

NETGEAR DSL Voice Gateway VVG2000

1. ADSL Setup Wizard
2. USB Setup Wizard
3. Add WPS Client

Setup

1. ADSL Settings
2. Basic Settings
3. Wireless Settings
4. USB Drive Settings

Telephony Setting

1. VoIP Status
2. Call Log

Security

1. Logs
2. Block Sites
3. Firewall Rules
4. Services
5. Schedule
6. E-mail

Maintenance

1. Router Status
2. Attached Devices
3. Backup Settings
4. Set Password
5. Diagnostics
6. Router Upgrade

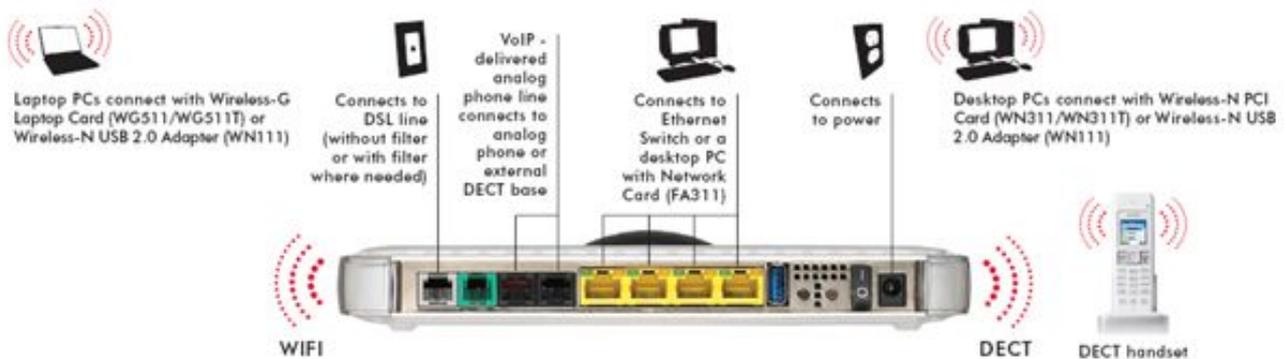
Advanced

1. VLAN Group Settings
2. QoS Setup
3. WAN Setup
4. Dynamic DNS
5. LAN IP Setup
6. Wireless Settings
7. Advanced Wireless Settings
8. Remote Management
9. Static Routes
10. UPnP

Web Support

1. Knowledge Base
2. Documentation

Picture of router.



Speed test.



Jeg var så heldig at have denne hastighed I ca. 14 dage inden FULLRATE fik rettet konfigurationen, det kørte bare hurtigt. Desværre er det slut nu har jeg de 25/4 Mbit som jeg betaler for. Jeg kunne ellers godt vende mig til den anden hastighed.

Dette er en simpel copy/paste manual, som indeholder det samme som brugerinterface, men det er hurtigere at slå op i denne manual.

Håber at I kan bruge det.

Med venlig hilsen

Martin Lohse.

Router Status Help

You can use the *Router Status* page to check the current settings and statistics for your router. This page shows you the current settings. If something needs to be changed, you'll have to change it on the relevant page.

Account Name: This is the Account Name that you entered in the *Setup Wizard* or *Basic Settings*.

Firmware Version: This is the current software the router is using. This will change if you upgrade your router.

ADSL Port: These are the current settings that you set in the *Setup Wizard* or *Basic Settings* pages.

- MAC Address - the physical address of the Router, as seen from the Internet.
- IP Address - current Internet IP address. If assigned dynamically, and no Internet connection exists, this will be blank or 0.0.0.0
- DHCP - indicates either *Client* (IP address is obtained dynamically) or *None*.
- IP Subnet Mask - the subnet mask associated with the Internet IP address Domain Name Server - displays the address of the current DNS.

LAN Port: These are the current settings, as set in the *LAN IP Setup* page.

- MAC Address - the physical address of the Router, as seen from the local LAN.
- IP Address - LAN IP address of the Router.
- DHCP - indicates if the Router is acting as a DHCP Server for devices on your LAN.
- IP Subnet Mask - subnet mask associated with the LAN IP address.

Modem: The current Modem status and settings are shown in this section.

- ADSL Firmware Version - This is the version number of the low-level ADSL firmware. This is contained within the Router Firmware.
- Modem Status - the current state of the ADSL connection to your phone company.
- DownStream Connection Speed - the connection speed of the ADSL connection from the phone company to your Router.
- UpStream Connection Speed - the connection speed of the ADSL connection from your Router to the phone company.
- VPI - the VPI setting entered on the ADSL Settings page.
- VCI - the VCI setting entered on the ADSL Settings page.

Wireless Port: These are the current settings, as set in the *Wireless Settings* page.

- Name (SSID) - SSID of the Router.
- Region - the location (country).
- Channel - the current channel in use.
- Mode - indicates the current mode (g & b, g, or b)
- Wireless AP - indicates if the Access Point feature of the Router is enabled or not. If not enabled, the Wireless LED on the front panel will be off.
- Broadcast Name - indicates if the Router is broadcasting its SSID.

Click **Show Statistics** to see router performance statistics such as the number of packets sent and number of packets received for each port.

Smart Setup Wizard - USB Drive Help

The VVG2000 allows file sharing if a USB hard drive or flash memory is connected to the USB port. Please consult the Reference Manual for detailed configuration information.

As soon as a USB hard disk or flash memory is attached to VVG2000 USB port, users on the local area network can access the USB drive with full read and write access.

Users from local area network or the Internet can also access the USB drive using FTP access. The Smart Setup Wizard will guide you through the FTP setup process.

Enter the folder name to share

When the user accesses files via FTP, this is the root folder that will be displayed.

Enter the FTP login name to give access to this folder

Type the FTP login account name that you want to have accessed to the folder.

Enter the FTP login password

Type a password for the FTP login account.

Select the FTP access rights

Selecting Read only will allow the user to retrieve data files using FTP. Selecting Read and Write will allow the user to read and write data files.

Note: Any FTP accesses from the Internet will have Read only access rights, regardless of the account rights granted here.

To Continue or Stop Wizard

Click **Continue** to come to the next page.

Click **Stop Wizard** to stop wizard and come to USB Drive Settings.

Add WPS Client Help

WPS stands for Wi-Fi Protected Setup. This is a process that let you add a wireless client to the network easily, and you don't have to specifically configure the wireless settings like SSID, security mode, and passphrase.

You can select to add a wireless client either through the "Push Button" or "PIN Number".

With the "Push Button" method, you have to complete the process by clicking a button on the client (either a hardware button or a software button on the client's utility GUI).

With the "PIN Number" method, you have to enter the client's PIN here. You have to start the client WPS process at the same time, and you can fins the client's PIN on the client's utility GUI.

ADSL Settings Help

The default parameters should be correct to match the system used by your ISP

- Multiplexing Method - Your ISP will indicate whether your Multiplexing Method is VC-BASED or LLC-BASED.
- Virtual Circuit - Your ISP will indicate which VPI/VCI combination is used for your service.

Connection service guarantees are specified per ATM VPI/VCI by a set of measurable connection parameters. Please check your ISP to set the proper parameters. If you don't know how to configure them, please keep them as default.

- UBR (Unspecified Bit Rate): The protocol that provides spare bandwidth to non-critical services such as file transfers. The actual rate depend on the bandwidth of the current network.
- CBR(Constant Bit Rate): Real-time connection with a specified amount of guaranteed bandwidth (PCR) that is continuously available during the connection life-time.
- VBR-rt (Real-Time Variable Bit Rate): Similar as CBR intended for real-time applications with constrained delay and delay variation values, but which can benefit from variable bit-rates. The average guaranteed bandwidth is SCR, but data up to PCR may be sent for a limited amount of data specified by MBS. A VBR-rt connection is characterized by PCR, SCR, MBS.
- VBR-nrt (Non-Real-Time Variable Bit Rate): Intended for non-real-time applications that have bursty traffic characteristics and no strict transfer delay requirements but which require an amount of guaranteed bandwidth. A VBR-nrt connection is characterized by an average guaranteed bandwidth (SCR) up to a maximum guaranteed bandwidth (PCR) for a burst with specified maximum size (MBS).
- PCR (Peak Cell Rate): Maximum number of ATM cells per second that may be sent on the connection.
- SCR (Sustainable Cell Rate): Average number of ATM cells per second that may be sent on the connection.
- MBS (Maximum Burst. Size): Maximum number of ATM cells that may be sent in a burst, and thus exceeding the average number of cells (SCR) up to the maximum number of cells (PCR) for a limited number of ATM cells defined by MBS.

To Apply or Cancel

Click **Apply** to save the new settings to the Router.

Click **Cancel** to disregard any unsaved changes.

Help

The VVG2000 Settings pages allow you to configure, upgrade and check the status of your NETGEAR Router.

Click an item in the leftmost column. The current settings or information for that area appear in the center column.

Helpful information related to the selected Settings page appears in this column. If you are using Internet Explorer, you may click an item in the center column to jump directly to the related help section; otherwise, scroll down until you reach it.

Basic Settings Help

Note: If you are setting up the Router for the first time, the default settings may work for you with no changes.

Does Your Internet Connection Require A Login?

Select this option based on the type of account you have with your ISP. If you need to enter login information every time you connect to the Internet or you have a PPPoE account with your ISP, select **Yes**. Otherwise, select **No**.

Note: If you have installed PPP software such as WinPoET (from Earthlink) or Enternet (from PacBell), then you have PPPoE. Select **Yes**. After selecting Yes and configuring your Router, you will not need to run the PPP software on your PC to connect to the Internet.

Account Name

(also known as Host Name or System Name)

For most users, type your account name or user name in this box. For example, if your main mail account is JerAB@ISP.com, then put JerAB in this box.

If your ISP has given you a specific Host name, then type it (for example, CCA7324-A).

Domain Name

For most users, you may leave this box blank, unless required by your ISP. You may type the domain name of your ISP. For example, if your ISP's mail server is mail.xxx.yyy.zzz, you would type xxx.yyy.zzz as the Domain Name.

If you have a Domain name given to you by your ISP, type it in this box. (For example, Earthlink Cable may require a Host name of 'home' and Comcast sometimes supplies a Domain name.)

Internet IP Address

If you log in to your service or your ISP did not provide you with a fixed IP address, the Router will find an IP address for you automatically when you connect. Select **Get Dynamically From ISP**.

If you have a fixed (or static IP) address, your ISP will have provided you with the required information. Select **Use Static IP Address** and type the IP Address, Subnet Mask and Gateway IP Address into the correct boxes.

For example:

- IP Address: 24.218.156.183
- Subnet Mask: 255.255.255.0
- Gateway IP Address: 24.218.156.1

If your ISP uses Classical IP (RFC1577) or Routed RFC1483, select **Use IP over ATM (IPOA)**. Fill in the information provided to you by your ISP. Type the IP Address, Subnet Mask, and Gateway IP address into the correct boxes.

Note: It is not always necessary to fill in the IPOA **Gateway IP Address**. In a RFC1577 environment, the gateway can be discovered automatically.

DNS Address

The DNS server is used to look up site addresses based on their names.

If your ISP gave you one or two DNS addresses, select **Use These DNS Servers** and type the primary and secondary addresses.

Otherwise, select **Get Automatically From ISP**.

Note: If you get 'Address not found' errors when you go to a Web site, it is likely that your DNS servers aren't set up properly. You should contact your ISP to get DNS server addresses.

NAT (Network Address Translation)

NAT allows all LAN PCs to gain Internet access via this Router, by sharing this Router's WAN IP address. In most situations, NAT is essential for Internet access via this Router. You should only disable NAT if you are sure you do not require it. When NAT is disabled, only standard routing is performed by this Router. Disabling the Firewall will change the default incoming rule from "Block" to "Allow", so the protections normally provided by the firewall will be disabled. Protections against DoS attacks and Port Scans will still be enabled and can be modified in the WAN Setup page.

Router MAC Address

Your computer's local address is its unique address on your network. This is also referred to as the computer's MAC (Media Access Control) address.

Usually, select Use Default MAC Address.

If your ISP requires MAC authentication, then select either **Use Computer MAC address** to disguise the Router's MAC address with the Computer's own MAC address or **Use This MAC Address** to manually type the MAC address for a different computer. The format for the MAC address is XX:XX:XX:XX:XX:XX. This value may be changed if the **Use Computer MAC Address** is selected once a value has already been set in the **Use This MAC Address** selection.

Apply, Cancel and Test

Click **Apply** when you finish changing the settings.

Click **Cancel** to return to the original settings.

Click **Test** to connect to the NETGEAR Web site. If you connect successfully, your settings work and you may click **Logout** to exit these pages and... enjoy surfing the **'net!**

If you don't connect successfully,

- Go through the settings and make sure you've selected the correct options and typed

everything correctly.

- Contact your ISP to verify the configuration information.
- Read the Troubleshooting section in the VVG2000 Installation Guide.
- On the VVG2000 Resource CD, read the Troubleshooting Guide or the Troubleshooting section in the Reference Manual.
- Contact NETGEAR Technical Support.

Wireless Settings Help

NOTE: To ensure proper agency compliance and compatibility between similar products in your area; the operating channel & region must be set correctly by you.

Placement of the Router to Optimize Wireless Connectivity

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the Router. For best results, place your Router:

- Near the center of the area in which your PCs will operate,
- In an elevated location such as a high shelf,
- Away from potential sources of interference, such as PCs, microwaves, and cordless phones,
- Away from large metal surfaces.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Router.

Wireless Network

Name (SSID)

Enter a value of up to 32 alphanumeric characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is NETGEAR, but NETGEAR strongly recommends that you change your networks Name (SSID) to a different value. This value is also case-sensitive. For example, *Wireless* is not the same as *wireless*.

Region

Select your region from the drop-down list. This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the Router in a region other than the region shown here. If your country or region is not listed, please check with your local government agency or check our website for more information on which channels to use.

Channel

This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point.

Mode

Select the desired wireless mode. The options are:

- Up to 54 Mbps - Legacy Mode with maximum speed of up to 54 Mbps for b/g networks.
- Up to 130 Mbps - Neighbor Friendly Mode - Default speed up to 130 Mbps in presence of neighboring wireless networks.
- Up to 270 Mbps - Performance Mode - Maximum Wireless-N speed up to 270 Mbps.

The default is "Up to 130Mbps", which allows all 11b and 11g wireless stations. The NETGEAR WN511B runs at 130 Mbps when accessing this router.

Wireless Access Point

Enable Wireless Access Point

The Wireless Access Point of this Router can be enabled or disabled to allow wireless access. The wireless icon on the front of the Router will also display the current status of the Wireless Access Point to let you know if it is disabled or enabled.

If Enabled, wireless stations will be able to access the Internet.

If Disabled, wireless stations will not be able to access the Internet.

Allow Broadcast of Name (SSID)

If Enabled, the SSID will broadcast its name to all Wireless Stations. Stations which have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point.

Wireless Isolation

If Enabled, the Wireless Stations will be hidden from each other, and will not be able to communicate with each other. For normal situations, this setting should be left at the default value of **Disabled**.

Wireless Station Access List

By default, any wireless PC that is configured with the correct SSID will be allowed access to your wireless network. For increased security, you can restrict access to the wireless network to only allow specific PCs based on their MAC addresses. From the *Wireless Settings* menu, click the **Setup Access List** button to display the Wireless Station Access List menu.

Security Options

Select the desired option, and ensure all your Wireless stations have the same setting:

- **Disable** - This will disable the security function. Data will not be encrypted before transmission.
- **WEP** - WEP (Wired Equivalent Privacy), if used, encrypts data before transmission. This provides greater security and privacy. All Wireless Stations need to use the same settings (WEP Key size and WEP key).
- **WPA-PSK** - This version of WPA uses a PSK (Pre-shared Key) for authentication, so you don't need a Radius Server. All Wireless stations need to use the same PSK (Pre-shared Key). Data transmissions are encrypted using a 256 Bit key derived from the PSK. This key changes regularly, providing greater protection. WPA is more secure than WEP, and should be used if possible.
- **WPA-802.1x** - This version of WPA requires the use of a Radius server for authentication. Each user (Wireless Client) must have a "user" login on the Radius Server, and this device must have a "client" login on the Radius server. Data transmissions are encrypted using a key which is automatically generated.

WEP Security Encryption

Authentication Type

Normally this can be left at the default value of "Automatic." If that fails, select the appropriate

value - "Open System" or "Shared Key." Check your wireless card's documentation to see what method to use.

Encryption Strength

Select the WEP Encryption level:

- 64-bit (sometimes called 40-bit) encryption
- 128-bit encryption

WEP Key

You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.

Automatic Key Generation (Passphrase)

Enter a word or group of printable characters in the Passphrase box and click the Generate button to automatically configure the WEP Key(s). If encryption strength is set to 64 bit, then each of the four key boxes will automatically be populated with key values. If encryption strength is set to 128 bit, then only the selected WEP key box will automatically be populated with key values.

Manual Entry Mode

Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key box.

For 64 bit WEP - Enter ten hexadecimal digits (any combination of 0-9, A-F).

For 128 bit WEP - Enter twenty-six hexadecimal digits (any combination of 0-9, A-F).

Be sure to click Apply to save your settings in this menu.

WPA-PSK Security Encryption

Network Key

For WPA-PSK, you need to enter the **Network Key** here. The Key must be from 8 to 63 ASCII characters. Your Wireless Stations must use the same key.

WPA Encryption

Currently, only TKIP is supported. Ensure your Wireless Stations are also using TKIP. Normally, this is the default. If there is no choice of encryption methods for WPA-PSK, then you can assume TKIP will be used.

WPA-802.1x Security Encryption

Radius Server Name/IP Address

Enter the name or IP address of the Radius Server on your LAN.

- Each user (Wireless Client) must have a "user" login on the Radius Server.
- This device must have a "client" login on the Radius server. The login name is the name of this device.

Radius Port

Enter the port number which is used for connections to your Radius Server.

Shared Key

Enter the shared key, as configured on your Radius server, for the "client" login for this device.

To Save Or Cancel Changes

Click **Apply** to have your changes take effect.

Click **Cancel** to return to the previous unsaved settings.

USB Drive Settings Help

The VVG2000 allows file sharing when a USB hard drive or flash memory is connected to the USB port.

Please consult the Reference Manual for detailed configuration information.

To access the USB Drive via FTP, use any FTP tool or type **ftp://ipaddress** in a Web browser such as Microsoft Internet Explorer or Netscape. The ipaddress entered is the Web IP address of the router, which can be located on the Router Status menu as the IP address of the Internet Port.

To access the USB Drive via Microsoft network connections, click Windows Start -> Run and type **\\ipaddress**. The ipaddress entered is the local IP address of the router, for example, 192.168.0.1. Typing **\\hostname** in Windows Explorer is also an alternative. The hostname entered is the Host Name specified in the Network Access section, for example, VVG2000.

Network Access

Host Name & Workgroup

The Host Name and workgroup combination is the name used to identify the router in your network. The attached USB drive can be easily accessed by typing **\\hostname** in Windows Explorer.

FTP Port

FTP port is the TCP port number of the embedded FTP server. The default value is 21. You can also change to any port between 1024 and 65535.

To Apply

Click **Apply** to save the new settings to the Router.

FTP Access

FTP accounts can be created by clicking the Add button. These FTP accounts will allow users on the LAN or Internet to access the files on the attached USB drive.

To Add, Edit, Delete or Eject Disk

Click **Add** to add a new information.

Click **Edit** to edit the selected information.

Click **Delete** to delete the selected information.

Click **Eject Disk** to eject the USB device.

Attached Device

This table shows the partition information of the attached USB drive, including the share name and file system type.

To Refresh

Click **Refresh** to update the Attached Device table.

VoIP Status Help

This page shows the current status of your VoIP (Voice over Internet Protocol) connection.

Line 1/Line 2

- **Display Name:** This is the name you have already chosen when you first opened your account. Your "Display Name" will be visible to other individuals with caller ID. If your display name appears as "UNAVAILABLE", either your account has not been established or your router has been unable to connect to the Internet.
- **Telephone Number:** This is the telephone number other people will use when they call you. This number was assigned to your router when you first established your account. Each line can have a different telephone number. If your Telephone Number appears as "phonenumber", either your account has not been established or your router has been unable to connect to the Internet.

Line Status

- **Hook State:** The "Hook State" displays the condition of the telephone receiver. ON indicates the receiver is "on-the-hook", while OFF indicates the receiver is "off-the-hook".
 - **Registration State:** When your router has successfully connected to the VoIP servers, the "Registration State" will be displayed as "registered". However, if you do not have a VOIP account or if the router could not connect to the VoIP servers, the "Registration State" will be displayed as "not registered".
-

To see the most recent entries:

- Click **Refresh**.

Call Log Help

This page indicates recent call activities including Call missed, successful calls and incoming calls.

To delete all log entries:

- Click **Clear Log**.

To see the most recent entries:

- Click **Refresh**.

Logs Help

Your Router will log security-related events such as denied incoming service requests, hacker probes, and administrator logins, according to your settings on this screen.

If you have set up content filtering on the *Block Sites* page, you can also log when someone on your network tried to access a blocked site.

If you have e-mail notification on, you'll receive these logs in an e-mail message. If you don't have e-mail notification set up, you can view the logs here.

To delete all log entries:

- Click **Clear Log**.

To see the most recent entries:

- Click **Refresh**.

To email the log now:

- Click **Send Log**.

Include in Log

Use these checkboxes to determine which events are included in the log. Checking all options will increase the size of the log, so it is good practice to disable any events which are not really required.

- Attempted access to blocked sites - If checked, attempted Internet accesses which were blocked are logged.
- Connections to the Web-based interface of this Router - If checked, this will log connections TO this Router, rather than through this Router to the Internet.
- Router operation - If checked, other Router operations (not covered by the selections above) will be logged.
- Known DoS attacks and Port Scans - If checked, Denial of Service attacks, as well as port scans, will be logged.

Syslog

The Logs can be send to a Syslog server. Enable one of these three options, as required:

- Disable - Select this if you don't have a Syslog server.
- Broadcast on LAN - the Syslog data is broadcast, rather than sent to a specific Syslog server. Use this if your Syslog Server does not have a fixed IP address.
- Send to this Syslog server IP address - If your Syslog server has a fixed IP address, select this option, and enter the IP address of your Syslog server.

Block Sites Help

If you want to limit access to certain sites on the Internet, you need to set up content filtering. There are two ways to filter content:

- blocking access to certain domains (for example, pornoXXXsiteXXX.com) or
- blocking sites that contains certain words (like profanity or explicit sexual material).

When users try to access a blocked site, they will get a message: "Blocked by NETGEAR".

To Enable Block Sites:

Click **Per Schedule** to turn on Block Sites and block according to the settings on the *Schedule* page.

Click **Always** to turn on Block Sites to allow blocking all of the time, independant of the *Schedule* page.

Note: On the *Schedule* page you can set when keyword and domain name blocking occurs.

To Disable Block Sites:

Click **Never** to turn off Block Sites.

To Block Keywords Or Internet Domains:

1. Select when to turn on **Keyword Blocking** (Never, Per Schedule, or Always).
2. In the box where you see **Type Keyword Or Domain Name Here**, type the word or domain name you want to block.
3. Click **Add Keyword**.
4. The word or domain name will appear in the list below.
5. Continue adding names and keywords until you are finished.
6. Click **Apply** when finished.

Block List - The list under the heading "Block Sites Containing these Keywords or Domain Names" contains the current list of items to block.

To Delete A Keyword Or Domain Name:

1. Select the word or domain name in the list.
2. Click **Delete Keyword**.
3. Continue selecting and deleting names and keywords until you are finished.
4. Click **Apply**.

To Delete All Keywords And Domain Names:

1. Click **Clear List**.
 2. Click **Apply**.
-

To Allow One Computer To Have Unrestricted Access To The Internet:

1. Select the **Allow Trusted IP Address To Visit Blocked Sites** check box.

2. Type the IP address of the computer in the **Trusted IP Address** area.
You should only need to type a number in the last box.
3. Click **Apply**.

To Allow Unrestricted Access To The Internet:

1. Select **Never** in the **Keyword Blocking** menu.
2. Click **Apply**.

Firewall Rules Help

You can use this screen to create Firewall rules to block or allow specific traffic. **This feature is for Advanced Administrators only!** Incorrect configuration will cause serious problems.

Outbound Services

This lists all existing rules for outbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule allows all outgoing traffic.

To create a new rule:

1. Click the "Add" button. (It does not matter which radio button is selected)
2. The "Outbound Service" screen will be displayed. This screen has its own help file.
3. Complete the "Outbound Service" screen, and save the data. The new rule will be listed in the table when you return to this screen.

To make changes to an existing rule:

1. Click the radio button next to an row in the table.
2. Click the button for the desired actions:
 - Edit - to make any changes to the rule definition. The "Outbound Service" screen will be displayed, with the data for the selected rule.
 - Move - to move the selected rule to a new position in the table. You will be prompted for the new position.
 - Delete - to delete the selected rule.

Inbound Services

This lists all existing rules for inbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule blocks all inbound traffic.

To create a new rule:

1. Click the "Add" button. (It does not matter which radio button is selected)
2. The "Inbound Service" screen will be displayed. This screen has its own help file.
3. Complete the "Inbound Service" screen, and save the data. The new rule will be listed in the table when you return to this screen.

To make changes to an existing rule:

1. Click the radio button next to an row in the table.
2. Click the button for the desired actions:
 - Edit - to make any changes to the rule definition. The "Inbound Service" screen will be displayed, with the data for the selected rule.
 - Move - to move the selected rule to a new position in the table. You will be prompted for the new position.
 - Delete - to delete the selected rule.

To Accept Or Cancel

Click **Accept** to update changes to the **Outbound Services** and **Inbound Services** tables.

Outbound Service Help

You can use this screen to define a new Outbound Firewall rule, or edit an existing rule. Outbound Firewall rules are used to block or allow access by computers on your network to services or applications on the Internet.

Service

Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu.

Action

Select the desired action for packets covered by this rule:

- BLOCK always
- BLOCK by schedule, otherwise Allow
- ALLOW always
- ALLOW by schedule, otherwise Block

Note:

- Any outbound traffic which is not blocked by rules you create will be allowed by the Default rule.
- ALLOW rules are only useful if the traffic is already covered by a BLOCK rule. (That is, you wish to allow a subset of traffic which is currently blocked by another rule.)
- To define the Schedule used in these selections, use the "Schedule" screen.

LAN users

These settings determine which computers on your network are affected by this rule, based on their source (LAN) IP address. Select the desired option:

- Any - All local IP addresses are covered by this rule.
- Address range - If this option is selected, you must enter the "Start" and "Finish" fields.
- Single address - Enter the required address in the "Start" fields.

WAN Servers

These settings determine which Internet locations are covered by the rule, based on their destination (WAN) IP address. Select the desired option:

- Any - All Internet IP address are covered by this rule.
- Address range - If this option is selected, you must enter the "Start" and "Finish" fields.
- Single address - Enter the required address in the "Start" fields.

Log

This determines whether packets covered by this rule are logged. Select the desired action:

- Always - always log traffic considered by this rule, whether it matches or not. (This is useful when debugging your rules.)
- Never - never log traffic considered by this rule, whether it matches or not.
- Match - Log traffic only it matches this rule. (The action is determined by this rule.)
- Not Match - Log traffic which is considered by this rule, but does not match (The action is NOT determined by this rule.)

Click **Apply** to have your changes take effect.

Inbound Service Help

You can use this screen to define a new Inbound Firewall rule, or edit an existing rule. Firewall rules can be used to block or allow specific traffic. **This feature is for Advanced Administrators only!** Incorrect configuration will cause serious problems.

Service

Select the desired Service. This determines which packets are covered by this rule. If necessary, you can define a new Service on the "Services" screen, by defining the protocols and port numbers used by the Service.

Action

Select the desired action for packets covered by this rule:

- ALLOW always
- ALLOW by schedule, otherwise Block
- BLOCK always
- BLOCK by schedule, otherwise Allow

Note:

- Any inbound traffic which is not allowed by rules you create will be blocked by the Default rule.
- BLOCK rules are only useful if the traffic is already covered by an ALLOW rule. (That is, you wish to block a sub-set of traffic which is currently allowed by another rule.)
- To define the Schedule used in these selections, use the "Schedule" screen.

LAN Server

Enter the IP address of the PC or Server on your LAN which will receive the inbound traffic covered by this rule.

WAN Users

These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option:

- Any All IP addresses are covered by this rule.
- Address range If this option is selected, you must enter the "Start" and "Finish" fields.
- Single address Enter the required address in the "Start" fields.

Log

This determines whether packets covered by this rule are logged. Select the desired action.

- Always - always log traffic considered by this rule, whether it matches or not. (This is useful when debugging your rules.)
- Never - never log traffic considered by this rule, whether it matches or not.
- Match - Log traffic only it matches this rule. (The action is determined by this rule.)
- Not Match - Log traffic which is considered by this rule, but does not match (The action is NOT determined by this rule.)

Click **Apply** to have your changes take effect.

Click **Back** to return to the previous screen

Services Help

The Services menu contains a list of user-defined Services for creating firewall rules. If a service does not appear in the predefined Services list in the Firewall Rules menu, you can define the service in this menu. The new service will then appear in the Firewall Rules menu Services list.

Service Table

This table lists all Services you have defined. If you have not defined any Services, the table will be empty.

To Create a Service

1. Click **Add Custom Service**
2. Enter the data for the service as required.
3. Click **Apply** to save the new service.

To Edit a Service

1. Click the radio button next to a service in the table.
2. Click **Edit Service** to display the service's data in the "Service Definition" section.
3. Change the data for the service as required.
4. Click **Apply** to save your changes.

To Delete a Service

1. Click the radio button next to a service in the table.
2. Click **Delete Service** to delete the selected service.

Schedule Help

If you have set Firewall Rules on the "Rules" screen or Keyword Filtering on the "Block Sites" screen, you can set up a schedule for when the rules are applied.

To apply Rules based on a schedule:

1. On the "Rules" screen, create the required Rules, using either "Block by Schedule" or "Allow by Schedule" for each rule, as required.
2. Select the **Use this schedule for rules** checkbox on this screen.
3. Select the days and times on this screen, as required.
4. Click **Apply**.

Note: If the schedule is disabled on this screen, this affects ALL Rules which are using a schedule.

Days

Select the required days

- Every Day - all days will automatically be selected
- Sunday, Monday .. If "Every Day" is NOT selected, you can choose the required days individually.

Time of day

This determines when the schedule is applied, for each day selected above. Enter the desired Start and Finish times.

Note: Enter the values as 24-hour time. For example, 10:30 am would be 10 hours and 30 minutes and 10:30 pm would be 22 hours and 30 minutes.

Timezone

The Router will determine the current time and date by contacting a Network Time (NTP) Server on the Internet. In order to display your local time, you must select your **Time Zone** from the list.

If your region uses Daylight Savings Time, you must manually check **Adjust for Daylight Savings Time** at the beginning of the adjustment period, and uncheck it at the end of the Daylight Savings period.

Use this NTP Server

If you prefer to use a particular NTP server as the primary server, check the checkbox **Use this NTP Server** and enter the Server's IP address under **Use this NTP Server**.

If this setting is not enabled, the default NTP Servers are used.

To Accept Or Cancel

Click **Apply** to save changes.

Click **Cancel** to disregard any unsaved changes.

E-mail Help

Your Router can periodically email you the system log. (On the *Logs* screen, you can choose what events are to be included in the log.) The Router can also send an immediate alert when it detects a significant security incident such as

- A known hacker attack is directed at your IP address
- A computer on the Internet scans your IP address for open ports
- Someone on your LAN (Local Area Network) tries to visit a blocked site.

If you'd like to have alerts and logs sent to you by e-mail, fill out the settings on this form.

You can always check the logs manually by viewing the *Logs* page. If you don't want to receive e-mails, simply leave the **Turn e-mail notification on** checkbox unchecked.

Send alerts and logs by e-mail

To receive alerts and logs by e-mail:

1. Select the **Turn E-mail Notification On** check box above.
2. In the **Send To This E-mail Address** box, type the e-mail address where the alerts and logs will be sent. Use a full e-mail address (for example, ChrisXY@myISP.com).
3. In the **Outgoing Mail Server** box, type the name or IP address of the outgoing SMTP mail server of your ISP (for example, mail.myISP.com).
If you leave this box blank, no alerts or logs will be sent to you.
4. Check **My Mail Server requires authentication** if you need to "login" to your SMTP Server in order to send E-mail. If this is checked, you must enter the user name and password for the Mail Server.
Tip: You used this information when you set up your e-mail program. If you can't remember it, check the settings in your e-mail program.

Send E-Mail alerts immediately

If you want **E-mail alerts** sent immediately whenever a security incident occurs, select the appropriate checkboxes.

Send logs according to this schedule

If you want logs sent, select one of the options:

- If you selected **Weekly**, then select which day of the week.
- If you selected **Weekly** or **Daily**, select the time of day for the e-mail to be sent.

Note: If E-mail logging is enabled, and the log is filled before the day/time specified to send it, it will be sent when full.

Click **Apply** to have your changes take effect.

Click **Cancel** to disregard any unsaved changes.

Router Status Help

You can use the *Router Status* page to check the current settings and statistics for your router. This page shows you the current settings. If something needs to be changed, you'll have to change it on the relevant page.

Account Name: This is the Account Name that you entered in the *Setup Wizard* or *Basic Settings*.

Firmware Version: This is the current software the router is using. This will change if you upgrade your router.

ADSL Port: These are the current settings that you set in the *Setup Wizard* or *Basic Settings* pages.

- MAC Address - the physical address of the Router, as seen from the Internet.
- IP Address - current Internet IP address. If assigned dynamically, and no Internet connection exists, this will be blank or 0.0.0.0
- DHCP - indicates either *Client* (IP address is obtained dynamically) or *None*.
- IP Subnet Mask - the subnet mask associated with the Internet IP address Domain Name Server - displays the address of the current DNS.

LAN Port: These are the current settings, as set in the *LAN IP Setup* page.

- MAC Address - the physical address of the Router, as seen from the local LAN.
- IP Address - LAN IP address of the Router.
- DHCP - indicates if the Router is acting as a DHCP Server for devices on your LAN.
- IP Subnet Mask - subnet mask associated with the LAN IP address.

Modem: The current Modem status and settings are shown in this section.

- ADSL Firmware Version - This is the version number of the low-level ADSL firmware. This is contained within the Router Firmware.
- Modem Status - the current state of the ADSL connection to your phone company.
- DownStream Connection Speed - the connection speed of the ADSL connection from the phone company to your Router.
- UpStream Connection Speed - the connection speed of the ADSL connection from your Router to the phone company.
- VPI - the VPI setting entered on the ADSL Settings page.
- VCI - the VCI setting entered on the ADSL Settings page.

Wireless Port: These are the current settings, as set in the *Wireless Settings* page.

- Name (SSID) - SSID of the Router.
- Region - the location (country).
- Channel - the current channel in use.
- Mode - indicates the current mode (g & b, g, or b)
- Wireless AP - indicates if the Access Point feature of the Router is enabled or not. If not enabled, the Wireless LED on the front panel will be off.
- Broadcast Name - indicates if the Router is broadcasting its SSID.

Click **Show Statistics** to see router performance statistics such as the number of packets sent and number of packets received for each port.

Attached Devices Help

This page shows the IP Address, Device Name and MAC (Media Access Control) Address for each computer attached to the router.

You cannot change any of the values on this page. To update this page and to show the current attached devices, click on the *Refresh* button.

Backup Settings Help

This page allows you to backup, restore and erase the router's current settings.

Once you have the router working properly, you should backup the information to have it available if something goes wrong. When you backup the settings, they are saved as a file on your computer. You can restore the router's settings from this file.

To create a backup file of the current settings:

1. Click **Backup**.
2. If you don't have your browser set up to save downloaded files automatically, locate where you want to save the file, rename it if you like, and click **Save**.
If you have your browser set up to save downloaded files automatically, the file is saved to the your browser's download location on the hard disk and is called *NETGEAR_VVG2000.cfg*.

IMPORTANT! Once you start restoring settings or erasing the router, do NOT try to go online, turn off the router, shutdown the computer or do anything else to the router until it finishes restarting! This should only take a minute or so. When the Test light stops blinking, wait a few more seconds before doing anything with the router.

To restore settings from a backup file:

1. Click **Browse**.
2. Locate and select the previously saved backup file (by default, *NETGEAR_VVG2000.cfg*).
3. Click **Restore**.
A window appears letting you know that the router has been successfully restored to previous settings. The router will restart. This will take about one minute.
IMPORTANT! Do not try to go online, turn off the router, shutdown the computer or do anything else to the router until it finishes restarting! When the Test light stops blinking, wait a few more seconds before doing anything with the router.
4. Close the message window.

To erase the current settings and reset the router to the original factory default settings:

- Click **Erase**.
IMPORTANT! Do not try to go online, turn off the router, shutdown the computer or do anything else to the router until the router finishes restarting! When the Test light stops blinking, wait a few more seconds before doing anything with the router.

After you have erased the router's current settings, the router's password will be *password*, the LAN IP address will be **192.168.0.1** and the router will act as a DHCP server on the LAN and act as a DHCP client to the Internet.

Set Password Help

You use the *Set Password* page to change the password you use to access the *Settings* pages -- NOT your ISP account password.

To change the password:

1. Type the old password.
The default password for the router is: password.
2. Type a new password and type it again in the **Repeat New Password** box to confirm it.
Note: Be sure to write it down in a secure location.
3. Click **Apply** to have the password changed or click **Cancel** to keep the current password.

Note: If you have backed up the router settings previously, you should do a new backup so that the settings file includes the new password.

Diagnostics Help

You can use this page to perform various diagnostics. For normal operation, these are not required.

Ping an IP address

Use this to send a "ping" packet request to the specified IP address. This is often used to test a connection. If the request "times out" (no reply is received), this usually means the destination is unreachable.

However, some network devices can be configured not to respond to a ping.

Perform a DNS Lookup

A DNS (Domain Name Server) converts the Internet name (e.g. www.netgear.com) to an IP address. If you need the IP address of a Web, FTP, Mail or other Server on the Internet, you can do a DNS lookup to find the IP address.

Display the Routing Table

This operation will display the internal routing table. This information is used by Technical Support and other staff who understand Routing Tables.

Reboot the Router

Use this button to perform a remote reboot (restart). You can use this if the Router seems to have become unstable or is not operating normally.

Note Rebooting will break any existing connections either to the Router (such as this one) or through the Router (for example, LAN users accessing the Internet). However, connections to the Internet will automatically be re-established when possible

Router Upgrade Help

You install new versions of the router's software using the *Router Upgrade* page.

Go to the NETGEAR Web site to get new versions of the router software. After downloading the file, you'll need to unzip (or unstuff) it before upgrading the router.

IMPORTANT! Once you click **Upload** do NOT interrupt the process of sending the software to the router and restarting the router. If you think the process may be interrupted in some way, click **Cancel** to keep the current router software.

To upgrade router software:

1. Go to www.NETGEAR.com and download the updated software.
2. If not done automatically, uncompress the file.
You may want to read the *Release Notes* before continuing.
3. Click **Browse**.
4. Locate and select the file you just downloaded and uncompressed.
5. Click **Upload** to send the software to the router.

This loads the new software in the router and causes the router to restart.

Note: Do not try to go online, turn off the router, shutdown the computer or do anything else to the router until the router finishes restarting! When the Ready light stops blinking, wait a few more seconds before doing anything.

6. Click **Router Status** and check the Firmware Version to verify that your router now has the new software installed.

IMPORTANT! In some cases, such as a major upgrades, you may need to reconfigure your router after upgrading it. Refer to the *Release Notes* included with the software to find out if you need to reconfigure the router.

If you are unable to successfully upgrade using this method, refer to the *Reference Manual* on the *Router GearBox CD* for other ways to upgrade the router.

VLAN Group

QoS Settings Help

QoS is an advanced feature that can be used to priority some internet applications and on-line gaming, and to minimize the impact when the bandwidth is busy.

Wi-Fi Multi-media (WMM) Settings

WMM (Wireless Multimedia) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video or audio, will have a higher priority than normal traffic. For WMM to function correctly, Wireless clients must also support WMM.

Turn Internet Access QoS On

If Turn On, the QoS function will work to priority the Internet access traffic. For the applications, On-line Gaming, Ethernet LAN Port, or specified MAC address, that already exist in the pull-down list, you can modify the Priority level by clicking the **Edit** button, or clicking the **Delete** button to erase the priority rule. Otherwise, you may also define the priority policy for each On-line gaming, Application, LAN port, or the computer's MAC address by clicking the **Add Priority Rule** button.

To Save Or Cancel Changes

Click **Apply** to have your changes take effect.
Click **Cancel** to return to the previous settings.

For Applications or On-line Gaming

To setup the priority for an Application or On-line Gaming:

1. Choose the Applications or On-line Gaming from the Priority Category lists.
2. Select the Internet application or game you want to use from one of the relevant lists.
3. Choose the priority level: Highest, High, Normal, or Low.
4. You may also type the name in the **QoS Policy for** box for this rule you preferred.
5. Click **Apply**.

For Ethernet LAN port

To setup the priority for LAN port:

1. Choose the LAN port number you plan to specify the priority level for those computers connecting on this LAN port.
2. Choose the priority level: Highest, High, Normal, or Low.
3. You may also type the name in the **QoS Policy for** box for this rule you preferred.
4. Click **Apply**.

For MAC address

To setup the priority for specified computer via MAC address:

1. Choose the MAC Address from the Priority Category lists.
2. Click the **Refresh** button to update those computers already connected with routers.

3. Select the entry's radio button of the table.
4. Modify the information from the **MAC address**, and the **Device Name** boxes for easily remember.
5. Choose the priority level: Highest, High, Normal, or Low.
6. You may also type the name in the **QoS Policy for** box for this rule you preferred.
7. Click **Edit** button.
8. Click **Apply**.

To add the priority for specified computer via MAC address:

1. Choose MAC Address selection from the Priority Category lists.
2. Input the **MAC address** value for the computer you plan to define the priority on it.
3. You may also input the **Device Name** boxes for easily remember.
4. Choose the priority level: Highest, High, Normal, or Low.
5. You may also type the name in the **QoS Policy for** box for this rule you preferred.
6. Click **Add** button.
7. Click **Apply**.

To delete a service entry

1. Select the entry's radio button of the table.
2. Click **Delete** button.
3. Click **Apply** button.

WAN Setup Help

Using this page, you can set up several parameters related the the WAN connection.

The wan number is which you set in basic settings. When wan setting is changed ,you must set the rules again. **Multiplexing Method,VPI,VPI and The current active protocol** just display the selected wan information

Connect Automatically, as Required

This option just can act when ppp is not set to be always on line. Normally, this option should be Enabled, so that an Internet connection will be made automatically, whenever Internet-bound traffic is detected. If this causes high connection costs, you can disable this setting.

If disabled, you must connect manually, using the sub-screen accessed from the "Connection Status" button on the **Status** screen.

If you have an "Always on" connection, this setting has no effect.

Disable Port Scan and DOS Protection - The Firewall protects your LAN against Port Scans and Denial of Service (DOS) attacks. This should be disabled only in special circumstances.

Respond To Ping On Internet Port

If you want the VVG2000 to respond to a 'Ping' from the Internet, click this check box. This can be used as a diagnostic tool. This can be a security problem. You shouldn't check this box unless you have a specific reason to do so.

MTU Size

The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes, or 1492 Bytes for PPPoE connections. For some ISPs you may need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

DNS Server Configuration

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will only accept the received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) from WAN1 during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses.

Routing -- Default Gateway

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will only accept the received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) from WAN1. If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface.

To Apply Or Cancel

Click **Apply** to update changes to the **MTU Size**.

Click **Cancel** to disregard any unsaved changes.

Dynamic DNS Help

A Dynamic DNS (DDNS) Service provides a central public database where information (such as e-mail addresses, host names and IP addresses) can be stored and retrieved. The Dynamic DNS server also stores password-protected information and accepts queries based on e-mail addresses.

If you want to use a DDNS service, you must register for it. The Dynamic DNS client service provider will give you a password or key.

To set up for DDNS:

1. If you have registered with a DDNS service provider, select the **Use A Dynamic DNS Service** check box.
2. Select the name of your dynamic DNS **Service Provider**.
3. Type the **Host Name** that your dynamic DNS service provider gave you.
The DDNS service provider may call this the domain name.
4. Type the **User Name** for your DDNS account.
5. Type the **Password** (or key) for your DDNS account.
6. Click **Apply** to have the DDNS service used.

Use Wildcards - If you have DYNDNS as your DDNS service provider, you may select the **Use Wildcards** check box to activate this optional feature.

Note: The Router supports only basic DDNS and the login and password may not be secure. If you have a private WAN IP address, do not use DDNS service as it may lead to problems.

LAN IP Setup Help

The DHCP and TCP/IP default values work for most users.

Group Number Select

GROUP number is related to VLAN Group settings. The default setting is 4 lan ports in GROUP1

LAN TCP/IP Setup

These are advanced settings that you may configure if you are a network administrator and your network contains multiple Routers. If you make any changes to these settings you will need to restart your computer(s) for the settings to take effect.

- **IP Address:** Type the IP address of your Router in dotted decimal notation (factory default: 192.168.0.1).
- **IP Subnet Mask:** The subnet mask specifies the network number portion of an IP address. Your Router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask (computed by the Router).
- **RIP Direction:** RIP (Routing Information Protocol, RFC1058 and RFC1389) allows a Router to exchange routing information with other Routers. The RIP Direction selection controls how the Router sends and receives RIP packets. Both is the default.
 - When set to **Both** or **Out Only**, the Router will broadcast its routing table periodically.
 - When set to **Both** or **In Only**, it will incorporate the RIP information that it receives.
 - When set to **None**, it will not send any RIP packets and will ignore any RIP packets received.
- **RIP Version:** This controls the format and the broadcasting method of the RIP packets that the Router sends. (It recognizes both formats when receiving.) By default, this is set for RIP-1.
 - RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
 - RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format.
 - RIP-2B uses subnet broadcasting.
 - RIP-2M uses multicasting. (See note below.)

Note: Multicasting can reduce the load on non-Router machines because they do not listen to the RIP multicast address and will not receive the RIP packets. However, if one Router uses multicasting, then all Routers on your network must use multicasting.

Default DMZ Server

Specifying a Default DMZ Server allows you to set up a computer or server that is available to anyone on the Internet for services that you haven't defined. There are security issues with doing this, so only do this if you're willing to risk open access. If you do not assign a Default DMZ Server, the Router discards any incoming service requests which are undefined. This can be a

security problem. You shouldn't check this box unless you have a specific reason to do so.

To assign a computer or server to be a DMZ server:

1. Click the *Default DMZ Server* checkbox
 2. Type the IP address for that server.
 3. Click **Apply**.
-

Use Router As DHCP Server

The VVG2000 Router is set up by default as a DHCP (Dynamic Host Configuration Protocol) Server, which provides the TCP/IP configuration for the all the computers that are connected to the Router.

Unless told to change these settings by your ISP, leave the **Use Router As DHCP Server** check box checked.

If your ISP has you clear this check box, you must have another DHCP server within your network or else you must manually configure the computer.

- **Starting IP Address:** This box specifies the first of the contiguous addresses in the IP address pool. 192.168.0.2 is the default start address.
 - **Ending IP Address:** This box specifies the last of the contiguous addresses in the IP address pool. 192.168.0.254 is the default ending address.
-

Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

To Reserve An IP Address:

1. Click the **Add** button.
2. Check the Computer you wish to add to the **Address Reservation Table** at first.
3. If the Computer is not on the **Address Reservation Table**; Enter the IP Address, MAC Address, and Device Name of the computer you wish to add.
4. Click the **Add** button when finished.

To Edit A Reserved IP Address:

1. Select the radio button next to the reserved address you want to edit.
2. Click the **Edit** button.
3. Edit the IP Address, MAC Address or Device Name.
4. Click the **Accept** button when finished.

To Delete A Reserved IP Address:

1. Select the radio button next to the reserved address you want to delete.
 2. Click the **Delete** button.
-

To Save Or Cancel Changes

Click **Apply** to save the new settings to the Router.If the lan ip changed,the Router need to be reboot

Click **Cancel** to disregard any unsaved changes

Wireless Settings Help

NOTE: To ensure proper agency compliance and compatibility between similar products in your area; the operating channel & region must be set correctly by you.

Placement of the Router to Optimize Wireless Connectivity

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the Router. For best results, place your Router:

- Near the center of the area in which your PCs will operate,
- In an elevated location such as a high shelf,
- Away from potential sources of interference, such as PCs, microwaves, and cordless phones,
- Away from large metal surfaces.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Router.

Wireless Network

Name (SSID)

Enter a value of up to 32 alphanumeric characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is NETGEAR, but NETGEAR strongly recommends that you change your networks Name (SSID) to a different value. This value is also case-sensitive. For example, *Wireless* is not the same as *wireless*.

Region

Select your region from the drop-down list. This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the Router in a region other than the region shown here. If your country or region is not listed, please check with your local government agency or check our website for more information on which channels to use.

Channel

This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point.

Mode

Select the desired wireless mode. The options are:

- Up to 54 Mbps - Legacy Mode with maximum speed of up to 54 Mbps for b/g networks.
- Up to 130 Mbps - Neighbor Friendly Mode - Default speed up to 130 Mbps in presence of neighboring wireless networks.
- Up to 270 Mbps - Performance Mode - Maximum Wireless-N speed up to 270 Mbps.

The default is "Up to 130Mbps", which allows all 11b and 11g wireless stations. The NETGEAR WN511B runs at 130 Mbps when accessing this router.

Wireless Access Point

Enable Wireless Access Point

The Wireless Access Point of this Router can be enabled or disabled to allow wireless access. The wireless icon on the front of the Router will also display the current status of the Wireless Access Point to let you know if it is disabled or enabled.

If Enabled, wireless stations will be able to access the Internet.

If Disabled, wireless stations will not be able to access the Internet.

Allow Broadcast of Name (SSID)

If Enabled, the SSID will broadcast its name to all Wireless Stations. Stations which have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point.

Wireless Isolation

If Enabled, the Wireless Stations will be hidden from each other, and will not be able to communicate with each other. For normal situations, this setting should be left at the default value of **Disabled**.

Wireless Station Access List

By default, any wireless PC that is configured with the correct SSID will be allowed access to your wireless network. For increased security, you can restrict access to the wireless network to only allow specific PCs based on their MAC addresses. From the *Wireless Settings* menu, click the **Setup Access List** button to display the Wireless Station Access List menu.

Security Options

Select the desired option, and ensure all your Wireless stations have the same setting:

- **Disable** - This will disable the security function. Data will not be encrypted before transmission.
- **WEP** - WEP (Wired Equivalent Privacy), if used, encrypts data before transmission. This provides greater security and privacy. All Wireless Stations need to use the same settings (WEP Key size and WEP key).
- **WPA-PSK** - This version of WPA uses a PSK (Pre-shared Key) for authentication, so you don't need a Radius Server. All Wireless stations need to use the same PSK (Pre-shared Key). Data transmissions are encrypted using a 256 Bit key derived from the PSK. This key changes regularly, providing greater protection. WPA is more secure than WEP, and should be used if possible.
- **WPA-802.1x** - This version of WPA requires the use of a Radius server for authentication. Each user (Wireless Client) must have a "user" login on the Radius Server, and this device must have a "client" login on the Radius server. Data transmissions are encrypted using a key which is automatically generated.

WEP Security Encryption

Authentication Type

Normally this can be left at the default value of "Automatic." If that fails, select the appropriate

value - "Open System" or "Shared Key." Check your wireless card's documentation to see what method to use.

Encryption Strength

Select the WEP Encryption level:

- 64-bit (sometimes called 40-bit) encryption
- 128-bit encryption

WEP Key

You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.

Automatic Key Generation (Passphrase)

Enter a word or group of printable characters in the Passphrase box and click the Generate button to automatically configure the WEP Key(s). If encryption strength is set to 64 bit, then each of the four key boxes will automatically be populated with key values. If encryption strength is set to 128 bit, then only the selected WEP key box will automatically be populated with key values.

Manual Entry Mode

Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key box.

For 64 bit WEP - Enter ten hexadecimal digits (any combination of 0-9, A-F).

For 128 bit WEP - Enter twenty-six hexadecimal digits (any combination of 0-9, A-F).

Be sure to click Apply to save your settings in this menu.

WPA-PSK Security Encryption

Network Key

For WPA-PSK, you need to enter the **Network Key** here. The Key must be from 8 to 63 ASCII characters. Your Wireless Stations must use the same key.

WPA Encryption

Currently, only TKIP is supported. Ensure your Wireless Stations are also using TKIP. Normally, this is the default. If there is no choice of encryption methods for WPA-PSK, then you can assume TKIP will be used.

WPA-802.1x Security Encryption

Radius Server Name/IP Address

Enter the name or IP address of the Radius Server on your LAN.

- Each user (Wireless Client) must have a "user" login on the Radius Server.
- This device must have a "client" login on the Radius server. The login name is the name of this device.

Radius Port

Enter the port number which is used for connections to your Radius Server.

Shared Key

Enter the shared key, as configured on your Radius server, for the "client" login for this device.

To Save Or Cancel Changes

Click **Apply** to have your changes take effect.

Click **Cancel** to return to the previous unsaved settings.

WPS Settings Help

WPS Settings

Router's PIN

This is the PIN number you use on a registrar (e.g. from the Network Explorer on a Vista Windows PC) to configure the router's wireless settings through WPS.

You can also find the PIN on the router's product label too.

Keep Existing Wireless Settings

This shows whether the router is in the WPS Configured state.

If the this option is not checked, adding a new wireless client will change the router's wireless settings to an automatically generated random SSID and security key. Besides, if this option is checked, some external registrar (e.g. Network Explorer on Vista Windows) may not see the router. Configuring basic wireless settings from the router's management GUI makes this option checked.

To Save Or Cancel Changes

Click **Apply** to have your changes take effect.

Click **Cancel** to return to the previous settings.

Remote Management Help

Using the Remote Management menu, you can allow a user on the Internet to configure, upgrade and check the status of your router.

IMPORTANT: *Be sure to change the router's default password to a very secure password.*

Turn Remote Management On

1. Click the check box to **Turn Remote Management On** .
 2. Click the **Apply** button to save changes .
-

Remote Management Address

This is the current address you will use When accessing your router from the Internet. To access the router, you will type your router's WAN IP address into your browser's Address (in IE) or Location (in Netscape) box, followed by a colon (:) and the custom port number. For example, if your external address is 10.0.0.123 and you use port number 8080, enter in your browser:

http://10.0.0.123:8080

Allow Remote Access

For security, you should restrict access to as few external IP addresses as practical.

Click **Only This Computer** to allow access by only one IP address.

Click **IP Address Range** to allow access from a range of IP addresses on the Internet, enter a beginning and ending IP address to define the allowed range.

Click **Everyone** to allow access by everyone on the Internet.

Port Number

Web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65534, but do not use the number of any common service port.

To Save Or Cancel Changes

Click **Apply** to have your changes take effect.

Click **Cancel** to return to the previous unsaved settings

Static Routes Help

Static routes give the router information that it cannot learn automatically through other means. This can happen when RIP is disabled on the LAN. (See the *LAN IP Setup* page.) All defined static routes appear in the table. To add or delete a route, work in the area under the Static Routes table.

To Set Up A Static Route:

1. Click the **Add** button.
2. Type a route name for this static route in the **Route Name** box under the table. (This is for identification purposes only.)
3. Select **Private** if you want to limit access to the LAN only.
4. Select **Active** to make this route effective.
5. Type the **Destination IP Address** of the final destination.
6. Type the **IP Subnet Mask** for this destination.
If this is for a single host, type 255.255.255.255.
7. Type the **Gateway IP Address**, which must be a router on the same segment.
8. Type a number between 2 and 15 as the **Metric** value.
This represents the number of other routers on your network. Usually, setting this to 2 or 3 works the best, but if this is a direct connection, set it to 2.
9. Click **Apply** to have the static route entered into the table.

To Edit A Static Route:

1. Click the radio button next to route you want to edit.
2. Update the information.
3. Click **Apply** when finished.

To Delete A Static Route:

1. Click the radio button next to route you want to delete.
2. Click **Delete**.
3. Click **Apply** to have the static route deleted from the table.

UPnP Help

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

Turn UPnP On

UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If disabled, the router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the router.

Advertisement Period

The Advertisement Period is how often the router will advertise (broadcast) its UPnP information. This value can range from 1 to 1440 minutes. The default period is for 30 minutes. Shorter durations will ensure that control points have current device status at the expense of additional network traffic. Longer durations may compromise the freshness of the device status but can significantly reduce network traffic.

Advertisement Time To Live

The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it may be necessary to increase this value a little.

UPnP Portmap Table

The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.

To Save, Cancel or Refresh the Table

Click **Apply** to save the new settings to the router.

Click **Cancel** to discard any unsaved changes.

Click **Refresh** to update the portmap table and to show the active ports that are currently opened by UPnP devices.

<http://kserver.netgear.com/products/DVG834NOUD.asp>

http://kserver.netgear.com/products_automatic/DVG834NOUD.asp