Accounts List** page,



Accounts List

Select List Type

Access Key	Attrib	Paid Time	Remaining Time	Charge	Creation Date	
fhf2hf6h	Disable/Local	1 hour	1 hour	1.00	2005-12-06 16:00:05	Export

All Local Accounts Setup

The following table describes the columns in the **Accounts List** screen:

Column	Description
Access Key	This field is auto-generated when a new account is added by pressing the keypad. Click the heading to sort the entries in ascending or descending order based on this column.

Attrib	This field displays the status of the account that is active, not active, disabled or pending for a while. Click the heading to sort the entries in ascending or descending order based on this column.
Paid Time	This field is the amount of time that a subscriber will use to surf the Internet. It can be entered in the number of hours. Click the heading to sort the entries in ascending or descending order based on this column.
Remaining Time	This field is the amount of time that a subscriber account remains idle for a specified time. Click the heading to sort the entries in ascending or descending order based on this column.
Charge	This field displays how much a customer is charged for using the internet per hour.
Creation Time	This field displays when the subscriber account was created (in yyyy/mm/dd hh/mm/ss format). Click the heading to sort the entries in ascending or descending order based on this column.

2. Use the keypad to create subscriber accounts. Press the **Num Lock** key on until you see the green LED light up.

3. Press the keypad hot key from '0' to '9'. For example, press '1' for the one hour account.

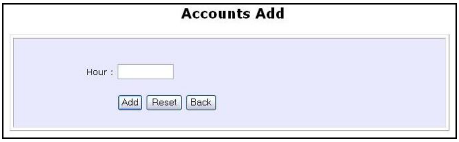
   See **Examples** for entering the **Paid Time**.

4. Then press **Enter**. Then you will see this entry automatically appear under the **Paid Time** column in the **Accounts List** page. At the same time, the printer will start printing your bill document.

You can use the **Add** button to generate a new account only if the keypad is not used or not working. In this case, the printer cannot print. Enter the number of hours in the **Hour** field, then followed by clicking **Add**.

Examples:

Hot Keys	Buy Time
1 Enter	**I hour**
1 2 Enter	**12 hours**

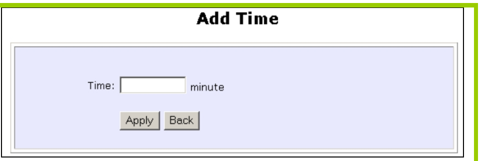


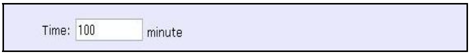
Adding Time Credits to a subscriber

Increasing a subscriber's usage time is the operator's responsibility when the subscriber's **Paid Time** expires and the subscriber requests for more time credits. This time credit will be accumulated in the subscriber's billing profile.

1. Under **HotSpot** on the command menu, click on **Accounts**. This page shows up with the sections, **Accounts List** and **All Local Accounts Setup**.

2. Go to the **All Local Accounts Setup** section and select **Add Time**. For example, 100 minutes. Then click **Apply** to effect the time.



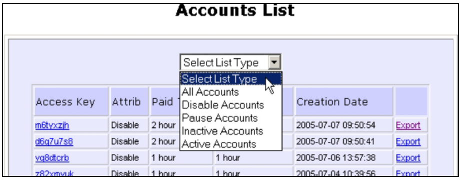

Time: 100 minute

Viewing Subscriber Accounts

When viewing a new or current subscriber account, you can use **Select List Type** to sort all accounts based on the selected attribute.

1. Go to the **Select List Type** dropdown menu list.

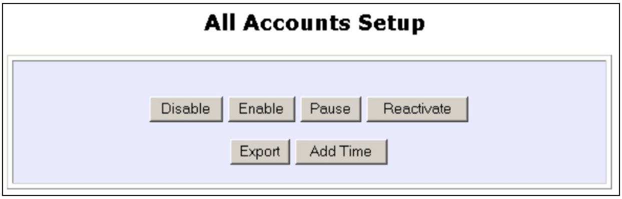
2. If you want all accounts to be displayed in the **Accounts List** table, select **All Accounts**.



Access Key	Attrib	Paid		Creation Date	
m6tyxzjh	Disable	2 hour		2005-07-07 09:50:54	Export
d6q7u7s8	Disable	2 hour		2005-07-07 09:50:41	Export
vq8dtcrb	Disable	1 hour	1 hour	2005-07-06 13:57:38	Export
z82xmyuk	Disable	1 hour	1 hour	2005-07-04 10:39:56	Export

The table below describes the types of the Select List:

Select List Type	Description
All Accounts	Retrieve and display all accounts that are disabled, paused, activated and deactivated.
Disable Accounts	Retrieve and display all accounts that are disabled.
Pause Accounts	Retrieve and display all accounts that are paused.
Not Active Accounts	Retrieve and display all accounts that are not activated.
Active Accounts	Retrieve and display all accounts that are activated.



All Accounts Setup

Disable :
This button disables all accounts.

Enable:
This button enables all accounts.

Pause:
This button stalls the time assigned to all accounts.

Reactive:
This button resumes the time assigned to all accounts.

Export:
This button saves the user account's billing statement into the text format.

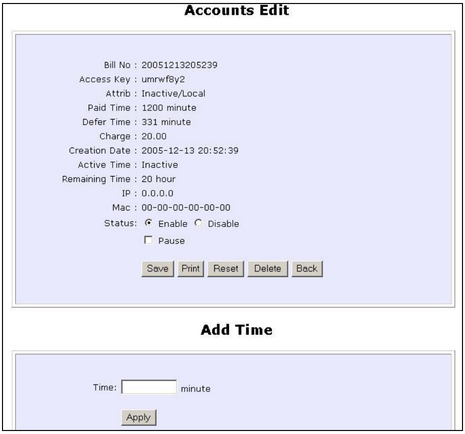
Add Time:
This button adds time credits to all accounts.

Editing Subscriber Accounts

When editing a subscriber account, you can only enable, disable or pause the account.

1. Under the **Accounts List** section, select and click the hyperlink of the selected access key. This will bring up the **Accounts Edit page** of the selected account.

2. Make some required changes. Click **Save** to effect the new change.



Accounts Edit

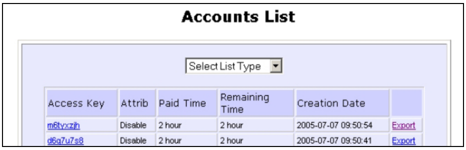
Bill No : 20051213205239
Access Key : umrwf8y2
Attrib : Inactive/Local
Paid Time : 1200 minute
Defer Time : 331 minute
Charge : 20.00
Creation Date : 2005-12-13 20:52:39
Active Time : Inactive
Remaining Time : 20 hour
IP : 0.0.0.0
Mac : 00-00-00-00-00-00
Status: ● Enable ○ Disable
□ Pause

Add Time

Time: ______ minute

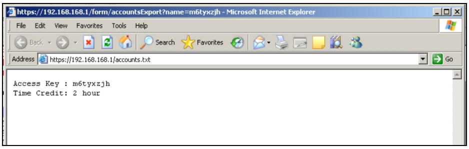
1. Under the **Accounts List** section, select and click the **Export** hyperlink of the selected access key. This will bring up the web browser of the selected account.

2. Then you will be directed to the web browser where you can view the information on the time credit.



Accounts List

Access Key	Attrib	Paid Time	Remaining Time	Creation Date	
m6tyxzjh	Disable	2 hour	2 hour	2005-07-07 09:50:54	Export
d6q7u7s8	Disable	2 hour	2 hour	2005-07-07 09:50:41	Export



https://192.168.168.1/form/accountsExport?name=m6tyxzjh - Microsoft Internet Explorer

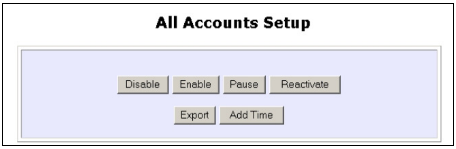
Address: https://192.168.168.1/accounts.txt

```
Access Key : m6tyxzjh
Time Credit: 2 hour
```

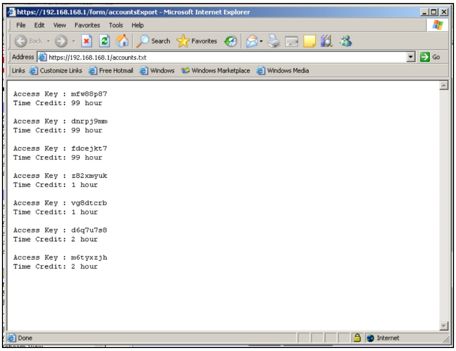
Exporting all existing subscriber Accounts

When exporting all subscriber accounts, you can view the list of all user account's access key and time credit.

1. Under the **Accounts List** section, go to **All Accounts Setup**. select and click on the **Export** button. This will bring up the web browser of all available accounts.



2. Then you will be directed to the web browser where you can view the listing on all exported accounts.

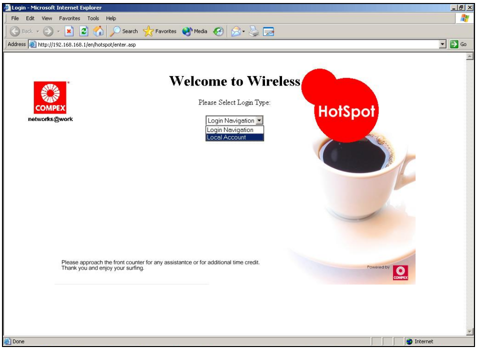


```
Access Key : mfw88p87
Time Credit: 99 hour

Access Key : dnrpj9mm
Time Credit: 99 hour

Access Key : fdcejkt7
Time Credit: 99 hour

Access Key : z82xmyuk
Time Credit: 1 hour

Access Key : vg8dtcrb
Time Credit: 1 hour

Access Key : d6q7u7s8
Time Credit: 2 hour

Access Key : m6tyxzjh
Time Credit: 2 hour
```

For a subscriber to access the Internet

Once the operator creates a time account for a subscriber, if a subscriber is authenticated, he/she can log in the given access key in order to surf the Internet.

1. At the subscriber's side, you can open a web browser and key in any URL. The **Welcome to CyberSing** page will show up.


Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.1/en/hotspot/enter.asp
Go
COMPEX
networks@work
HotSpot
Powered by
COMPEX
Done
Internet

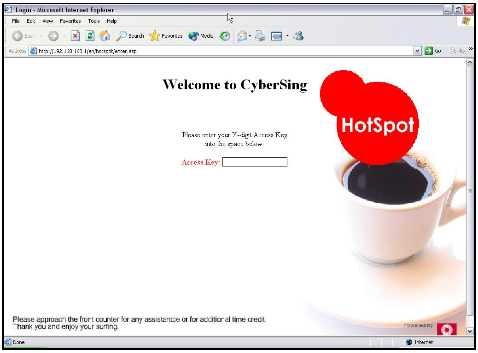
Welcome to Wireless

Please Select Login Type:

Login Navigation
Login Navigation
Local Account

Please approach the front counter for any assistantce or for additional time credit.
Thank you and enjoy your surfing.

2. Enter the **Access Key**. The access key will be provided by the operator to the subscriber. Alternatively, the subscriber can find it in the bill issued to him.

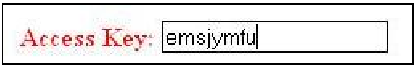

Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.1/en/hotspot/enter.asp
Go Links
HotSpot
Powered by
Done
Internet

Welcome to CyberSing

Please enter your X-digit Access Key
into the space below.

Access Key:

Please approach the front counter for any assistantce or for additional time credit.
Thank you and enjoy your surfing.

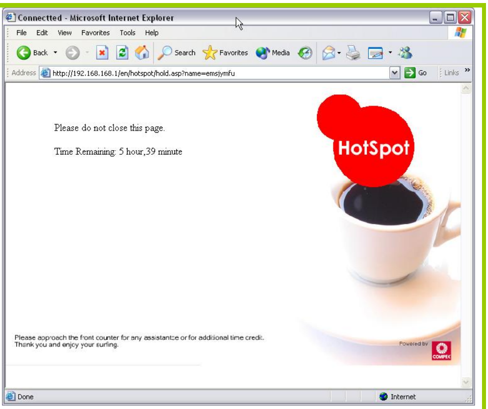


Access Key: emsjymfu

3. Press **Enter** on the keyboard.

4. Then the Remaining Time page will appear. You can open another web browser to start surfing.

5. At the same time, the status of the selected access key is changed from 'Not Active to 'Active' on the **Accounts List** page.



Connectted - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links

http://192.168.168.1/en/hotspot/hold.asp?name=emsjymfu

Please do not close this page.

Time Remaining: 5 hour,39 minute

Please approach the front counter for any assistantce or for additional time credit.
Thank you and enjoy your surfing.

Powered by
COMPEX
Done
Internet

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 which you encounter. If you cannot find an answer here, you may visit the corporate Compex website at www.compex.com.sg or www.cpx.com.

1. I want to know if the router is connected to the Internet.

A. Open a Command Prompt

- For Windows 98SE and ME, please click the **Start** button and **Run**. In the **Open** field within the **Run** dialog box, type in **command**. Press the **Enter** key or click the **OK** button.
- For Windows 2000 and XP, please click the **Start** button and **Run**. In the **Open** field within the **Run** dialog box, type in **cmd**. Press the **Enter** key or click the **OK** button.

B. In the Command Prompt, type **ping 192.168.168.1** and press the **Enter** key.

- If you get a reply, the computer is communicating with the router.
- If you do NOT get a reply, please check the cables and make the settings are correct as mentioned in Parts 1 and 2 of Chapter 4.

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

- If you get a reply, the computer is connected to the Internet.
- If you do not get a reply, you may want to ping another known host. No reply from the host implies a problem with the connection.

2. I am not getting an IP address on my connection and 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 on the WAN port information page. Then refer to Problem 1 (steps A & B), and verify connectivity with the router.

B. Ensure that you are using the correct WAN settings suitable for your broadband connection. You may contact your ISP to see if your Internet connection type should be that of Dynamic IP or Static IP addressing, or if it is PPPoE (commonly used for ADSL subscriptions). Please refer to Part 2 of Chapter 4 for WAN Setup.

C. If you are able to surf the Internet when your Cable/ADSL modem is connected directly to your PC, but after verifying the settings in steps A & B above, your NetPassage is unable to get an IP address from the ISP, then you may need to refer to Chapter 4 Part 2(d)i 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.

3. I am not able to access the web-based configuration page of the router

A. Refer to Problem 1, and first verify connectivity with the router.

B. 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 for PPPoE users. 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**.
    - Make sure that the **Direct connection to the Internet** option is selected.
    - Close all windows to finish.

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

A. 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 it for 8 to 10 seconds before releasing it.

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

A. 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 default 'password'.

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

A. You 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.

B. You MUST give your PC a static IP address of 192.168.168.100 with a subnet mask of 255.255.255.0. By default your PC will also learn the IP address of 192.168.168.100 from the router.

- If you are using Windows 98SE or Windows Millennium, follow Part 1(c) of the manual to set the static IP address.
- If you are using Windows 2000 or Windows XP, follow Part 1(d) of the manual to set the static IP address

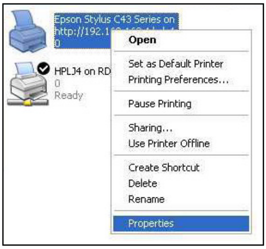
C. Depress and hold the "Reset" button on the router, and at the same time power ON the device and hold the button for 5 seconds.

D. Insert the Product CD into the CD-ROM drive of your PC, where the CD-ROM drive is X:\, double-click "np28grcv.bat" to begin the firmware recovery process.

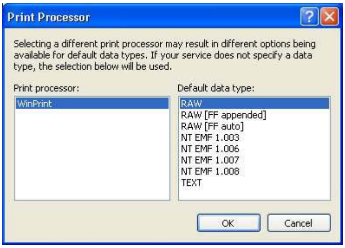
E. It takes about 1 minute to complete the whole process. Power OFF and then power ON the router to continue with normal operation.

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

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



B. 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:



Print Processor

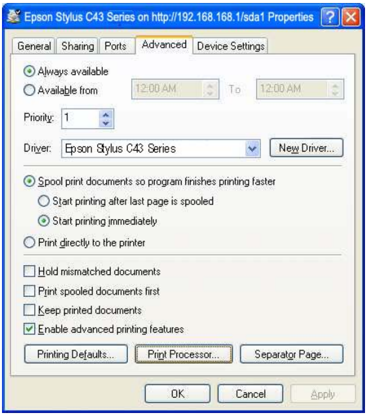
Selecting a different print processor may result in different options being available for default data types. If your service does not specify a data type, the selection below will be used.

Print processor:

WinPrint

Default data type:

RAW
RAW [FF appended]
RAW [FF auto]
NT EMF 1.003
NT EMF 1.006
NT EMF 1.007
NT EMF 1.008
TEXT



Epson Stylus C43 Series on http://192.168.168.1/sda1 Properties

● Always available

○ Available from 12:00 AM To 12:00 AM

Priority: 1

Driver: Epson Stylus C43 Series

● Spool print documents so program finishes printing faster

○ Start printing after last page is spooled

● Start printing immediately

○ Print directly to the printer

☐ Hold mismatched documents

☐ Print spooled documents first

☐ Keep printed documents

☑ Enable advanced printing features

Appendix B: Frequently Asked Questions

Answers to Frequently Asked Questions

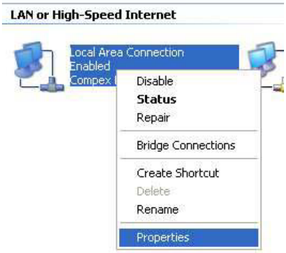
In the section, we have compiled a short list of answers to some frequently asked questions about the router product. If you cannot find an answer here, you may visit the corporate Compex website at www.compex.com.sg or www.cpx.com.

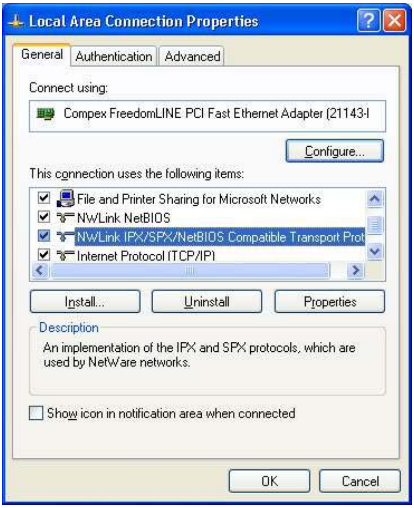
	Question	Answer
1.	**IPSec pass-through supported by the router?**	Yes. It is an automatically enabled feature supported by the router.
2.	**Does the router support other operating systems other than Windows 98SE, ME, 2000 and XP?**	Yes. However, Compex does not provide technical support for the set up, configuration or troubleshooting of these 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 is Network Address Translation and what is it used for?**	Network Address Translation multiplexes multiple private IP addresses for 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. *Learn more from our* ***NAT*** ***Technology Primer***
6.	**What is a 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.

Appendix C: NETBIOS Protocol Installation

To check if you have installed your NETBIOS protocol,

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





Connect using:

Compex FreedomLINE PCI Fast Ethernet Adapter (21143-I

This connection uses the following items:

☑ File and Printer Sharing for Microsoft Networks
☑ NWLink NetBIOS
☑ NWLink IPX/SPX/NetBIOS Compatible Transport Prot
☑ Internet Protocol (TCP/IP)

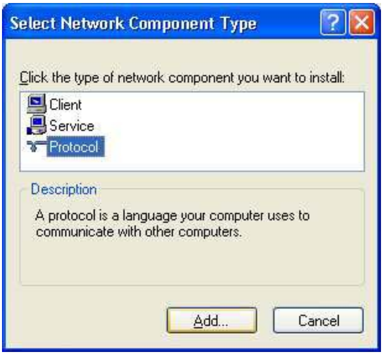
Description

An implementation of the IPX and SPX protocols, which are used by NetWare networks.

☐ Show icon in notification area when connected

2. Next, from the **General** tab, scroll down to look for *NwLink IPX/SPX/NetBIOS Compatible Transport Protocol*. If you have found this protocol, this means that NETBIOS protocol has installed to 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.

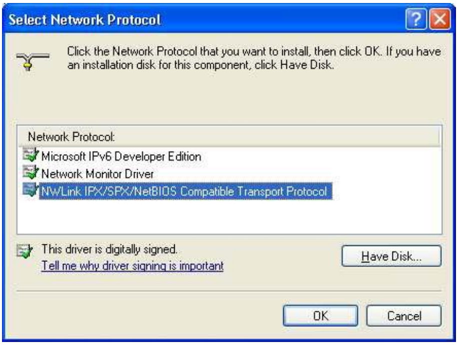


Click the type of network component you want to install:

Description

A protocol is a language your computer uses to communicate with other computers.

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



Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

Network Protocol:

- Microsoft IPv6 Developer Edition
- Network Monitor Driver
- NWLink IPX/SPX/NetBIOS Compatible Transport Protocol

This driver is digitally signed.
Tell me why driver signing is important

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 A draft standard proposed by IEEE that is awaiting ratification, to be an extension of the IEEE 802.11 standard. It specifies a data transfer rate of 54Mbps using ODFM modulation and an operating frequency of 2.4GHz, as well as backward compatibility with the 802.11b devices.

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.

CAT 5 It is a standard developed by the Electronics Industries Association that specifies network cabling which consists for twisted pairs of copper wire with a sustainable data rate of 100Mbps.

Database A database is a collection of information that is organized so that the contents may be easily accessed/managed.

Data Packet In an IP network, packet switching is the method employed to transmit data and the smallest chunk of data is called a packet (packet size can vary).

DHCP Dynamic Host Configuration Protocol. It is a protocol that allows the network administrator to centrally manage and assign IP addresses to devices in the network. For more information on DHCP, please refer to the DHCP Technology Primer found on the Product CD.

Learn more from our ***DHCP*** **Technology Primer**

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 which has to run specialized applications requiring multiple TCP/IP ports to be opened.

DNS Domain Name System translates Internet domain names to IP addresses, giving meaningful and easy-to-remember names to otherwise arcane IP addresses.

Driver A piece of software developed to interface a piece of hardware with its immediate upper-layer software (i.e. operating system) so that it can be recognized and operated.

DSSS Direct Sequence Spread Spectrum is a modulation scheme employed by the 802.11b standard that uses a chipping code (redundant bit) during its transmission to reject interference.

Dynamic IP Address It is an IP address that is dynamically allocated or assigned to a client device within a TCP/IP network, typically by a DHCP server.

Encryption Encryption is a security method applying specific algorithms to make sure that all the data from one computer is encoded into a form that only the other intended party will be able to decode and view the information.

Ethernet An IEEE standard network protocol that specifies how data is transmitted over a common medium. It uses CSMA/CD which stands for Carrier Sense Multiple Access with Collision Detection. It has a defined data rate of 10Mbps.

Fast Ethernet An IEEE standard extended from 10Base-T Ethernet to support 100Mbps data rate.

Firewall It is a software layer that controls network access from within and without so that any undesired activity may be prevented by malicious or snooping parties.

Firmware It is a software code written and saved within the read-only memory (ROM) or programmable read-only memory (PROM). The firmware that is written on the ROM/PROM is retained even when the device is powered off.

FTP File Transfer Protocol. It is a protocol designed to transfer files over a TCP/IP network.

Full Duplex It defines the ability of a device to transmit data simultaneously in both upstream and downstream directions over a single line.

Router A router is a device that interconnects networks.

Half Duplex It defines the ability of a device to transmit in one direction at a time over a single line.

HTTP HyperText Transport Protocol is a common protocol used to connect servers on the World Wide Web, with its primary function being to establish a connection with a web server and transmit HTML pages to the client's browser.

ICMP Internet Control Message Protocol is a message control and error reporting protocol between a host server and a 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.

NAT Network Address Translations multiplexes multiple private IP addresses for 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.

Learn more from our ***NAT*** ***Technology Primer***

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 IP address is available online. It works by sending out a packet and waiting for a response from the recipient.

PPPoE Point-to-Point Protocol over Ethernet is a method for the encapsulation of PPP packets over Ethernet frames.

PPTP 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 which holds up to eight wires.

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.

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 **W**i Fi **P**rotected **A**ccess **P**re **S**hared **K**ey. 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	Wired: - IEEE 802.3 10Base-T - IEEE 802.3u 100Base-Tx - IEEE 802.3x Flow Control Wireless: - IEEE 802.11b - IEEE 802.11g
WAN Interface	- 1x Auto MDI/MDI-X RJ45 Ethernet Port for external Cable/ADSL modem
WAN Type	- Static IP - Dynamic IP - PPP over Ethernet (PPPoE) - Point to Point Tunneling Protocol (PPTP)
LAN/WLAN Interface	Wired: - Integrated 3x Auto MDI/MDI-X 10/100Mbps Switch Wireless: - 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: 108Mbps, 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	4X integrated USB ports supporting: - Print Server
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
Configuration Interface	Web-based Configuration Menus
Profile Backup and Restore	Yes
Firmware Upgradeable	Yes
Environment Requirement	Temperature: - Operating : 0°C to 40°C - Storage : -20°C to 70°C Humidity: - 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 Fax	Tel: +1 (714) 482-0333 (8 a.m.-5 p.m. Pacific time) Tel: +1 (800) 279-8891 (Ext.122 Technical Support) Fax: +1 (714) 482-0332
Asia, Australia, New Zealand, Middle East and the rest of the World	
✉ Write	**Compex Systems Pte Ltd** 135, Joo Seng Road #08-01, PM Industrial Building Singapore 368363
☎ Call Fax	Tel: (65) 6286-1805 (8 a.m.-5 p.m. local time) Tel: (65) 6286-2086 (Ext.199 Technical Support) Fax: (65) 6283-8337
Internet access/	E-mail: **support@compex.com.sg** FTPsite: **ftp.compex.com.sg**
Website:	**http://www.cpx.com** *or* **http://www.compex.com.sg**