Table 33 Network > Wireless LAN > General: WPA/WPA2

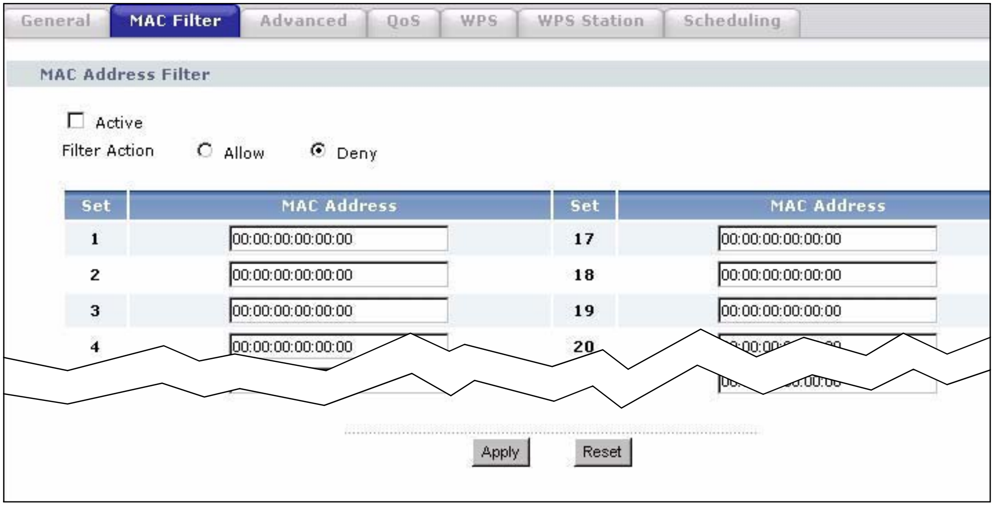
LABEL	DESCRIPTION
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK/ WPA2-PSK** key management) or RADIUS server (if using **WPA/WPA2** key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA-PSK/WPA2-PSK** mode. The NBG420N default is **1800** seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the NBG420N. The key must be the same on the external authentication server and your NBG420N. The key is not sent over the network.
Accounting Server	
Active	Select **Yes** from the drop down list box to enable user accounting through an external authentication server.
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the NBG420N. The key must be the same on the external accounting server and your NBG420N. The key is not sent over the network.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.6 MAC Filter

The MAC filter screen allows you to configure the NBG420N to give exclusive access to up to 32 devices (Allow) or exclude up to 32 devices from accessing the NBG420N (Deny). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your NBG420N’s MAC filter settings, click **Network** > **Wireless LAN** > **MAC Filter**. The screen appears as shown.

Figure 66 Network > Wireless LAN > MAC Filter



MAC Address Filter

□ Active

Filter Action ○ Allow ● Deny

Set	MAC Address	Set	MAC Address
1	00:00:00:00:00:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	[illegible]

The following table describes the labels in this menu.

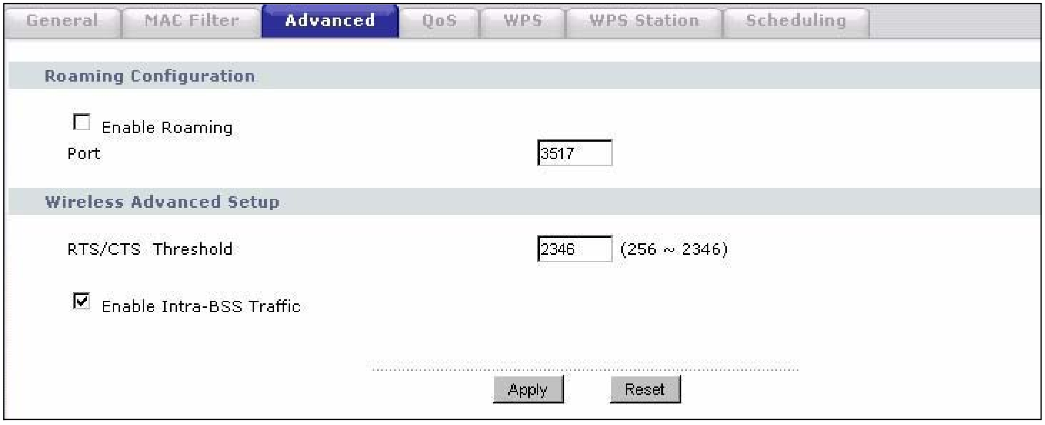
Table 34 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Active	Select **Yes** from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny** to block access to the NBG420N, MAC addresses not listed will be allowed to access the NBG420N Select **Allow** to permit access to the NBG420N, MAC addresses not listed will be denied access to the NBG420N.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the NBG420N in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.7 Wireless LAN Advanced Screen

Click **Network** > **Wireless LAN** > **Advanced**. The screen appears as shown.

Figure 67 Network > Wireless LAN > Advanced



Roaming Configuration

☐ Enable Roaming

Port 3517

Wireless Advanced Setup

RTS/CTS Threshold 2346 (256 ~ 2346)

☑ Enable Intra-BSS Traffic

The following table describes the labels in this screen.

Table 35 Network > Wireless LAN > Advanced

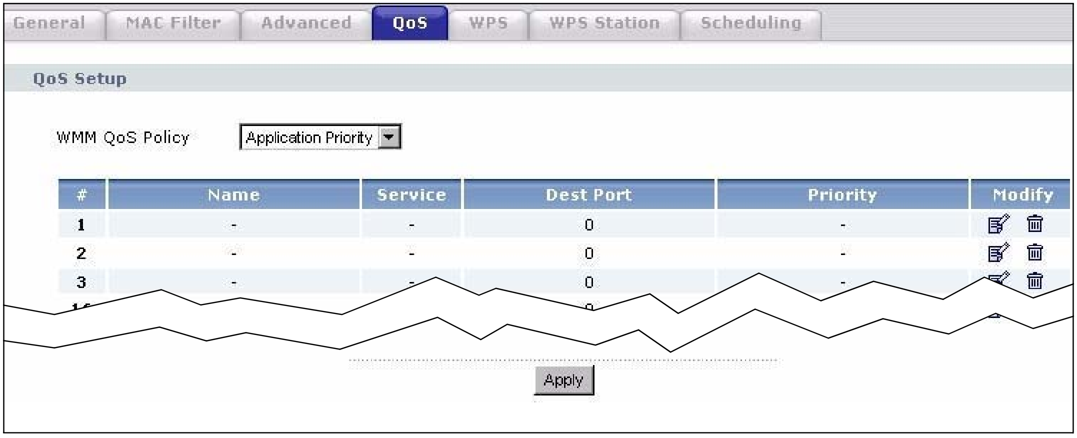
LABEL	DESCRIPTION
Roaming Configuration	
Enable Roaming	Select this option if your network environment has multiple APs and you want your wireless device to be able to access the network as you move between wireless networks.
Wireless Advanced Setup	
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2432.
Enable Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.8 Quality of Service (QoS) Screen

The QoS screen allows you to automatically give a service (such as e-mail, VoIP or FTP) a priority level.

Click **Network** > **Wireless LAN** > **QoS**. The following screen appears.

Figure 68 Network > Wireless LAN > QoS



QoS Setup

WMM QoS Policy: Application Priority

#	Name	Service	Dest Port	Priority	Modify
1	-	-	0	-	✎ 🗑
2	-	-	0	-	✎ 🗑
3	-	-	0	-	✎ 🗑

The following table describes the labels in this screen.

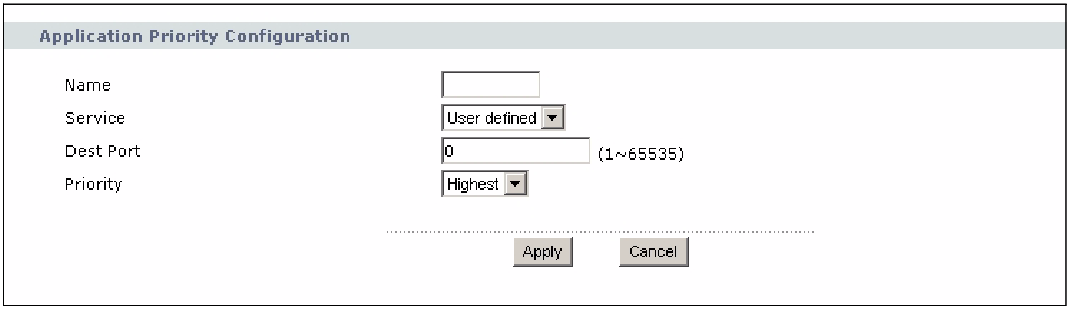
Table 36 Network > Wireless LAN > QoS

LABEL	DESCRIPTION
WMM QoS Policy	Select **Default** to have the NBG420N automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. Select **Application Priority** from the drop-down list box to display a table of application names, services, ports and priorities to which you want to apply WMM QoS.
	The table appears only if you select **Application Priority** in **WMM QoS Policy**.
#	This is the number of an individual application entry.
Name	This field displays a description given to an application entry.
Service	This field displays either **FTP**, **WWW**, **E-mail** or a **User Defined** service to which you want to apply WMM QoS.
Dest Port	This field displays the destination port number to which the application sends traffic.
Priority	This field displays the priority of the application. **Highest** - Typically used for voice or video that should be high-quality. **High** - Typically used for voice or video that can be medium-quality. **Mid** - Typically used for applications that do not fit into another priority. For example, Internet surfing. **Low** - Typically used for non-critical “background” applications, such as large file transfers and print jobs that should not affect other applications.
Modify	Click the **Edit** icon to open the **Application Priority Configuration** screen. Modify an existing application entry or create a application entry in the **Application Priority Configuration** screen. Click the **Remove** icon to delete an application entry.
Apply	Click **Apply** to save your changes to the NBG420N.

7.8.1 Application Priority Configuration

Use this screen to edit a WMM QoS application entry. Click the edit icon under **Modify**. The following screen displays.

Figure 69 Network > Wireless LAN > QoS: Application Priority Configuration



Application Priority Configuration

Name

Service: User defined

Dest Port: 0 (1~65535)

Priority: Highest

See Appendix F on page 321 for a list of commonly-used services and destination ports. The following table describes the fields in this screen.

Network > Wireless LAN > QoS: Application Priority Configuration

LABEL	DESCRIPTION
Application Priority Configuration	
Name	Type a description of the application priority.
Service	The following is a description of the applications you can prioritize with WMM QoS. Select a service from the drop-down list box. • **E-Mail** Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80 • **FTP** File Transfer Protocol enables fast transfer of files, including large files that it may not be possible to send via e-mail. FTP uses port number 21. • **WWW** The World Wide Web is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser. • **User-Defined** User-defined services are user specific services configured using known ports and applications.
Dest Port	This displays the port the selected service uses. Type a port number in the field provided if you want to use a different port to the default port.
Priority	Select a priority from the drop-down list box.
Apply	Click **Apply** to save your changes back to the NBG420N.
Cancel	Click **Cancel** to return to the previous screen.

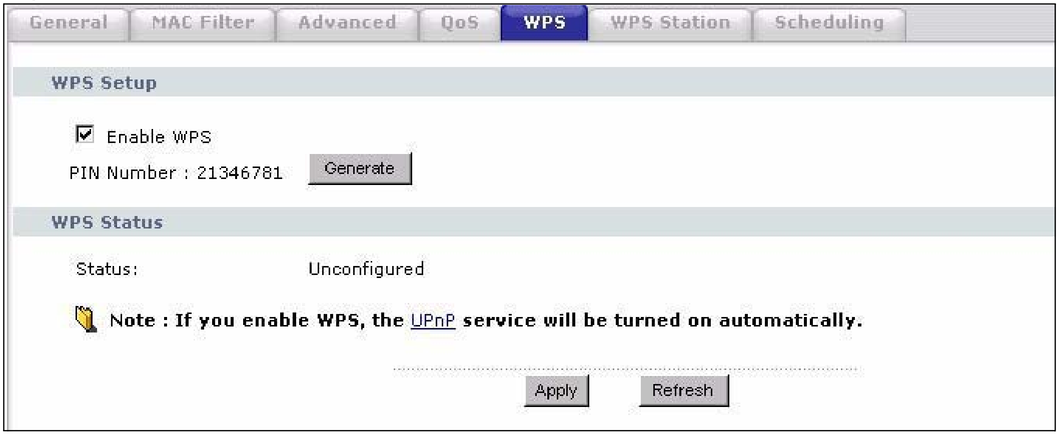
7.9 WiFi Protected Setup

WiFi Protected Setup (WPS) is an industry standard specification, defined by the WiFi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the Section 6.1.2 on page 73.

7.9.1 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Network** > **Wireless LAN** > **WPS** tab.

Figure 70 WPS



☑ Enable WPS

PIN Number : 21346781

Status: Unconfigured

Note : If you enable WPS, the UPnP service will be turned on automatically.

The following table describes the labels in this screen.

Table 37 WPS

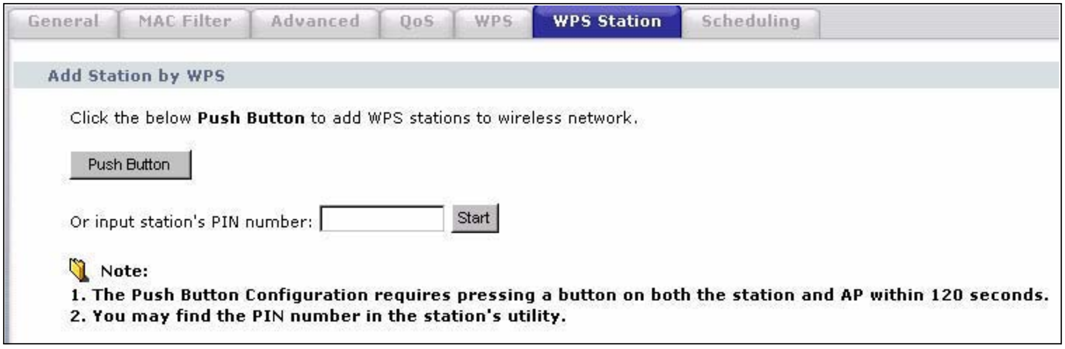
LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select this to enable the WPS feature.
PIN Number	This displays a PIN number last time system generated. Click **Generate** to generate a new PIN number.
WPS Status	
Status	This displays **Configured** when the NBG420N has connected to a wireless network using WPS or when **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there are no wireless or wireless security changes on the NBG420N or you click **Release_Configuration** to remove the configured wireless and wireless security settings.
Release Configuration	This button is only available when the WPS status displays **Configured**. Click this button to remove all configured wireless and wireless security settings for WPS connections on the NBG420N.
Apply	Click **Apply** to save your changes back to the NBG420N.
Refresh	Click **Refresh** to get this screen information afresh.

7.9.2 WPS Station Screen

Use this screen when you want to add a wireless station using WPS. To open this screen, click **Network** > **Wireless LAN** > **WPS Station** tab.

Note: After you click **Push Button** on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.

Figure 71 WPS Station



Add Station by WPS

Click the below **Push Button** to add WPS stations to wireless network.

Or input station's PIN number:

Note:
1. The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2. You may find the PIN number in the station's utility.

The following table describes the labels in this screen.

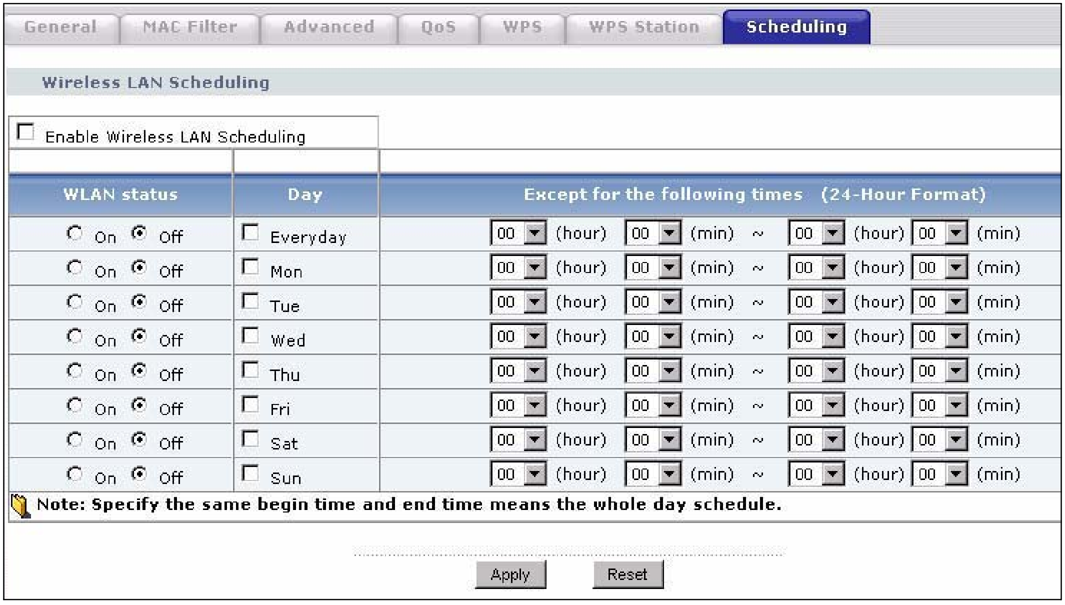
Table 38 WPS Station

LABEL	DESCRIPTION
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. See Section 6.1.2.1 on page 74. Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
Or input station's PIN number	Use this button when you use the PIN Configuration method to configure wireless station's wireless settings. See Section 6.1.2.2 on page 75. Type the same PIN number generated in the wireless station's utility. Then click **Start** to associate to each other and perform the wireless security information synchronization.

7.9.3 Scheduling

Use this screen to set the times your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default. The wireless LAN can be scheduled to turn on or off on certain days and at certain times. To open this screen, click **Network** > **Wireless LAN** > **Scheduling** tab.

Figure 72 Scheduling



Wireless LAN Scheduling

□ Enable Wireless LAN Scheduling

WLAN status	Day	Except for the following times (24-Hour Format)
○ On ● Off	□ Everyday	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Mon	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Tue	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Wed	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Thu	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Fri	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Sat	00 (hour) 00 (min) ~ 00 (hour) 00 (min)
○ On ● Off	□ Sun	00 (hour) 00 (min) ~ 00 (hour) 00 (min)

Note: Specify the same begin time and end time means the whole day schedule.

The following table describes the labels in this screen.

Table 39 Scheduling

LABEL	DESCRIPTION
Enable Wireless LAN Scheduling	Select this to enable Wireless LAN scheduling.
WLAN Status	Select **On** or **Off** to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the **Day** and **Except for the following times** fields.
Day	Select **Everyday** or the specific days to turn the Wireless LAN on or off. If you select **Everyday** you can not select any specific days. This field works in conjunction with the **Except for the following times** field.
Except for the following times (24-Hour Format)	Select a begin time using the first set of **hour** and minute (**min**) drop down boxes and select an end time using the second set of **hour** and minute (**min**) drop down boxes. If you have chosen **On** earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields. If you have chosen **Off** earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. Note: Entering the same begin time and end time will mean the whole day.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.10 iPod Touch Web Configurator

The iPod Touch web configurator displays when you are connecting to the NBG420N wirelessly with an iPod Touch device through a web browser. It is different to the web configurator that you access from your computer.

To connect wirelessly to the iPod Touch web configurator with your iPod Touch follow the steps below:

1 Make sure the Wireless LAN on the NBG420N is enabled and that you know the security settings (if any). To do this check the **Wireless LAN** > **General** screen in the web configurator from your computer.

2 On the iPod Touch's main screen press **Settings** > **Wi-fi** and from the list press the NBG420N's network name (SSID) to connect to it. If you are prompted for any security settings enter them and press connect. If you cannot connect check your security settings in the web configurator from your computer and try again.

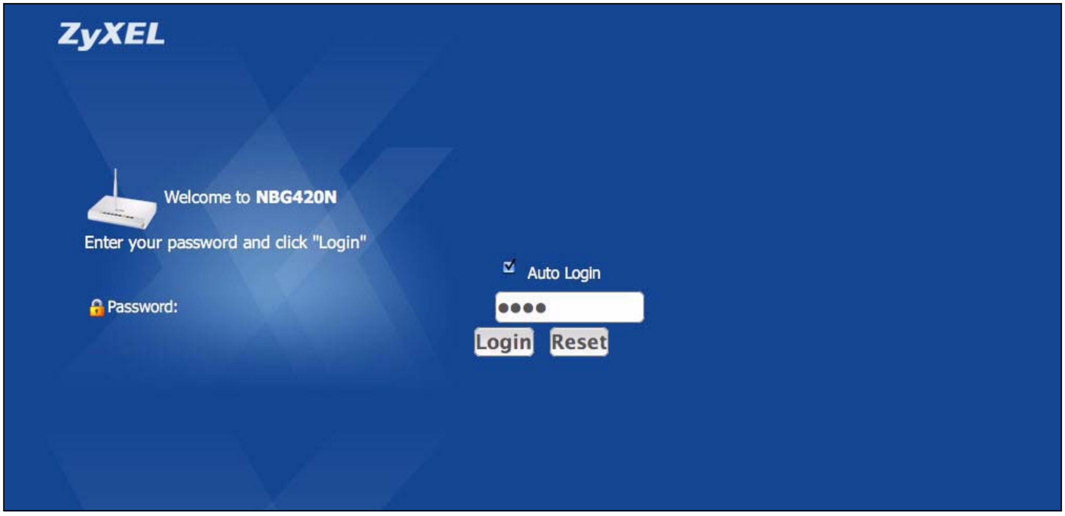
3 After connecting to the NBG420N's wireless LAN network launch the iPod Touch Internet browser and enter the NBG420N's IP address (default: 192.168.1.1) into the address bar. The login screen displays.

7.10.1 Login Screen

After accessing the NBG420N's IP address in the iPod Touch web browser the screen below will display.

You cannot change your password in the iPod Touch web configurator. To change your password log into the web configurator using your computer.

Figure 73 Login Screen



The following table describes the labels in this screen.

Table 40 Login Screen

LABEL	DESCRIPTION
Auto Login	Select this checkbox to automatically log into the iPod Touch web configurator when accessing it through the same iPod Touch device.
Password	Enter the password for the NBG420N. If you haven't changed the default password earlier this is "**1234**".
Login	Press the **Login** button to log into the iPod Touch web configurator.
Reset	Press the **Reset** button to clear your selections and start over.

7.10.2 System Status

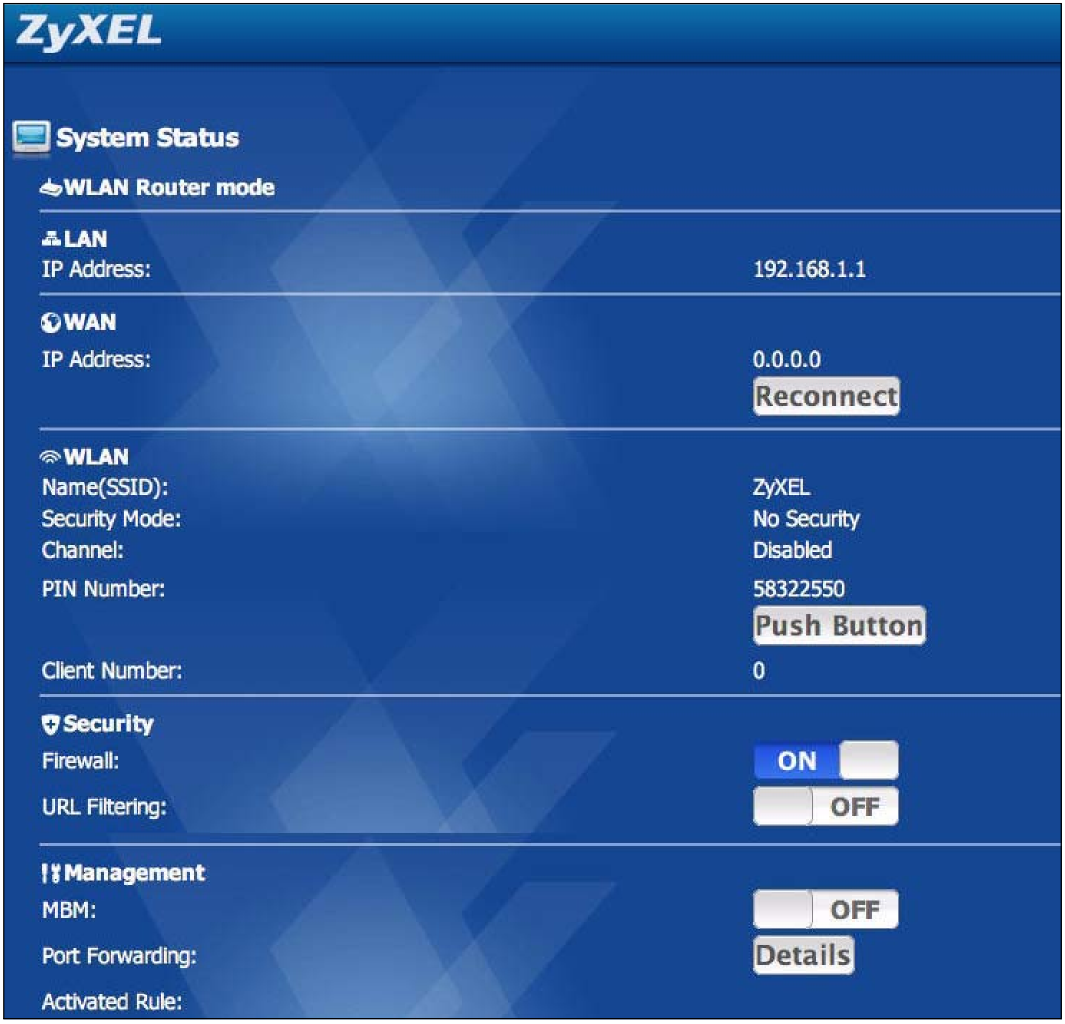
After successfully logging into the iPod Touch web configurator the **System Status** screen displays.

Your changes in the iPod Touch web configurator are saved automatically after pressing a button.

If you are going to use the WPS (Wi-Fi Protected Setup) function in the iPod Touch Web Configurator it is recommended to configure your WPS settings first from your computer.

If WPS has not been configured previously the iPod Touch will lose it's wireless connection to the NBG420N after the NBG420N has connected to another device using WPS through the iPod Touch web configurator. To reconnect to the wireless network using your iPod Touch you must find out the new WPS settings by logging into the web configurator from your computer and going to the **Wireless LAN** screen.

Figure 74 System Status screen



ZyXEL

System Status

WLAN Router mode

LAN

IP Address: 192.168.1.1

WAN

IP Address: 0.0.0.0

Reconnect

WLAN

Name(SSID): ZyXEL

Security Mode: No Security

Channel: Disabled

PIN Number: 58322550

Push Button

Client Number: 0

Security

Firewall: ON

URL Filtering: OFF

Management

MBM: OFF

Port Forwarding: Details

Activated Rule:

The following table describes the labels in this screen.

Table 41 System Status screen

LABEL	DESCRIPTION
Logout	Press this to logout of the iPod Touch web configurator.
LAN	
IP Address	This field displays the NBG420N's LAN (Local Area Network) IP address.
WAN	
IP Address	This field displays the NBG420N's WAN IP address. If this field displays "-" it means the WAN is not connected. Try pressing **Reconnect** if your WAN connection is not working.
Reconnect	Press **Reconnect** to renew your NBG420N's WAN connection.
WLAN	
Name (SSID)	This field displays the SSID (Service set identifier) of the NBG420N's Wireless LAN.
Security Mode	This field displays the security authentication mode of the NBG420N's Wireless LAN. This can be **No Security**, **WPA-PSK**, **WPA2-PSK** or **WEP**.

Table 41 System Status screen

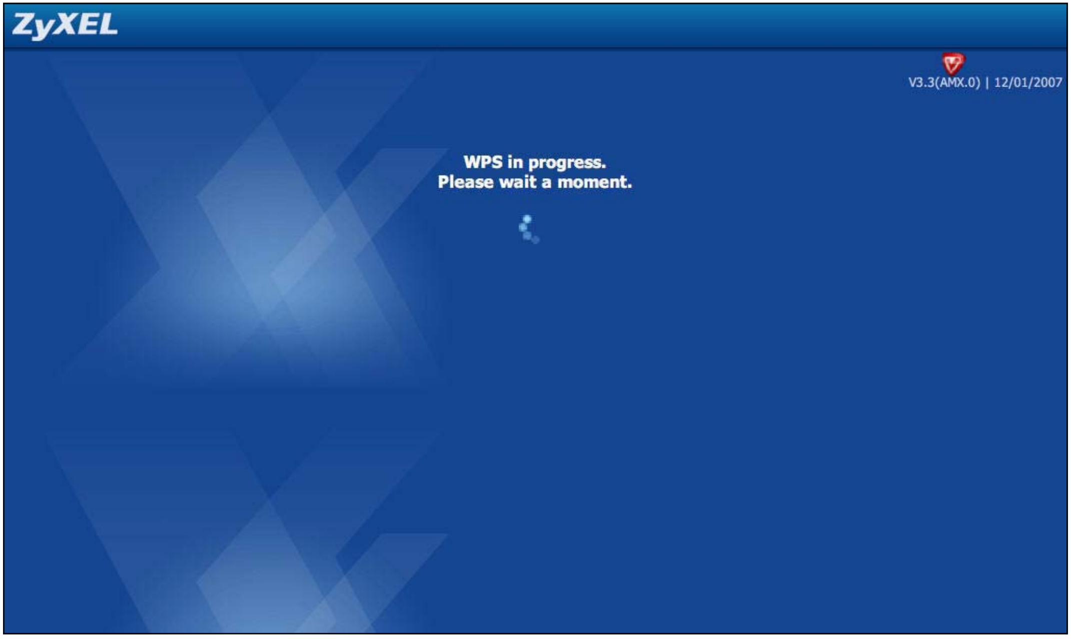
LABEL	DESCRIPTION
Channel	This field displays the channel the NBG420N's Wireless LAN operates on. This will display as disabled if auto channel selection mode is on.
PIN Number	This field displays the NBG420N's WPS (Wi-Fi Protected Setup) PIN number. WPS allows you to connect wireless clients to your wireless LAN easily. See Section 7.9 on page 106 for more information on WPS and the PIN method of configuration.
Push Button	Press the **Push Button** to start either the PBC (Push Button Configuration) or PIN method of WPS configuration. The WPS in progress screen will display, see Section 7.10.3 on page 112.
Client Number	This field displays the number of wireless clients on the network.
Security	
Firewall	Press the left side of the button to turn the firewall **ON**. Press the right side of the button to turn the firewall **OFF**. To configure the firewall access the web configurator from your computer. A Firewall enables the NBG420N to act as a secure gateway between the LAN and the Internet.
URL Filtering	Press the left side of the button to turn URL Filtering **ON**. Press the right side of the button to turn URL Filtering **OFF**. To configure URL filtering access the web configurator from your computer and go to the content filtering screens. Content filtering enables you to block certain web features or specific URL keywords.
Management	
MBM	Press the left side of the button to turn MBM (Media Bandwidth Management) **ON**. Press the right side of the button to turn MBM **OFF**. To configure Media Bandwidth Management access the web configurator from your computer and go to the Bandwidth Management screens. When accessed from a computer the web configurator allows you to specify bandwidth management rules based on an application and/or subnet.
Port Forwarding	Press **Details** to go to another screen to manage the port forwarding rules.
Activated Rule	This field displays the currently activated port forwarding rules.

7.10.3 WPS in Progress

After pressing **Push Button** in the **System Status** screen the WPS in Progress screen will display.

It can take around two minutes for a successful WPS connection to be made. The **System Status** screen will display after a connection has been made or if it has failed. For more information on WPS see Section 7.9 on page 106.

Figure 75 WPS In Progress



WPS in progress.
Please wait a moment.

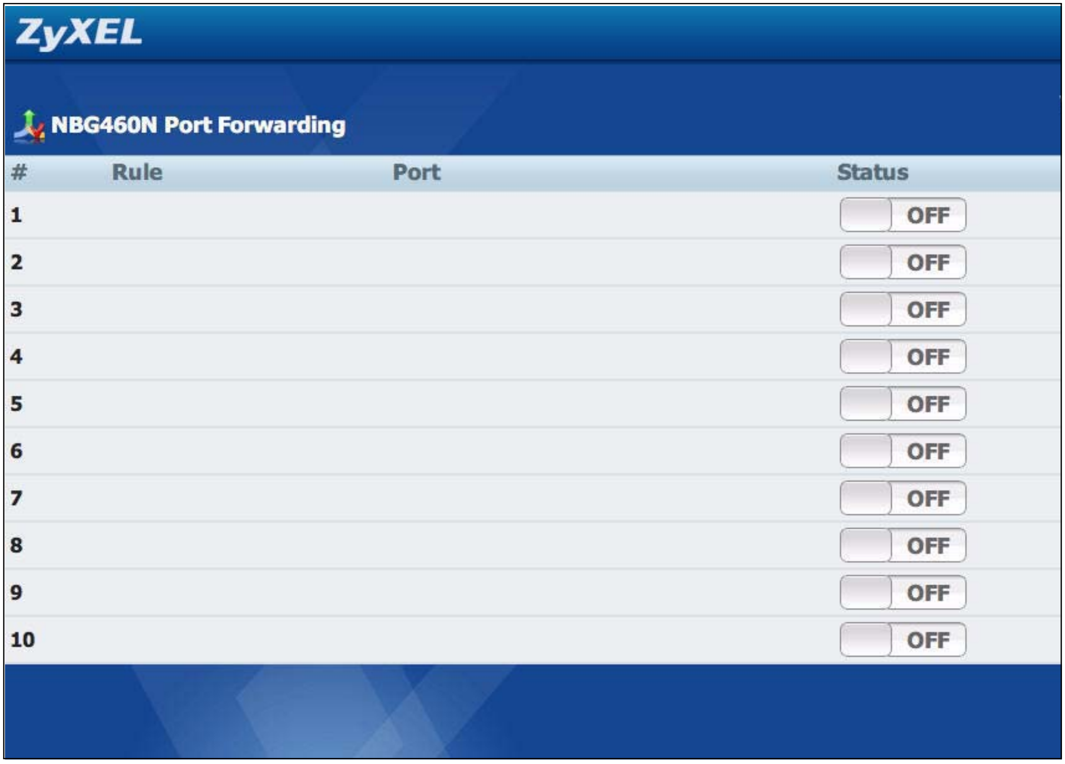
7.10.4 Port Forwarding

After pressing the **Details** button in the **System Status** screen the port forwarding screen will display. Use this screen to change the status of port forwarding rules that have been set up in the web configurator from your computer. See Section 11.4 on page 139 for more information on configuring port forwarding rules.

To go back to the **System Status** screen press the ZyXEL logo at the top of the page.

To see any changes on the **System Status** screen you will need to refresh the page first. Use the browser’s refresh function. See the iPod Touch’s documentation if you cannot find it.

Figure 76 Port Forwarding



ZyXEL

NBG460N Port Forwarding

#	Rule	Port	Status
1			OFF
2			OFF
3			OFF
4			OFF
5			OFF
6			OFF
7			OFF
8			OFF
9			OFF
10			OFF

The following table describes the labels in this screen.

Table 42 Port Forwarding

LABEL	DESCRIPTION
#	This is the number of an individual port forwarding entry.
Rule	This column displays the configured port forwarding rules. To configure a new rule you must use the web configurator from your computer.
Port	This column displays the port number(s) which are forwarded when the rule is turned on.
Status	Use this column to manage the status of the rules. Press the left side of the button to turn the rule **ON** and press the right side of the button to turn the rule **OFF**.

7.11 Accessing the iPod Touch Web Configurator

To access the iPod Touch web configurator through your iPod Touch you must first connect it to the NBG420N's wireless network. Follow the steps below to do this.

If you have not configured your wireless settings yet you can do so by using the Wizard in the web configurator you access from your computer. Click the Wizard icon or the **Go To Wizard Setup** web link you see after logging into the web configurator from your computer. See Chapter 4 on page 49 for more information on using the Wizard.

1. On the iPod Touch's main screen press **Settings** and then press **Wi-fi**.
2. On the list of networks press the NBG420N's network name (SSID) to connect to it. If you are prompted for any security settings enter them and press connect.

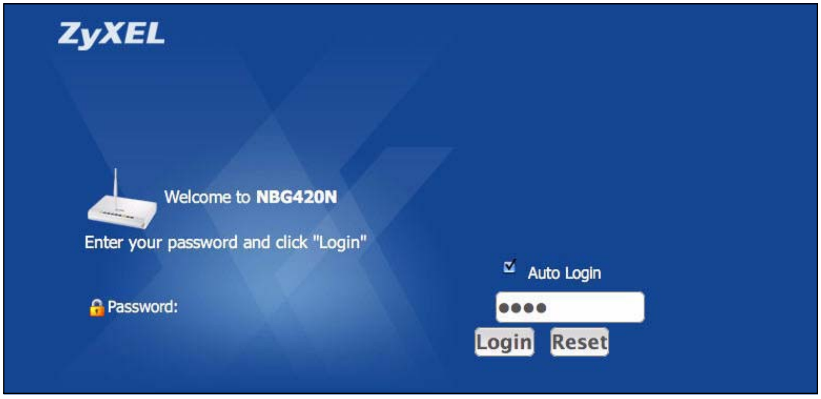
The pre-shared key is case-sensitive. If you have problems connecting then try checking the security settings in the web configurator from your computer and try again.

7.11.1 Accessing the iPod Touch Web Configurator

Now that you are connected to the NBG420N's wireless network you can access the iPod Touch web configurator. To do this follow the steps below:

1. Launch the iPod Touch's web browser from the main screen. The default web browser is Safari.
2. Enter the IP address of the NBG420N into the address bar and go to that address. The default IP address for the NBG420N is 192.168.1.1.
3. The login screen should display.

Figure 77 Login Screen



ZyXEL

Welcome to **NBG420N**

Enter your password and click "Login"

☑ Auto Login

Password: ●●●●

If the login screen does not display properly, check that you are accessing the correct IP address. Also check your iPod Touch web browser's security settings as they may affect how the page displays.

4 If you wish to login automatically in the future make sure the **Auto Login** checkbox is selected.

5 Enter your password and press login. The default password for the NBG420N is "**1234**".

6 The **System Status** screen will display after successfully logging in. Congratulations! For information on using the configurator see Section 7.10 on page 108.

8

WAN

This chapter describes how to configure WAN settings.

8.1 WAN Overview

See the chapter about the connection wizard for more information on the fields in the WAN screens.

8.2 WAN MAC Address

The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

8.3 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The NBG420N supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the NBG420N queries all directly connected networks to gather group membership. After that, the NBG420N periodically updates this information. IP multicasting can be enabled/disabled on the NBG420N LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

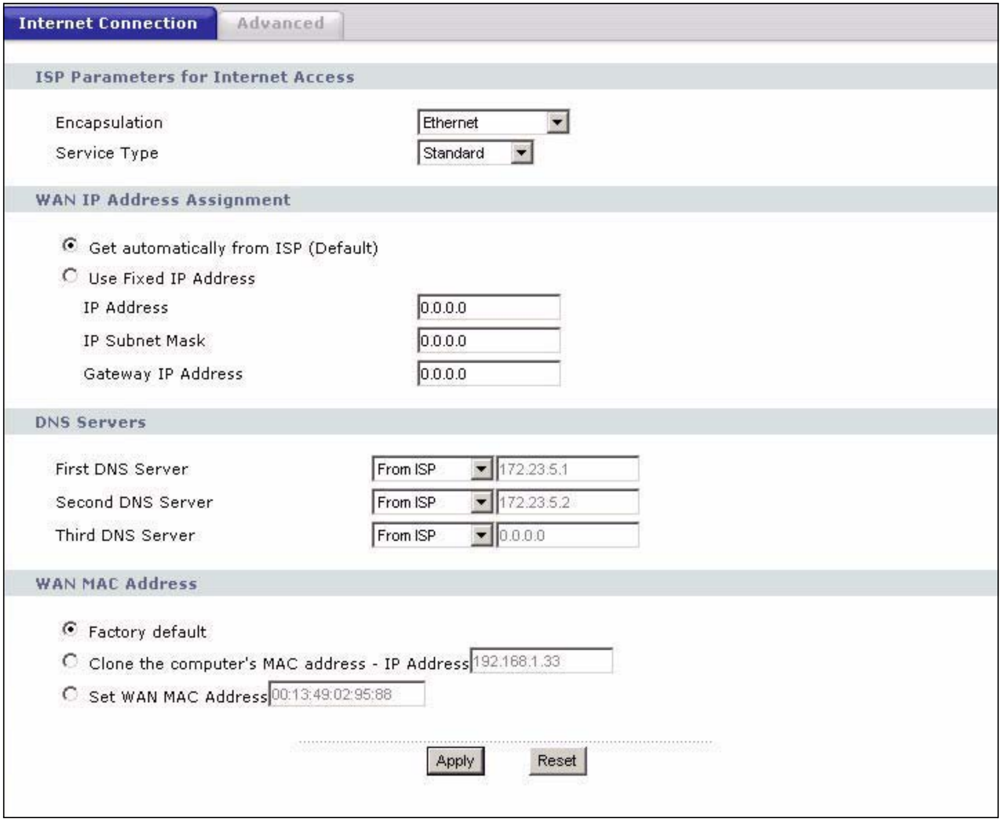
8.4 Internet Connection

Use this screen to change your NBG420N's Internet access settings. Click **Network** > **WAN**. The screen differs according to the encapsulation you choose.

8.4.1 Ethernet Encapsulation

This screen displays when you select **Ethernet** encapsulation.

Figure 78 Network > WAN > Internet Connection: Ethernet Encapsulation



ISP Parameters for Internet Access

Encapsulation	Ethernet
Service Type	Standard

WAN IP Address Assignment

● Get automatically from ISP (Default)

○ Use Fixed IP Address

IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0

DNS Servers

First DNS Server	From ISP	172.23.5.1
Second DNS Server	From ISP	172.23.5.2
Third DNS Server	From ISP	0.0.0.0

WAN MAC Address

● Factory default

○ Clone the computer's MAC address - IP Address 192.168.1.33

○ Set WAN MAC Address 00:13:49:02:95:88

The following table describes the labels in this screen.

Table 43 Network > WAN > Internet Connection: Ethernet Encapsulation

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from **Standard**, **RR-Telstra** (RoadRunner Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Toshiba** (Roadrunner Toshiba authentication method) or **Telia Login**. The following fields do not appear with the **Standard** service type.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
IP Subnet Mask	Enter the **IP Subnet Mask** in this field.
Gateway IP Address	Enter a **Gateway IP Address** (if your ISP gave you one) in this field.
DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG420N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG420N's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4.2 PPPoE Encapsulation

The NBG420N supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius).

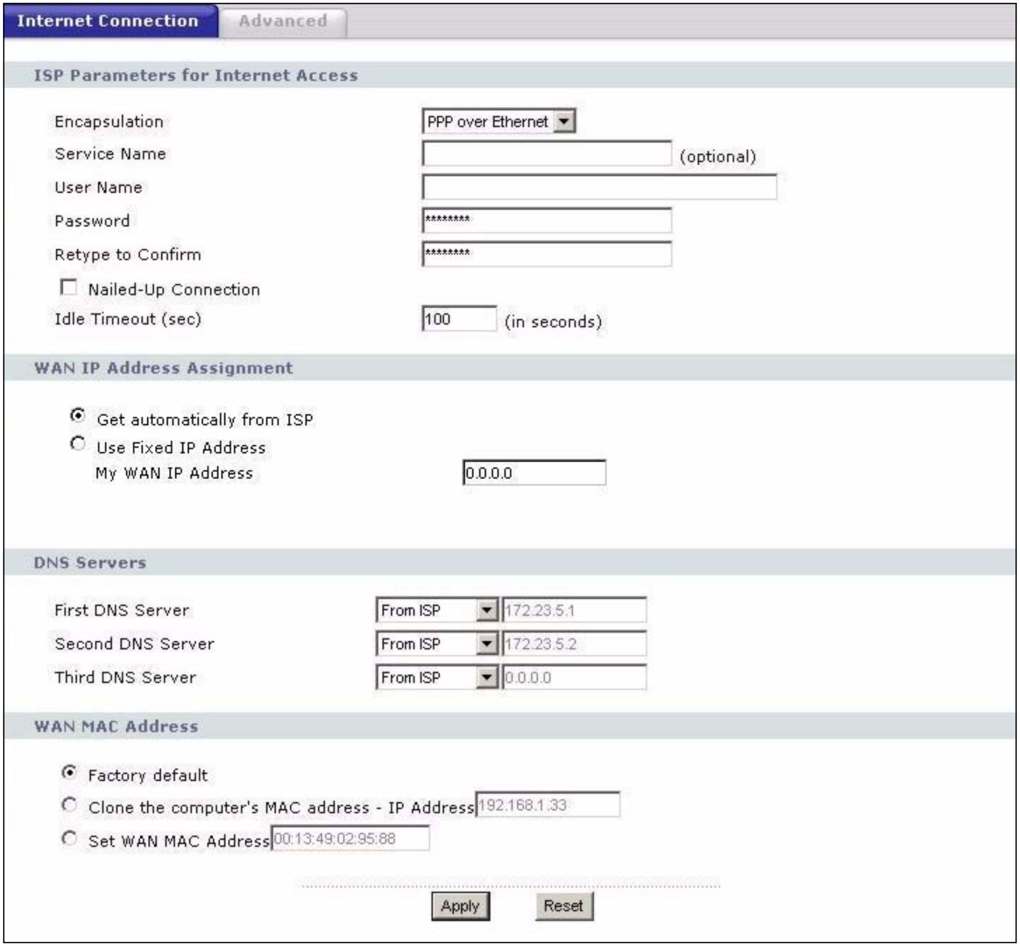
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the NBG420N (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG420N does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

This screen displays when you select **PPPoE** encapsulation.

Figure 79 Network > WAN > Internet Connection: PPPoE Encapsulation



ISP Parameters for Internet Access

Encapsulation	PPP over Ethernet
Service Name	(optional)
User Name	
Password	********
Retype to Confirm	********
□ Nailed-Up Connection	
Idle Timeout (sec)	100 (in seconds)

WAN IP Address Assignment

● Get automatically from ISP

○ Use Fixed IP Address

My WAN IP Address 0.0.0.0

DNS Servers

First DNS Server	From ISP	172.23.5.1
Second DNS Server	From ISP	172.23.5.2
Third DNS Server	From ISP	0.0.0.0

WAN MAC Address

● Factory default

○ Clone the computer's MAC address - IP Address 192.168.1.33

○ Set WAN MAC Address 00:13:49:02:95:88

The following table describes the labels in this screen.

Table 44 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The **PPP over Ethernet** choice is for a dial-up connection using PPPoE. The NBG420N supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG420N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the NBG420N's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.

Table 44 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

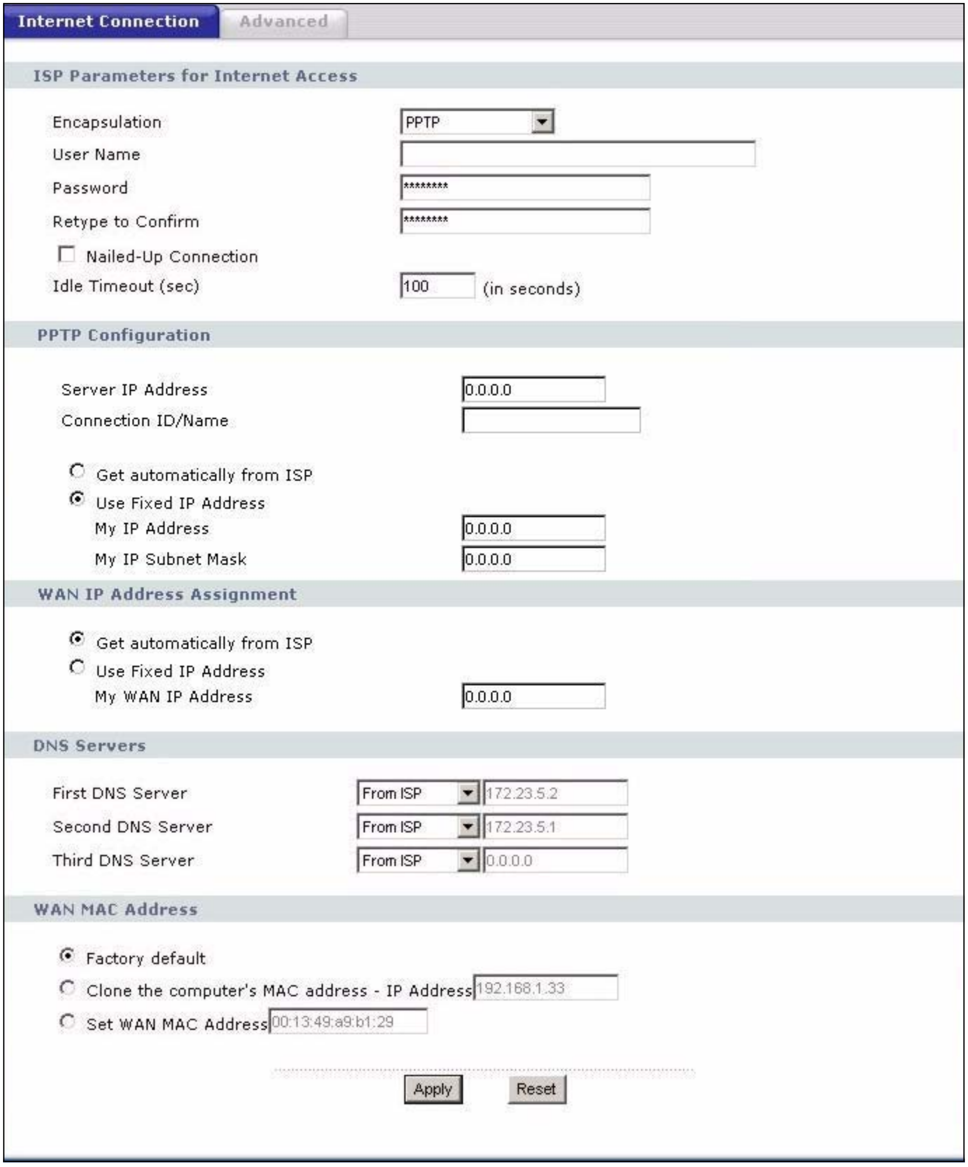
8.4.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

This screen displays when you select **PPTP** encapsulation.

Figure 80 Network > WAN > Internet Connection: PPTP Encapsulation



ISP Parameters for Internet Access

Encapsulation	PPTP
User Name	
Password	********
Retype to Confirm	********
□ Nailed-Up Connection	
Idle Timeout (sec)	100 (in seconds)

PPTP Configuration

Server IP Address	0.0.0.0
Connection ID/Name	
○ Get automatically from ISP	
● Use Fixed IP Address	
My IP Address	0.0.0.0
My IP Subnet Mask	0.0.0.0

WAN IP Address Assignment

● Get automatically from ISP	
○ Use Fixed IP Address	
My WAN IP Address	0.0.0.0

DNS Servers

First DNS Server	From ISP	172.23.5.2
Second DNS Server	From ISP	172.23.5.1
Third DNS Server	From ISP	0.0.0.0

WAN MAC Address

● Factory default

○ Clone the computer's MAC address - IP Address 192.168.1.33

○ Set WAN MAC Address 00:13:49:a9:b1:29

The following table describes the labels in this screen.

Table 45 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The NBG420N supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.

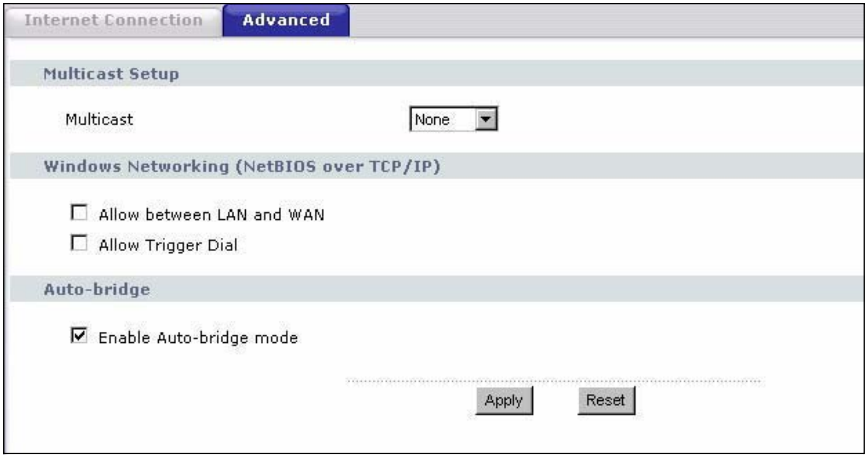
Table 45 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the NBG420N automatically disconnects from the PPTP server.
PPTP Configuration	
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Type your identification name for the PPTP server.
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Your NBG420N will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the NBG420N.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG420N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG420N’s MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer’s MAC address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

8.5 Advanced WAN Screen

To change your NBG420N's advanced WAN settings, click **Network** > **WAN** > **Advanced**. The screen appears as shown.

Figure 81 Network > WAN > Advanced



Internet Connection | Advanced

Multicast Setup

Multicast: None

Windows Networking (NetBIOS over TCP/IP)

□ Allow between LAN and WAN

□ Allow Trigger Dial

Auto-bridge

☑ Enable Auto-bridge mode

The following table describes the labels in this screen.

Table 46 WAN > Advanced

LABEL	DESCRIPTION
Multicast Setup	
Multicast	Select **IGMP V-1**, **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.

Table 46 WAN > Advanced

LABEL	DESCRIPTION
Enable Auto-bridge mode	Select this option to have the NBG420N switch to bridge mode automatically when the NBG420N gets a WAN IP address in the range of 192.168.x.y (where x and y are from zero to nine) no matter what the LAN IP address is. This might happen if you put the NBG420N behind a NAT router that assigns it this IP address. When the NBG420N is in bridge mode, the NBG420N acts as an AP and all the interfaces (LAN, WAN and WLAN) are bridged. In this mode, your NAT, DHCP server, firewall and bandwidth management (rules) on the NBG420N are not available. You do not have to reconfigure them if you return to router mode. Note: The NBG420N automatically turns back to **Router Mode** when the NBG420N gets a WAN IP address that is not in the 192.168.x.y range. Auto-bridging only works under the following conditions: • The WAN IP must be 192.168.x.y (where x and y must be from zero to nine). If the LAN IP address and the WAN IP address are in the same subnet but x or y is greater than nine, the device operates in router mode (with firewall and bandwidth management available). • The device must be in **Router Mode** (see Chapter 24 on page 259 for more information) for auto-bridging to become active.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

9

LAN

This chapter describes how to configure LAN settings.

9.1 LAN Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

9.1.1 IP Pool Setup

The NBG420N is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the NBG420N itself) in the lower range (192.168.1.2 to 192.168.1.32) for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

9.1.2 System DNS Servers

Refer to the IP address and subnet mask section in the **Connection Wizard** chapter.

9.2 LAN TCP/IP

The NBG420N has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

9.2.1 Factory LAN Defaults

The LAN parameters of the NBG420N are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

9.2.2 IP Address and Subnet Mask

Refer to the IP address and subnet mask section in the **Connection Wizard** chapter for this information.

9.2.3 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The NBG420N supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the NBG420N queries all directly connected networks to gather group membership. After that, the NBG420N periodically updates this information. IP multicasting can be enabled/disabled on the NBG420N LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

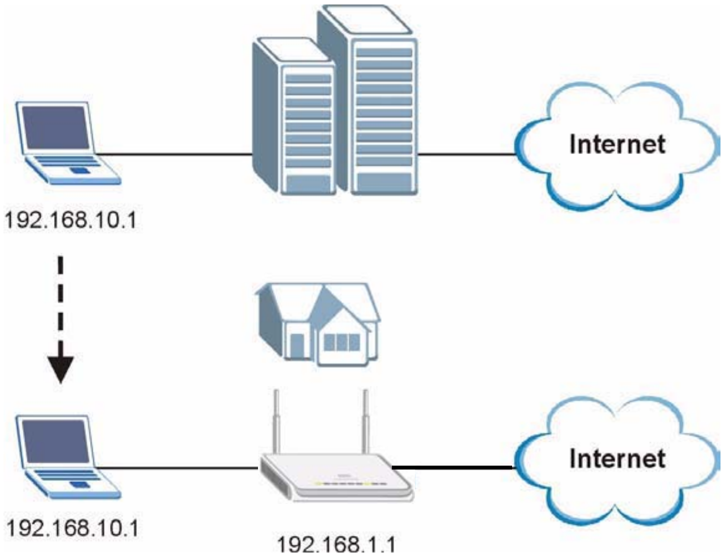
9.2.4 Any IP

Traditionally, you must set the IP addresses and the subnet masks of a computer and the NBG420N to be in the same subnet to allow the computer to access the Internet (through the NBG420N). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the NBG420N.

With the Any IP feature and NAT enabled, the NBG420N allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the NBG420N are not in the same subnet. Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the NBG420N and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a NBG420N is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the NBG420N are not in the same subnet.

Figure 82 Any IP Example



The Any IP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the NBG420N's IP address.

You *must* enable NAT to use the Any IP feature on the NBG420N.

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. IP routing table is defined on IP Ethernet devices (the NBG420N) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the NBG420N.

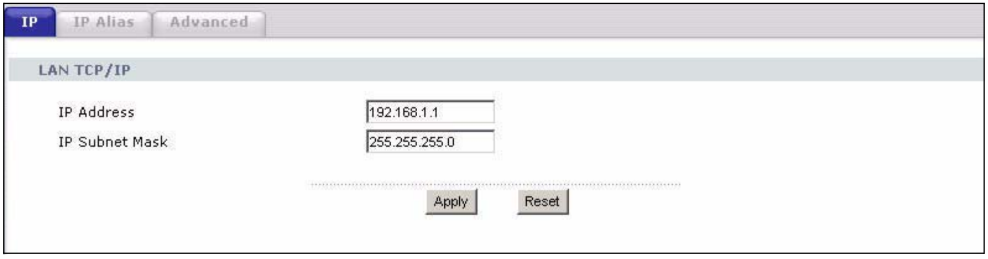
1. When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the NBG420N) by looking at the MAC address in its ARP table.
2. When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.
3. The NBG420N receives the ARP request and replies to the computer with its own MAC address.
4. The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the NBG420N.
5. When the NBG420N receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

After all the routing information is updated, the computer can access the NBG420N and the Internet as if it is in the same subnet as the NBG420N.

9.3 LAN IP Screen

Use this screen to change your basic LAN settings. Click **Network** > **LAN**.

Figure 83 Network > LAN > IP



LAN TCP/IP

IP Address: 192.168.1.1

IP Subnet Mask: 255.255.255.0

The following table describes the labels in this screen.

Table 47 Network > LAN > IP

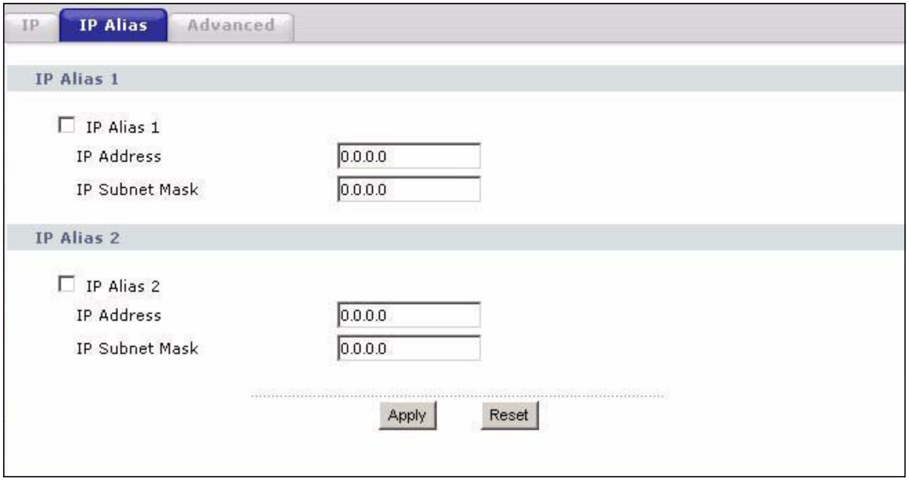
LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Type the IP address of your NBG420N in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG420N will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the NBG420N.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

9.4 LAN IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The NBG420N supports three logical LAN interfaces via its single physical Ethernet interface with the NBG420N itself as the gateway for each LAN network.

To change your NBG420N’s IP alias settings, click **Network** > **LAN** > **IP Alias**. The screen appears as shown.

Figure 84 Network > LAN > IP Alias



IP Alias 1

☐ IP Alias 1

IP Address 0.0.0.0

IP Subnet Mask 0.0.0.0

IP Alias 2

☐ IP Alias 2

IP Address 0.0.0.0

IP Subnet Mask 0.0.0.0

The following table describes the labels in this screen.

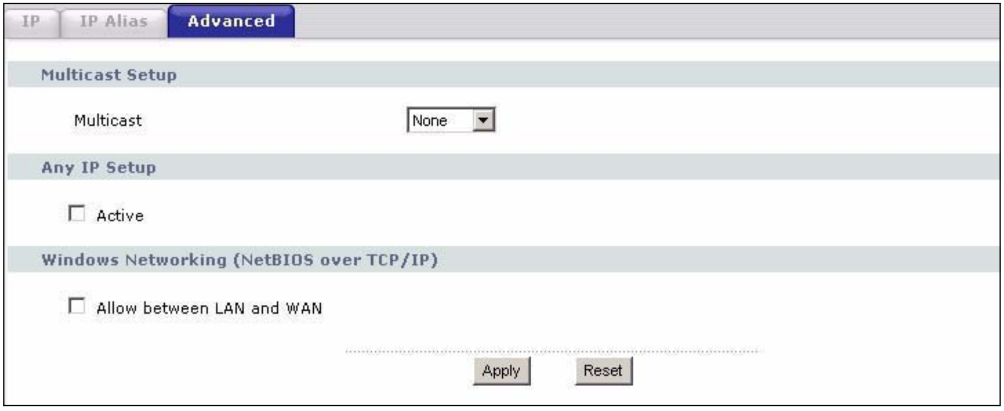
Table 48 Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias 1,2	Select the check box to configure another LAN network for the NBG420N.
IP Address	Enter the IP address of your NBG420N in dotted decimal notation.
IP Subnet Mask	Your NBG420N will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the NBG420N.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

9.5 Advanced LAN Screen

To change your NBG420N’s advanced IP settings, click **Network** > **LAN** > **Advanced**. The screen appears as shown.

Figure 85 Network > LAN > Advanced



Multicast Setup

Multicast None

Any IP Setup

☐ Active

Windows Networking (NetBIOS over TCP/IP)

☐ Allow between LAN and WAN

The following table describes the labels in this screen.

Table 49 Network > LAN > Advanced

LABEL	DESCRIPTION
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Any IP Setup	
Active	Select this if you want to let computers on different subnets use the NBG420N.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

10

DHCP

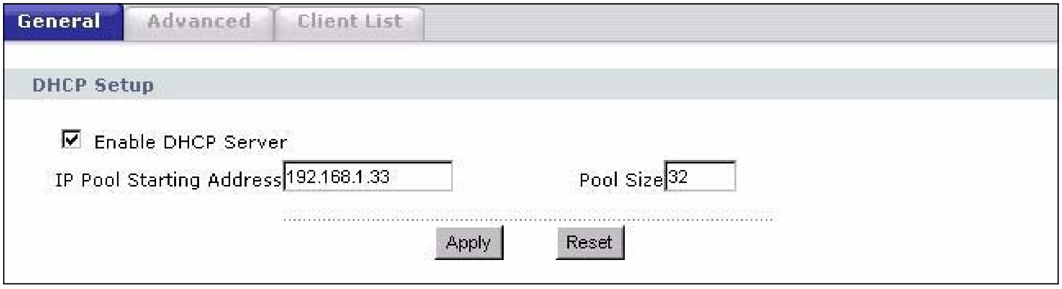
10.1 DHCP

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the NBG420N's LAN as a DHCP server or disable it. When configured as a server, the NBG420N provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

10.2 DHCP General Screen

Click **Network** > **DHCP**. The following screen displays.

Figure 86 Network > DHCP > General



DHCP Setup

☑ Enable DHCP Server

IP Pool Starting Address 192.168.1.33

Pool Size 32

The following table describes the labels in this screen.

Table 50 Network > DHCP > General

LABEL	DESCRIPTION
LAN DHCP Setup	
Enable DHCP Server	Enable or Disable DHCP for LAN. DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Leave the **Enable DHCP Server** check box selected unless your ISP instructs you to do otherwise. Clear it to disable the NBG420N acting as a DHCP server. When configured as a server, the NBG420N provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool for LAN.
Pool Size	This field specifies the size, or count of the IP address pool for LAN.

Table 50 Network > DHCP > General

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

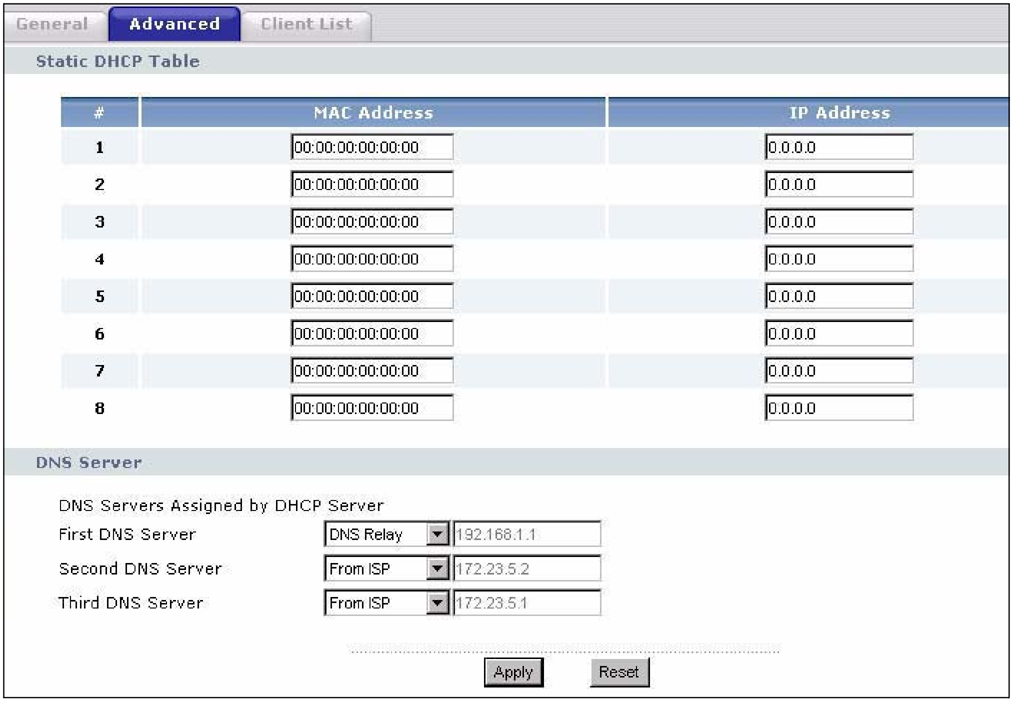
10.3 DHCP Advanced Screen

This screen allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses. You can also use this screen to configure the DNS server information that the NBG420N sends to the DHCP clients.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

To change your NBG420N's static DHCP settings, click **Network** > **DHCP** > **Advanced**. The following screen displays.

Figure 87 Network > DHCP > Advanced



Static DHCP Table

#	MAC Address	IP Address
1	00:00:00:00:00:00	0.0.0.0
2	00:00:00:00:00:00	0.0.0.0
3	00:00:00:00:00:00	0.0.0.0
4	00:00:00:00:00:00	0.0.0.0
5	00:00:00:00:00:00	0.0.0.0
6	00:00:00:00:00:00	0.0.0.0
7	00:00:00:00:00:00	0.0.0.0
8	00:00:00:00:00:00	0.0.0.0

DNS Server

DNS Servers Assigned by DHCP Server

First DNS Server: DNS Relay 192.168.1.1

Second DNS Server: From ISP 172.23.5.2

Third DNS Server: From ISP 172.23.5.1

The following table describes the labels in this screen.

Table 51 Network > DHCP > Advanced

LABEL	DESCRIPTION
Static DHCP Table	
#	This is the index number of the static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	Type the LAN IP address of a computer on your LAN.

Table 51 Network > DHCP > Advanced

LABEL	DESCRIPTION
DNS Server	
DNS Servers Assigned by DHCP Server	The NBG420N passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The NBG420N only passes this information to the LAN DHCP clients when you select the **Enable DHCP Server** check box. When you clear the **Enable DHCP Server** check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG420N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **DNS Relay** to have the NBG420N act as a DNS proxy. The NBG420N's LAN IP address displays in the field to the right (read-only). The NBG420N tells the DHCP clients on the LAN that the NBG420N itself is the DNS server. When a computer on the LAN sends a DNS query to the NBG420N, the NBG420N forwards the query to the NBG420N's system DNS server (configured in the **WAN > Internet Connection** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

10.4 Client List Screen

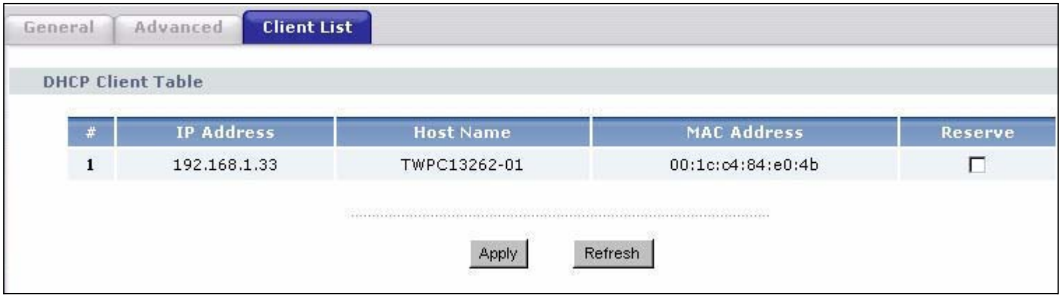
The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of network clients using the NBG420N's DHCP servers.

Configure this screen to always assign an IP address to a MAC address (and host name). Click **Network** > **DHCP Server** > **Client List**.

You can also view a read-only client list by clicking the **DHCP Table (Details...)** hyperlink in the **Status** screen.

The following screen displays.

Figure 88 Network > DHCP > Client List



DHCP Client Table

#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.33	TWPC13262-01	00:1c:c4:84:e0:4b	□

The following table describes the labels in this screen.

Table 52 Network > DHCP > Client List

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select this check box in the **DHCP Setup** section to have the NBG420N always assign the IP address(es) to the MAC address(es) (and host name(s)). After you click **Apply**, the MAC address and IP address also display in the **Advanced** screen (where you can edit them).
Apply	Click **Apply** to save your settings.
Refresh	Click **Refresh** to reload the DHCP table.

11

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the NBG420N.

11.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

11.2 Using NAT

You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the NBG420N.

11.2.1 Port Forwarding: Services and Port Numbers

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use the **Application** screen to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

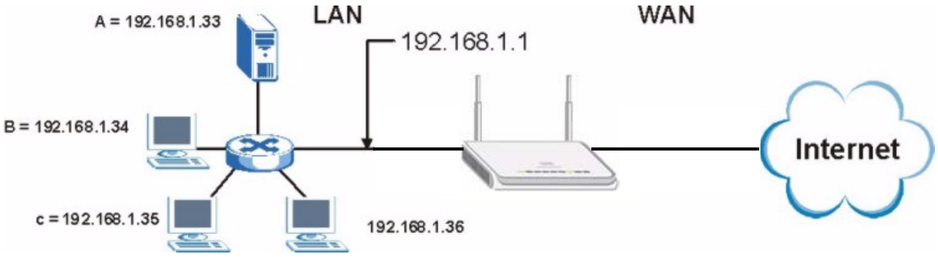
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

11.2.2 Configuring Servers Behind Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

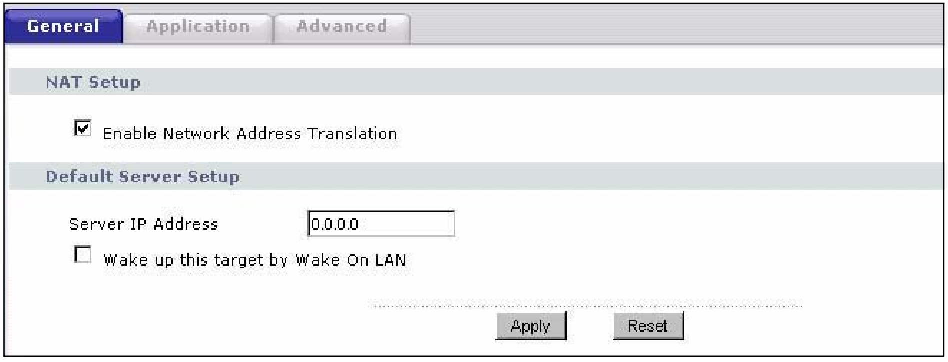
Figure 89 Multiple Servers Behind NAT Example



11.3 General NAT Screen

Click **Network** > **NAT** to open the **General** screen.

Figure 90 Network > NAT > General



NAT Setup

☑ Enable Network Address Translation

Default Server Setup

Server IP Address 0.0.0.0

☐ Wake up this target by Wake On LAN

The following table describes the labels in this screen.

Table 53 Network > NAT > General

LABEL	DESCRIPTION
Enable Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select the check box to enable NAT.
Default Server Setup	
Server IP Address	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in the **Application** screen. If you do not assign a **Default Server IP address**, the NBG420N discards all packets received for ports that are not specified in the **Application** screen or remote management.
Wake up this target by Wake On LAN	Select this to use WoL (Wake On LAN) to turn on the server specified in the **Server IP Address** field when packets are received on ports not specified in the **Application** screen. Note: For more information on Wake On LAN see Section 22.4 on page 255.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

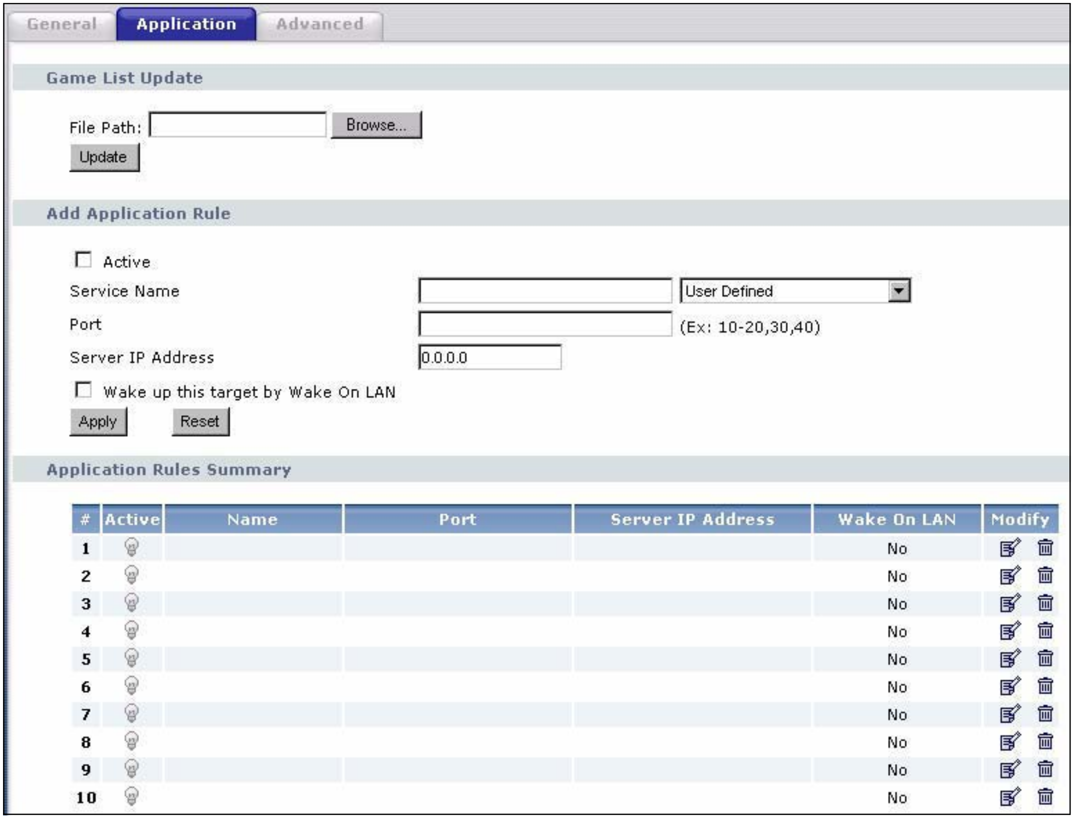
11.4 NAT Application Screen

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your NBG420N's port forwarding settings, click **Network** > **NAT** > **Application**. The screen appears as shown.

If you do not assign a **Default Server IP address** in the **NAT > General** screen, the NBG420N discards all packets received for ports that are not specified in this screen or remote management.

Refer to Appendix F on page 321 for port numbers commonly used for particular services.

Figure 91 Network > NAT > Application



Game List Update

File Path: Browse...

Update

Add Application Rule

☐ Active

Service Name | User Defined

Port (Ex: 10-20,30,40)

Server IP Address 0.0.0.0

☐ Wake up this target by Wake On LAN

Apply Reset

Application Rules Summary

#	Active	Name	Port	Server IP Address	Wake On LAN	Modify
1					No	
2					No	
3					No	
4					No	
5					No	
6					No	
7					No	
8					No	
9					No	
10					No	

The following table describes the labels in this screen.

Table 54 NAT Application

LABEL	DESCRIPTION
Game List Update	A game list includes the pre-defined service name(s) and port number(s). You can edit and upload it to the NBG420N to replace the existing entries in the second field next to **Service Name**.
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the.txt file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Update	Click **Update** to begin the upload process. This process may take up to two minutes.
Add Application Rule	
Active	Select the check box to enable this rule and the requested service can be forwarded to the host with a specified internal IP address. Clear the checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Service Name	Type a name (of up to 31 printable characters) to identify this rule in the first field next to **Service Name**. Otherwise, select a predefined service in the second field next to **Service Name**. The predefined service name and port number(s) will display in the **Service Name** and **Port** fields.

Table 54 NAT Application (continued)

LABEL	DESCRIPTION
Port	Type a port number(s) to be forwarded. To specify a range of ports, enter a hyphen (-) between the first port and the last port, such as 10-20. To specify two or more non-consecutive port numbers, separate them by a comma without spaces, such as 123,567.
Server IP Address	Type the inside IP address of the server that receives packets from the port(s) specified in the **Port** field.
Wake up this target by Wake On LAN	Select this to use WoL (Wake On LAN) to turn on the server specified in the **IP address** field when packets are received on the ports specified in the **Port** field. Note: For more information on Wake On LAN see Section 22.4 on page 255.
Apply	Click **Apply** to save your changes to the **Application Rules Summary** table.
Reset	Click **Reset** to not save and return your new changes in the **Service Name** and **Port** fields to the previous one.
Application Rules Summary	
#	This is the number of an individual port forwarding server entry.
Active	This icon is turned on when the rule is enabled.
Name	This field displays a name to identify this rule.
Port	This field displays the port number(s).
Server IP Address	This field displays the inside IP address of the server.
Wake On LAN	This field displays **No** when **Wake On LAN** is disabled and **Yes** when **Wake On LAN** is enabled.
Modify	Click the **Edit** icon to display and modify an existing rule setting in the fields under **Add Application Rule**. Click the **Remove** icon to delete a rule.

11.4.1 Game List Example

Here is an example game list text file. The index number, service name and associated port(s) are specified by semi-colons (no spaces). Use the name=xxx (where xxx is the service name) to create a new service. Port range can be separated with a hyphen (-) (no spaces). Multiple (non-consecutive) ports can be separated by commas.

Figure 92 Game List Example

```
version=1
1;name=Battlefield 1942;port=14567,22000,23000-23009,27900,28900
2;name=Call of Duty;port=28960
3;name=Civilization IV;port=2056
4;name=Diablo I and II;port=6112-6119,4000
5;name=Doom 3;port=27666
6;name=F.E.A.R;port=27888
7;name=Final Fantasy XI;port=25,80,110,443,50000-65535
8;name=Guild Wars;port=6112,80
9;name=Half Life;port=6003,7002,27005,27010,27011,27015
10;name=Jedi Knight III: Jedi Academy;port=28060-28062,28070-28081
11;name=Need for Speed: Hot Pursuit 2;port=1230,8511-
8512,27900,28900,61200-61230
12;name=Neverwinter Nights;port=5120-5300,6500,27900,28900
13;name=Quake 2;port=27910
14;name=Quake 3;port=27660,27960
15;name=Rainbow Six 3: Raven Shield;port=7777-7787,8777-8787
16;name=Serious Sam II;port=25600-25605
17;name=Silent Hunter III;port=17997-18003
18;name=Soldier of Fortune II;port=20100-20112
19;name=Starcraft;port=6112-6119,4000
20;name=Star Trek: Elite Force II;port=29250,29256
21;name=SWAT 4;port=10480-10483
22;name=Warcraft II and III;port=6112-6119,4000
23;name=World of Warcraft;port=3724
```

11.5 Trigger Port Forwarding

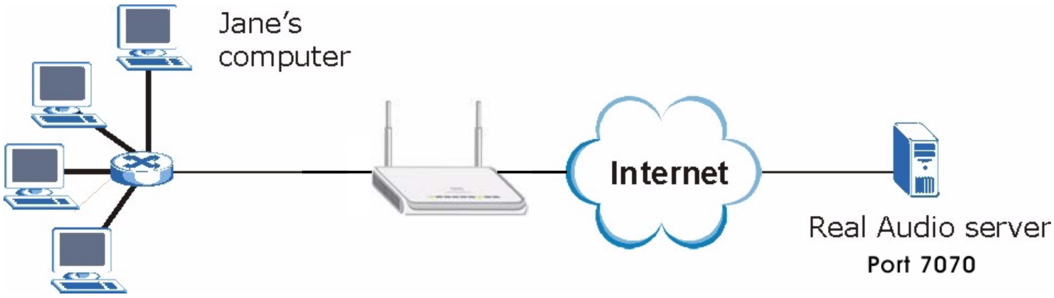
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The NBG420N records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the NBG420N's WAN port receives a response with a specific port number and protocol ("incoming" port), the NBG420N forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

11.5.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 93 Trigger Port Forwarding Process: Example



1. Jane requests a file from the Real Audio server (port 7070).
2. Port 7070 is a "trigger" port and causes the NBG420N to record Jane's computer IP address. The NBG420N associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The NBG420N forwards the traffic to Jane's computer IP address.
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The NBG420N times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

11.5.2 Two Points To Remember About Trigger Ports

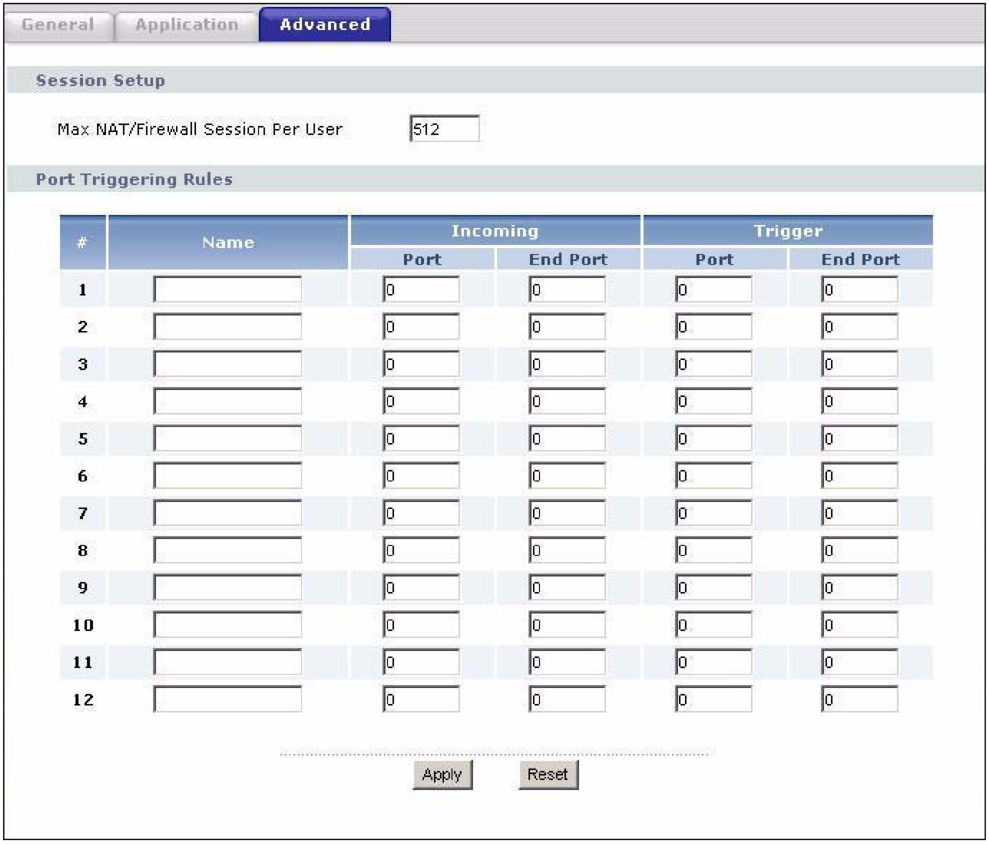
1. Trigger events only happen on data that is going coming from inside the NBG420N and going to the outside.
2. If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

11.6 NAT Advanced Screen

To change your NBG420N's trigger port settings, click **Network > NAT** > **Advanced**. The screen appears as shown.

Only one LAN computer can use a trigger port (range) at a time.

Figure 94 Network > NAT > Advanced



Session Setup

Max NAT/Firewall Session Per User: 512

Port Triggering Rules

#	Name	Incoming		Trigger	
		Port	End Port	Port	End Port
1		0	0	0	0
2		0	0	0	0
3		0	0	0	0
4		0	0	0	0
5		0	0	0	0
6		0	0	0	0
7		0	0	0	0
8		0	0	0	0
9		0	0	0	0
10		0	0	0	0
11		0	0	0	0
12		0	0	0	0

The following table describes the labels in this screen.

Table 55 Network > NAT > Advanced

LABEL	DESCRIPTION
Max NAT/Firewall Session Per User	Type a number ranging from 1 to 2048 to limit the number of NAT/firewall sessions that a host can create. When computers use peer to peer applications, such as file sharing applications, they may use a large number of NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet. Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/firewall sessions each client computer can establish through the NBG420N. If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using all of the available NAT sessions.
Port Triggering Rules	
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.

Table 55 Network > NAT > Advanced

LABEL	DESCRIPTION
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The NBG420N forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the NBG420N to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

12

Dynamic DNS

12.1 Dynamic DNS Introduction

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

12.1.1 DynDNS Wildcard

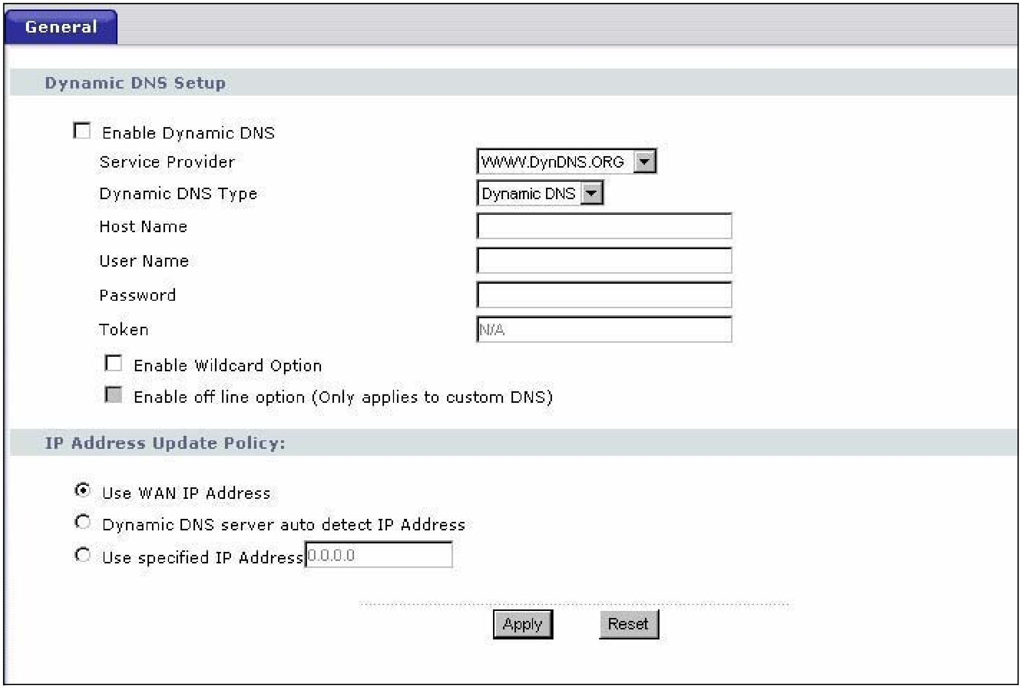
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

12.2 Dynamic DNS Screen

To change your NBG420N’s DDNS, click **Network** > **DDNS**. The screen appears as shown.

Figure 95 Dynamic DNS



Dynamic DNS Setup

☐ Enable Dynamic DNS

Service Provider: WWW.DynDNS.ORG

Dynamic DNS Type: Dynamic DNS

Host Name:

User Name:

Password:

Token: N/A

☐ Enable Wildcard Option

☐ Enable off line option (Only applies to custom DNS)

IP Address Update Policy:

● Use WAN IP Address

○ Dynamic DNS server auto detect IP Address

○ Use specified IP Address 0.0.0.0

The following table describes the labels in this screen.

Table 56 Dynamic DNS

LABEL	DESCRIPTION
Enable Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Enter a host names in the field provided. You can specify up to two host names in the field separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Token	Enter your client authorization key provided by the server to update DynDNS records. This field is configurable only when you select **WWW.REGFISH.COM** in the **Service Provider** field.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when **CustomDNS** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy:	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.
Dynamic DNS server auto detect IP Address	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.

Table 56 Dynamic DNS

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

PART III
Security

13

Firewall

This chapter gives some background information on firewalls and explains how to get started with the NBG420N's firewall.

13.1 Introduction to ZyXEL's Firewall

13.1.1 What is a Firewall?

Originally, the term "firewall" referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from a network that is not trusted. Of course, firewalls cannot solve every security problem. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

13.1.2 Stateful Inspection Firewall

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

13.1.3 About the NBG420N Firewall

The NBG420N firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The NBG420N's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG420N can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The NBG420N is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The NBG420N has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

13.1.4 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via web configurator.
2. Think about access control before you connect to the network in any way, including attaching a modem to the port.
3. Limit who can access your router.
4. Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

13.2 Triangle Routes

If an alternate gateway on the LAN has an IP address in the same subnet as the NBG420N’s LAN IP address, return traffic may not go through the NBG420N. This is called an asymmetrical or “triangle” route. This causes the NBG420N to reset the connection, as the connection has not been acknowledged.

You can have the NBG420N permit the use of asymmetrical route topology on the network (not reset the connection).

Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the NBG420N. A better solution is to use IP alias to put the NBG420N and the backup gateway on separate subnets.

13.2.1 Triangle Routes and IP Alias

You can use IP alias instead of allowing triangle routes. IP Alias allow you to partition your network into logical sections over the same interface.

By putting your LAN and Gateway **A** in different subnets, all returning network traffic must pass through the NBG420N to your LAN. The following steps describe such a scenario.

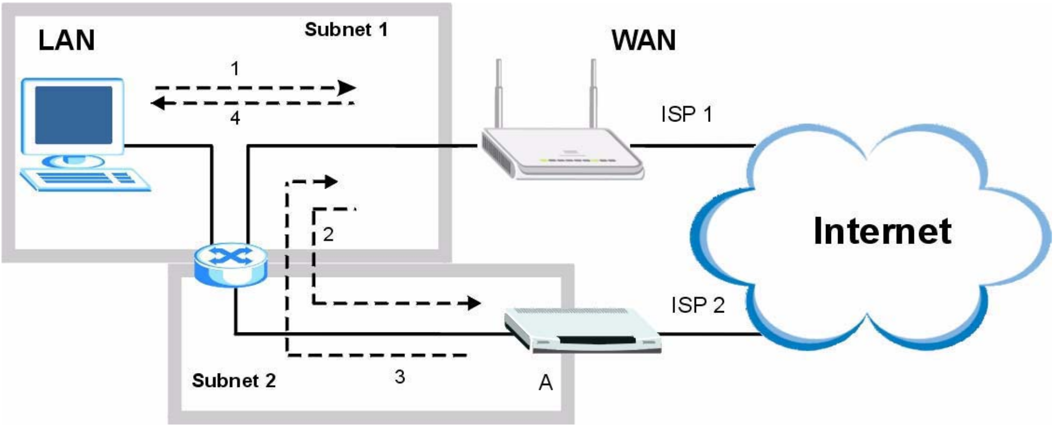
1 A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.

2 The NBG420N reroutes the packet to Gateway **A**, which is in **Subnet 2**.

3 The reply from the WAN goes to the NBG420N.

4 The NBG420N then sends it to the computer on the LAN in **Subnet 1**.

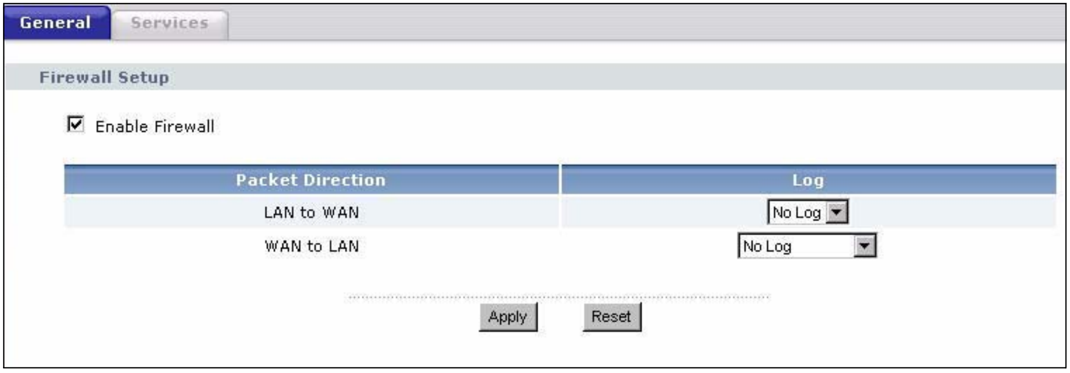
Figure 96 Using IP Alias to Solve the Triangle Route Problem



13.3 General Firewall Screen

Click **Security** > **Firewall** to open the **General** screen. Use this screen to enable or disable the NBG420N's firewall, and set up firewall logs.

Figure 97 Security > Firewall > General I



☑ Enable Firewall

Packet Direction	Log
LAN to WAN	No Log
WAN to LAN	No Log

The following table describes the labels in this screen.

Table 57 Security > Firewall > General

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The NBG420N performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Packet Direction	This is the direction of travel of packets. Firewall rules are grouped based on the direction of travel of packets to which they apply.

Table 57 Security > Firewall > General

LABEL	DESCRIPTION
Log	Select whether to create a log for packets that are traveling in the selected direction when the packets are blocked (**Log All**) or forwarded (**Log Forward**). Or select **Not Log** to not log any records. To log packets related to firewall rules, make sure that **Access Control** under **Log** is selected in the **Logs** > **Log Settings** screen.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

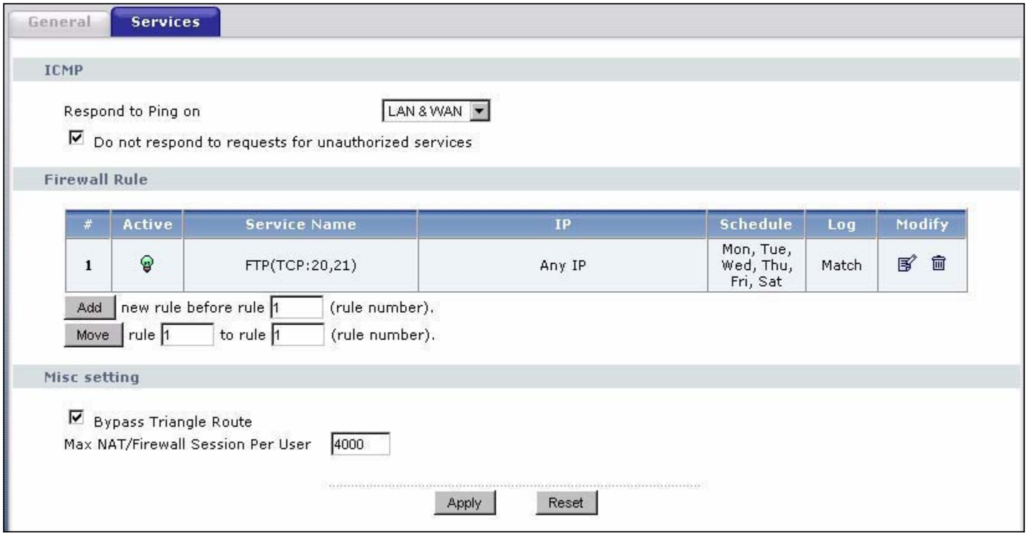
13.4 Services Screen

Click **Security** > **Firewall** > **Services**. The screen appears as shown next.

If an outside user attempts to probe an unsupported port on your NBG420N, an ICMP response packet is automatically returned. This allows the outside user to know the NBG420N exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your NBG420N when unsupported ports are probed.

You can also use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

Figure 98 Security > Firewall > Services



ICMP

Respond to Ping on: LAN & WAN

☑ Do not respond to requests for unauthorized services

Firewall Rule

#	Active	Service Name	IP	Schedule	Log	Modify
1	●	FTP(TCP:20,21)	Any IP	Mon, Tue, Wed, Thu, Fri, Sat	Match	✎ 🗑

Add new rule before rule 1 (rule number).

Move rule 1 to rule 1 (rule number).

Misc setting

☑ Bypass Triangle Route

Max NAT/Firewall Session Per User: 4000

The following table describes the labels in this screen.

Table 58 Security > Firewall > Services

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The NBG420N will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** to reply to all incoming LAN and WAN Ping requests.

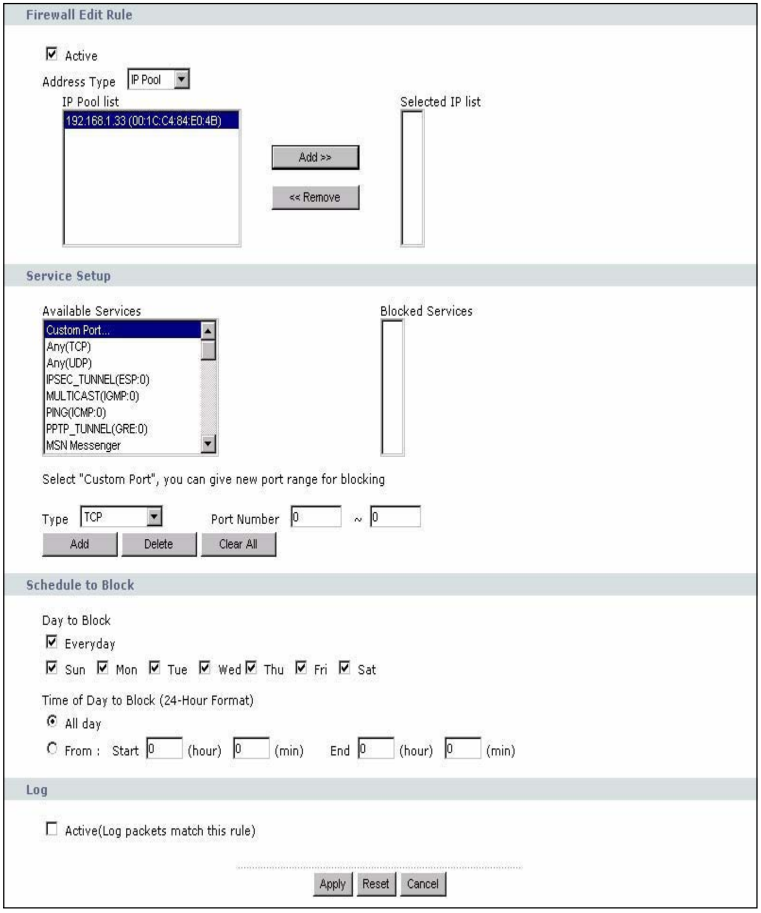
Table 58 Security > Firewall > Services

LABEL	DESCRIPTION
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the NBG420N by probing for unused ports. If you select this option, the NBG420N will not respond to port request(s) for unused ports, thus leaving the unused ports and the NBG420N unseen. By default this option is not selected and the NBG420N will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the NBG420N's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the NBG420N reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcprst rst [on|off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. Use the **Move** button to rearrange the order of the rules.
Active	This icon is green when the rule is turned on. The icon is grey when the rule is turned off.
Service Name	This field displays the services and port numbers to which this firewall rule applies.
IP	This field displays the IP address(es) the rule applies to.
Schedule	This field displays the days the firewall rule is active.
Log	This field shows you whether a log will be created when packets match the rule (**Match**) or not (**No**).
Modify	Click the **Edit** icon to modify an existing rule setting in the fields under the **Add Firewall Rule** screen. Click the **Remove** icon to delete a rule. Note that subsequent firewall rules move up by one when you take this action.
Add	Click the **Add** button to display the screen where you can configure a new firewall rule. Modify the number in the textbox to add the rule before a specific rule number.
Move	The **Move** button moves a rule to a different position. In the first text box enter the number of the rule you wish to move. In the second text box enter the number of the rule you wish to move the first rule to and click the **Move** button.
Misc setting	
Bypass Triangle Route	Select this check box to have the NBG420N firewall ignore the use of triangle route topology on the network.
Max NAT/Firewall Session Per User	Type a number ranging from 1 to 2048 to limit the number of NAT/firewall sessions that a host can create.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

13.4.1 The Add Firewall Rule Screen

If you click Add or the Modify icon on an existing rule, the Add Firewall Rule screen is displayed. Use this screen to add a firewall rule or to modify an existing one.

Figure 99 Security > Firewall > Services > Adding a Rule



Firewall Edit Rule

☑ Active

Address Type [IP Pool]

IP Pool list

192.168.1.33 (00:1C:C4:84:E0:4B)

Selected IP list

Service Setup

Available Services

- Custom Port...
- Any(TCP)
- Any(UDP)
- IPSEC_TUNNEL(ESP:0)
- MULTICAST(IGMP:0)
- PING(ICMP:0)
- PPTP_TUNNEL(GRE:0)
- MSN Messenger

Blocked Services

Select "Custom Port", you can give new port range for blocking

Type [TCP] Port Number [0] ~ [0]

Schedule to Block

Day to Block

☑ Everyday

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time of Day to Block (24-Hour Format)

● All day

○ From : Start [0] (hour) [0] (min) End [0] (hour) [0] (min)

Log

□ Active(Log packets match this rule)

The following table describes the labels in this screen.

Table 59 Security > Firewall > Services > Adding a Rule

LABEL	DESCRIPTION
Active	Select this check box to turn the rule on.
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50), a pool of IP address or any IP address? Select an option from the drop-down list box that includes: **Any IP**, **Single IP**, **IP Range** and **IP Pool**.
IP Address	Enter the single IP address here. This field is only available when **Single IP** is selected as the **Address Type**.
Start IP Address	Enter the starting IP address in a range here. This field is only available when **IP Range** is selected as the **Address Type**.
End IP Address	Enter the ending IP address in a range here. This field is only available when **IP Range** is selected as the **Address Type**.
IP Pool List	Add an IP address from the **IP Pool List** to the **Selected IP List** by highlighting an IP address and clicking **Add**. To delete an IP address from the Selected IP List highlight an IP address and click the **Remove** button. These fields are only available when **IP Pool** is selected as the **Address Type**. The IP Pool list gathers its IPs from entries in the ARP table. The ARP table contains the IP addresses and MAC addresses of the devices that have sent traffic to the NBG420N.
Service Setup	

Table 59 Security > Firewall > Services > Adding a Rule

LABEL	DESCRIPTION
Available Services	This is a list of pre-defined services (ports) you may prohibit your LAN computers from using. Select the port you want to block using the drop-down list and click **Add** to add the port to the **Blocked Services** field.
Blocked Services	This is a list of services (ports) that will be inaccessible to computers on your LAN once you enable service blocking.
Custom Port	A custom port is a service that is not available in the pre-defined **Available Services** list and you must define using the next two fields.
Type	Choose the IP port (**TCP** or **UDP**) that defines your customized port from the drop down list box.
Port Number	Enter the port number range that defines the service. For example, if you want to define the Gnutella service, then select **TCP** type and enter a port range from 6345 to 6349.
Add	Select a service from the **Available Services** drop-down list and then click **Add** to add a service to the **Blocked Services**
Delete	Select a service from the **Blocked Services** list and then click **Delete** to remove this service from the list.
Clear All	Click **Clear All** to empty the **Blocked Services**.
Schedule to Block	
Day to Block:	Select a check box to configure which days of the week (or everyday) you want service blocking to be active.
Time of Day to Block (24-Hour Format)	Select the time of day you want service blocking to take effect. Configure blocking to take effect all day by selecting **All Day**. You can also configure specific times by selecting **From** and entering the start time in the **Start (hour)** and **Start (min)** fields and the end time in the **End (hour)** and **End (min)** fields. Enter times in 24-hour format, for example, "3:00pm" should be entered as "15:00".
Log	
Active (Log packets match this rule)	Select this to log packets that match this rule. Go to the **Log Settings** page and select the **Access Control** logs category to have the NBG420N record these logs.
Misc setting	
Bypass Triangle Route	Select this check box to have the NBG420N firewall ignore the use of triangle route topology on the network.
Max NAT/Firewall Session Per User	Type a number ranging from 1 to 2048 to limit the number of NAT/firewall sessions that a host can create.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.
Cancel	Click **Cancel** to return to the **Services** screen without saving any changes.

14

Content Filtering

This chapter provides a brief overview of content filtering using the embedded web GUI.

14.1 Introduction to Content Filtering

Internet content filtering allows you to create and enforce Internet access policies tailored to your needs. Content filtering is the ability to block certain web features or specific URL keywords.

14.2 Restrict Web Features

The NBG420N can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.

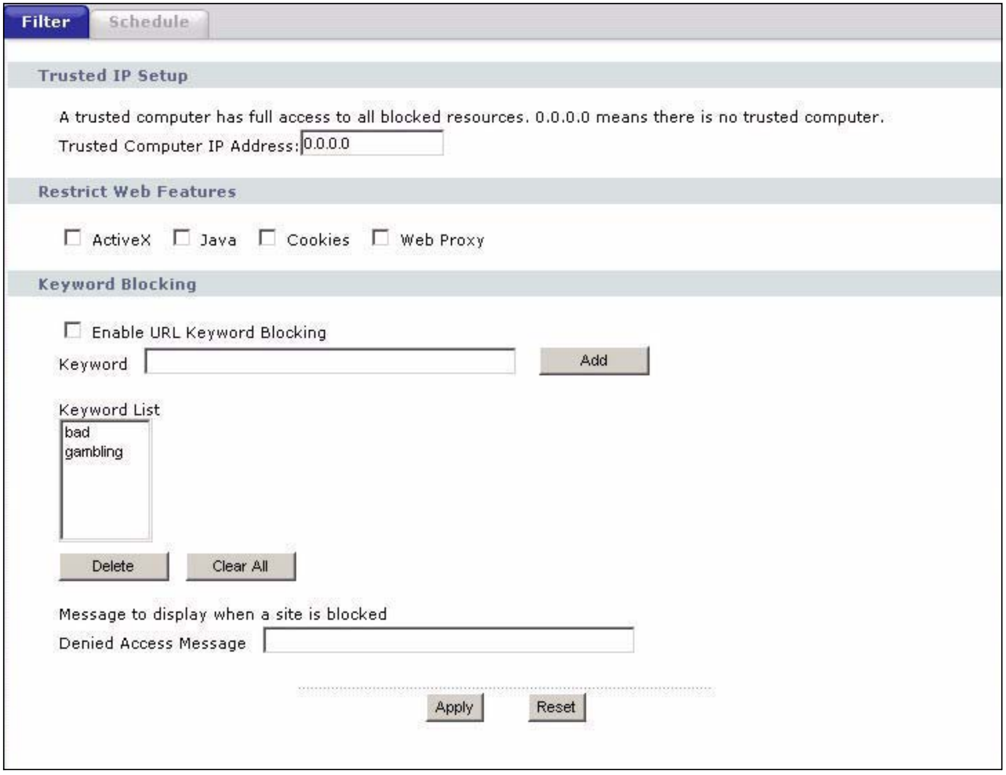
14.3 Days and Times

The NBG420N also allows you to define time periods and days during which the NBG420N performs content filtering.

14.4 Filter Screen

Click **Security** > **Content Filter** to open the **Filter** screen.

Figure 100 Security > Content Filter > Filter



A trusted computer has full access to all blocked resources. 0.0.0.0 means there is no trusted computer.

Trusted Computer IP Address: 0.0.0.0

□ ActiveX □ Java □ Cookies □ Web Proxy

□ Enable URL Keyword Blocking

bad
gambling

Message to display when a site is blocked

The following table describes the labels in this screen.

Table 60 Security > Content Filter > Filter

LABEL	DESCRIPTION
Trusted Computer IP Address	To enable this feature, type an IP address of any one of the computers in your network that you want to have as a trusted computer. This allows the trusted computer to have full access to all features that are configured to be blocked by content filtering. Leave this field blank to have no trusted computers.
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Keyword Blocking	
Enable URL Keyword Blocking	The NBG420N can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL http://www.website.com/bad.html would be blocked. Select this check box to enable this feature.

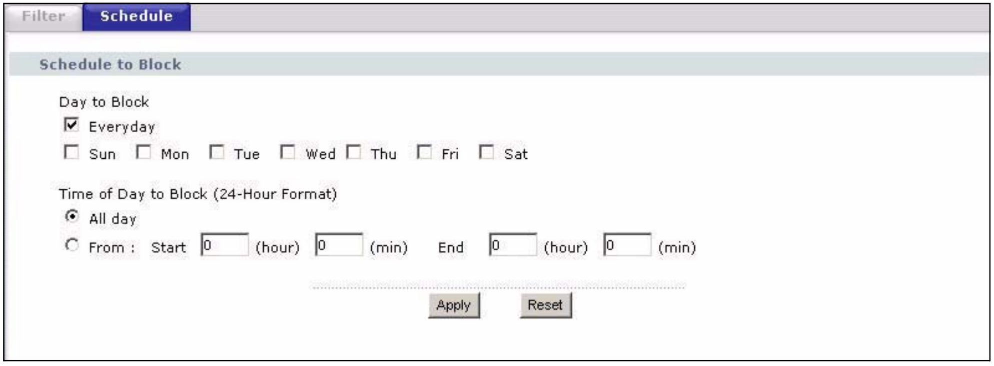
Table 60 Security > Content Filter > Filter

LABEL	DESCRIPTION
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.
Add	Click **Add** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click **Delete** to remove it. The keyword disappears from the text box after you click **Apply**.
Clear All	Click this button to remove all of the listed keywords.
Denied Access Message	Enter a message to be displayed when a user tries to access a restricted web site. The default message is “Please contact your network administrator!!”
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh

14.5 Schedule

Use this screen to set the day(s) and time you want the NBG420N to use content filtering. Click **Security** > **Content Filter** > **Schedule**. The following screen displays.

Figure 101 Security > Content Filter > Schedule



Schedule to Block

Day to Block

☑ Everyday

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Time of Day to Block (24-Hour Format)

● All day

○ From : Start 0 (hour) 0 (min) End 0 (hour) 0 (min)

The following table describes the labels in this screen.

Table 61 Security > Content Filter > Schedule

LABEL	DESCRIPTION
Day to Block	Select check boxes for the days that you want the NBG420N to perform content filtering. Select the **Everyday** check box to have content filtering turned on all days of the week.
Time of Day to Block (24-Hour Format)	**Time of Day to Block** allows the administrator to define during which time periods content filtering is enabled. **Time of Day to Block** restrictions only apply to the keywords (see above). Restrict web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected. Select **All Day** to have content filtering always active on the days selected in **Day to Block** with time of day limitations not enforced. Select **From** and enter the time period, in 24-hour format, during which content filtering will be enforced.

Table 61 Security > Content Filter > Schedule

LABEL	DESCRIPTION
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh

14.6 Customizing Keyword Blocking URL Checking

You can use commands to set how much of a website's URL the content filter is to check for keyword blocking. See the appendices for information on how to access and use the command interpreter.

14.6.1 Domain Name or IP Address URL Checking

By default, the NBG420N checks the URL's domain name or IP address when performing keyword blocking.

This means that the NBG420N checks the characters that come before the first slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, content filtering only searches for keywords within www.zyxel.com.tw.

14.6.2 Full Path URL Checking

Full path URL checking has the NBG420N check the characters that come before the last slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, full path URL checking searches for keywords within www.zyxel.com.tw/news/.

Use the `ip urlfilter customize actionFlags 6 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's full path.

14.6.3 File Name URL Checking

Filename URL checking has the NBG420N check all of the characters in the URL.

For example, filename URL checking searches for keywords within the URL www.zyxel.com.tw/news/pressroom.php.

Use the `ip urlfilter customize actionFlags 8 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's complete filename.

15

IPSec VPN

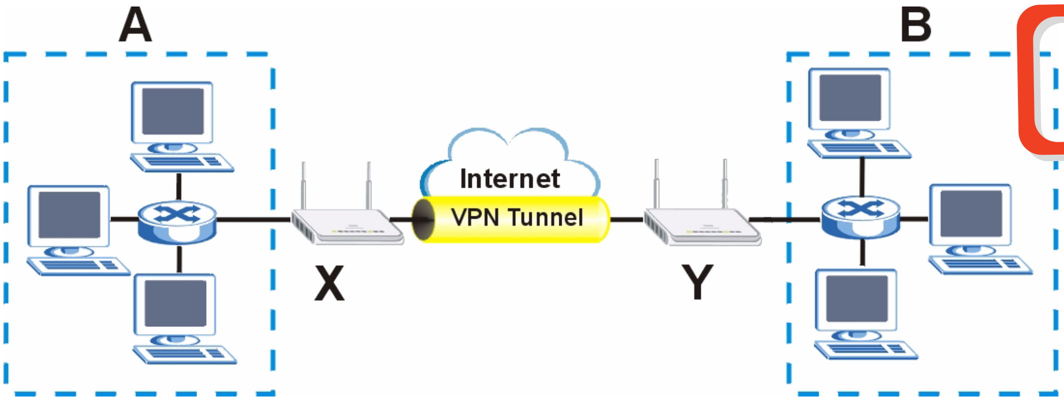
15.1 IPSec VPN Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

The following figure provides one perspective of a VPN tunnel.

Figure 102 IPSec VPN: Overview



The VPN tunnel connects the NBG420N (**X**) and the remote IPSec router (**Y**). These routers then connect the local network (**A**) and remote network (**B**).

15.1.1 What You Can Do in the IPSec VPN Screens

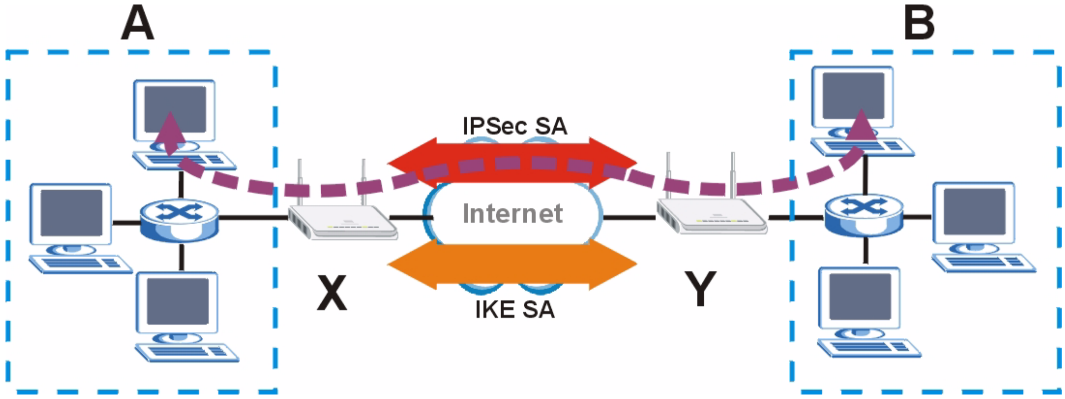
Use the **General** Screen (Section 15.2 on page 167) to display and manage the NBG420N's VPN rules (tunnels).

Use the **SA Monitor** Screen (Section 15.3 on page 183) to display and manage active VPN connections.

15.1.2 What You Need To Know About IPSec VPN

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the NBG420N and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the NBG420N and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the NBG420N and remote IPSec router can send data between computers on the local network and remote network. The following figure illustrates this.

Figure 103 VPN: IKE SA and IPSec SA



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is established securely using the IKE SA that routers **X** and **Y** established first.

15.1.3 IKE SA (IKE Phase 1) Overview

The IKE SA provides a secure connection between the NBG420N and remote IPSec router.

It takes several steps to establish an IKE SA. The negotiation mode determines the number of steps to use. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Note: Both routers must use the same negotiation mode.

These modes are discussed in more detail in Negotiation Mode on page 187. Main mode is used in various examples in the rest of this section.

15.1.3.1 IP Addresses of the NBG420N and Remote IPSec Router

In the NBG420N, you have to specify the IP addresses of the NBG420N and the remote IPSec router to establish an IKE SA.

You can usually provide a static IP address or a domain name for the NBG420N. Sometimes, your NBG420N might also offer another alternative, such as using the IP address of a port or interface.

You can usually provide a static IP address or a domain name for the remote IPSec router as well. Sometimes, you might not know the IP address of the remote IPSec router (for example, telecommuters). In this case, you can still set up the IKE SA, but only the remote IPSec router can initiate an IKE SA.

15.1.4 IPSec SA (IKE Phase 2) Overview

Once the NBG420N and remote IPSec router have established the IKE SA, they can securely negotiate an IPSec SA through which to send data between computers on the networks.

Note: The IPSec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of an IPSec SA.

15.1.4.1 Local Network and Remote Network

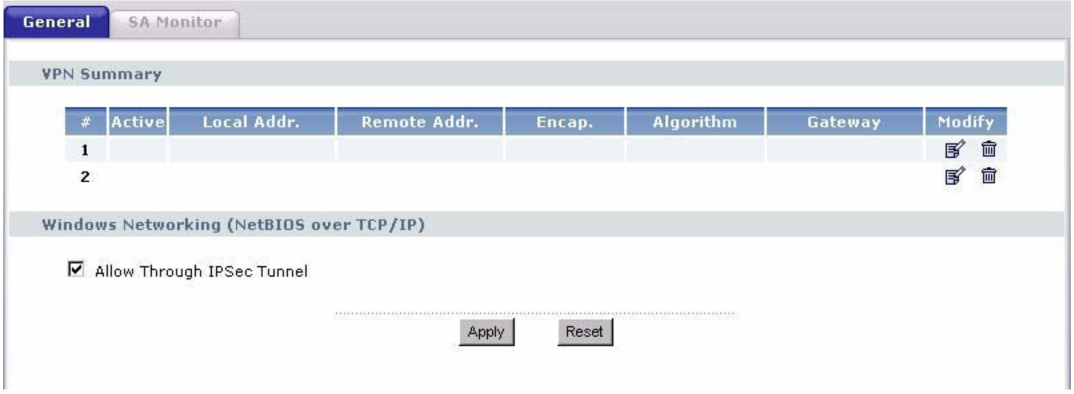
In an IPSec SA, the local network consists of devices connected to the NBG420N and may be called the local policy. Similarly, the remote network consists of the devices connected to the remote IPSec router and may be called the remote policy.

Note: It is not recommended to set a VPN rule's local and remote network settings both to 0.0.0.0 (any). This causes the NBG420N to try to forward all access attempts (to the local network, the Internet or even the NBG420N) to the remote IPSec router. In this case, you can no longer manage the NBG420N.

15.2 The General Screen

Click **Security** > **VPN** to display the **Summary** screen. This is a read-only menu of your VPN rules (tunnels). Edit a VPN rule by clicking the **Edit** icon.

Figure 104 Security > VPN > General



VPN Summary

#	Active	Local Addr.	Remote Addr.	Encap.	Algorithm	Gateway	Modify
1							✎ 🗑
2							✎ 🗑

Windows Networking (NetBIOS over TCP/IP)

☑ Allow Through IPSec Tunnel

The following table describes the fields in this screen.

Table 62 Security > VPN > General

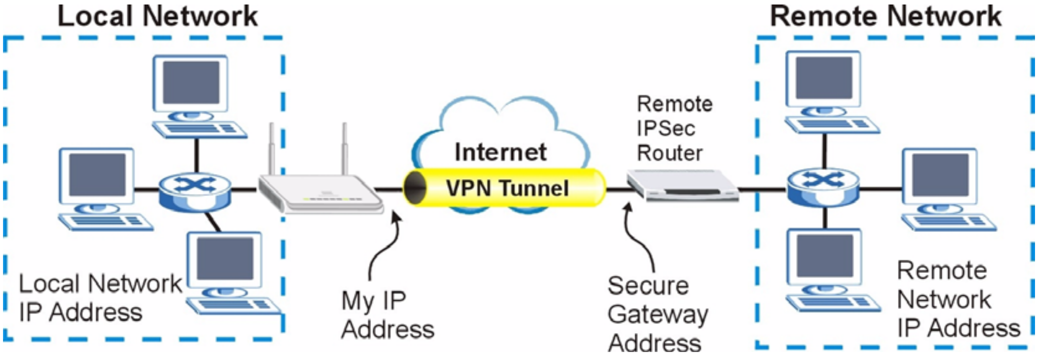
LABEL	DESCRIPTION
#	This is the VPN policy index number.
Active	This field displays whether the VPN policy is active or not. This icon is turned on when the rule is enabled.
Local Addr.	This displays the beginning and ending (static) IP addresses or a (static) IP address and a subnet mask of computer(s) on your local network behind your NBG420N.
Remote Addr.	This displays the beginning and ending (static) IP addresses or a (static) IP address and a subnet mask of computer(s) on the remote network behind the remote IPSec router. This field displays **0.0.0.0** when the **Secure Gateway Address** field displays **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN.
Encap.	This field displays **Tunnel** or **Transport** mode (**Tunnel** is the default selection).
Algorithm	This field displays the security protocol, encryption algorithm and authentication algorithm used for an SA.
Gateway	This is the static WAN IP address or URL of the remote IPSec router. This field displays **0.0.0.0** when you configure the **Secure Gateway Address** field in the **Rule Setup** screen to **0.0.0.0.**
Modify	Click the **Edit** icon to go to the screen where you can edit the VPN rule. Click the **Remove** icon to remove an existing VPN rule.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.
Allow NetBIOS Traffic Through IPSec Tunnel	Select this check box to send NetBIOS packets through the VPN connection.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

15.2.1 VPN Rule Setup (Basic)

Click the **Edit** icon in the **General** screen to display the **Rule Setup** screen.

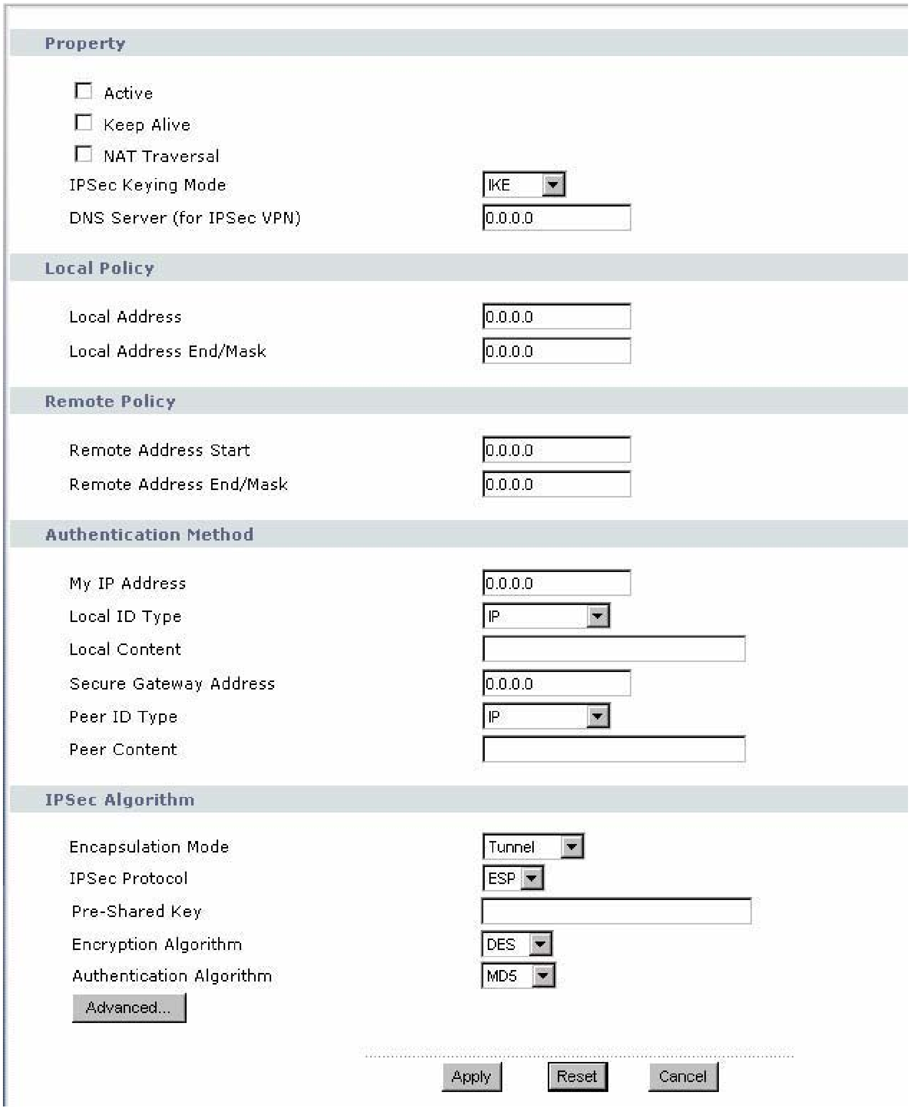
This figure helps explain the main fields.

Figure 105 IPSec Fields Summary



Use this screen to configure a VPN rule.

Figure 106 Security > VPN > General > Rule Setup: IKE (Basic)



Property

□ Active

□ Keep Alive

□ NAT Traversal

IPSec Keying Mode	IKE
DNS Server (for IPSec VPN)	0.0.0.0

Local Policy

Local Address	0.0.0.0
Local Address End/Mask	0.0.0.0

Remote Policy

Remote Address Start	0.0.0.0
Remote Address End/Mask	0.0.0.0

Authentication Method

My IP Address	0.0.0.0
Local ID Type	IP
Local Content	
Secure Gateway Address	0.0.0.0
Peer ID Type	IP
Peer Content	

IPSec Algorithm

Encapsulation Mode	Tunnel
IPSec Protocol	ESP
Pre-Shared Key	
Encryption Algorithm	DES
Authentication Algorithm	MD5

The following table describes the labels in this screen.

Table 63 SECURITY > VPN > Rule Setup: IKE (Basic)

LABEL	DESCRIPTION
Property	
Active	Select this check box to activate this VPN policy.
Keep Alive	Select this check box to have the NBG420N automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
NAT Traversal	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers. **Note:** The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP ports 500 and 4500 to the IPSec router behind the NAT router.
IPSec Keying Mode	Select **IKE** or **Manual** from the drop-down list box. **IKE** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The NBG420N assigns this additional DNS server to the NBG420N's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local Policy	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
Local Address	For a single IP address, enter a (static) IP address on the LAN behind your NBG420N. For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on your LAN behind your NBG420N. To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the LAN behind your NBG420N.
Local Address End /Mask	When the local IP address is a single address, type it a second time here. When the local IP address is a range, enter the end (static) IP address, in a range of computers on the LAN behind your NBG420N. When the local IP address is a subnet address, enter a subnet mask on the LAN behind your NBG420N.

Table 63 SECURITY > VPN > Rule Setup: IKE (Basic) (continued)

LABEL	DESCRIPTION
Remote Policy	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the **Secure Gateway IP Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address	For a single IP address, enter a (static) IP address on the network behind the remote IPSec router. For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the network behind the remote IPSec router.
Remote Address End /Mask	When the remote IP address is a single address, type it a second time here. When the remote IP address is a range, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the remote IP address is a subnet address, enter a subnet mask on the network behind the remote IPSec router.
Authentication Method	
My IP Address	Enter the NBG420N's static WAN IP address (if it has one) or leave the field set to **0.0.0.0**. The NBG420N uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. If the WAN connection goes down, the NBG420N uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. Otherwise, you can enter one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the NBG420N use that dynamic domain name's IP address. The VPN tunnel has to be rebuilt if **My IP Address** changes after setup.
Local ID Type	Select **IP** to identify this NBG420N by its IP address. Select **Domain Name** to identify this NBG420N by a domain name. Select **E-mail** to identify this NBG420N by an e-mail address.
Local Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the **Local Content** field. The NBG420N automatically uses the IP address in the **My IP Address** field (refer to the **My IP Address** field description) if you configure the **Local Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the **Local Content** field or use the **Domain Name** or **E-mail** ID type in the following situations. • When there is a NAT router between the two IPSec routers. • When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **Domain Name** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this NBG420N in the **Local Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.

Table 63 SECURITY > VPN > Rule Setup: IKE (Basic) (continued)

LABEL	DESCRIPTION
Secure Gateway Address	Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address (the **IPSec Keying Mode** field must be set to **IKE**). In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**. **Note:** You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The NBG420N has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **Domain Name** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Peer Content	The configuration of the peer content depends on the peer ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the NBG420N will use the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description). For **Domain Name** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than **0.0.0.0** or use the **Domain Name** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the NBG420N to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.
IPSec Algorithm	
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
IPSec Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase processing requirements and communications latency (delay). If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below).

Table 63 SECURITY > VPN > Rule Setup: IKE (Basic) (continued)

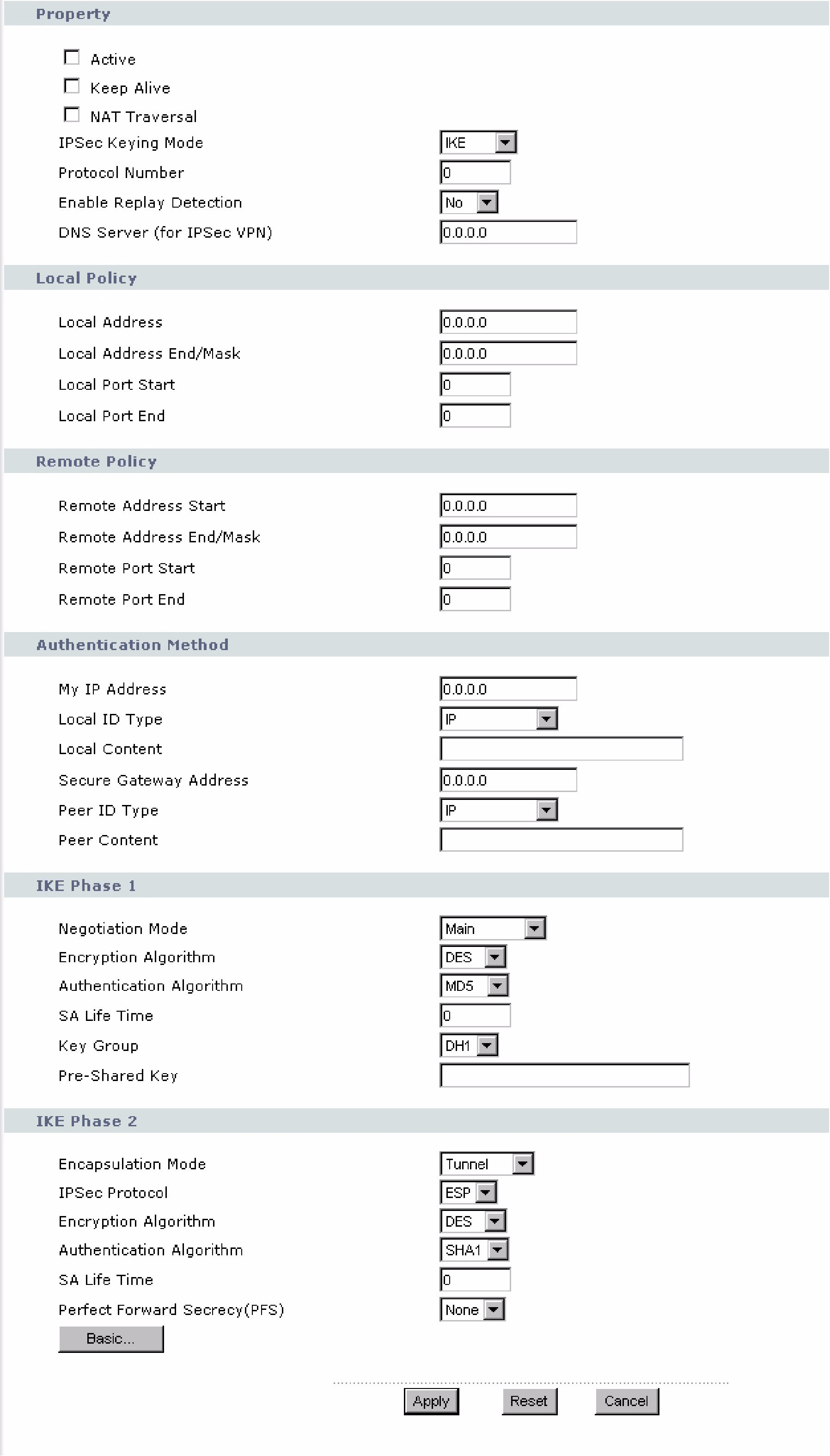
LABEL	DESCRIPTION
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a “PYLD_MALFORMED” (payload malformed) packet if the same pre-shared key is not used on both ends.
Encryption Algorithm	Select which key size and encryption algorithm to use for data communications. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm The NBG420N and the remote IPSec router must use the same algorithms and key , which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
Advanced...	Click **Advanced...** to configure more detailed settings of your IKE key management.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.
Cancel	Click **Cancel** to exit the screen without making any changes.

15.2.2 VPN Rule Setup (Advanced)

Click the **Advanced...** button in the **Rule Setup** screen to open this screen.

Use this screen to configure a VPN rule.

Figure 107 Security > VPN > General > Rule Setup: IKE (Advanced)



Property

□ Active	
□ Keep Alive	
□ NAT Traversal	
IPSec Keying Mode	IKE
Protocol Number	0
Enable Replay Detection	No
DNS Server (for IPSec VPN)	0.0.0.0

Local Policy

Local Address	0.0.0.0
Local Address End/Mask	0.0.0.0
Local Port Start	0
Local Port End	0

Remote Policy

Remote Address Start	0.0.0.0
Remote Address End/Mask	0.0.0.0
Remote Port Start	0
Remote Port End	0

Authentication Method

My IP Address	0.0.0.0
Local ID Type	IP
Local Content	
Secure Gateway Address	0.0.0.0
Peer ID Type	IP
Peer Content	

IKE Phase 1

Negotiation Mode	Main
Encryption Algorithm	DES
Authentication Algorithm	MD5
SA Life Time	0
Key Group	DH1
Pre-Shared Key	

IKE Phase 2

Encapsulation Mode	Tunnel
IPSec Protocol	ESP
Encryption Algorithm	DES
Authentication Algorithm	SHA1
SA Life Time	0
Perfect Forward Secrecy(PFS)	None

The following table describes the labels in this screen.

Table 64 Security > VPN > Rule Setup: IKE (Advanced)

LABEL	DESCRIPTION
Property	
Active	Select this check box to activate this VPN policy.
Keep Alive	Select this check box to have the NBG420N automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
NAT Traversal	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers. **Note:** The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP ports 500 and 4500 to the IPSec router behind the NAT router.
IPSec Keying Mode	Select **IKE** or **Manual** from the drop-down list box. **IKE** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
Protocol Number	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Select **Yes** from the drop-down menu to enable replay detection, or select **No** to disable it.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The NBG420N assigns this additional DNS server to the NBG420N's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local Policy	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
Local Address	For a single IP address, enter a (static) IP address on the LAN behind your NBG420N. For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on your LAN behind your NBG420N. To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the LAN behind your NBG420N.

Table 64 Security > VPN > Rule Setup: IKE (Advanced) (continued)

LABEL	DESCRIPTION
Local Address End / Mask	When the local IP address is a single address, type it a second time here. When the local IP address is a range, enter the end (static) IP address, in a range of computers on the LAN behind your NBG420N. When the local IP address is a subnet address, enter a subnet mask on the LAN behind your NBG420N.
Local Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Local Port End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Local Port Start** is left at 0, **Local Port End** will also remain at 0.
Remote Policy	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the **Secure Gateway IP Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address	For a single IP address, enter a (static) IP address on the network behind the remote IPSec router. For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the network behind the remote IPSec router.
Remote Address End /Mask	When the remote IP address is a single address, type it a second time here. When the remote IP address is a range, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the remote IP address is a subnet address, enter a subnet mask on the network behind the remote IPSec router.
Remote Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Remote Port End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Remote Port Start** is left at 0, **Remote Port End** will also remain at 0.
Authentication Method	
My IP Address	Enter the NBG420N's static WAN IP address (if it has one) or leave the field set to **0.0.0.0**. The NBG420N uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. If the WAN connection goes down, the NBG420N uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. Otherwise, you can enter one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the NBG420N use that dynamic domain name's IP address. The VPN tunnel has to be rebuilt if **My IP Address** changes after setup.
Local ID Type	Select **IP** to identify this NBG420N by its IP address. Select **Domain Name** to identify this NBG420N by a domain name. Select **E-mail** to identify this NBG420N by an e-mail address.

Table 64 Security > VPN > Rule Setup: IKE (Advanced) (continued)

LABEL	DESCRIPTION
Local Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the **Local Content** field. The NBG420N automatically uses the IP address in the **My IP Address** field (refer to the **My IP Address** field description) if you configure the **Local Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the **Local Content** field or use the **Domain Name** or **E-mail** ID type in the following situations. • When there is a NAT router between the two IPSec routers. • When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **Domain Name** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this NBG420N in the **Local Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Secure Gateway Address	Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address (the **IPSec Keying Mode** field must be set to **IKE**). In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**. **Note:** You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The NBG420N has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **Domain Name** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Peer Content	The configuration of the peer content depends on the peer ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the NBG420N will use the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description). For **Domain Name** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than **0.0.0.0** or use the **Domain Name** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the NBG420N to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.

Table 64 Security > VPN > Rule Setup: IKE (Advanced) (continued)

LABEL	DESCRIPTION
IKE Phase 1	
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm The NBG420N and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data in the IKE SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 180 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	Select which Diffie-Hellman key group (DH*x*) you want to use for encryption keys. Choices are: **DH1** - use a 768-bit random number **DH2** - use a 1024-bit random number
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x” (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a “PYLD_MALFORMED” (payload malformed) packet if the same pre-shared key is not used on both ends.
IKE Phase 2	
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode.
IPSec Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase processing requirements and communications latency (delay). If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below).
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm The NBG420N and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.

Table 64 Security > VPN > Rule Setup: IKE (Advanced) (continued)

LABEL	DESCRIPTION
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
SA Life Time	Define the length of time before an IPSec SA automatically renegotiates in this field. The minimum value is 180 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secrecy (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: **None** - disable PFS **DH1** - enable PFS and use a 768-bit random number **DH2** - enable PFS and use a 1024-bit random number PFS changes the root key that is used to generate encryption keys for each IPSec SA. It is more secure but takes more time.
Basic...	Click **Basic...** to go to the previous VPN configuration screen.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to begin configuring this screen afresh.
Cancel	Click **Cancel** to exit the screen without making any changes.

15.2.3 VPN Rule Setup (Manual)

Use this screen to configure VPN rules (tunnels) that use manual keys. Manual key management is useful if you have problems with IKE key management.

Select **Manual** in the **IPSec Keying Mode** field on the **Rule Setup** screen to open the screen as shown in Figure 108 on page 180.

15.2.3.1 IPSec SA Using Manual Keys

You might set up an IPSec SA using manual keys when you want to establish a VPN tunnel quickly, for example, for troubleshooting. You should only do this as a temporary solution, however, because it is not as secure as a regular IPSec SA.

In IPSec SAs using manual keys, the NBG420N and remote IPSec router do not establish an IKE SA. They only establish an IPSec SA. As a result, an IPSec SA using manual keys has some characteristics of IKE SA and some characteristics of IPSec SA. There are also some differences between IPSec SA using manual keys and other types of SA.

15.2.3.2 IPSec SA Proposal Using Manual Keys

In IPSec SA using manual keys, you can only specify one encryption algorithm and one authentication algorithm. There is no DH key exchange, so you have to provide the encryption key and the authentication key the NBG420N and remote IPSec router use.

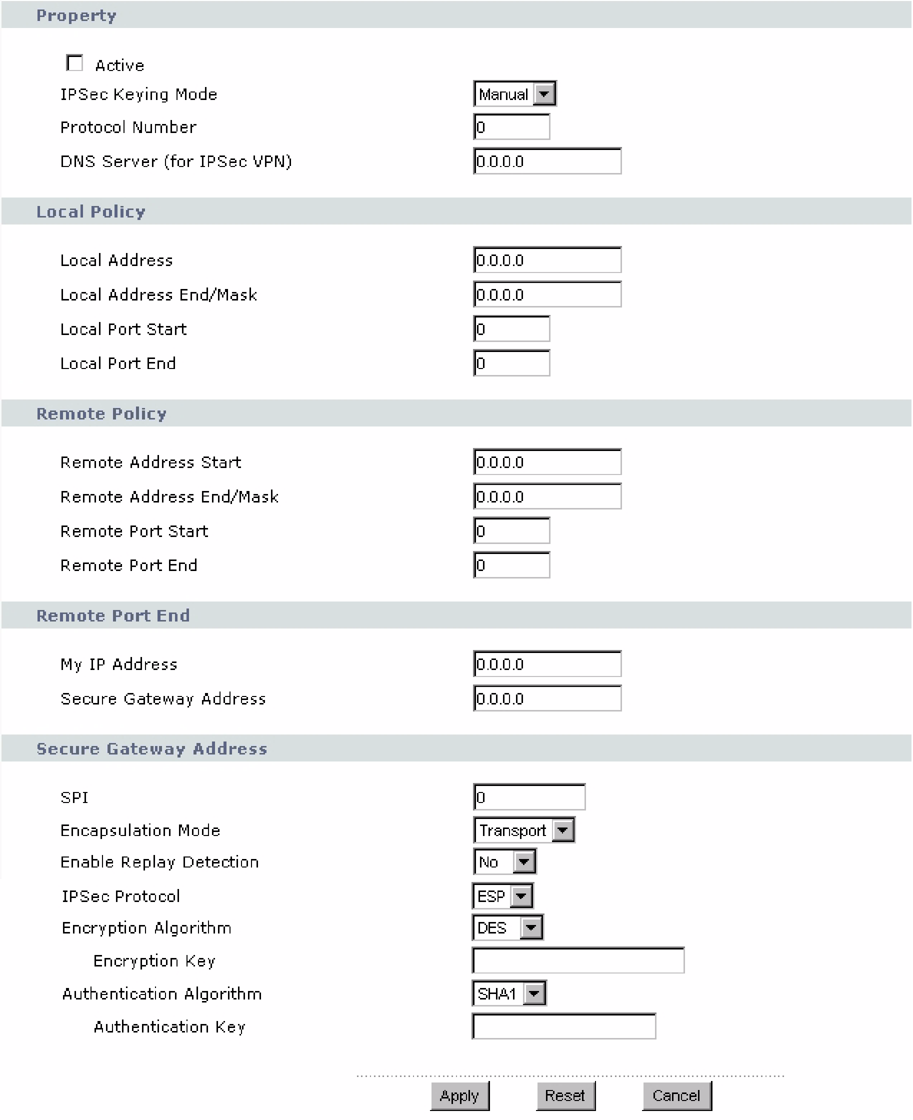
Note: The NBG420N and remote IPSec router must use the same encryption key and authentication key.

15.2.3.3 Authentication and the Security Parameter Index (SPI)

For authentication, the NBG420N and remote IPSec router use the SPI, instead of pre-shared keys, ID type and content. The SPI is an identification number.

Note: The NBG420N and remote IPSec router must use the same SPI.

Figure 108 Security > VPN > General > Rule Setup: Manual



Property

□ Active	
IPSec Keying Mode	Manual
Protocol Number	0
DNS Server (for IPSec VPN)	0.0.0.0

Local Policy

Local Address	0.0.0.0
Local Address End/Mask	0.0.0.0
Local Port Start	0
Local Port End	0

Remote Policy

Remote Address Start	0.0.0.0
Remote Address End/Mask	0.0.0.0
Remote Port Start	0
Remote Port End	0

Remote Port End

My IP Address	0.0.0.0
Secure Gateway Address	0.0.0.0

Secure Gateway Address

SPI	0
Encapsulation Mode	Transport
Enable Replay Detection	No
IPSec Protocol	ESP
Encryption Algorithm	DES
Encryption Key	
Authentication Algorithm	SHA1
Authentication Key	

The following table describes the labels in this screen.

Table 65 Security > VPN > Rule Setup: Manual

LABEL	DESCRIPTION
Property	
Active	Select this check box to activate this VPN policy.

Table 65 Security > VPN > Rule Setup: Manual (continued)

LABEL	DESCRIPTION
IPSec Keying Mode	Select **IKE** or **Manual** from the drop-down list box. **IKE** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
Protocol Number	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The NBG420N assigns this additional DNS server to the NBG420N's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local Policy	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN’s full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
Local Address	For a single IP address, enter a (static) IP address on the LAN behind your NBG420N. For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on your LAN behind your NBG420N. To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the LAN behind your NBG420N.
Local Address End /Mask	When the local IP address is a single address, type it a second time here. When the local IP address is a range, enter the end (static) IP address, in a range of computers on the LAN behind your NBG420N. When the local IP address is a subnet address, enter a subnet mask on the LAN behind your NBG420N.
Local Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Local Port End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Local Port Start** is left at 0, **Local Port End** will also remain at 0.
Remote Policy	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the **Secure Gateway IP Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.

Table 65 Security > VPN > Rule Setup: Manual (continued)

LABEL	DESCRIPTION
Remote Address	For a single IP address, enter a (static) IP address on the network behind the remote IPSec router. For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the network behind the remote IPSec router.
Remote Address End /Mask	When the remote IP address is a single address, type it a second time here. When the remote IP address is a range, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the remote IP address is a subnet address, enter a subnet mask on the network behind the remote IPSec router.
Remote Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Remote Port End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Remote Port Start** is left at 0, **Remote Port End** will also remain at 0.
My IP Address	Enter the NBG420N's static WAN IP address (if it has one) or leave the field set to **0.0.0.0**. The NBG420N uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. If the WAN connection goes down, the NBG420N uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. Otherwise, you can enter one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the NBG420N use that dynamic domain name's IP address. The VPN tunnel has to be rebuilt if **My IP Address** changes after setup.
Secure Gateway Address	Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address (the **IPSec Keying Mode** field must be set to **IKE**). In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**. **Note:** You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The NBG420N has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).
SPI	Type a unique **SPI** (Security Parameter Index) from one to four characters long. Valid Characters are "0, 1, 2, 3, 4, 5, 6, 7, 8, and 9".
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.

Table 65 Security > VPN > Rule Setup: Manual (continued)

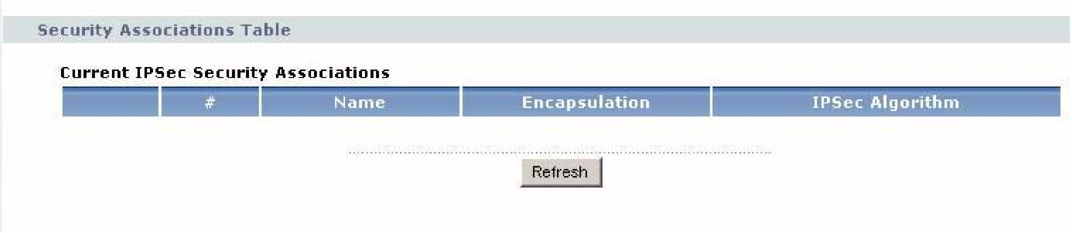
LABEL	DESCRIPTION
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Select **Yes** from the drop-down menu to enable replay detection, or select **No** to disable it.
IPSec Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase processing requirements and communications latency (delay). If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below).
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm The NBG420N and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Encryption Key	This field is applicable when you select **ESP** in the **IPSec Protocol** field above. With **DES**, type a unique key 8 characters long. With **3DES**, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA-1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.
Cancel	Click **Cancel** to exit the screen without making any changes.

15.3 The SA Monitor Screen

In the web configurator, click **Security > VPN > SA Monitor**. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections.

Figure 109 Security > VPN > SA Monitor



Security Associations Table
Current IPSec Security Associations
#
Name
Encapsulation
IPSec Algorithm
Refresh

The following table describes the labels in this screen.

Table 66 Security > VPN > SA Monitor

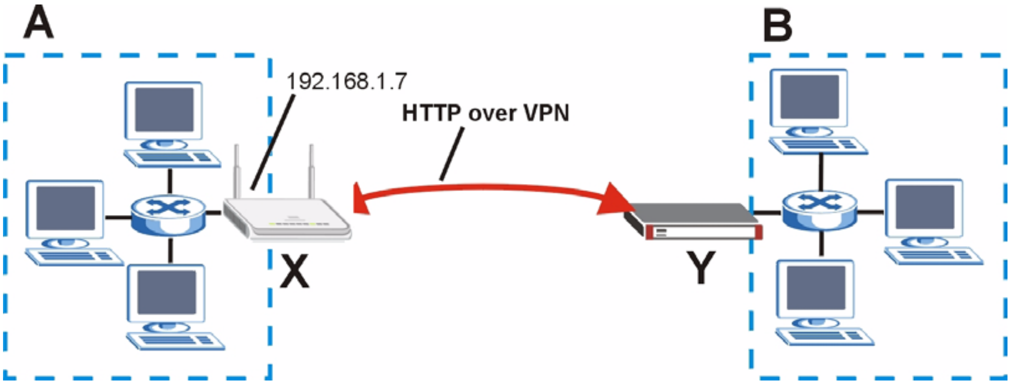
LABEL	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase NBG420N processing requirements and communications latency (delay).
Refresh	Click **Refresh** to display the current active VPN connection(s).

15.4 VPN and Remote Management

You can allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the NBG420N. One of the NBG420N's ports must be part of the VPN rule's local network. This can be the NBG420N's LAN port if you do not want to allow remote management on the WAN port. You also have to configure remote management (**REMOTE MGMT**) to allow management access for the service through the specific port.

In the following example, the VPN rule's local network (A) includes the NBG420N's LAN IP address of 192.168.1.7. Someone in the remote network (B) can use a service (like HTTP for example) through the VPN tunnel to access the NBG420N's LAN interface. Remote management must also be configured to allow HTTP access on the NBG420N's LAN interface.

Figure 110 VPN for Remote Management Example

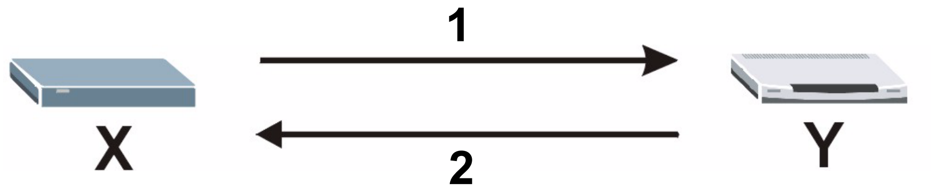


15.5 IPSec VPN Technical Reference

IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the NBG420N and remote IPSec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated below.

Figure 111 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal



The NBG420N sends a proposal to the remote IPSec router. Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the NBG420N wants to use in the IKE SA. The remote IPSec router sends the accepted proposal back to the NBG420N. If the remote IPSec router rejects the proposal (for example, if the VPN tunnel is not configured correctly), the NBG420N and remote IPSec router cannot establish an IKE SA.

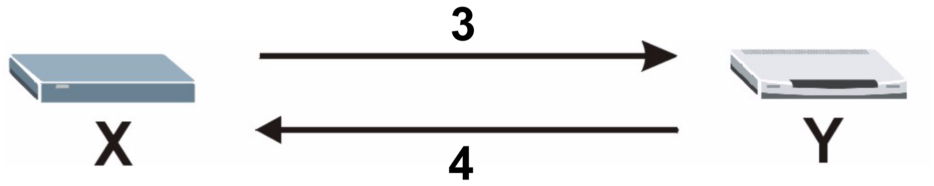
Note: Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

See the field descriptions for information about specific encryption algorithms, authentication algorithms, and DH key groups. See Diffie-Hellman (DH) Key Exchange on page 185 for more information about DH key groups.

Diffie-Hellman (DH) Key Exchange

The NBG420N and the remote IPSec router use a DH key exchange to establish a shared secret, which is used to generate encryption keys for IKE SA and IPSec SA. In main mode, the DH key exchange is done in steps 3 and 4, as illustrated below.

Figure 112 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



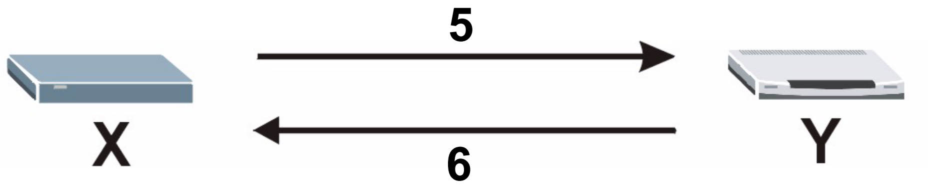
The DH key exchange is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption keys, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 encryption keys take longer to encrypt and decrypt.

Authentication

Before the NBG420N and remote IPSec router establish an IKE SA, they have to verify each other's identity. This process is based on pre-shared keys and router identities.

In main mode, the NBG420N and remote IPSec router authenticate each other in steps 5 and 6, as illustrated below. Their identities are encrypted using the encryption algorithm and encryption key the NBG420N and remote IPSec router selected in previous steps.

Figure 113 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication



The NBG420N and remote IPSec router use a pre-shared key in the authentication process, though it is not actually transmitted or exchanged.

Note: The NBG420N and the remote IPSec router must use the same pre-shared key.

Router identity consists of ID type and ID content. The ID type can be IP address, domain name, or e-mail address, and the ID content is a specific IP address, domain name, or e-mail address. The ID content is only used for identification; the IP address, domain name, or e-mail address that you enter does not have to actually exist.

The NBG420N and the remote IPSec router each has its own identity, so each one must store two sets of information, one for itself and one for the other router. Local ID type and ID content refers to the ID type and ID content that applies to the router itself, and peer ID type and ID content refers to the ID type and ID content that applies to the other router in the IKE SA.

Note: The NBG420N's local and peer ID type and ID content must match the remote IPSec router's peer and local ID type and ID content, respectively.

In the following example, the ID type and content match so the NBG420N and the remote IPSec router authenticate each other successfully.

Table 67 VPN Example: Matching ID Type and Content

NBG420N	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

In the following example, the ID type and content do not match so the authentication fails and the NBG420N and the remote IPSec router cannot establish an IKE SA.

Table 68 VPN Example: Mismatching ID Type and Content

NBG420N	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: **1.1.1.2**
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: **1.1.1.15**	Peer ID content: tom@yourcompany.com

Negotiation Mode

There are two negotiation modes: main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1-2: The NBG420N sends its proposals to the remote IPSec router. The remote IPSec router selects an acceptable proposal and sends it back to the NBG420N.

Steps 3-4: The NBG420N and the remote IPSec router participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

Steps 5-6: Finally, the NBG420N and the remote IPSec router generate an encryption key from the shared secret, encrypt their identities, and exchange their encrypted identity information for authentication.

In contrast, aggressive mode only takes three steps to establish an IKE SA.

Step 1: The NBG420N sends its proposals to the remote IPSec router. It also starts the Diffie-Hellman key exchange and sends its (unencrypted) identity to the remote IPSec router for authentication.

Step 2: The remote IPSec router selects an acceptable proposal and sends it back to the NBG420N. It also finishes the Diffie-Hellman key exchange, authenticates the NBG420N, and sends its (unencrypted) identity to the NBG420N for authentication.

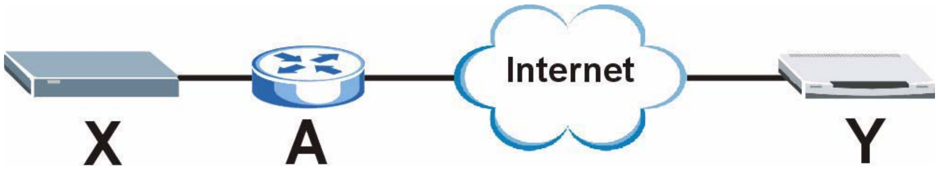
Step 3: The NBG420N authenticates the remote IPSec router and confirms that the IKE SA is established.

Aggressive mode does not provide as much security as main mode because the identity of the NBG420N and the identity of the remote IPSec router are not encrypted. It is usually used when the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication (for example, telecommuters).

VPN, NAT, and NAT Traversal

In the following example, there is another router (**A**) between router **X** and router **Y**.

Figure 114 VPN/NAT Example



If router **A** does NAT, it might change the IP addresses, port numbers, or both. If router **X** and router **Y** try to establish a VPN tunnel, the authentication fails because it depends on this information. The routers cannot establish a VPN tunnel.

Most routers like router **A** now have an IPSec pass-through feature. This feature helps router **A** recognize VPN packets and route them appropriately. If router **A** has this feature, router **X** and router **Y** can establish a VPN tunnel as long as the IPSec protocol is ESP. (See IPSec Protocol on page 188 for more information about active protocols.)

If router **A** does not have an IPSec pass-through or if the IPSec protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router **X** and router **Y** add an extra header to the IKE SA and IPSec SA packets. If you configure router **A** to forward these packets unchanged, router **X** and router **Y** can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the NBG420N and remote IPSec router.
- Configure the NAT router to forward packets with the extra header unchanged.

The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the NBG420N and remote IPSec router support.

IPSec Protocol

The IPSec protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPSec VPN includes two IPSec protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

Note: The NBG420N and remote IPSec router must use the same IPSec protocol.

Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

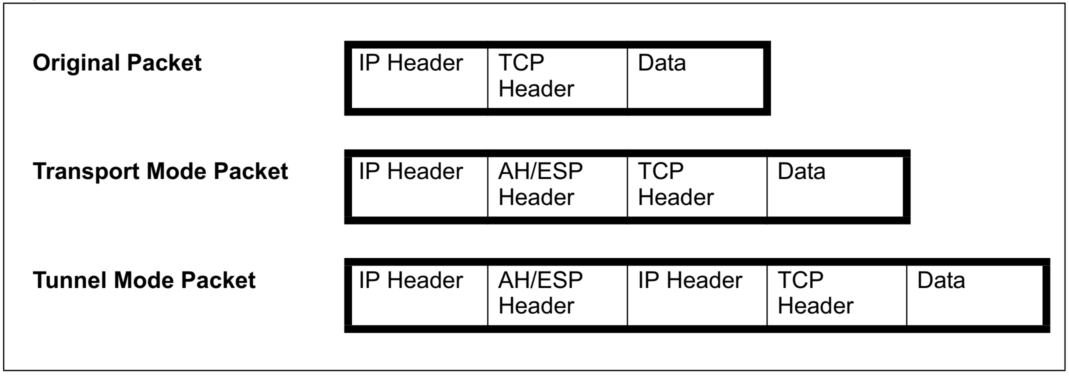
Encapsulation

There are two ways to encapsulate packets. Usually, you should use tunnel mode because it is more secure. Transport mode is only used when the IPSec SA is used for communication between the NBG420N and remote IPSec router (for example, for remote management), not between computers on the local and remote networks.

Note: The NBG420N and remote IPSec router must use the same encapsulation.

These modes are illustrated below.

Figure 115 VPN: Transport and Tunnel Mode Encapsulation



Original Packet	IP Header	TCP Header	Data		
Transport Mode Packet	IP Header	AH/ESP Header	TCP Header	Data	
Tunnel Mode Packet	IP Header	AH/ESP Header	IP Header	TCP Header	Data

In tunnel mode, the NBG420N uses the IPSec protocol to encapsulate the entire IP packet. As a result, there are two IP headers:

- Outside header: The outside IP header contains the IP address of the NBG420N or remote IPSec router, whichever is the destination.
- Inside header: The inside IP header contains the IP address of the computer behind the NBG420N or remote IPSec router. The header for the IPSec protocol (AH or ESP) appears between the IP headers.

In transport mode, the encapsulation depends on the IPSec protocol. With AH, the NBG420N includes part of the original IP header when it encapsulates the packet. With ESP, however, the NBG420N does not include the IP header when it encapsulates the packet, so it is not possible to verify the integrity of the source IP address.

IPSec SA Proposal and Perfect Forward Secrecy

An IPSec SA proposal is similar to an IKE SA proposal (see IKE SA Proposal on page 185), except that you also have the choice whether or not the NBG420N and remote IPSec router perform a new DH key exchange every time an IPSec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the NBG420N and remote IPSec router perform a DH key exchange every time an IPSec SA is established, changing the root key from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys remain secure.

If you do not enable PFS, the NBG420N and remote IPSec router use the same root key that was generated when the IKE SA was established to generate encryption keys.

The DH key exchange is time-consuming and may be unnecessary for data that does not require such security.

Additional IPSec VPN Topics

This section discusses other IPSec VPN topics that apply to either IKE SAs or IPSec SAs or both. Relationships between the topics are also highlighted.

SA Life Time

SAs have a lifetime that specifies how long the SA lasts until it times out. When an SA times out, the NBG420N automatically renegotiates the SA in the following situations:

- There is traffic when the SA life time expires
- The IPSec SA is configured on the NBG420N as nailed up (see below)

Otherwise, the NBG420N must re-negotiate the SA the next time someone wants to send traffic.

Note: If the IKE SA times out while an IPSec SA is connected, the IPSec SA stays connected.

An IPSec SA can be set to **keep alive** Normally, the NBG420N drops the IPSec SA when the life time expires or after two minutes of outbound traffic with no inbound traffic. If you set the IPSec SA to keep alive , the NBG420N automatically renegotiates the IPSec SA when the SA life time expires, and it does not drop the IPSec SA if there is no inbound traffic.

Note: The SA life time and keep alive settings only apply if the rule identifies the remote IPSec router by a static IP address or a domain name. If the **Secure Gateway Address** field is set to **0.0.0.0**, the NBG420N cannot initiate the tunnel (and cannot renegotiate the SA).

Encryption and Authentication Algorithms

In most NBG420Ns, you can select one of the following encryption algorithms for each proposal. The encryption algorithms are listed here in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data.
- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.

You can select one of the following authentication algorithms for each proposal. The algorithms are listed here in order from weakest to strongest.

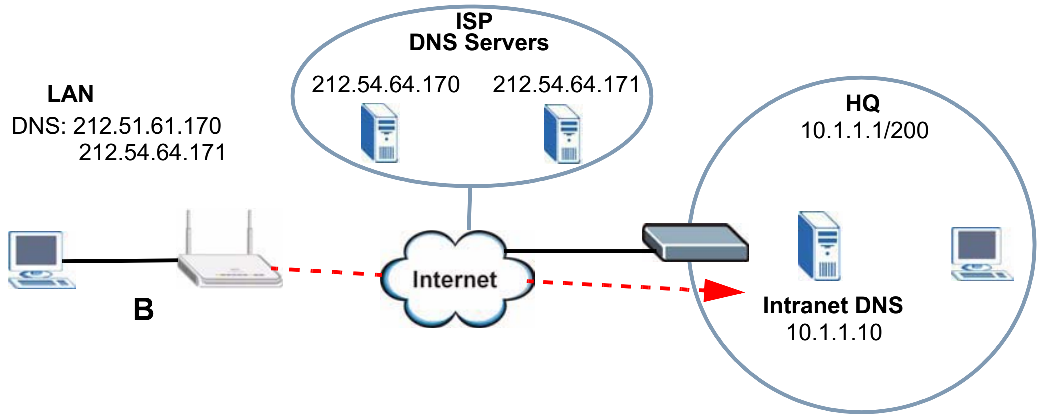
- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

Private DNS Server

In cases where you want to use domain names to access Intranet servers on a remote private network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote private network.

The following figure depicts an example where one VPN tunnel is created from an NBG420N at branch office (**B**) to headquarters (**HQ**). In order to access computers that use private domain names on the **HQ** network, the NBG420N at **B** uses the Intranet DNS server in headquarters.

Figure 116 Private DNS Server Example



If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote private network.

PART IV
Management

16

Static Route Screens

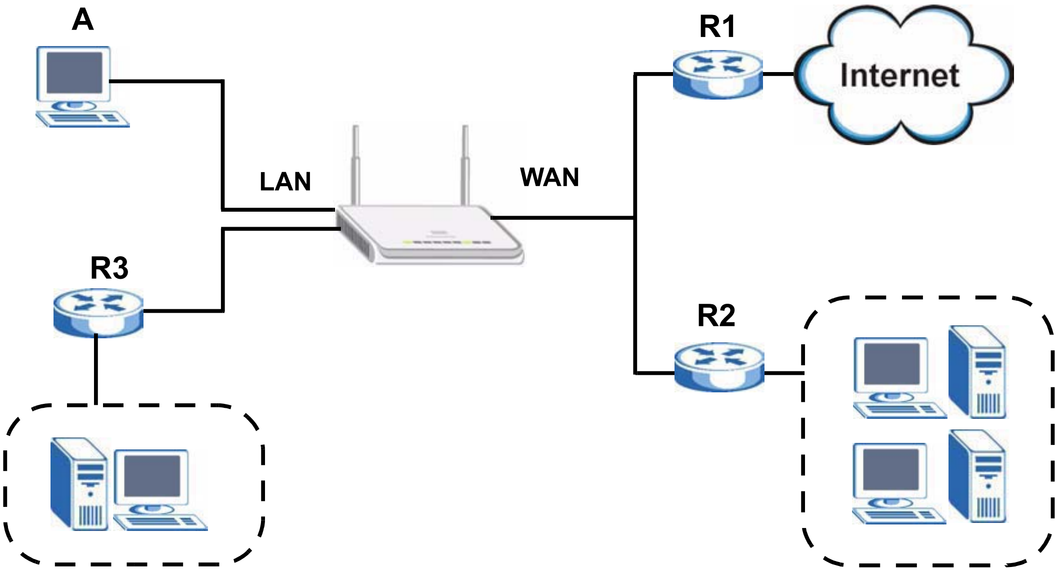
This chapter shows you how to configure static routes for your NBG420N.

16.1 Static Route Overview

The NBG420N usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the NBG420N send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the NBG420N's LAN interface. The NBG420N routes most traffic from **A** to the Internet through the NBG420N's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

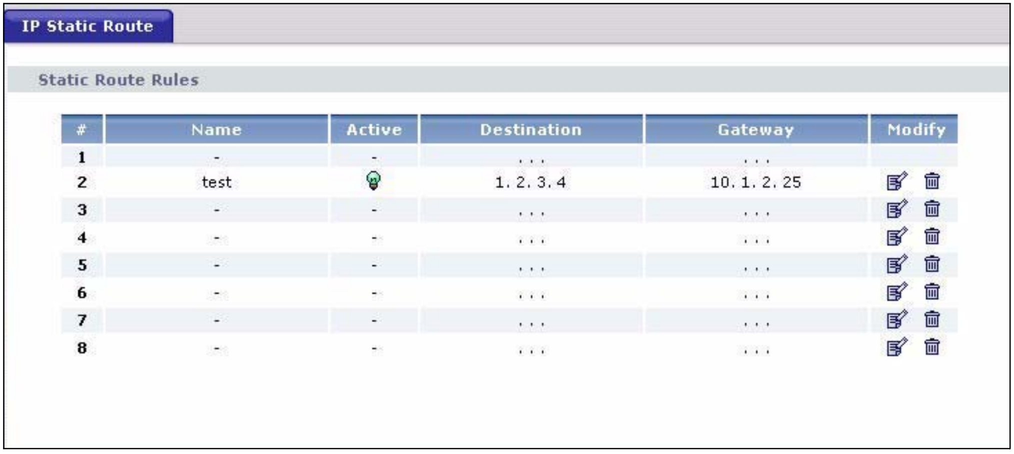
Figure 117 Example of Static Routing Topology



16.2 IP Static Route Screen

Click **Management** > **Static Route** to open the **IP Static Route** screen. The following screen displays.

Figure 118 Management > Static Route > IP Static Route



Static Route Rules

#	Name	Active	Destination	Gateway	Modify
1	-	-	. . .	. . .	
2	test	●	1. 2. 3. 4	10. 1. 2. 25	✎ 🗑
3	-	-	. . .	. . .	✎ 🗑
4	-	-	. . .	. . .	✎ 🗑
5	-	-	. . .	. . .	✎ 🗑
6	-	-	. . .	. . .	✎ 🗑
7	-	-	. . .	. . .	✎ 🗑
8	-	-	. . .	. . .	✎ 🗑

The following table describes the labels in this screen.

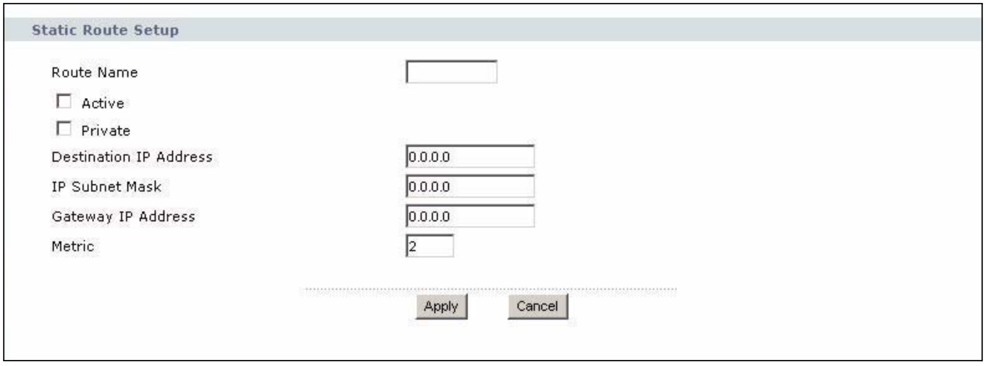
Table 69 Management > Static Route > IP Static Route

LABEL	DESCRIPTION
#	This is the index number of an individual static route. The first entry is for the default route and not editable.
Name	This is the name that describes or identifies this route.
Active	This icon is turned on when this static route is active. Click the **Edit** icon under **Modify** and select the **Active** checkbox in the **Static Route Setup** screen to enable the static route. Clear the checkbox to disable this static route without having to delete the entry.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is an immediate neighbor of your NBG420N that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your NBG420N; over the WAN, the gateway must be the IP address of one of the remote nodes.
Modify	Click the **Edit** icon to open the static route setup screen. Modify a static route or create a new static route in the **Static Route Setup** screen. Click the **Remove** icon to delete a static route.

16.2.1 Static Route Setup Screen

To edit a static route, click the edit icon under **Modify**. The following screen displays. Fill in the required information for each static route.

Figure 119 Management > Static Route > IP Static Route: Static Route Setup



Static Route Setup

Route Name	
□ Active	
□ Private	
Destination IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0
Metric	2

The following table describes the labels in this screen.

Table 70 Management > Static Route > IP Static Route: Static Route Setup

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Private	This parameter determines if the NBG420N will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this checkbox to propagate this route to other hosts through RIP broadcasts.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your NBG420N that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your NBG420N; over the WAN, the gateway must be the IP address of one of the Remote Nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Apply	Click **Apply** to save your changes back to the NBG420N.
Cancel	Click **Cancel** to return to the previous screen and not save your changes.

17

Bandwidth Management

This chapter contains information about configuring bandwidth management, editing rules and viewing the NBG420N's bandwidth management logs.

17.1 Bandwidth Management Overview

ZyXEL's Bandwidth Management allows you to specify bandwidth management rules based on an application and/or subnet. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth rules.

The NBG420N applies bandwidth management to traffic that it forwards out through an interface. The NBG420N does not control the bandwidth of traffic that comes into an interface.

Bandwidth management applies to all traffic flowing out of the router, regardless of the traffic's source.

Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the NBG420N and be managed by bandwidth management.

- The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WLAN to WAN, WAN to WAN / NBG420N) must be less than or equal to the **Upstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen.
- The sum of the bandwidth allotments that apply to the LAN port (WAN to LAN, WLAN to LAN, LAN to LAN / NBG420N) must be less than or equal to 100,000 kbps (you cannot configure the bandwidth budget for the LAN port).
- The sum of the bandwidth allotments that apply to the WLAN port (LAN to WLAN, WAN to WLAN, WLAN to WLAN / NBG420N) must be less than or equal to 54,000 kbps (you cannot configure the bandwidth budget for the WLAN port).

17.2 Application-based Bandwidth Management

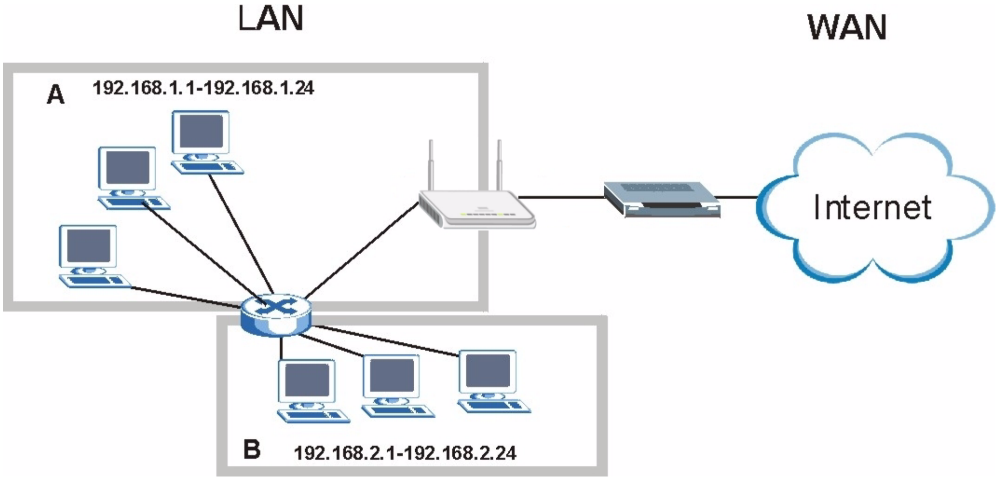
You can create bandwidth classes based on individual applications (like VoIP, Web, FTP, E-mail and Video for example).

17.3 Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets.

The following figure shows LAN subnets. You could configure one bandwidth class for subnet **A** and another for subnet **B**.

Figure 120 Subnet-based Bandwidth Management Example



17.4 Application and Subnet-based Bandwidth Management

You could also create bandwidth classes based on a combination of a subnet and an application. The following example table shows bandwidth allocations for application specific traffic from separate LAN subnets.

Table 71 Application and Subnet-based Bandwidth Management Example

TRAFFIC TYPE	FROM SUBNET A	FROM SUBNET B
VoIP	64 Kbps	64 Kbps
Web	64 Kbps	64 Kbps
FTP	64 Kbps	64 Kbps
E-mail	64 Kbps	64 Kbps
Video	64 Kbps	64 Kbps

17.5 Bandwidth Management Priorities

The following table describes the priorities that you can apply to traffic that the NBG420N forwards out through an interface.

Table 72 Bandwidth Management Priorities

PRIORITY LEVELS: TRAFFIC WITH A HIGHER PRIORITY GETS THROUGH FASTER WHILE TRAFFIC WITH A LOWER PRIORITY IS DROPPED IF THE NETWORK IS CONGESTED.	
High	Typically used for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay).