NETPASSAGE NP25G

User Manual

Table of Contents

Overview the Product

Introduction

NetPassage NP25G is a high-performance and low-cost IEEE802.11b/g Router using the latest AR5007 technology. Using Atheros System-on-Chip (SoC) solution, NP25G supports high-speed data transmission of up to 54Mbps.

NetPassage NP25G combines 3 devices into one box. It works as a Wireless Access Point, which allows you to connect Wireless B/G devices to the network. It also has a 4-port full-duplex 10/100Mbps switch which connects your wired Ethernet devices directly to 4 PCs or to additional hubs and switches to create a larger network. NP25G also works as a router that lets your whole network share a high-speed cable or DSL Internet connection.

To ease the complexity of setting up a secured network, NetPassage NP25G features Wireless One-Touch Registration using WSC (Wireless Simple Config).
There no need to setup or remember the secure key as require by other wireless devices. The client automatically connect to NP25G with the using the WPA-PSK secured wireless connection.
A network administrator or home users just need to push a single access button on NP25G to allow it to enter the network.
The Client devices on running the JumpStart application automatically discover NP25G and automatically register the connection with NP25G. On completing the registration process, the client will create a wireless secured connection profile. Each time the client makes a connection with NP25G it automatically use this secured profile.

Features

Key Features

Wireless One-Touch Registration

Remove the complexity of setting up a secured network – at a touch of a single access button, a shared security key is set up in the network.

Wireless multimedia (WMM)

Suitable for simple applications that require Quality of Service (QoS), such as Voice over IP (VoIP), WMM prioritizes data traffic according to 4 access categories: Voice, Video, Best Effort and Background.

Bandwidth Control

Available in Routing Mode, this feature gives the administrator the ability to manage the bandwidth of subscribers to prevent massive data transfers from slowing down the Internet access of other users. The Upload / Download bandwidth at WAN / LAN ports can be limited using either IP address or MAC address.

Compatible with IEEE 802.11g and IEEE 802.11b standards

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

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

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

Auto MDI/MDI-X crossover support on all Ports

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

Virtual Servers based on Port-forwarding, IP-forwarding

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

Domain Name System (DNS) Redirection

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

Static Routing

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

Dynamic DNS

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

De-Militarized Zone (DMZ) hosting

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

Universal Plug and Play (UPnP)

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

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.

WDS2

WDS2 (Wireless Distributed System 2) links up access points to create a wider network in which mobile users can roam while still staying connected to available network resources.

Security Features

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

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

Built-in "NAT" firewall

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

Stateful Packet Inspection (SPI) firewall

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

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

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

Overview the LEDs

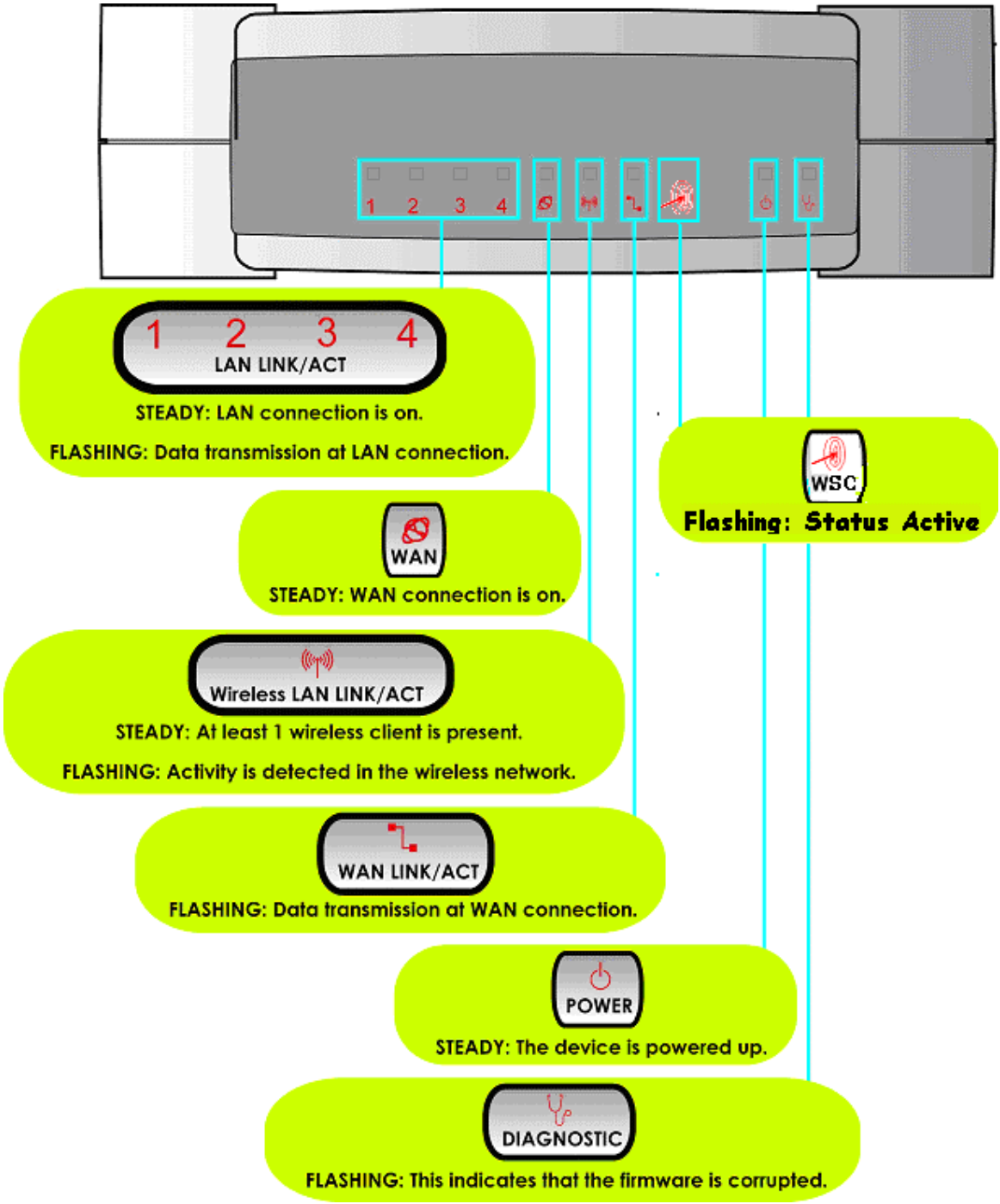


Figure 1

Setup the Software

PC Configuration

Configuring PCs to be Wired to the Router

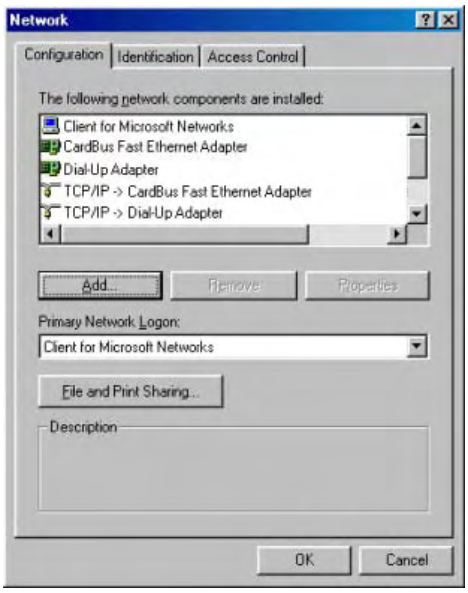
The first step is to make sure the PC gets an IP address that it will use to communicate with the router and with other PCs across the network. You can begin by setting up your PC to function as a DHCP client, which will obtain an IP address automatically from router. Alternatively, you may want to give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

Whether you choose to allocate static or dynamic IP settings, the next few pages will walk you through the TCP/IP configuration in a step-by-step process. Depending on the Microsoft Windows operating system used, you may skip some of the steps. Please ensure that you have an Ethernet or wireless adapter successfully installed in each PC you are configuring.

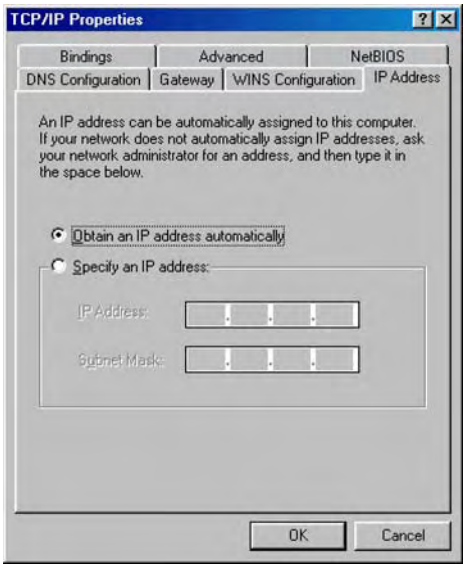
Important: By default, Windows 98SE, ME, 2000 and XP have the TCP/IP protocol installed and set to obtain an IP address automatically.

Configuring PC to dynamically obtain an IP address for Windows 98SE or ME…

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



2. On the **Configuration** tab, highlight the **TCP/IP** line corresponding to your Ethernet adapter and click on the **Properties** button. You will be brought to the **TCP/IP Properties** page below.



3. Click on the **IP Address** tab, and select **Obtain an IP address automatically**.

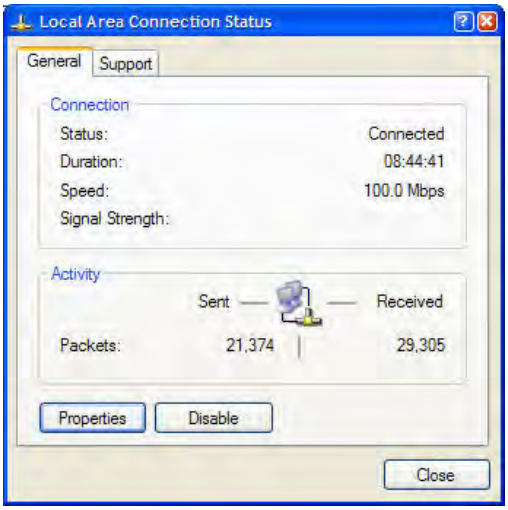
4. Next, click the **Gateway** tab, and verify that the **Installed Gateway** field is blank. Now, click the **OK** button

5. On the Network dialog page, click on the **OK** button.

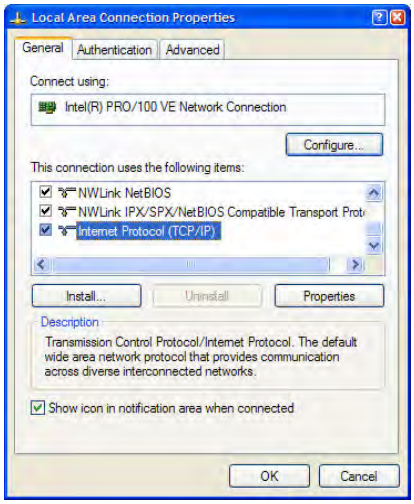
6. Windows may ask you to restart the PC, if so, click the **Yes** button and allow the PC to restart in order to complete the configuration.

Configure PC to dynamically obtain IP address for Windows 2K or XP

1. Click the **Start** button. Select **Settings** and click the **Control Panel** icon. Then double-click the **Network and Dial-up Connection** (Windows 2000) or **Network Connection** (Windows XP) icon.



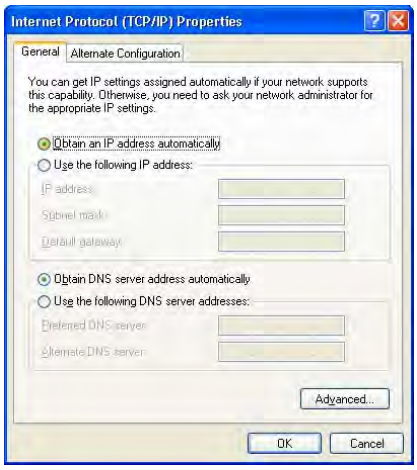
2. Double-click the **Local Area Connection** icon for the network adapter applicable to your Internet connection, and click the **Properties** button. You will be brought to the dialog page below.



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

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

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

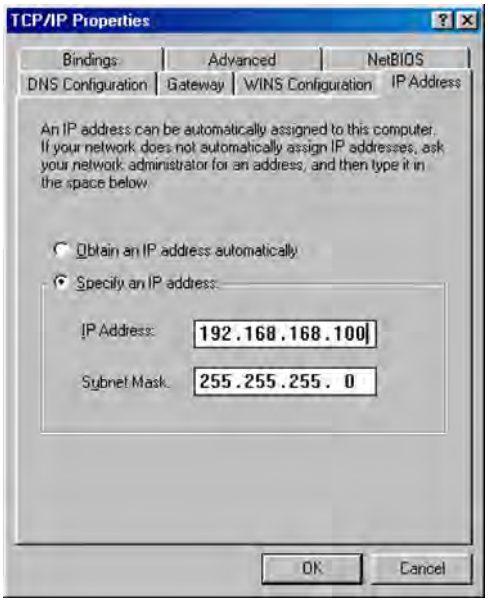


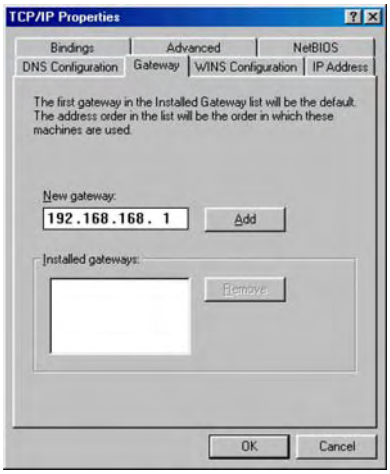
Configure PC with static IP address for Windows 98SE or ME

1. To begin the Static IP address configuration, follow steps 1 & 2 of Part 1(a) to get to the page on the right.

2. Click on the **IP Address** tab. Then type in an **IP address** and **Subnet Mask** as 192.168.168.X and 255.255.255.0 respectively, where X is any number from 2 to 254.

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



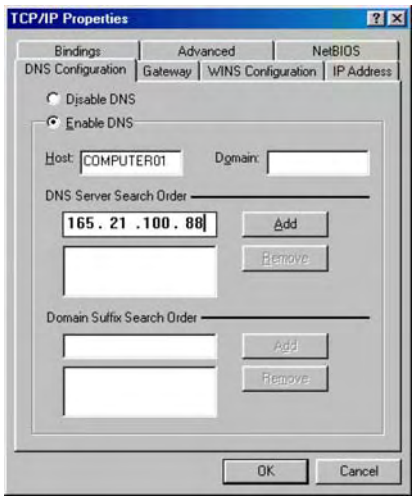


3. Next, click the **Gateway** tab to see the dialog page on the left.

4. Under the **New Gateway** field, key in the IP address of the router (which is 192.168.168.1 by default). Follow by clicking the **Add** button.

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

6. You complete by clicking the **OK** button, and then restarting the computer.



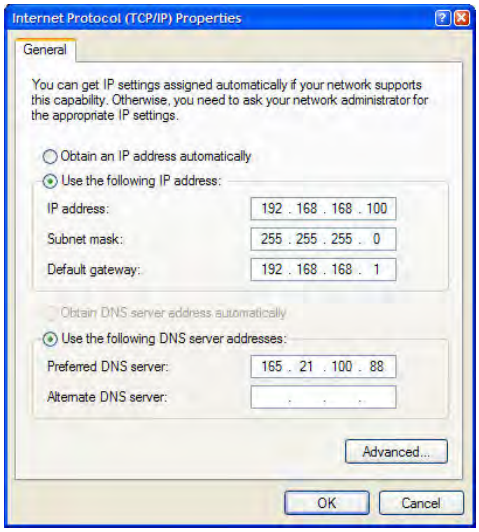
Configure PC with static IP address for Windows 2K or XP

1. To begin the Static IP address configuration, follow steps 1, 2 & 3 of Part 1(b) to get to the page on the right.

2. Select **Use the following IP address**, and then key in 192.168.168.X for the **IP address** field, where X is any number from 2 to 254. Following that, enter 255.255.255.0 for the **Subnet mask**, and key in the IP address of the router as the **Default gateway**.

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

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



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

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

Configuring PCs to be Wireless Clients

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

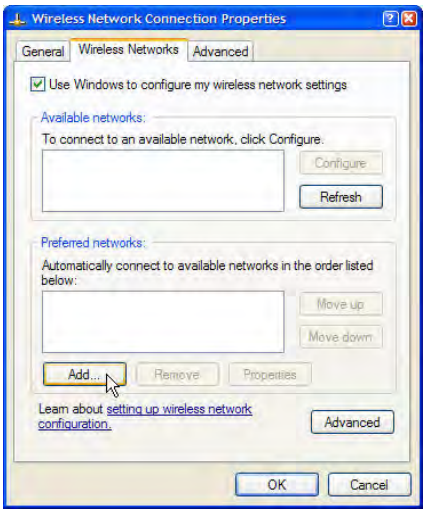
Hence, please note that in Windows XP, you will need to select the wireless network connection corresponding to the wireless adapter you use.

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

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

Configure Wireless Client for Windows XP

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



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

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

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

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

Perform Basic Router Setup

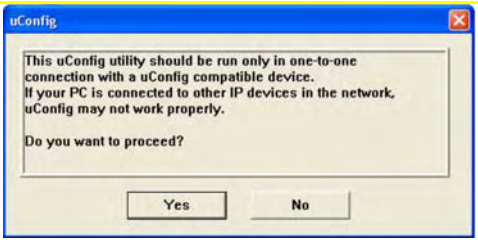
In this basic setup, you will find information on how you may configure the router to function in your network and to access the Internet.

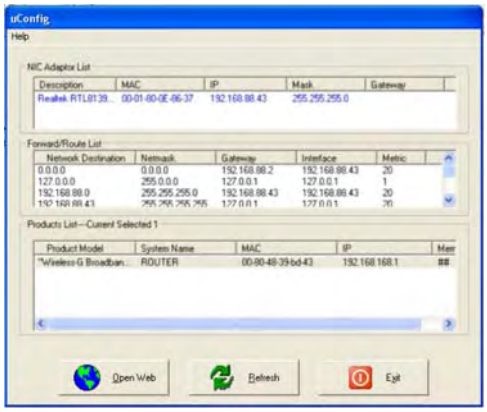
Use UConfig

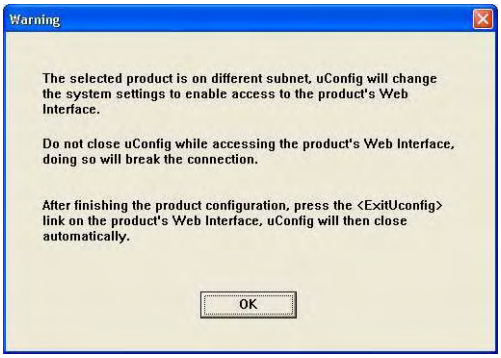
The powerful uConfig utility has been developed to provide you hassle-free access to the router's web-based configuration page. If you do not wish to modify the TCP/IP settings of your PC, or you have changed but forgotten the router's management IP address, uConfig will bring you to the router's setup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

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

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







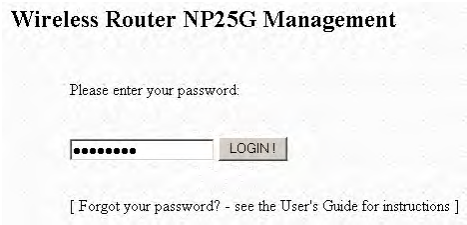
Step 3:
When the uConfig window is prompted, click **Yes** to proceed. With the router selected under **Products List**, click on **Open Web**. Click on **OK** and you are done!

Access Web Interface

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

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

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



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

Setup Secured Wireless Connection

Setup Secured Wireless Connection with One-Touch Registration

The router supports the new Wireless One-Touch Registration feature using WSC (Wireless Simple Config). WSC allows users unfamiliar with network security to set up a secured wireless connection.

The router has a Wireless One-Touch Registration button which when pressed lets router automatically setup a WPA-PSK secured wireless connection with the client computer. The client computer after the registration process will create a connection profile. Client computer will automatically use this profile to make the secured connection with router each time client computer starts up.

Setup Secured Wireless Connection with One-Touch Registration

Step 1:

Press the WSC button once.
WSC button is located at the back of NP25G between the WAN and LAN ports. See figure 1.
Notice the WSC light indicator at the front panel of NP25G will flash fast at rate of about 2 to 3 flashes per second after pressing the button.
This indicates the one-touch registration process is now started.
Its now listening for client to register.

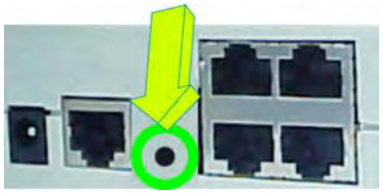


Figure 1

Step 2:

On the Client computer, run the JumpStart program.

In the **Welcome to JumpStart** page, select the **Join a wireless network** radio button.

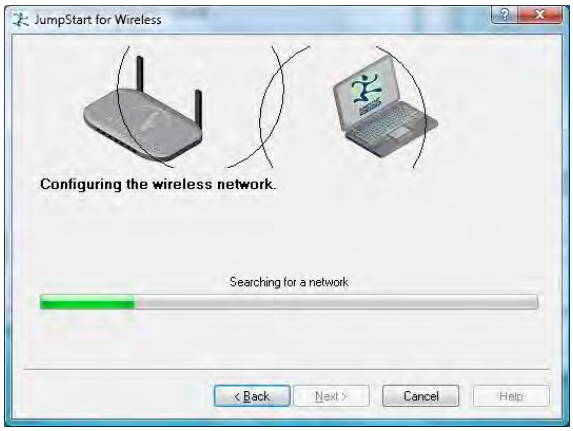
Click the **Next** button.

Step 3:

In the **Join a wireless network** page, select the **Push the button on my access point** radio button.

The **Automatically select the network** checkbox is selected by default, for convenient setting up of the connection, leave this option enabled.

Click the **Next** button.



Step 4:

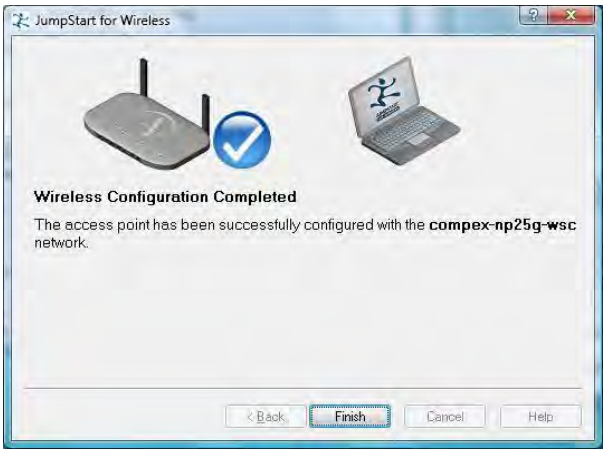
Configuring the wireless network screen appears.
The client device found NP25G and negotiating with NP25G to do the registration.

Step 5:

The **Wireless Configuration Completed** page displays, indicating that configuration was successfully.

Click on the **Finish** button to exit the page.

On NP25G the WSC light indicator will change to flash slowly at a rate of about 1 flash per second.
This indicates client registration has completed successfully.



WSC light indicator status

Action	Light indicator status	Remarks
After pressed once.	WSC light flash fast at a rate of 2 to 3 flashes per second.	Indicates One-Touch-Registration is activated
a) No respond from client after 2 minutes. Or b) Client JumpStart application started but failed to complete. Or c) More than one client try to register at the same time.	Light flashes 5 times and paused for 1 second and repeat. Status will display for about 2 minutes before it turn off.	Indicates registration failed

Setup Secured Wireless Connection Without Using One-Touch Registration

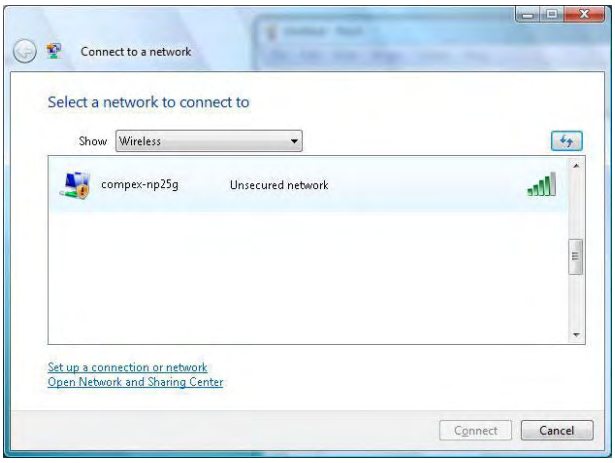
For users using older wireless adapters without Jumpstart support, a secondary SSID which by default has no wireless security enabled is available for connection setup.

*** Note:-**

This unsecured connection is only available in factory default mode and has not been registered a client before through the one-touch-registration process.
If there is already a client been registered first through the one-touch-registration process, then this unsecured connection will be disabled automatically.
To enabled it refer to configure your router section in the later chapters.

User can then connect to NP25G through this secondary unsecured wireless connection.
This section will show how to setup a secured wireless connection without using the Wireless One-Touch Registration, and setup WPA-Personal security. For other security modes, please refer to the Set Security Mode section.

Setup Secured Wireless Connection without using One-Touch Registration

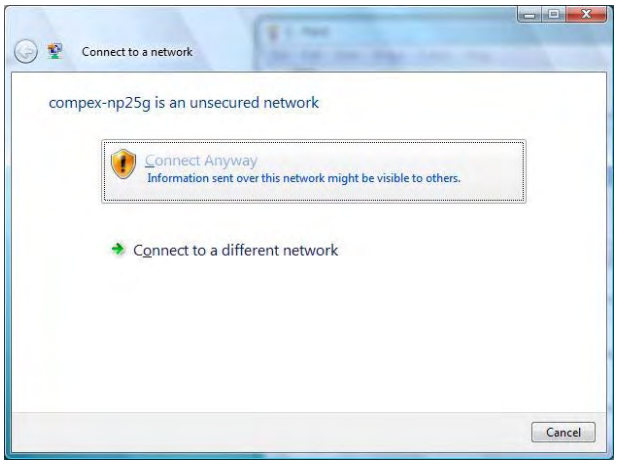


Step 1:

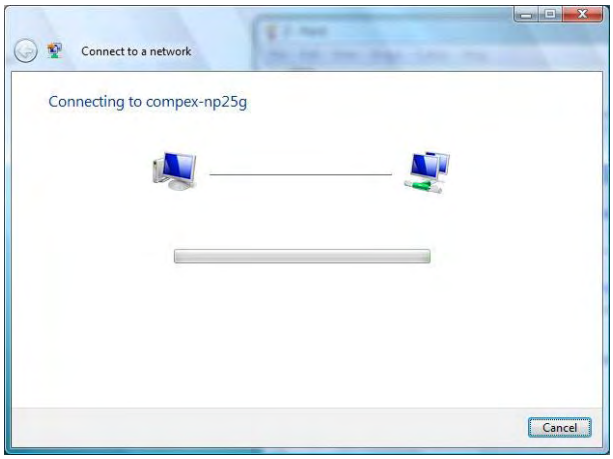
In the **Connect to a network** configuration page, select the secondary SSID (**compex-np25g**) and click the **Connect** button.

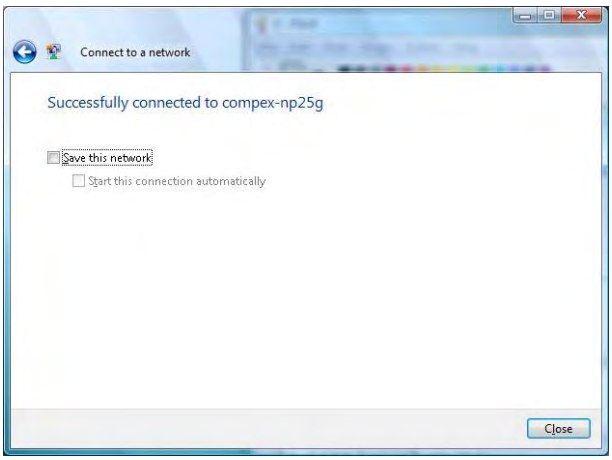
Step 2:

Click the **Connect Anyway** button when prompted.



Connection to the secondary SSID (**compex-np25g**) will commence.





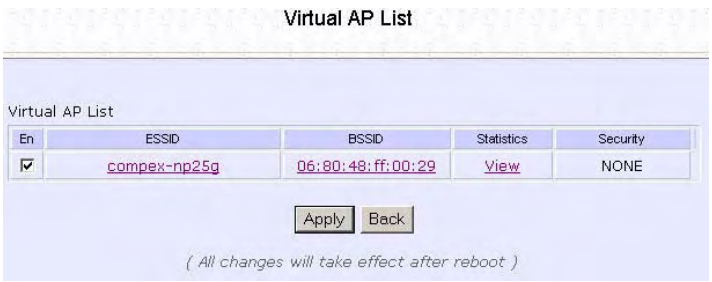
Step 3:

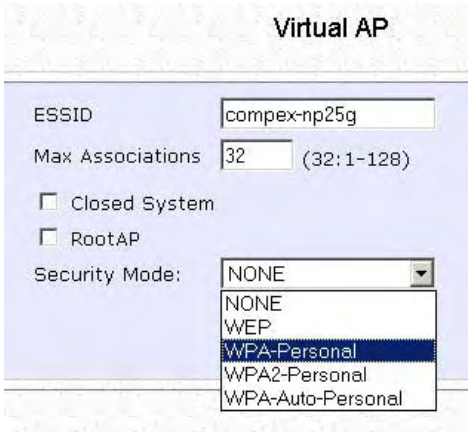
Click the **Close** button to complete the connection.

Step 4:

In the web-based configuration page, select **Configuration – WLAN Setup – Virtual AP** to view the **Virtual AP List**.

Select the secondary SSID (**compex-np25g**).





Step 5:

Set the **Security Mode** to **WPA-Personal** and click on the **Apply** button.

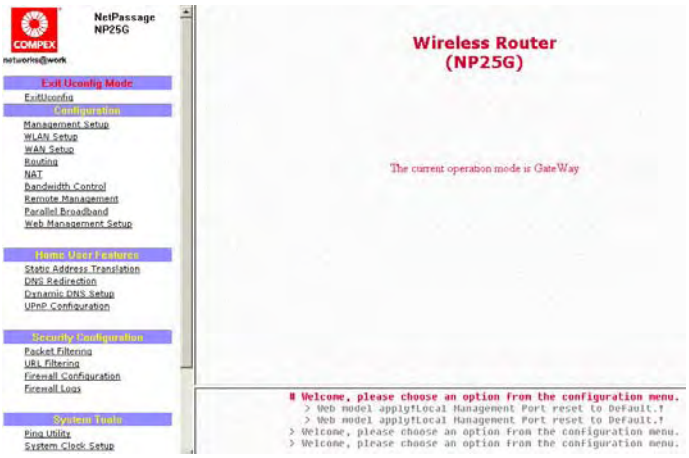
Please refer to the Setup WPA section for detailed configuration of the security mode.

Reboot the router to apply changes.

Perform Configuration

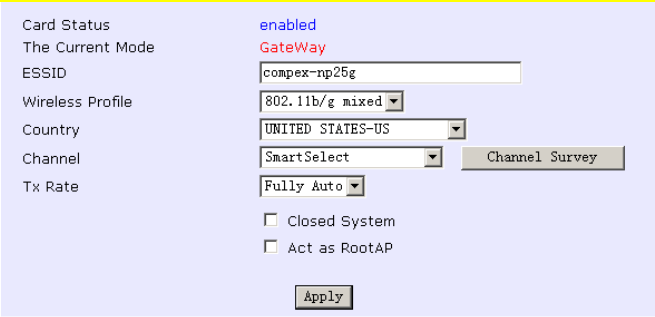
This part of the setup for the router is meant for the advanced user who requires more than the essential information to set up a wired/wireless network infrastructure. Adopting a top-down approach to explain the features found on the router, what follows is a detailed walkthrough of the configurable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

Once you have successfully logged in, you shall find a comprehensive list of configurable features as shown.



Configure Wireless Setup

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



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 Profile : Select from the list of wireless modes available:

a. 802.11b only
This mode supports wireless B clients with data rates of up to 11Mbps in the frequency range of 2.4Hz.

b. 802.11g only
This mode supports wireless G clients with data rates of up to 54Mbps in the frequency range of 2.4Hz.

c. 802.11b/g mixed
This mode supports both wireless B and G clients. The basic rates are 1Mbps, 2 Mbps, 5.5 Mbps, 11Mbps, 6 Mbps, 12 Mbps and 24 Mbps.

Country : This is where you are located during the connection.

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

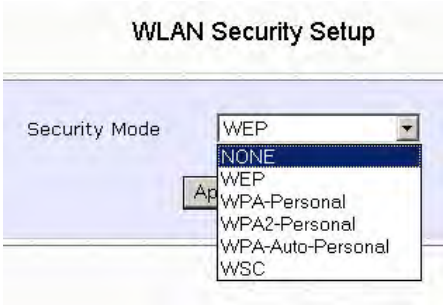
Tx Rate : This option allows you to select a specific transmit power for the wireless communication. The Transmit Power controls the signal strength transmitted by the antenna. If the antenna has a weak RF coverage, increase the Transmit Power. If the antenna has a strong RF coverage, decrease the Transmit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

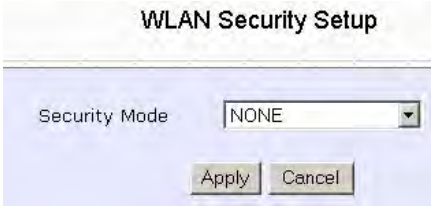
Set Security Mode

Security plays a vital role in securing wireless 802.11 networks to prevent unauthorised users from accessing and using the network resources.

Disable Security

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





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

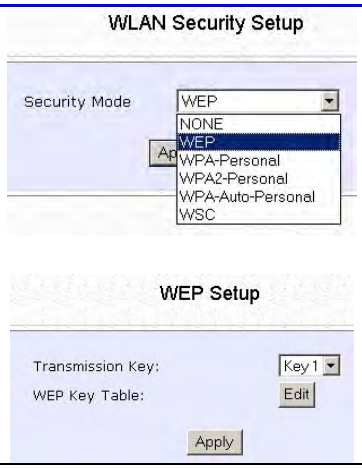
Setup WEP

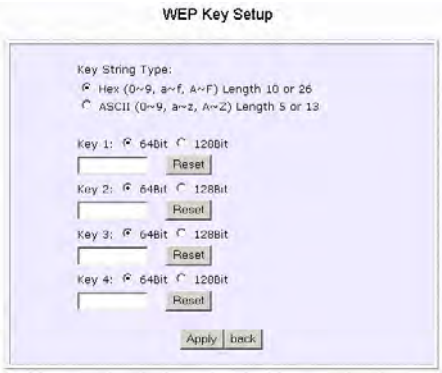
Wired **E**quivalent **P**rivacy is implemented in the network. It is a security protocol in a wireless local area network.
To set the Security mode to WEP, follow these instructions:

1

You can define up to 4 WEP keys.

Click **Edit** to set the keys.





2

For hexadecimal key entry:

1. Select the **Hex** radio button.
2. Select the radio button of the key to be entered.
3. Select the key encryption mode from the drop down menu.
4. Fill in the key value.

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

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

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

5. Click on **Apply**.
6. If the key format is valid, the page will refresh and the key will appear in

3

For **ASCII** key entry:

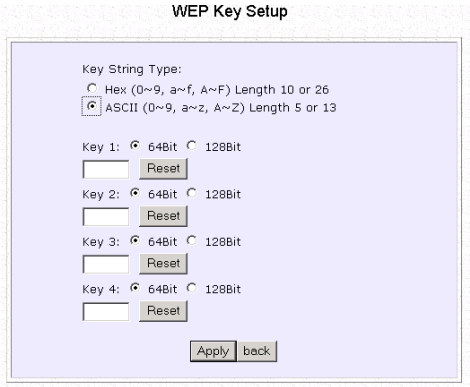
1. Select the **ASCII** radio button.
2. Select the radio button of the key to be entered.
3. Select the key encryption mode from the drop down menu.
4. Fill in the key value.

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

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

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

5. Click on **Save**.
6. If the key format is valid, the page will refresh and the key



4

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

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

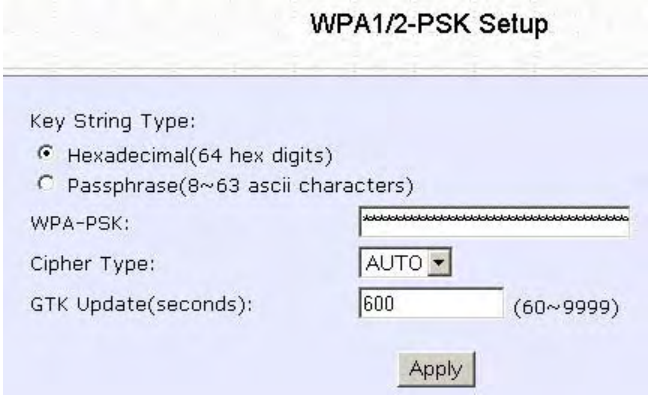
To specify which key to use:

1. Select the radio button of the key to be used.
2. Click on **Apply,** then on **Reboot** to apply the changes.

Setup WPA

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

At the **WPA1/2-PSK Setup** page,



Step 1:

Specify the **key entry type**, by selecting either:

- **Passphrase (Alphanumeric characters)**
- **Hexadecimal**

Step 2:

Fill in the pre-shared network key:
If you are using the **Passphrase** format, your entry can consist of a minimum of 8 alphanumeric characters or a maximum of 63 alphanumeric characters.

Otherwise, when using the **Hexadecimal** format, your entry MUST consist of 64 hexadecimal characters.

Step 3:

For WPA-Personal
Set the **Cipher Type** to **TKIP**.
WPA replaces WEP with a strong encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC).

For WPA2-Personal
Set the **Cipher Type** to **AES**.
Advanced **E**ncryption **S**tandard (AES) is a stronger symmetric 128-bit block data encryption technique. AES is a requirement of WPA2 under the IEEE 802.11i standard.

For WPA-Personal-AUTO

Set the **Cipher Type** to **Auto** to allow the router to automatically detect the cipher type to use.

Step 4:

Enter the **GTK (Group Transient Key) Updates**.
This is the length of time after which the router will automatically generate a new shared key to secure multicast/broadcast traffic among all stations that are communicating with it. By default, the value is 600 seconds.

Step 5:

Click the **Apply** button and reboot your system, after which your settings will become effective.

Setup WSC

Follow these steps to setup the router for using WSC.

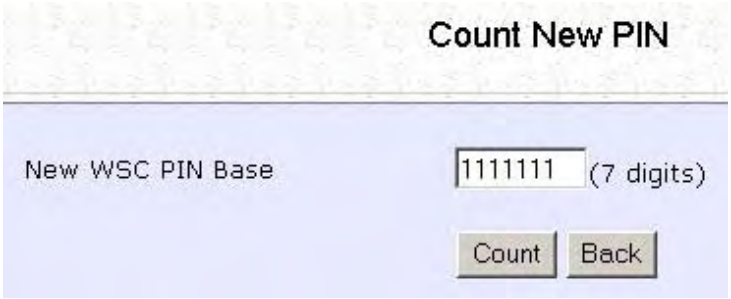
At the **WPA1/2-PSK Setup** page, in the **WSC Particular Setup** section,

Step 1:

Specify whether you wish to enable the **Pushbutton Mode**. Pushbutton Mode is required for Wireless One-Touch Registration.

Step 2:

If you wish to create a new PIN:
Click on the **Create New PIN** button and in the **Count New PIN** page, enter in the desired PIN and click on the **Count** button.



Step 3:

Click on the **Apply** button.

Configure the Advanced WLAN Settings

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

1

1. Click on **WLAN Setup** from the **CONFIGURATION** menu.
2. Select **Advanced**

2

1. Set the **Beacon Interval** (the time lapse between every beacon sent) to any value between 20 and 1000.

It is preset as 100 seconds.

2. Set the **Data Beacon Rate** from 1 to 16384.

This determines how often the beacon should contain a **Delivery Traffic Indication Message** (**DTIM**) that tells power-save clients that a packet is waiting for them. Is it preset to 1.

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

It is preset to 2346.

4. Set the **Frag Threshold** from 256 to 2346.

It is preset to 2346.

5. Transmission Power Control (TPC) offers the flexibility to set the **Transmit Power**. (802.11h compliant)

It is set to **Maximum** by default, but should be reduced if there is more than one unit using the same channel frequency.

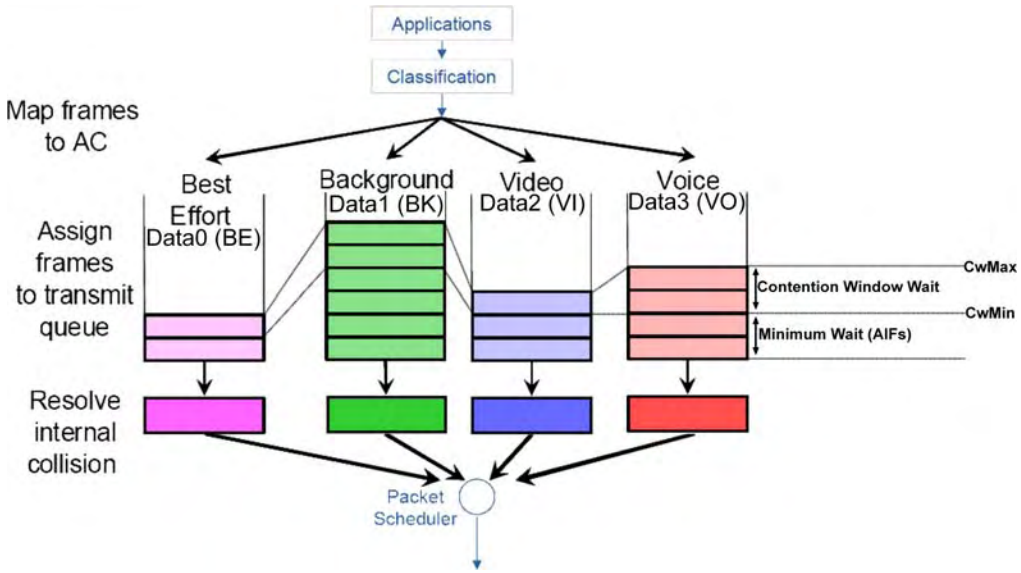
3

1. Click **Apply.**

Changes will be enabled after reboot.

Set Wireless Multimedia

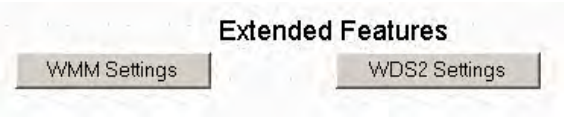
Wireless Multimedia (WMM) is a QoS (Quality of Service) standard in IEEE802.11E that we have adopted to improve and support the user experience for multimedia, video, and voice applications by prioritizing data traffic. QoS can be realized through 4 different Access Categories (AC). Each AC type consists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



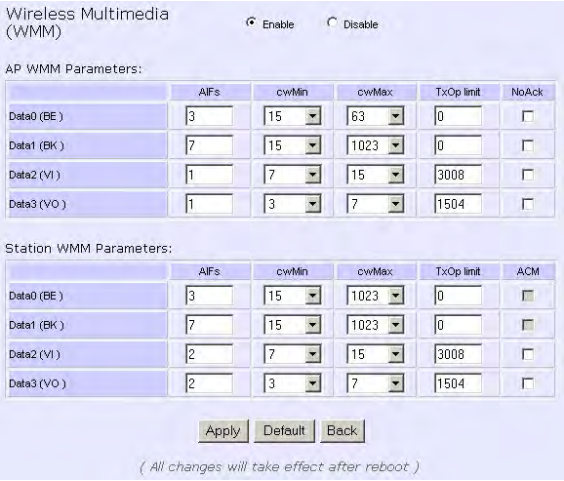
Follow these steps to change the setup Wireless Multimedia on your router.

1

1. Click on **WLAN Setup** from the **CONFIGURATION** menu.
2. Select **Advanced**.



2 Click **WMM Settings.**



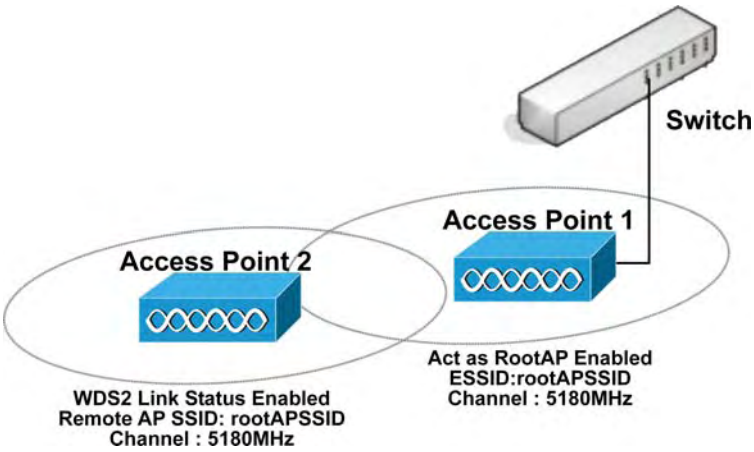
3

1. Select to Enable **Wireless Multimedia (WMM)**
2. Enter the desired WMM parameters. Using the default parameters is recommended.
3. Click **Apply** to apply the WMM settings, click **Default** to reset all parameters to default, or click **Back** to discard any changes and return to WLAN Basic Setup page.

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

Setup WDS2

WDS2 (Wireless Distributed System 2) links up access points to create a wider network in which mobile users can roam while still staying connected to available network resources. The wireless client and root access point has to be set up with the same channel frequency. This allows them to connect even when the link is lost, as the channel frequency setting is preserved.



In this example, there are 2 access points: Access Point 1 and Access Point 2, with Access Point 1 as the root access point.

Follow these steps to change the setup the root access point.

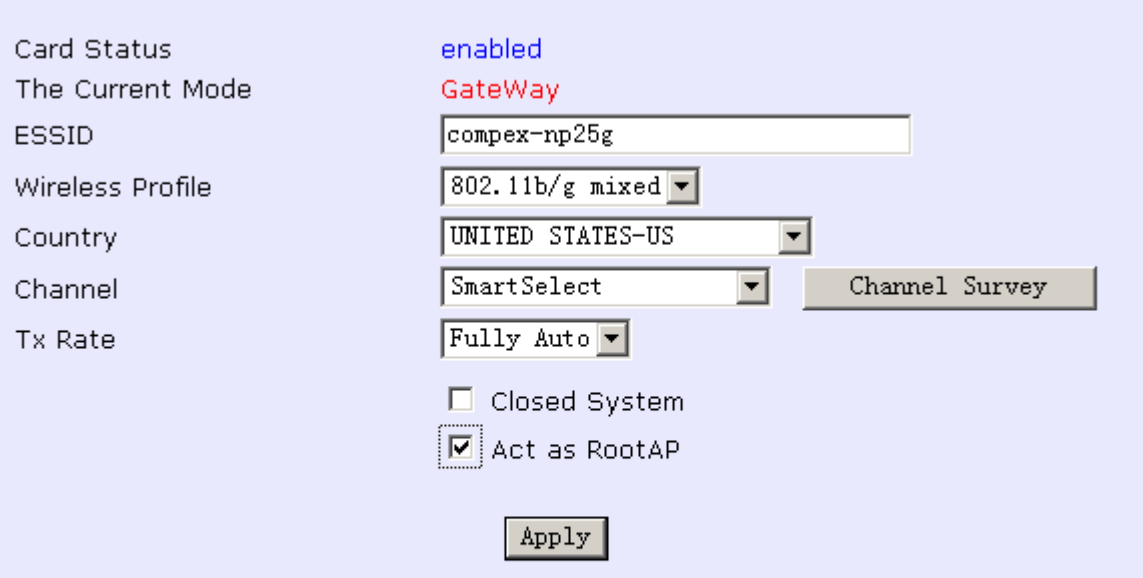
Setup access point 1:

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

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

Select **Act as RootAP**.

Select the **Channel** common to both access point 1 and access point 2.

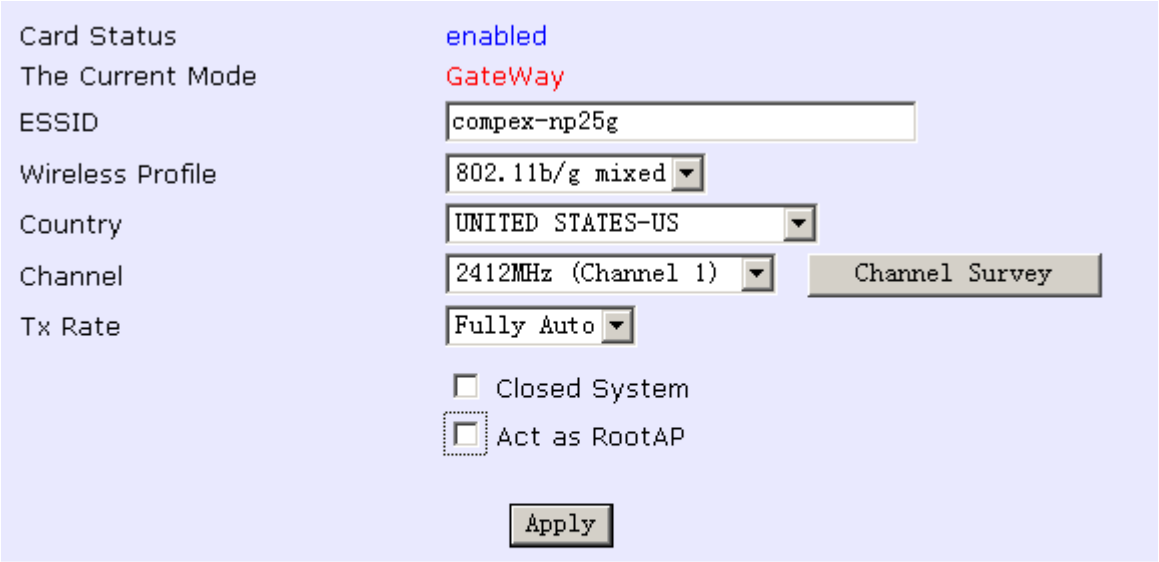


Follow these settings to setup access point 2.

Setup access point 2:

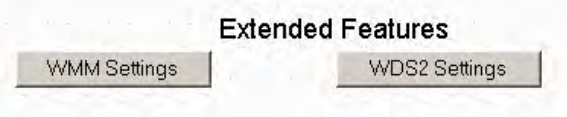
Click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Basic**.

Select the **Channel** common to both access point 1 and access point 2.



Configure WDS2 link:

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

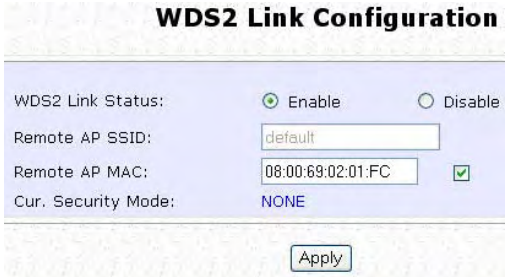


Under **Extended Features**, click on the **WDS2 Settings** button.

Set **WDS2 Link Status** to **Enable**.

Options for configuring WDS2 link:

- By Remote AP MAC – Enter the Remote AP MAC



OR

- By Remote AP SSID – Uncheck the Remote AP MAC checkbox and enter the Remote AP SSID.

Click **Apply**.

Setup Management Port

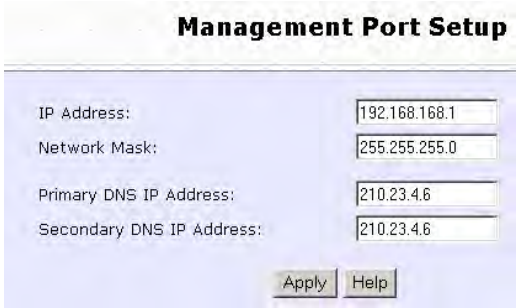
Follow these steps to define the IP addresses.

Step 1:

Click on **TCP/IP Settings** from **Management Setup** from the **CONFIGURATION** menu.

Step 2:

In the **Management Port Setup** page, refer to the table below to replace the default settings with appropriate values to suit the needs of your network.



Step 3:

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

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

Parameters	Description
IP Address	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. The IP address is set by default to *192.168.168.1*.
Network Mask	The Network Mask serves to identify the subnet in which your router resides. The default network mask is *255.255.255.0*.
Primary DNS IP Address	Your ISP usually provides the IP address of the DNS server.
Secondary DNS IP Address	This optional field is reserved for the IP address of a secondary DNS server.

To Setup DHCP Server

There are 3 DHCP Modes:

- NONE
  Select NONE if you do not wish to use a DHCP server.

- DHCP Server
  Select this mode to setup a DHCP server.

- DHCP Relay
  Select this mode to setup a DHCP relay.
  By default, DHCP broadcast messages do not cross router interfaces.
  DHCP Relay supports DHCP Clients and DHCP Servers on different networks by configuring the router to pass selective DHCP messages.

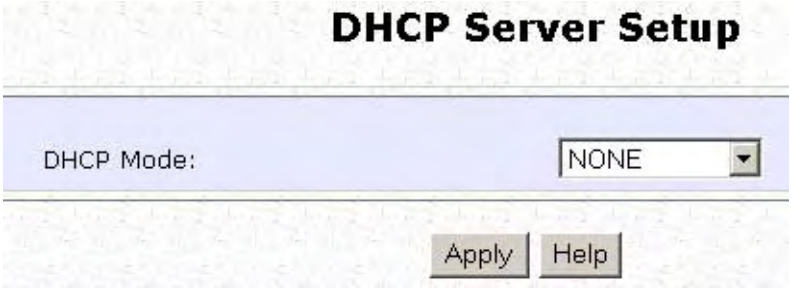
Follow these steps if you do not wish to use DHCP.

Step 1:

Click on **Advanced Settings** from **Management Setup** from the **CONFIGURATION** menu.

Step 2:

Set **DHCP Mode** to **NONE**.



Step 3:

Click on the **Apply** button.

The following will guide you to setup the DHCP Server.

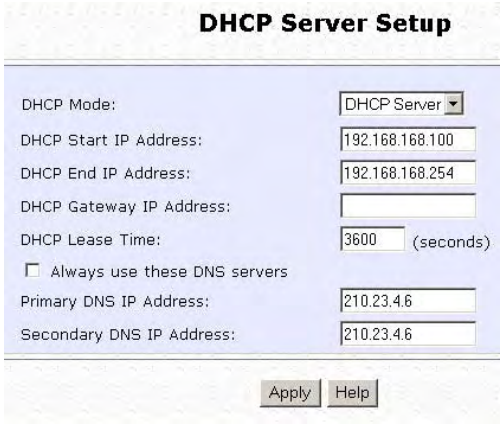
Step 1:

Click on **Advanced Settings** from **Management Setup** from the **CONFIGURATION** menu.

Step 2:

Set **DHCP Mode** to **DHCP Server**.

In **DHCP Server Setup**, refer to the table below to set the appropriate values to suit the needs of your network.



Step 3:

Click on the **Apply** button.

This table describes the parameters that can be modified in **DHCP Server Setup**.

Parameters	Description
The fields DHCP Start IP Address and DHCP End IP Address fields 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 and should belong to the same subnet as the router. For example if the router IP address is 192.168.168.1 and the network mask is 192.168.168.1 and 255.255.255.0, the DHCP Start IP Address should be 192.168.168.X, where X can be any number 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 and should also belong to the same subnet as your router. For example if the router IP address is 192.168.168.1 and the network mask is 192.168.168.1 and 255.255.255.0, the DHCP End IP Address should be 192.168.168.X, where X can be any number from 2 to 254. It is pre-set as *192.168.168.254*.
DHCP Gateway IP Address	Though the DHCP server usually also acts as the Default Gateway of the DHCP client, the router allows you to define a different Gateway IP Address which will be allocated as the Default Gateway IP of the DHCP client. The DHCP client will thus receive its dynamic IP address from the router but will access to the Internet or the other LAN through the Default Gateway defined by the DHCP Gateway IP Address. For instance if the unit in Access Point Client mode connects to an Internet gateway X, a PC wired to the unit will be unable to obtain a dynamic IP address directly from X. But if you enable the DHCP server of the unit and set the IP address of X as the DHCP Gateway IP Address, the PC will obtain its IP address from the unit and access the Internet through X.

DHCP Lease Time	This is the length of time that the client may use the assigned address before having to check with the DHCP server to see if the Address is still valid.

Always use these DNS servers	Enable this checkbox if you only want to use the DNS server(s) you have specified.
Primary DNS IP Address	Your ISP usually provides the IP address of the DNS server.
Secondary DNS IP Address	This optional setting is the IP address of a secondary DNS server.

The following will guide you to setup the DHCP Relay.

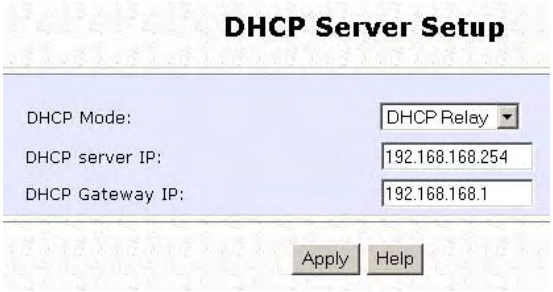
Step 1:

Click on **Advanced Settings** from **Management Setup** from the **CONFIGURATION** menu.

Step 2:

Set **DHCP Mode** to **DHCP Relay**.

In **DHCP Server Setup**, refer to the table below to set the appropriate values to suit the needs of your network.



Step 3:

Click on the **Apply** button.

This table describes the parameters that can be modified in **DHCP Server Setup**.

Parameters	Description
DHCP Server IP	This is the IP address of the DHCP server.
DHCP Gateway IP	Though the DHCP server usually also acts as the Default Gateway of the DHCP client, the router allows you to define a different Gateway IP Address which will be allocated as the Default Gateway IP of the DHCP client. The DHCP client will thus receive its dynamic IP address from the router but will access to the Internet or the other LAN through the Default Gateway defined by the DHCP Gateway IP Address. For instance if the unit in Access Point Client mode connects to an Internet gateway X, a PC wired to the unit will be unable to obtain a dynamic IP address directly from X. But if you enable the DHCP server of the unit and set the IP address of X as the DHCP Gateway IP Address, the PC will obtain its IP address from the unit and access the Internet through X.

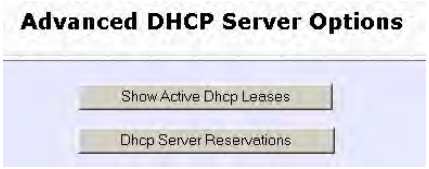
View Active DHCP Leases

Step 1:

Select **Management Setup** from the **CONFIGURATION** menu.

Step 2:

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



The **DHCP Active Leases** table displays:

- The **Host Name** of the DHCP client.
- The **IP Address** allocated to the DHCP client.
- The **Hardware (MAC) Address** of the DHCP client.
- The **Lease Expired Time.**

NOTE

Invalid date and time displayed in the **Lease Expired Time** column indicates that the clock of the router has not been set properly.

Reserve IP Addresses for Predetermined DHCP Clients

A reserved IP address is excluded from the pool of free IP addresses the DHCP server draws on for dynamic IP address allocation.
For instance if you set up a publicly accessible FTP or HTTP server within your private LAN, while that server requires a fixed IP address you would still want the DHCP server to dynamically allocate IP addresses to the rest of the PCs on the LAN.

Step 1:

From the **Advanced DHCP Server** Options section click on the **DHCP Server Reservations** button.

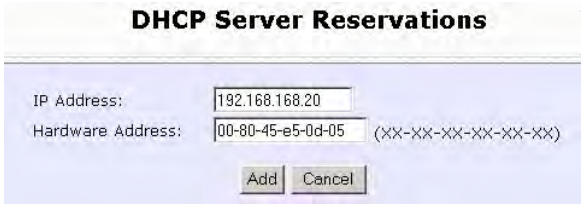
Step 2:

Click on the **Add** button.

Step 3:

Fill in:
The **IP Address** to be reserved.
The **Hardware Address**, in pairs of two hexadecimal values.

Press the **Apply** button to effect your new entry.



The **DHCP Server Reservations** page refreshes to display the currently reserved IP addresses.

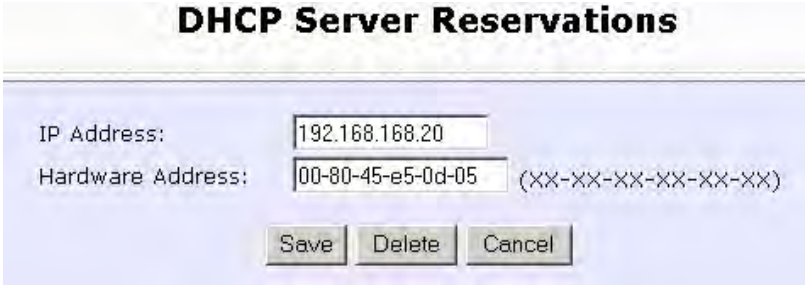
Delete DHCP Server Reservation

Step 1:

Select the reserved IP address to delete.

Step 2:

Click on the **Delete** button.



The **DHCP Server Reservations** table refreshes to display your changes.

View Statistics

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

1

1. Click on **WLAN Setup** from the **CONFIGURATION** menu.

2. Select **Statistics**.

2

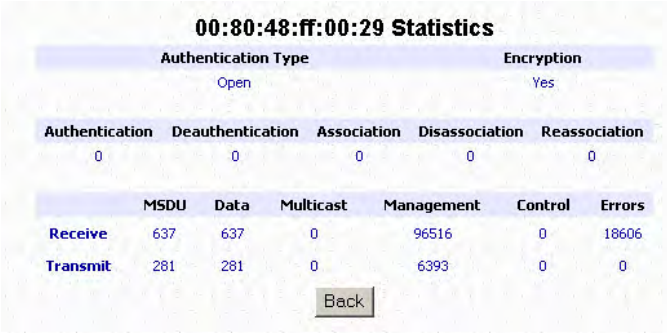
1. Select the WLAN connection to view statistics of.

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

3

The WLAN connection's statistics displays.

Click Back to return to WLAN Basic Setup page.



Set Virtual AP

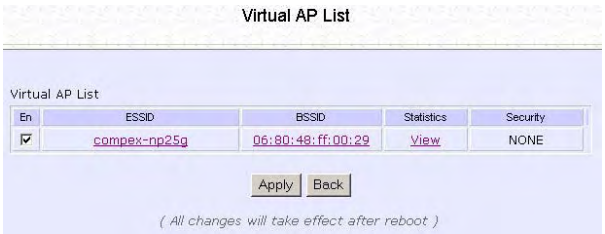
In Virtual AP a single wireless card can setup 2 virtual AP connections with different SSIDs or BSSID (Basic Service Set Identifier) and security modes.

Virtual AP delivers multiple services by network segmentation: making the network think there are many SSIDs available and channeling each connection through different segments to the respective virtual network segments on the Ethernet network.
Follow these steps to setup Virtual AP.

Virtual AP

1

Click on **WLAN Setup** from the **CONFIGURATION** menu.
Select **Virtual AP**.

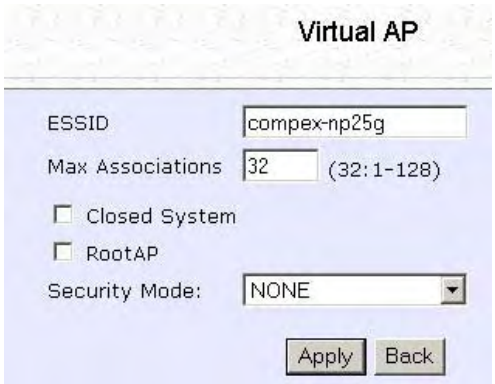


2

Virtual AP List page displays.

- Click Apply to register changes.
- Click Back to return to WLAN Basic Setup page.

Click on the link of the Virtual AP to go to the Virtual AP page.



3

1. Enter ESSID name.
2. Settings:
   - Max Associations
   - Closed System
   - RootAP
3. Select Security Mode
4. Click Apply to make changes or click Back to return to Virtual AP List

Setup WAN

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

i. ***Cable Internet where your ISP dynamically assigns a WAN IP address***

ii. ***Cable Internet where your ISP provides you with a fixed WAN IP address*** (or a range of fixed IP addresses)

iii. ***ADSL Internet that requires standard PPP over Ethernet (PPPoE)*** for authentication

iv. ***ADSL Internet that requires standard Point-to-Point Tunneling Protocol (PPTP)*** for authentication.

v. **ADSL Internet that requires standard Layer 2 Tunneling Protocol (L2TP)** for authentication. L2TP is an extension to the PPP protocol that enables ISPs to operate VPNs. It is the best combination of PPTP (from Microsoft) and L2F (from Cisco Systems). It has the most similar parameters of the PPTP except that it does not support the DHCP server.

Setup WAN for Cable Internet with Dynamic IP Assignment

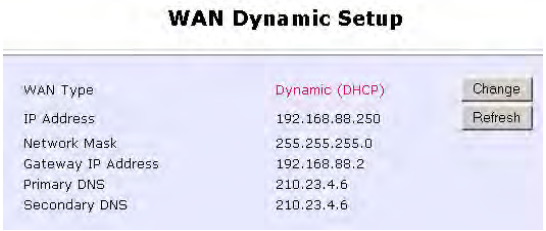
The router is pre-configured to support a WAN type that dynamically obtains an IP address from the ISP. However, you may verify the WAN settings with the following steps:

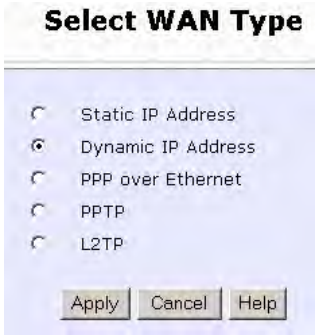
1. Under the **CONFIGURATION** on the command menu, click on **WAN Setup**.

2. On the **WAN Dynamic Setup** screen that follows, verify that the **WAN Type** reads **Dynamic (DHCP)** in red colour. Otherwise, click on the **Change** button.

3. Simply select **Dynamic IP Address** and hit the **Apply** button.

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





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

b. Certain ISPs log the MAC address of the first device used to connect to the broadband channel and will not release a WAN IP address unless the MAC address matches the one in their log. Therefore, if yours is not a new Cable Internet subscription (i.e. your PC was formerly connected directly to your cable modem); refer to **steps 5 - 7** to clone the "approved" MAC address onto the router.

c. Certain ISPs require authentication through a DHCP Client ID before releasing a public IP address to you. The router uses the System Name in the System Identity as the DHCP Client ID.

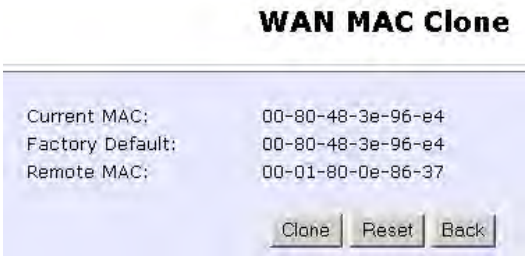
   Therefore, if this is the case, refer to your ISP for the correct DHCP Client ID to be set and follow **steps 8 - 10** to accomplish the setup.

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

   In the **WAN Setup** found under the **CONFIGURATION** command menu, click **MAC Clone** to continue.

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

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



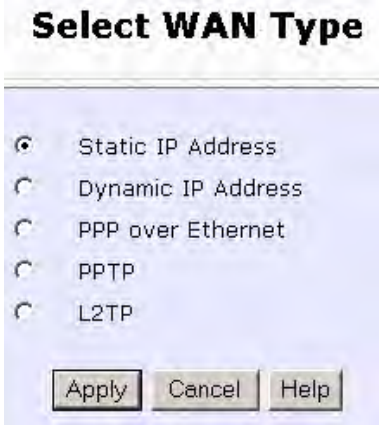
Take note: (If required, you may reset the router's MAC address to its factory default by clicking **Reset** on that same page)

Setup WAN for Cable Internet with Static IP Assignment

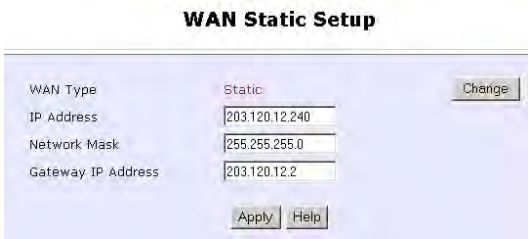
If you have an ISP that leases a static WAN IP for your subscription, you will need to configure your router's WAN type accordingly. For example, if the ISP provided you with the following setup information, you can set up your WAN as described below:

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

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



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

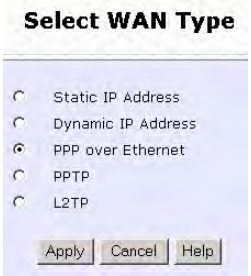


3. Fill in the information provided by your ISP in the **IP Address**, **Network Mask** and **Gateway IP Address** fields, before clicking the **Apply** button.

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

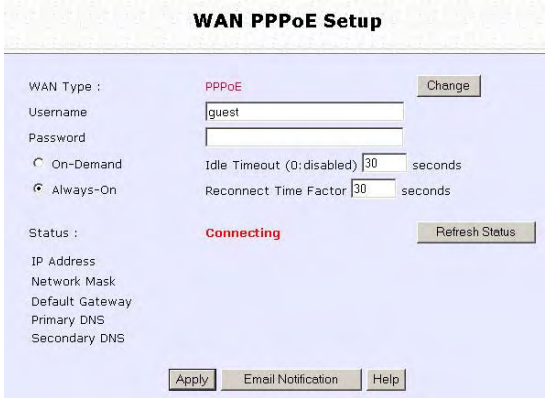
Setup WAN for ADSL Internet Using PPPoE

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



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

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



3. For **Username**, key in your ISP assigned account name (e.g. guest for this example), followed by your account **Password**.

4. Select **Always-On** if you want your router to always maintain a connection with the ISP. Otherwise, you may select **On-Demand**. The router will then connect to the ISP automatically when it receives Internet requests from the PCs in your network.

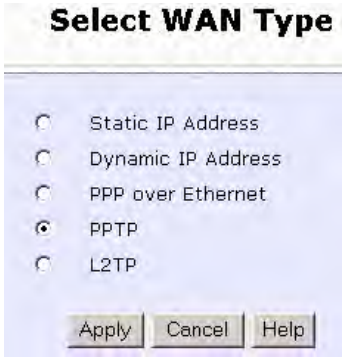
The **Idle Timeout** setting is associated with the **On-Demand** option, allowing you to specify the value (in seconds) after which the router will disconnect from the ISP after the last Internet activity. A value of "0" will disable idle timeout. **Reconnect Time Factor** is associated with the **Always-on**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

Setup WAN for ADSL Internet using PPTP

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

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

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



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

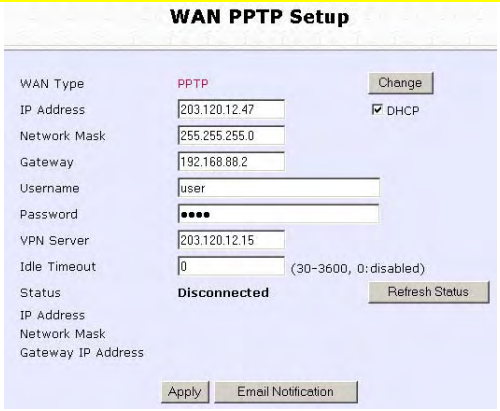
3. Fill in the information, followed by clicking the **Apply** button.

- Select whether to enable DHCP.
- Enter in the client **IP Address**.
- Enter in the **Network Mask**.
- Enter in the **Gateway**.
- Enter in the **Username** of your Internet account.
- Enter in the **Password** of your Internet account.
- Enter the IP address of your **VPN Server**.
- Enter an **Idle Timeout** value between 30-3600 seconds. Entering **0** will disable this feature.

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

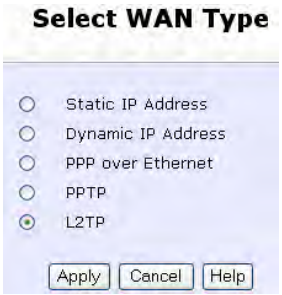
- The **Status** section gives you a summary of your connection settings such as: IP Address, Network mask, and gateway IP Address.
- If you are online, clicking **Disconnect** will disconnect your connection.

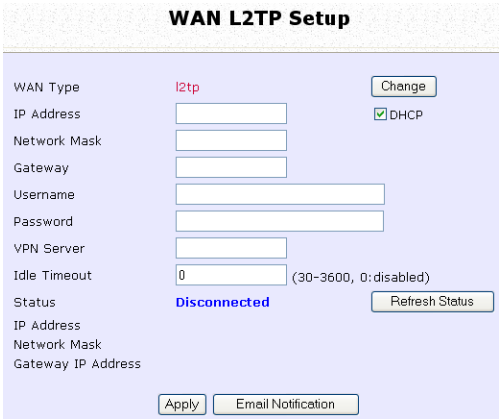
4. Please remember to click **Reboot Router** under **SYSTEM TOOLS** and hit the **Reboot** button to let the settings take effect.



Setup WAN for ADSL Internet using L2TP

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





1

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

2

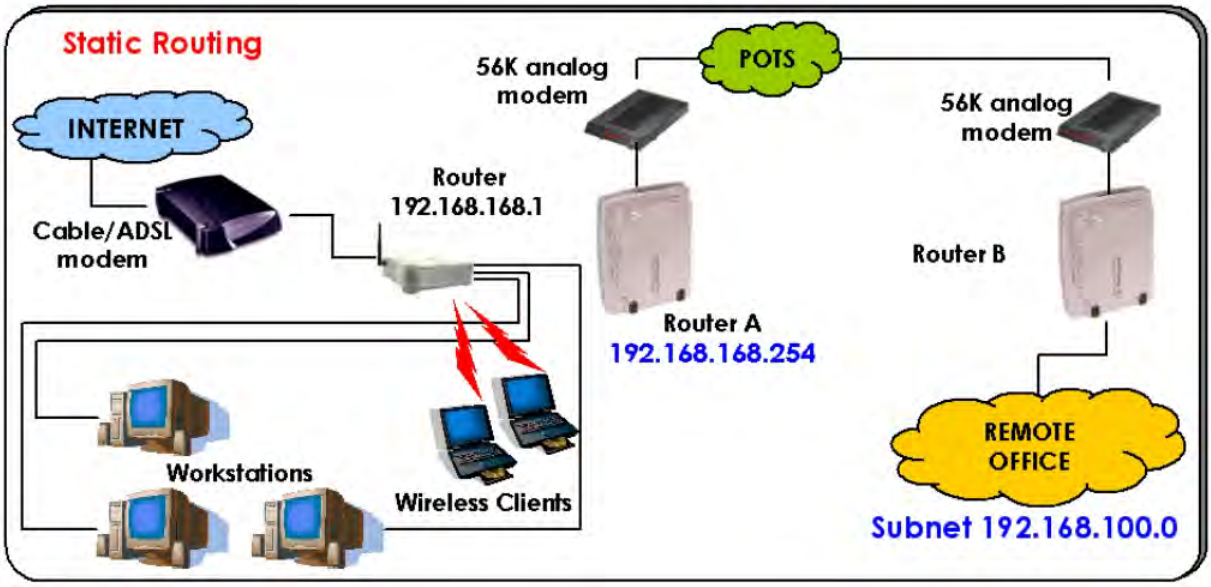
At the WAN L2TP Setup page:

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

Configure Static Routing

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

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

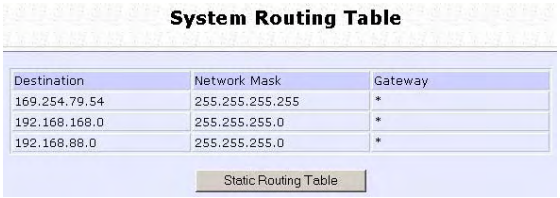


In this network, the main office of subnet 192.168.168.0 contains two routers: the office is connected to the Internet via the router (192.168.168.1) and to the remote office via Router A (192.168.168.254). The remote office resides on a subnet 192.168.100.0.

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

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

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

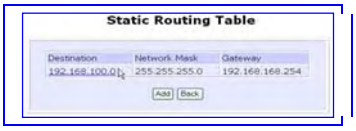


2. Click on the **Static Routing Table** button above.

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

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.

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



Configure NAT

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

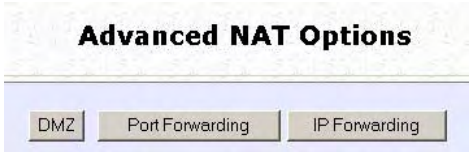
Due to NAT, computers in the private LAN behind the router will not be directly accessible from the Internet. However, employing virtual Servers lets you host Internet servers behind the NAT by way of IP/Port Forwarding as well as De-Militarized Zone hosting.

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

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

Configure Virtual Server Based on DMZ Host

When NAT is enabled, an Internet request from a client within the private network first goes to the router. Upon receiving a request, the router keeps track of which client is using which port number. Since any reply from Internet goes to the router first, the router (from the port number in the reply packet) knows to which client to forward the reply. If the router does not recognize the port number, it will discard the reply. When using DMZ on a PC, any reply not recognized by the router will be forwarded to the DMZ-enabled PC instead.
You may wish to set up a DMZ host if you intend to use a special-purpose Internet Service such as an online game for which no port range information is available. You can also host Web pages or public information that can be served to the outside world, on the DMZ host.



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

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

2. On **NAT DMZ IP Address** page, you have to define the **Private IP Address** of the DMZ host. In this example, show private IP address for the PC placed within the DMZ is 192.168.168.55

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

3. Remember to click **Apply** button.
4.

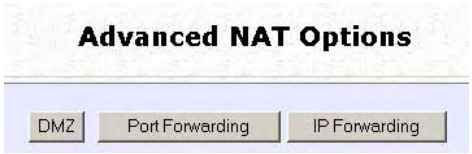
NOTE:
When you enable DMZ, the Static IP Address configuration is recommended for the DMZ host. Otherwise, if the address is allocated by DHCP, it may change and DMZ will not function properly.

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.

Configure Virtual Servers Based on Port Forwarding

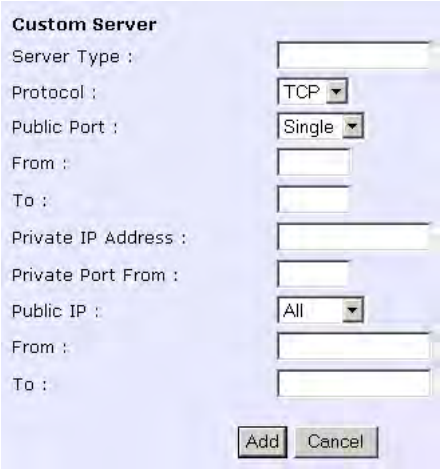
Virtual Server based on Port Forwarding is implemented to forward Internet requests arriving at the router's WAN interface, based on their TCP ports, to specific PCs in the private network.

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



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

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



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

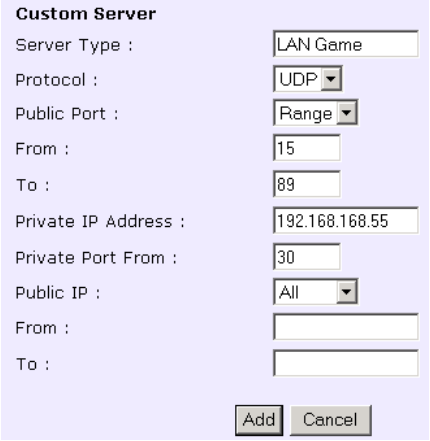
5.

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

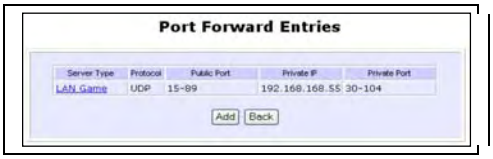
1. Enter the **Private IP Address**.
2. Pick the appropriate **Server Type**.
3. Enter the range in the **From:** and **To:** fields.
4. Click **Add**.

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

1. Enter the **Private IP Address**.
2. Define the **Port** numbers to use.
3. Select the relevant **Protocol** from the drop down list.
4. Identify the **Server Type**.
5. Enter the in the **From:** and **To:** fields.
6. Click on **Add**.



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



6.

NAT Static Port Based Entries reflects the new entry.

To assign more servers in your LAN:

1. Click **Add**.

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

2. Repeat Step 3 above.

To delete table entries:

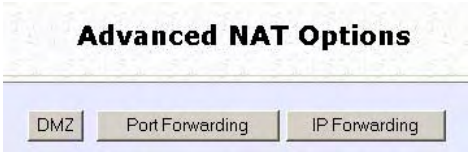
1. Select the entry to delete.

2. Click **Delete**.

   The table will refresh.

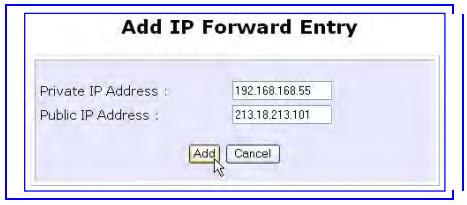
Configure Virtual Server Based on IP Forwarding

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

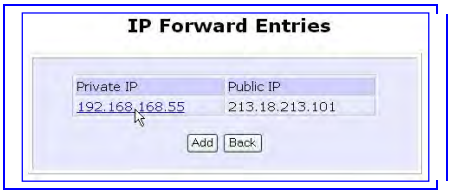


1. Under the **CONFIGURATION** command menu, click on **NAT**. You will find the **Advanced NAT Options** available near the bottom of the page.

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.



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

Please ensure that you have subscribed to the Public IP Address you intend to forward from.

Configure Bandwidth Control for WAN

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

Follow these steps to setup Bandwidth Control for WAN.

1

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

2

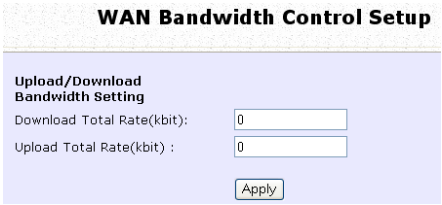
Select whether to Enable or Disable Bandwidth Control and click Apply.

3

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

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

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



Configure Bandwidth Control for LAN

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

Follow these steps to setup Bandwidth Control for LAN.

1

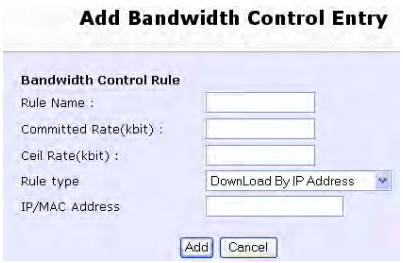
Click **Bandwidth Control** from the **CONFIGURATION** menu.

2

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

3

Click Add to add a Bandwidth Control Entry



3

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

Rule Types:

- Download by IP Address
- Download by MAC Address
- Upload by IP Address
- Upload by MAC Address

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

Use 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.

1. Under the **CONFIGURATION** command menu, click on **Remote Management**, and you will be brought to the following screen.

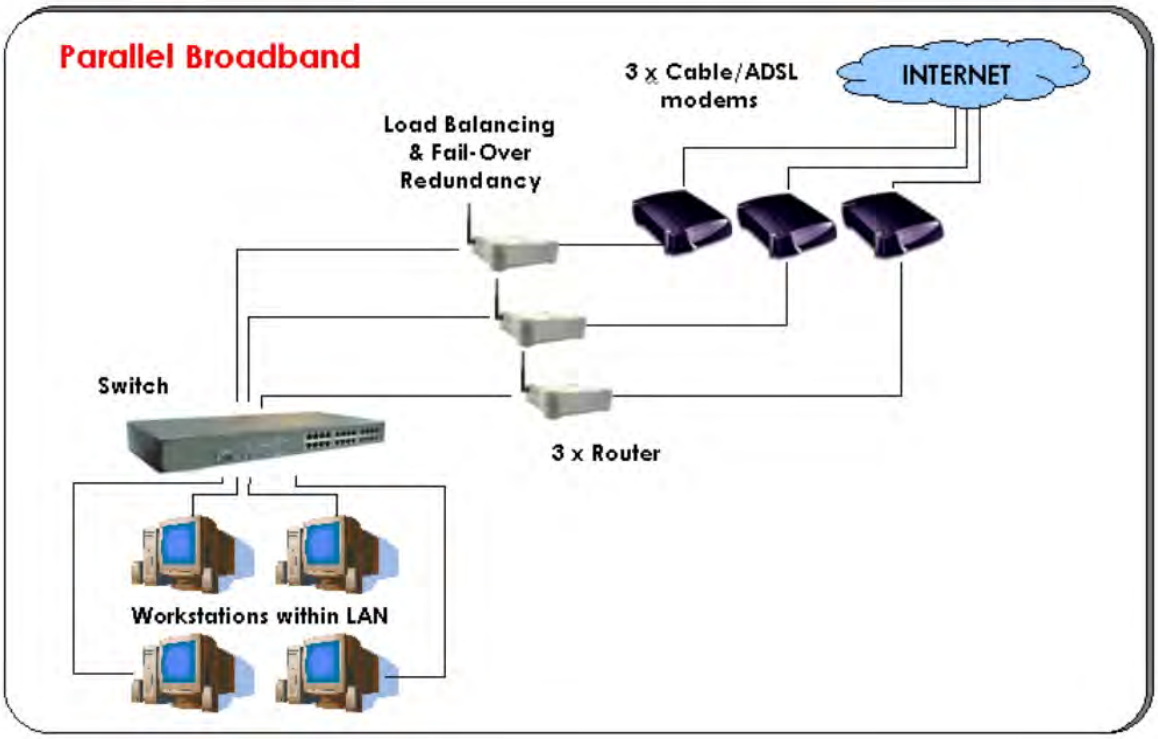
2. By default, **Remote Management** is disabled. (To disable Remote Management, just enter 0 for **Remote Http Port**).

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

Use Parallel Broadband

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

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



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

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

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

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

1. Under the **CONFIGURATION** command menu, click on **Parallel Broadband**.

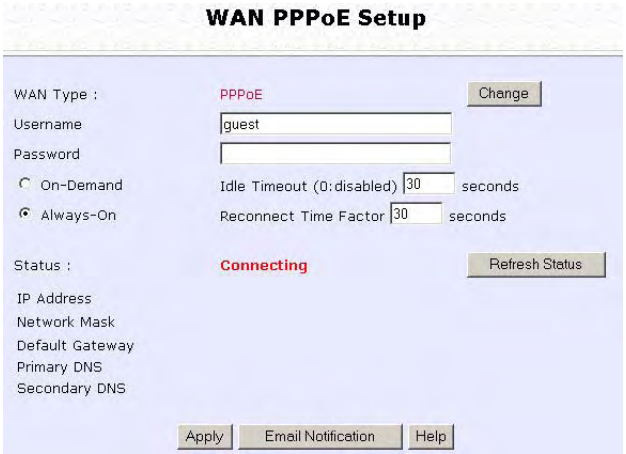
2. Next simply select **Enable** and click the **Apply** button to make the changes effective.

3. Repeat this for the other routers in your network and they will communicate with each other and assign each new user to the router that has the smallest load, so that there is approximately the same number of users on each router.

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

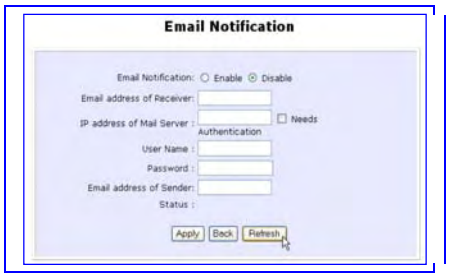
Configure Email Notification

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



1. Under the **CONFIGURATION** command menu, click on **WAN Setup**, and you will be brought to the following screen.

2. Click on the **Email Notification** button.



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

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

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

   User Name:

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

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

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

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

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

Use Static Address Translation

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

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

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

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

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

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

Note: For SAT to function properly:
The IP address of the notebook should belong to a different subnet from the LAN IP address of the router.
The <Default Gateway> in the TCP/IP settings of your notebook should NOT be left blank.

Use DNS Redirection

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

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

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

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

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

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

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

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

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.

Setup DDNS

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

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

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

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

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

Enable DDNS

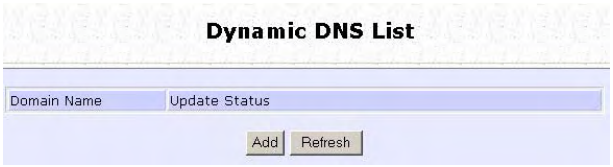
1. Under the **HOME USER FEATURES** command menu, click on **Dynamic DNS Setup**.

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

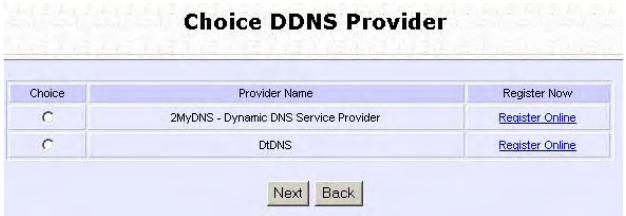
DDNS List

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

2. If you have already created a list earlier, click on the **Refresh** button to update the list.



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



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

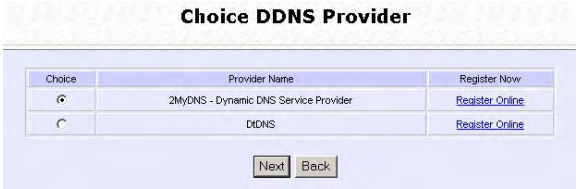
Provider Name :
This is the name of your preferred DDNS provider.

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

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

Select 2MyDNS as DDNS Service Provider

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

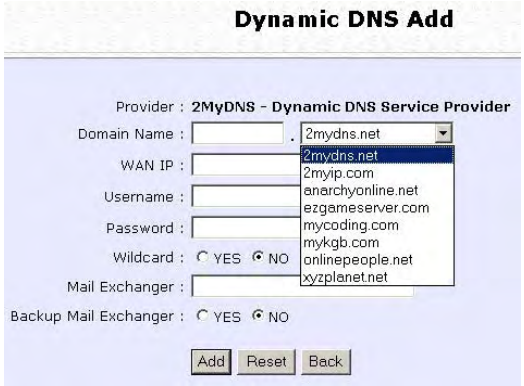


   Enter your **Domain Name**.

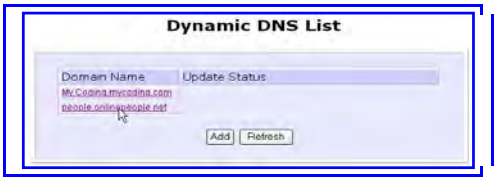
   Select **Auto Detect** to let the DDNS server learn your current WAN IP address. Enter your DDNS account **Username** and **Password**.

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

2. (Optional) In the Mail Exchanger field, enter the Static WAN IP address of the mail server configured to handle email for your domain. Select **Backup Mail Exchanger** to enable this service. Click on the Add button to save the new addition.



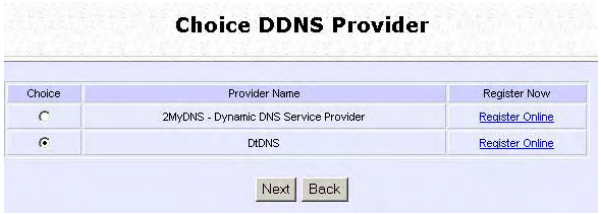
3. The new domain is added to the Dynamic DNS list table.



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

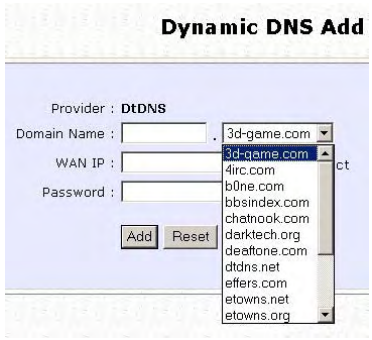
Select DtDNS as DDNS Service Provider

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.



Enter your **Domain Name**.

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



2. Then click on the Add button.

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

Configure UPnP

The following are issues that can arise when using NAT:

- Some network applications assume the IP address and port that the client has been assigned are global routable values that can be used on the Internet directly. Often, this is not the case as the client has been assigned a private IP address that can only be used on the LAN.

- Other network applications send requests using a socket on a port “A” and expect to receive the reply from a different listening socket on port “Z”. When the NAT router creates a port mapping for port “A”, it won't know that it has to match it with the reply packets addressed to port “Z”.

- A number of network protocols assume they will always be able to use certain globally routable well-known ports. However there are several clients in the LAN and at any given time, only one client can be allowed to use a specific well-known port. In the meantime, the other clients will not be able to run any web service requiring the same well-known port.

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

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

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

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

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

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

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

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

Configure Security

Configure 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.

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

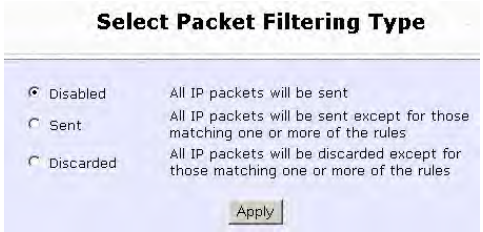
Example: **Packet Filtering Type** set to Disabled.

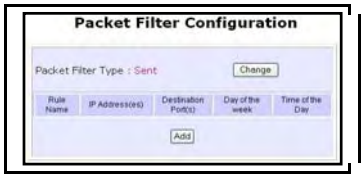
2. You must first choose the **Packet Filter Type** by clicking on the **Change** button.
   Default **Packet Filter Type** is Disabled.

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

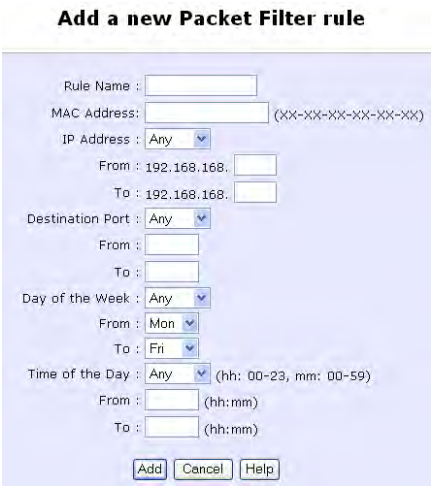
Example: **Packet Filtering Type** set to Discarded.

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



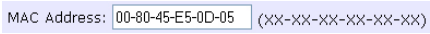


4. Click on the **Add** button and you will be able to define the details of your **Packet Filter Rule** from the screen on the right.



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

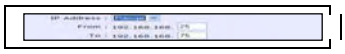
4b). Enter **MAC Address** for this new packet filtering rule.



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

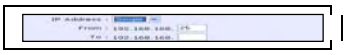
- A **Range** of IP addresses

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



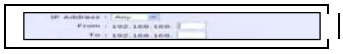
- A **Single** IP address

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



- **Any** IP address

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

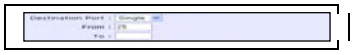


4d). At the **Destination Port** drop down list, select either:

- A **Range** of TCP ports

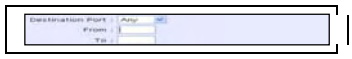
In this case, you will have to

define **(From)** which port **(To)** which port, your rule applies.



- A **Single** TCP port

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



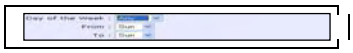
- **Any** IP port

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

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

- A **Range** of days

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



- **Any** day

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

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

- A **Range** of time

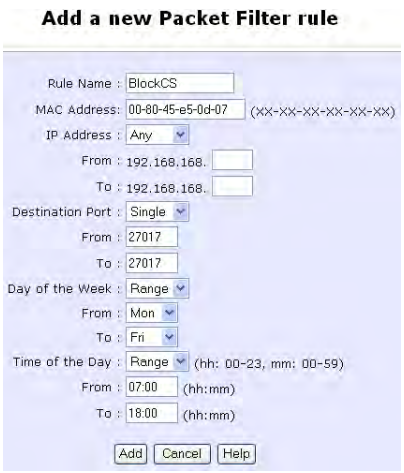
In which case, you have to specify the time in the format **HH:MM**, where **HH** may take any value from 00 to 23 and **MM**, any value from 00 to 59.

- **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.



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

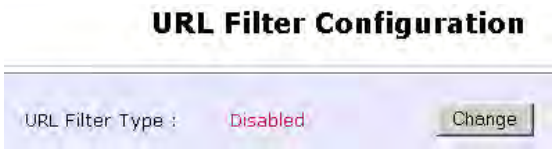
   Therefore, for a rule we name BlockCS, and add the entries depicted on the left. Clicking on the **Add** button will make your packet filter rule effective.

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

Configure URL Filtering

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

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



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

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

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

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

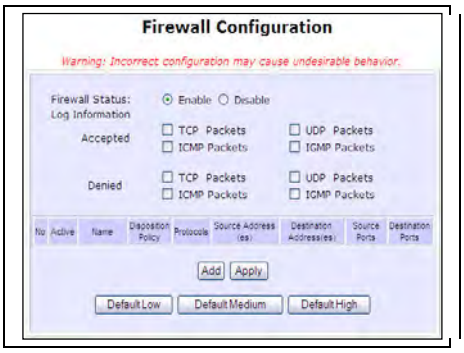
Configure Firewall

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

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

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

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

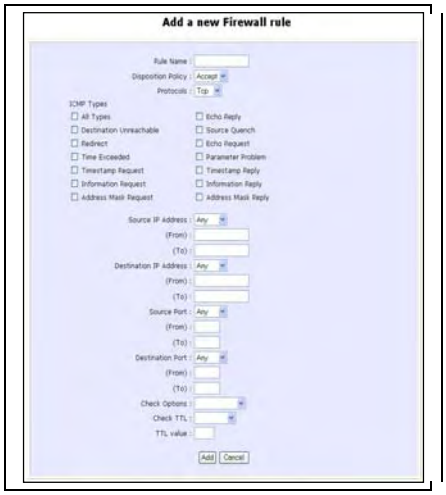


2. First, enable the firewall. You can choose among the **Default Low**, **Default Medium** or **Default High** security options for convenient setup.

3. Then you may choose the type of network activity information you wish to log for reference. Data activity arising from different types of protocol can be recorded.

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

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



Rule Name : Enter a unique name to identify this firewall rule.

Disposition Policy : This parameter determines whether the packets obeying the rule should be accepted or denied by the firewall. Choose between Accept and Deny.

Protocols : Users are allowed to select the type of data packet from: TCP, UDP, ICMP, IGMP or ALL.

Note: If users select either ICMP or IGMP, they are required to make further selection in the ICMP Types or IGMP Types respectively.

ICMP Types : This IP protocol is used to report errors in IP packet routing. ICMP serves as a form of flow control, although ICMP messages are neither guaranteed to be received or transmitted.

ICMP Packet Type	Description
Echo request	Determines whether an IP node (a host or a router) is available on the network.
Echo reply	Replies to an ICMP echo request.
Destination unreachabl e	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

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

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

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

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

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

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

Check Options : This parameter refers to the options in the packet header. The available selection options are abbreviated as follows:

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

Check TTL : This parameter would let you screen packets according

to their Time-To-Live (TTL) value available options are:

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

View Firewall Logs

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

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

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

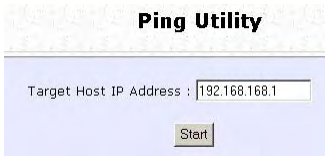
Administer the System

Use the SYSTEM TOOLS Menu

Use the Ping Utility

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

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



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

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

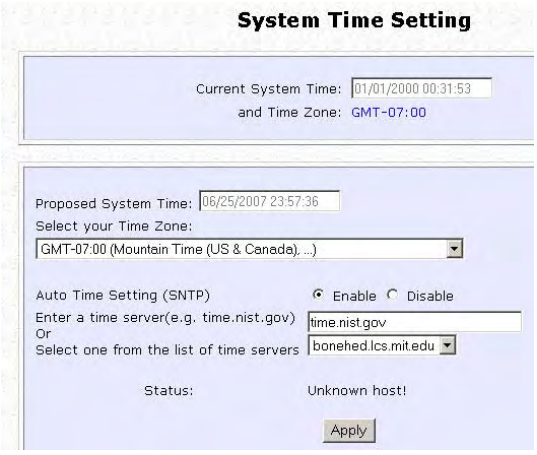
4. The Ping messages will be displayed.

Set the Time

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

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.



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.

Upgrade the Firmware

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

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

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

3. Click on the **Browse** button to search your hard drive for the new firmware file.

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

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

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

Settings Profile

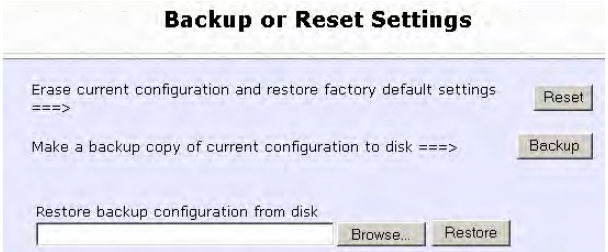
A useful feature is built into the router allowing you to save configuration profiles, especially the painstakingly crafted firewall security rules, and the intricate IP and Port settings of your Virtual Servers that effect a host of network applications.

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

1. From the **SYSTEMS TOOLS** command menu, click on the **Save or Reset Settings** option to arrive at the following screen below.

2. Press the **Reset** button to return the router to factory default (Note that this will discard the entire configuration you have done).

3. Press the **Backup** button if you wish to save the configuration profile as a file on your PC's hard disk drive.



4. If you wish to return the router to an earlier saved file from the hard disk drive, click **Browse** to search for the filename and click on **Restore**.

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

Reboot the System

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

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

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

Change Your Login Password

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

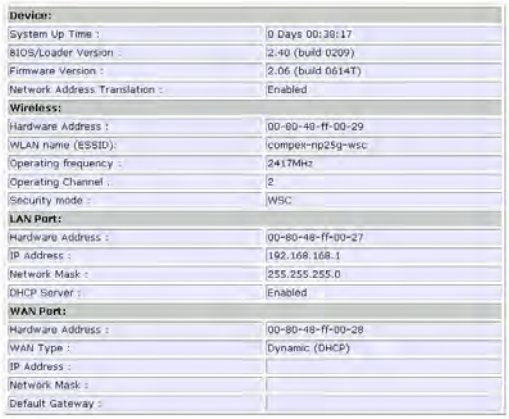
1. Select **Change Password** under the **SYSTEM TOOLS** command menu.

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

View System Information

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

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



Device:	
System Up Time :	0 Days 00:38:17
BIOS/Loader Version :	2.40 (build 0209)
Firmware Version :	2.06 (build 0614T)
Network Address Translation :	Enabled
Wireless:	
Hardware Address :	00-80-48-ff-00-29
WLAN name (ESSID):	compex-np25g-wsc
Operating frequency :	2417MHz
Operating Channel :	2
Security mode :	WSC
LAN Port:	
Hardware Address :	00-80-48-ff-00-27
IP Address :	192.168.168.1
Network Mask :	255.255.255.0
DHCP Server :	Enabled
WAN Port:	
Hardware Address :	00-80-48-ff-00-28
WAN Type :	Dynamic (DHCP)
IP Address :	
Network Mask :	
Default Gateway :	

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

Appendix: Learn About Commonly Used Terms

10Base-T	An IEEE Ethernet standard for 10Mbps data transmission using unshielded twisted pair wires
100Base-Tx	An IEEE Ethernet standard for 100Mbps data transmission using two pairs of Category 5 UTP wire
802.11b	An IEEE standard for wireless networking standard specifying a maximum data transmission rate of 11Mbps using DSSS modulation and an operating frequency of 2.4GHz.
802.11g	An IEEE standard for wireless networking standard that 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, eg. Internet Explorer, Netscape Navigator.
CAT 5	It is a standard developed by the Electronics Industries Association that specifies network cabling which consists of twisted pairs of copper wire with a sustainable data rate of 100Mbps.
Database	A database is a collection of information that is organized so that the contents may be easily accessed/managed.
Data Packet	In an IP network, the smallest chunk of data is called a packet (packet sizes can vary).
DHCP	Dynamic Host Configuration Protocol. It is a protocol that allows the network administrator to centrally manage and assign IP addresses to devices in the network.
DMZ	De-Militarized Zone hosting allows the administrator to expose a private IP address onto the Internet. It is used for a PC/Server assigned with a Static IP address that has to run specialized applications requiring multiple TCP/IP ports to be opened.
DNS	Domain Name System is transparent to the user and translates Internet domain names to IP addresses, so that the user only needs to remember meaningful and easy-to-remember names rather than arcane IP addresses.

Driver	A piece of software developed to interface a piece of hardware with its immediate upper-layer software (i.e. operating system) so that it can be recognized and operated.
DSSS	Direct Sequence Spread Spectrum is a modulation scheme employed by the 802.11b standard that uses a chipping code (redundant bit) during its transmission to reject interference.
Dynamic IP Address	It is an IP address that is dynamically allocated or assigned to a client device within a TCP/IP network, typically by a DHCP server.
Encryption	Encryption is a security method applying specific algorithms to make sure that all the data from one computer is encoded into a form that only the intended party will be able to decode to view the information.
Ethernet	An IEEE standard network protocol that specifies how data is transmitted over a common medium. It uses CSMA/CD, which stands for Carrier Sense Multiple Access with Collision Detection. It has a defined data rate of 10Mbps.
Fast Ethernet	An IEEE standard extended from 10Base-T Ethernet to support 100Mbps data rate.
Firewall	It is a software layer that controls network access from within and without so that undesired activity by malicious or snooping parties may be prevented.
Firmware	It is a software code written and saved within the read-only memory (ROM) of the device so that it is retained even when the device is powered off.
FTP	File Transfer Protocol. It is a protocol designed to transfer files over a TCP/IP network.
Full Duplex	It defines the ability of a device to transmit data simultaneously in both upstream and downstream directions over a single line.
Half Duplex	It defines the ability of a device to transmit in one direction at a time over a single line.
HTTP	HyperText Transport Protocol is a common protocol used to connect servers on the World Wide Web, with its primary function being to establish a connection with a web server and transmit HTML pages to the client's browser.
ICMP	Internet Control Message Protocol is a message control and error reporting protocol between a host server and a router to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.
IGMP	Internet Group Management Protocol is the standard for IP multicasting on the Internet. It is used to establish host memberships in particular multicast groups on a single network. The mechanisms of the protocol allow a host to inform its local router, using Host

	Membership Reports that it wants to receive messages addressed to a specific multicast group. All hosts conforming to level 2 of the IP multicasting specification require IGMP.
IEEE	It is the Institute of Electrical and Electronic Engineers. The IEEE is a professional technical body promoting the development and application of technology.
IP Address	At the moment, IP address is a 32-bit binary digit that defines each sender or receiver of information across an IP network.
IPSec	Internet Protocol Security. It is a suite of protocols used to implement secure exchange of packets at the IP layer.
ISP	Internet Service Provider. It is a company that provides individuals or corporations with Internet access and other related services.
LAN	Local Area Network is a group of computers and devices sharing a common communication medium within a small geographical area.
Latency	Latency is a time-delay.
MAC Address	MAC is the abbreviation for Media Access Control. The MAC address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter or router that allows a network to identify the hardware. Unlike IP addresses, this number is permanent and is therefore a valuable identifier.
Mbps	Mega bits per second. It is a unit of measurement for data transmission indicating a million bits per second.
MDI	Medium Dependent Interface. On a network hub/switch, a MDI port (uplink port) connects to another hub/switch using a straight cable. To connect a MDI port to a computer, a crossover cable is used.
MDI-X	Medium Dependent Interface Crossed. On a network hub/switch, a MDI-X port connects to a computer using a straight cable. To connect a MDI-X port to another hub/switch, use a crossover cable.
Multicast	A multicast is a packet that is sent to a subset of end stations in a LAN, or VLAN that belong to a *multicast group*. If the network is set up correctly, a multicast can only be sent to an end station if it has joined the relevant group.
NAT	Network Address Translations multiplexes multiple private IP addresses on the LAN to a single public IP address on the Internet.
OFDM	Orthogonal Frequency Division Multiplexing. It is a modulation scheme employed by the IEEE 802.11g standard, which combines numerous signals of different frequencies to form a single signal for transmission over a medium.
Packet Filtering	This is a means of discarding unwanted network traffic based on its originating addresses or the type of data transmitted.
Ping	Packet Internet Groper is a utility used to determine whether a

	particular network device (IP address) is available online. It works by sending out a packet to the device and waiting for its response.
PPPoE	Point-to-Point Protocol over Ethernet is a method for the encapsulation of PPP packets over Ethernet frames.
PPTP	PPTP stands for Point-to-Point Tunneling Protocol. It is a protocol that allows authorized users to extend their own networks through private "tunnels" over the ISP or online service. This kind of interconnection is known as VPN (Virtual Private Network)
RJ-45	A connector used for Ethernet devices that holds up to eight wires.
Router	A router is a device that interconnects networks.
Subnet Mask	Subnet masking is a method of splitting IP networks into subgroups.
TCP	Transmission Control Protocol enables two hosts to establish a connection and exchange streams of data, guaranteeing delivery of data and that packets will be delivered in the same order in which they were sent.
Throughput	It is the measurable amount of data moved from one place to another within a given time period.
UDP	User Datagram Protocol is a connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP provides a direct way to send and receive datagrams over an IP network and is used primarily for broadcasting messages over a network.
URL	Uniform Resource Locator is the address that defines the location of a file on the World Wide Web.
UTP	Unshielded Twisted Pair is the most common kind of copper wiring designed to reduce crosstalk between copper wires.
VPN	Virtual Private Network is a secure means to join remote networks using comprehensive authentication and encryption. They may be "virtually" joined even across a public network like the Internet by means of employing IPSec amongst others.
WAN	Wide Area Network. It is a communication network that extends over a large geographical area. For example, the Internet.
WEP	Wired Equivalent Privacy is a wireless data privacy encryption protocol based on a 64-bit or 128-bit shared key algorithm.
WLAN	Wireless Local Area Network is a group of computers and associated devices that communicate with each other wirelessly.
WPA-PSK	WPA-PSK is a special mode for home users without authentication server and yet provides the same strong encryption protection.

Appendix: View the 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) - L2TP
LAN/WLAN Interface	Wired: - Integrated 4x Auto MDI/MDI-X 10/100Mbps Switch Wireless: - Operating channels, frequency of: 11 Channels 2.412~2.462, US, Canada 13 Channels, 2.412~2.472, Europe 14 Channels 2.412~2.484, Japan - Direct Sequence Spread Spectrum modulation, Orthogonal Frequency Division Multiplexing modulation - Data rates: 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps, 6Mbps, 5.5Mbps, 2Mbps, 1Mbps - Security: WEP WPA-Personal

	WPA2-Personal WPA-Auto-Personal WSC
External Antenna Type	2dBi antenna
IP Addressing	All Classful/Classless subnets
Built-in DHCP Server	Yes
DHCP Reservation	Yes
NAT Firewall	Yes
Stateful Packet Inspection (SPI) Firewall	Yes
Load-Balancing/ Fail-Over Redundancy	Parallel Broadband
Virtual Server	IP and Port Forwarding, De-Militarized Zone hosting
IP Packet Filtering	Time-based, TCP Port, Source IP filtering
URL Filtering	Yes
IP Routing	Static Routing Entry
VPN Client Pass-Through	PPTP, IPSec
Multicast Filtering	Yes
Configuration Interface	Web-based Configuration Menu
Profile Backup and Restore	Yes
Firmware Upgradeable	Yes
Environment Requirement	Temperature: - Operating : 0ºC to 40ºC - Storage : -20ºC to 70ºC Humidity: - Operating : 10% to 80% RH - Storage : 5% to 90% RH
Physical Dimension	174mm x 104mm x 40mm (L x W x H)
Weight	~ 800 g (including power adapter)

Trademark Information

Compex® is a registered trademark 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 Daniel
Manual Number: U-0588-V1.2C Version 1.2 Nov 2007

Disclaimer

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

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.

Products that contain a radio transmitter are labelled with FCC ID and may also carry the FCC logo.

Caution: Exposure to Radio Frequency Radiation.

To comply with the FCC RF exposure compliance requirements, the following antenna installation and device operating configurations must be satisfied:

1. For configurations using the integral antenna, the separation distance between the antenna(s) and any person's body (including hands, wrists, feet and ankles) must be at least 2.5cm (1 inch).
2. For configurations using an approved external antenna, the separation distance between the antenna and any person's body (including hands, wrists, feet and ankles) must be at least 20cm (8 inch).

The transmitter shall not be collocated with other transmitters or antennas.

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

Declaration of Conformity

Compex, Inc. declares the following:
Product Name: Wireless-G Internet Router
Model No.: NP25G conforms to the following Product Standards:
The device complies with the Electromagnetic Compatibility Directive (89/336/EEC), Low Voltage Directive (73/23/EEC) and the Amendment Directive (93/68/EEC) issued by the Commission of the European Community. Compliance with these directives implies conformity to the following European Norms (in brackets are the equivalent international standards).
Electromagnetic Interference (Conduction and Radiation): EN 55022 (CISPR 22)
Electromagnetic Immunity: EN 55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11)
Low Voltage Directive: EN 60 950: 1992+A1: 1993+A2: 1993+A3: 1995+A4: 1996+A11: 1997.
EN 61000-3-2 (IEC610000-3-2) – **Power Line Harmonics**
EN 61000-3-3 (IEC610000-3-3) – **Product Safety**
Therefore, this product is in conformity with the following regional standards: **FCC Class B:** following the provisions of FCC Part 15 directive, **CE Mark:** following the provisions of the EC directive.

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

Compex, Inc. also declares that:
The wireless card in this product complies with the R&TTE Directive (1999/5/EC) issued by the Commission of the European Community. Compliance with this directive implies conformity to the following:
EMC Standards: FCC: Subpart B, Subpart C; CE: EN 300 328-2, EN 300 826 (EN 301 489-17)
Therefore, this product is in conformity with the following regional standards: **FCC Class B**: following the provisions of FCC Part 15 directive, **CE Mark:** following the provisions of the EC directive.

Firmware

This manual is written based on Firmware version 2

Technical Support Information

The warranty information and registration form are found in the Quick Install Guide.

For technical support, you may contact Compex or its subsidiaries. For your convenience, you may also seek technical assistance from the local distributor, or from the authorized dealer/reseller that you have purchased this product from. For technical support by email, write to support@compex.com.sg.

Refer to the table below for the nearest Technical Support Centres:

Technical Support Centres	
Contact the technical support centre that services your location.	
U.S.A., Canada, Latin America and South America	
✉ Write	Compex, Inc. 840 Columbia Street, Suite B Brea, CA 92821, USA
☎ Call 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

We value your feedback. If you have any suggestions on improving, we would like to hear from you.

Please contact us at:
Fax: (65) 62809947
Email: feedback@compex.com.sg

We hope this manual was helpful to you. For more Compex information, please visit us at www.Compex.com.sg

warning

Class B:

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT

This equipment 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 equipment 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 equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-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.

RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.