14

DHCP Server

14.1 Overview

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 NBG5615's LAN as a DHCP server or disable it. When configured as a server, the NBG5615 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.

14.1.1 What You Can Do

- Use the **General** screen to enable the DHCP server (Section 14.2 on page 133).
- Use the **Advanced** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 14.3 on page 134).
- Use the **Client List** screen to view the current DHCP client information (Section 14.4 on page 136).

14.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

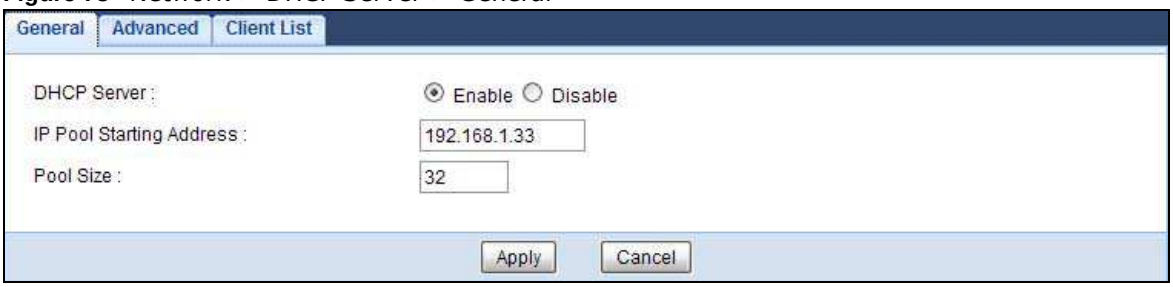
MAC Addresses

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. Find out the MAC addresses of your network devices if you intend to add them to the **DHCP Client List** screen.

14.2 DHCP Server General Screen

Use this screen to enable the DHCP server. Click **Network** > **DHCP Server**. The following screen displays.

Figure 78 Network > DHCP Server > General



The following table describes the labels in this screen.

Table 52 Network > DHCP Server > General

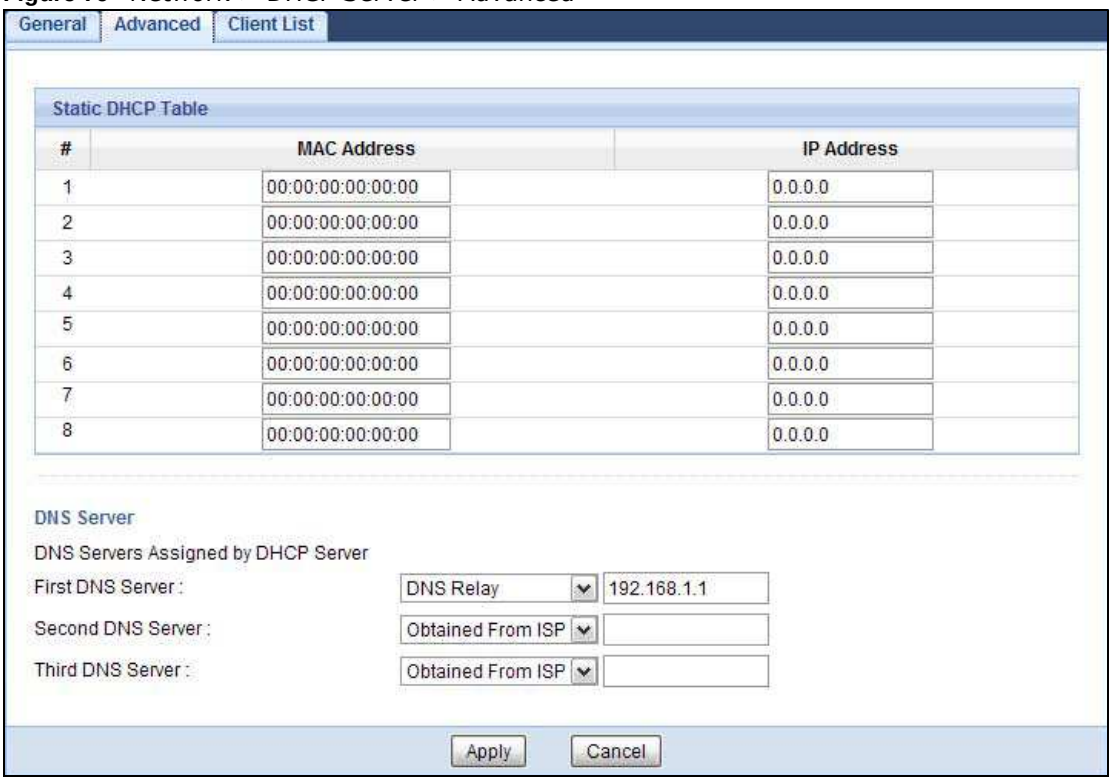
LABEL	DESCRIPTION
DHCP Server	Select **Enable** to activate DHCP for LAN. DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Enable the DHCP server unless your ISP instructs you to do otherwise. Select **Disable** to stop the NBG5615 acting as a DHCP server. When configured as a server, the NBG5615 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.
Apply	Click **Apply** to save your changes back to the NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.3 DHCP Server 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 NBG5615 sends to the DHCP clients.

To change your NBG5615's static DHCP settings, click **Network** > **DHCP Server** > **Advanced**. The following screen displays.

Figure 79 Network > DHCP Server > Advanced



The following table describes the labels in this screen.

Table 53 Network > DHCP Server > 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.
DNS Server	
DNS Servers Assigned by DHCP Server	The NBG5615 passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The NBG5615 only passes this information to the LAN DHCP clients when you enable **DHCP Server**. When you disable **DHCP Server**, 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.

Table 53 Network > DHCP Server > Advanced (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the NBG5615'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 NBG5615 act as a DNS proxy. The NBG5615's LAN IP address displays in the field to the right (read-only). The NBG5615 tells the DHCP clients on the LAN that the NBG5615 itself is the DNS server. When a computer on the LAN sends a DNS query to the NBG5615, the NBG5615 forwards the query to the NBG5615'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 NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

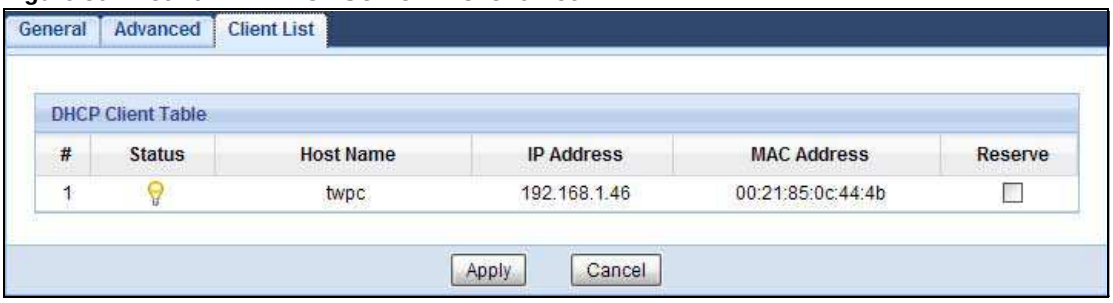
14.4 DHCP Client List Screen

The DHCP table shows current DHCP client information (including IP Address, Host Name and MAC Address) of network clients using the NBG5615'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**.

Note: You can also view a read-only client list by clicking **Monitor > DHCP Server**.

Figure 80 Network > DHCP Server > Client List



The following table describes the labels in this screen.

Table 54 Network > DHCP Server > Client List

LABEL	DESCRIPTION
#	This is the index number of the host computer.
Status	This field displays whether the connection to the host computer is up (a yellow bulb) or down (a gray bulb).

Table 54 Network > DHCP Server > Client List (continued)

LABEL	DESCRIPTION
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Reserve	Select this if you want to reserve the IP address for this specific MAC address.
Apply	Click **Apply** to save your changes back to the NBG5615.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

15 NAT

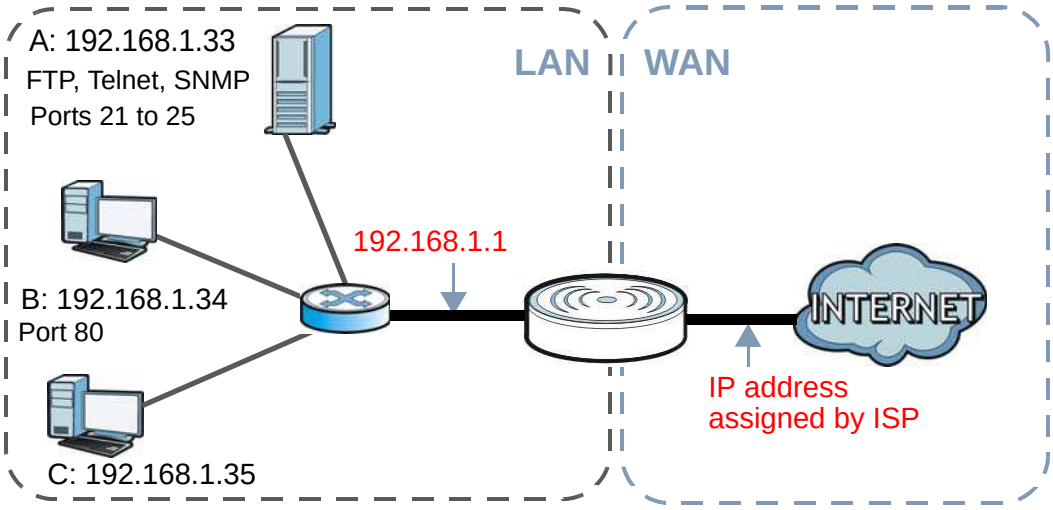
15.1 Overview

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.

The figure below is a simple illustration of a NAT network. 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 to the devices (**A** to **D**) connected to your NBG5615. The ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet. All traffic coming from **A** to **D** going out to the Internet use the IP address of the NBG5615, which is 192.168.1.1.

Figure 81 NAT Example



This chapter discusses how to configure NAT on the NBG5615.

Note: You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the NBG5615.

15.1.1 What You Can Do

- Use the **General** screen to enable NAT (Section 15.2 on page 141).

- Use the **Port Forwarding** screen to set a default server and change your NBG5615's port forwarding settings to forward incoming service requests to the server(s) on your local network (Section 15.3 on page 142).
- Use the **Port Trigger** screen to change your NBG5615's trigger port settings (Section 15.5.3 on page 147).

15.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

Inside/Outside

This denotes where a host is located relative to the NBG5615, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

This denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note: Inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet.

An inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 55 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

Note: NAT never changes the IP address (either local or global) of an outside host.

What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

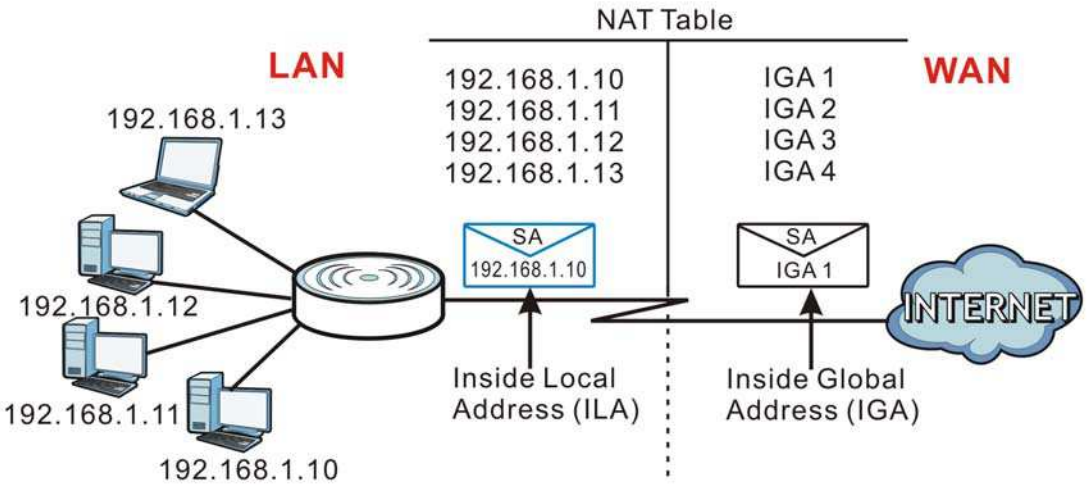
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local

network and make them accessible to the outside world. If you do not define any servers , NAT offers the additional benefit of firewall protection. With no servers defined, your NBG5615 filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address in each packet and then forwards it to the Internet. The NBG5615 keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 82 How NAT Works



15.2 General

Use this screen to enable NAT and set a default server. Click **Network > NAT** to open the **General** screen.

Figure 83 Network > NAT > General

The following table describes the labels in this screen.

Table 56 Network > NAT > General

LABEL	DESCRIPTION
Network Address Translation (NAT)	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 **Enable** to activate NAT. Select **Disable** to turn it off.
Apply	Click **Apply** to save your changes back to the NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.3 Port Forwarding Screen

Use this screen to forward incoming service requests to the server(s) on your local network and set a default server. 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.

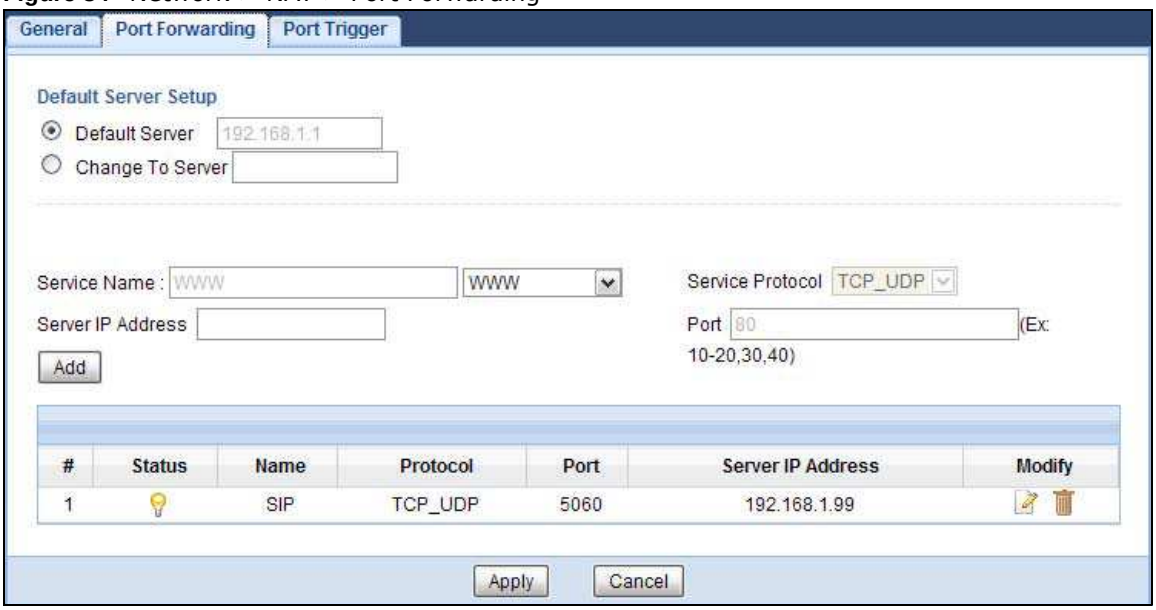
Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your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

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your NBG5615's port forwarding settings, click **Network > NAT** > **Port Forwarding**. The screen appears as shown.

Note: If you do not assign a **Default Server**, the NBG5615 discards all packets received for ports that are not specified in this screen or remote management.

Refer to Appendix C on page 249 for port numbers commonly used for particular services.

Figure 84 Network > NAT > Port Forwarding



The following table describes the labels in this screen.

Table 57 Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	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 **Port Forwarding** screen. You can decide whether you want to use the default server or specify a server manually. Select this to use the default server.
Change to Server	Select this and manually enter the server's IP address.
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will be displayed in the port forwarding summary table. Otherwise, select **User define** to manually enter the port number(s) and select the IP protocol.
Service Protocol	Select the transport layer protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP_UDP**. If you have chosen a pre-defined service in the **Service Name** field, the protocol will be configured automatically.
Server IP Address	Enter the inside IP address of the virtual server here and click **Add** to add it in the port forwarding summary table.
#	This is the number of an individual port forwarding server entry.
Status	This icon is turned on when the rule is enabled.
Name	This field displays a name to identify this rule.
Protocol	This is the transport layer protocol used for the service.
Port	This field displays the port number(s).
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the **Edit** icon to open the edit screen where you can modify an existing rule. Click the **Delete** icon to remove a rule.

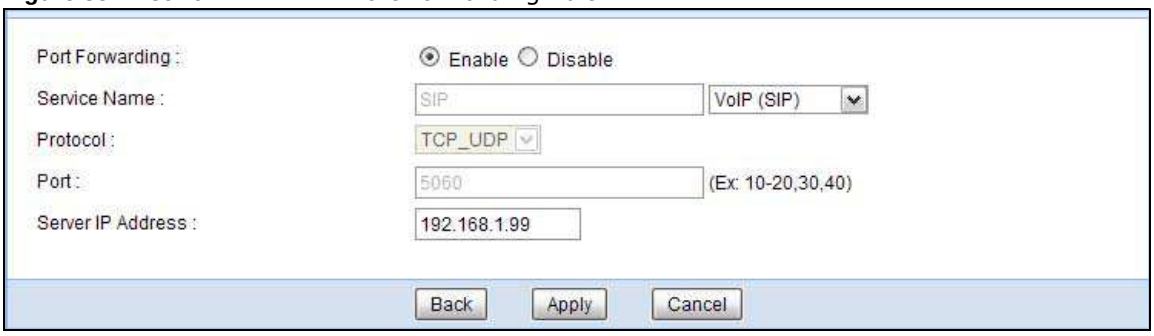
Table 57 Network > NAT > Port Forwarding (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.3.1 Port Forwarding Edit Screen

This screen lets you edit a port forwarding rule. Click a rule's **Edit** icon in the **Port Forwarding** screen to open the following screen.

Figure 85 Network > NAT > Port Forwarding Edit



The following table describes the labels in this screen.

Table 58 Network > NAT > Port Forwarding Edit

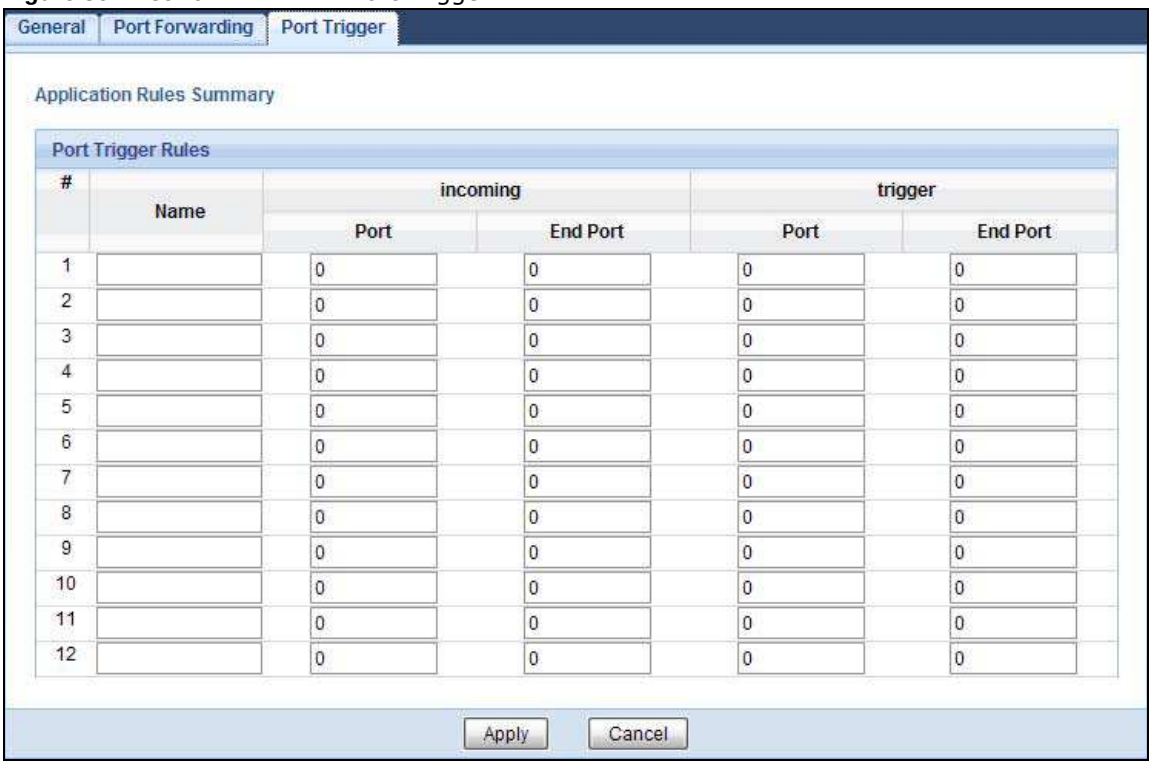
LABEL	DESCRIPTION
Port Forwarding	Select **Enable** to turn on this rule and the requested service can be forwarded to the host with a specified internal IP address. Select **Disable** to disallow forwarding of these ports to an inside server without having to delete the entry.
Service Name	Type a name (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.
Protocol	Select the transport layer protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP_UDP**. If you have chosen a pre-defined service in the **Service Name** field, the protocol will be configured automatically.
Port	Type a port number(s) to define the service to be forwarded to the specified server. To specify a range of ports, enter a hyphen (-) between the first port and the last port, such as 10-.
Server IP Address	Type the IP address of the server on your LAN that receives packets from the port(s) specified in the **Port** field.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.4 Port Trigger Screen

To change your NBG5615's trigger port settings, click **Network > NAT > Port Trigger**. The screen appears as shown.

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

Figure 86 Network > NAT > Port Trigger



The following table describes the labels in this screen.

Table 59 Network > NAT > Port Trigger

LABEL	DESCRIPTION
#	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.
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 NBG5615 forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
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 NBG5615 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
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 NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.5 Technical Reference

The following section contains additional technical information about the NBG5615 features described in this chapter.

15.5.1 NATPort 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 **Port Forwarding** 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.

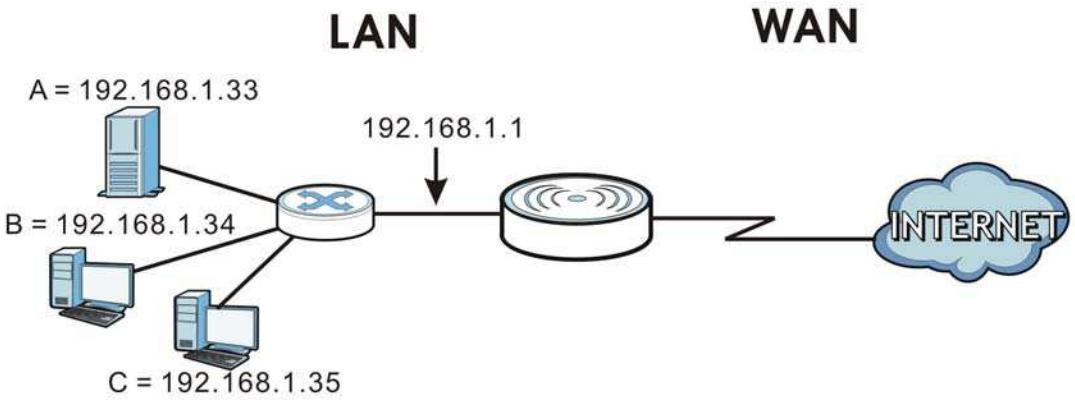
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Note: 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.

15.5.2 NAT 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 87 Multiple Servers Behind NAT Example



15.5.3 Trigger Port Forwarding

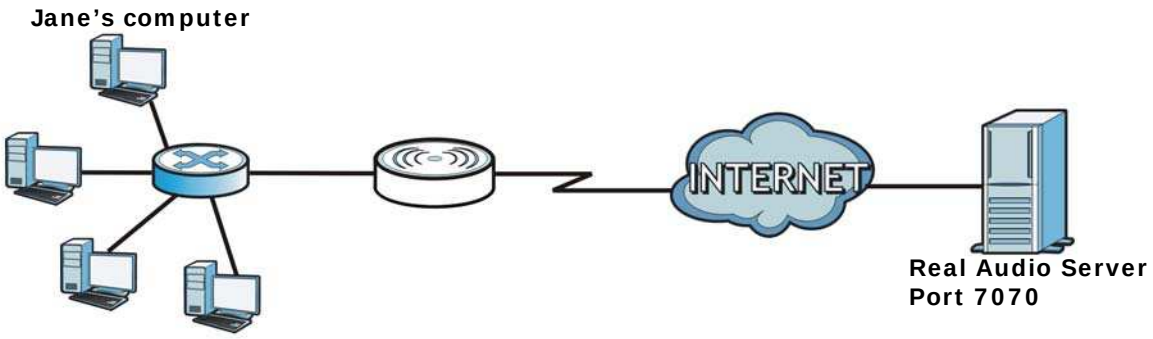
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem 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 NBG5615 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 NBG5615's WAN port receives a response with a specific port number and protocol ("incoming" port), the NBG5615 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.

15.5.4 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 88 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 NBG5615 to record Jane's computer IP address. The NBG5615 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 NBG5615 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 NBG5615 times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

15.5.5 Two Points To Remember About Trigger Ports

1. Trigger events only happen on data that is coming from inside the NBG5615 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.

16

DDNS

16.1 Overview

DDNS services let you use a domain name with a dynamic IP address.

16.1.1 What You Need To Know

The following terms and concepts may help as you read through this chapter.

What is DDNS?

Dynamic Domain Name Service (DDNS) services let you use a fixed domain name with a dynamic IP address. Users can always use the same domain name instead of a different dynamic IP address that changes each time to connect to the NBG5615 or a server in your network.

Note: The NBG5615 must have a public global IP address and you should have your registered DDNS account information on hand.

16.2 General

To change your NBG5615's DDNS, click **Network > DDNS**. The screen appears as shown.

Figure 89 Dynamic DNS

The following table describes the labels in this screen.

Table 60 Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS	Select **Enable** to use dynamic DNS. Select **Disable** to turn this feature off.
Service Provider	Select the name of 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 (",").
Usename	Enter your user name.
Password	Enter the password assigned to you.
Apply	Click **Apply** to save your changes back to the NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17

Static Route

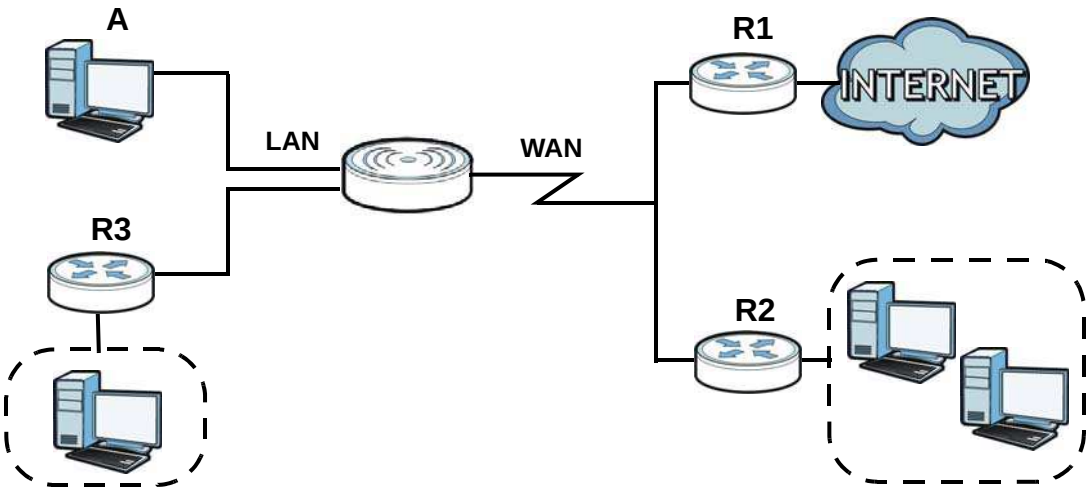
17.1 Overview

This chapter shows you how to configure static routes for your NBG5615.

The NBG5615 usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the NBG5615 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 NBG5615's LAN interface. The NBG5615 routes most traffic from **A** to the Internet through the NBG5615'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 90 Example of Static Routing Topology



17.2 IP Static Route Screen

Click **Network** > **Static Route** to open the **Static Route** screen.

Figure 91 Network > Static Route

The following table describes the labels in this screen.

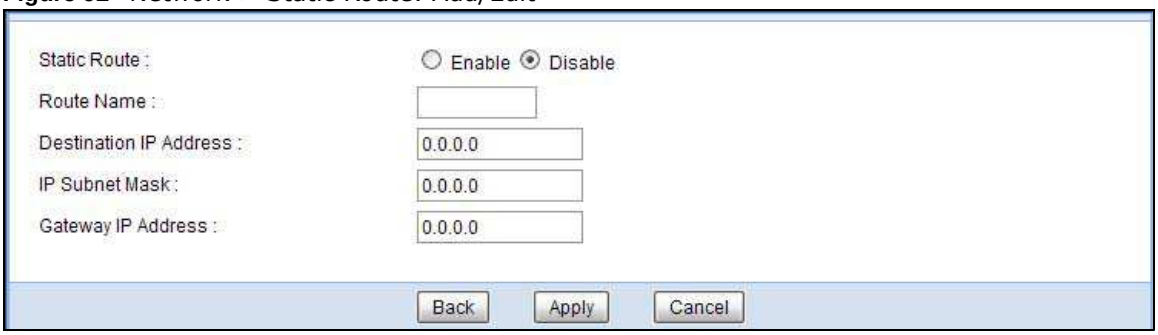
Table 61 Network > Static Route

LABEL	DESCRIPTION
Add Static Route	Click this to create a new rule.
#	This is the number of an individual static route.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Name	This field displays a name to identify this rule.
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 a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Subent Mask	This parameter specifies the IP network subnet mask of the final destination.
Modify	Click the **Edit** icon to open a screen where you can modify an existing rule. Click the **Delete** icon to remove a rule from the NBG5615.
Apply	Click **Apply** to save your changes back to the NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17.2.1 Add/Edit Static Route

Click the **Add Static Route** button or a rule's **Edit** icon in the **Static Route** screen. Use this screen to configure the required information for a static route.

Figure 92 Network > Static Route: Add/Edit



The following table describes the labels in this screen.

Table 62 Network > Static Route: Add/Edit

LABEL	DESCRIPTION
Static Route	Select to enable or disable this rule.
Route Name	Type a name to identify this rule. You can use up to printable English keyboard characters, including spaces.
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 next-hop gateway. The gateway is a router or switch on the same segment as your NBG5615's interface(s). The gateway helps forward packets to their destinations.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the NBG5615.
Cancel	Click **Cancel** to set every field in this screen to its last-saved value.

18 Firewall

18.1 Overview

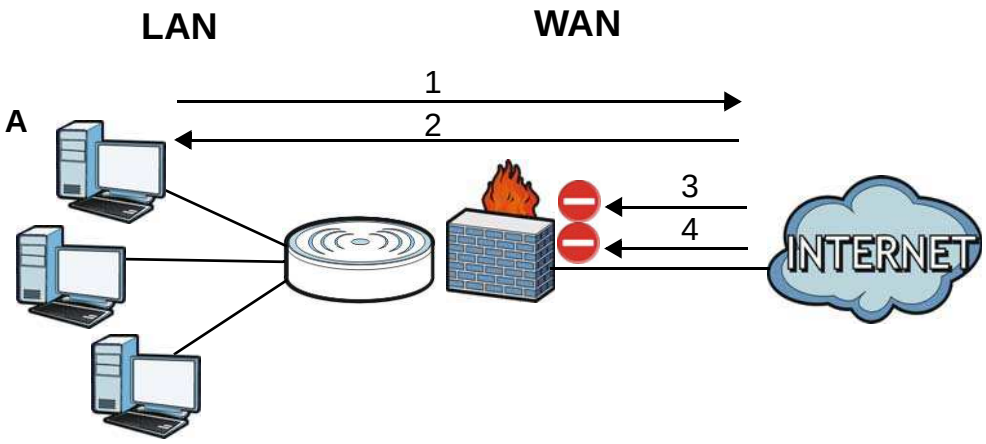
Use these screens to enable and configure the firewall that protects your NBG5615 and your LAN from unwanted or malicious traffic.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 93 Default Firewall Action



18.1.1 What You Can Do

- Use the **General** screen to enable or disable the NBG5615's firewall (Section 18.2 on page 157).
- Use the **Services** screen enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them (Section 18.3 on page 157).

18.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

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.

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.

About the NBG5615 Firewall

The NBG5615’s firewall feature physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks.

It 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 NBG5615's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG5615 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 NBG5615 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 NBG5615 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.

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 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.

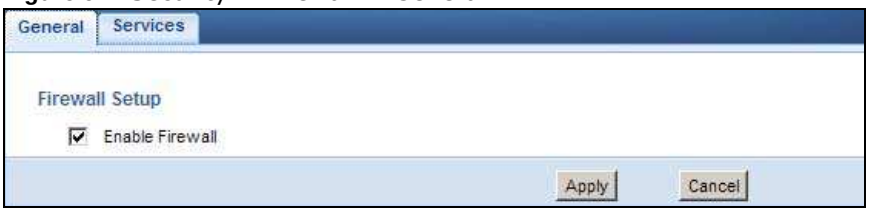
6 Protect against IP spoofing by making sure the firewall is active.

7 Keep the firewall in a secured (locked) room.

18.2 General Screen

Use this screen to enable or disable the NBG5615's firewall, and set up firewall logs. Click **Security** > **Firewall** to open the **General** screen.

Figure 94 Security > Firewall > General l



The following table describes the labels in this screen.

Table 63 Security > Firewall > General

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The NBG5615 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to start configuring this screen again.

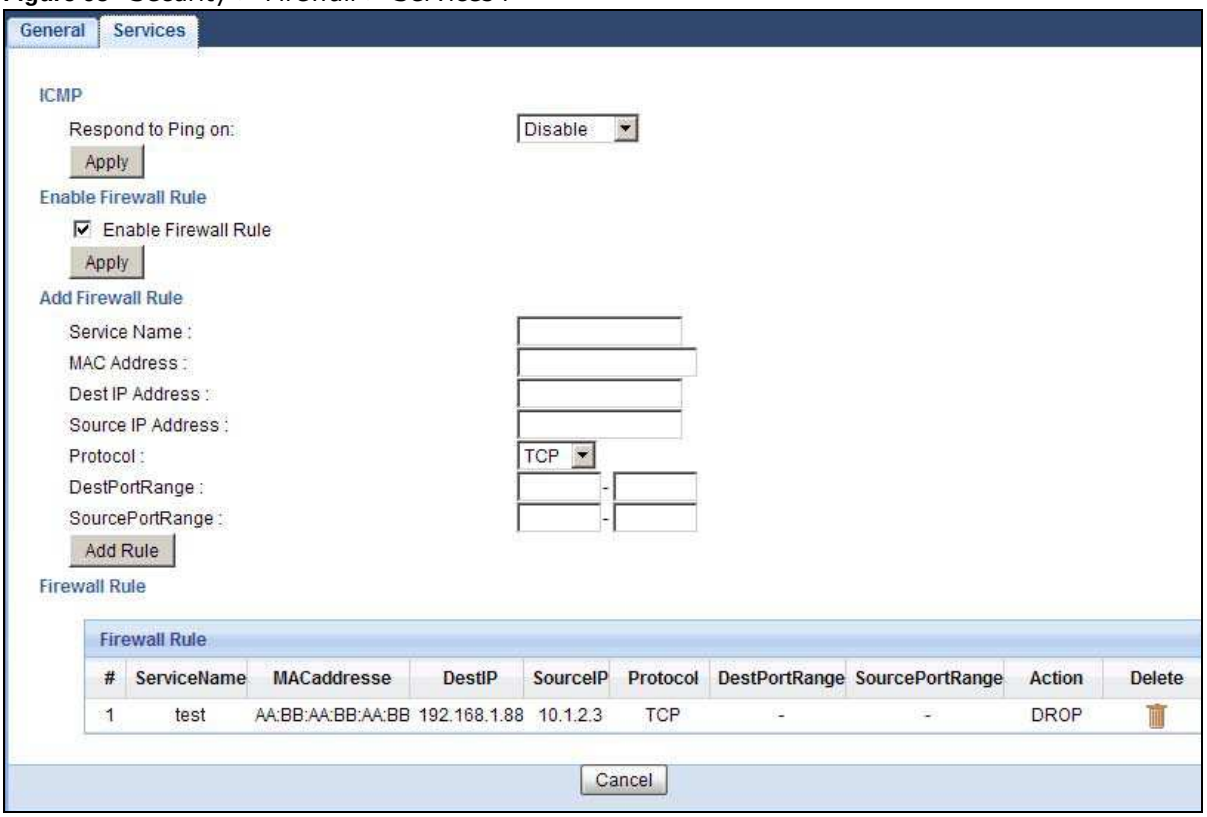
18.3 Services Screen

If an outside user attempts to probe an unsupported port on your NBG5615, an ICMP response packet is automatically returned. This allows the outside user to know the NBG5615 exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your NBG5615 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.

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

Figure 95 Security > Firewall > Services l



The following table describes the labels in this screen.

Table 64 Security > Firewall > Services

LABEL	DESCRIPTION
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 NBG5615 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.
Apply	Click **Apply** to save the settings.
Enable Firewall Rule	
Enable Firewall Rule	Select this check box to activate the firewall rules that you define (see **Add Firewall Rule** below).
Apply	Click **Apply** to save the settings.
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest IP Address	Enter the IP address of the computer to which traffic for the application or service is entering. The NBG5615 applies the firewall rule to traffic initiating from this computer.

Table 64 Security > Firewall > Services (continued)

LABEL	DESCRIPTION
Source IP Address	Enter the IP address of the computer that initializes traffic for the application or service. The NBG5615 applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Add Rule	Click **Add** to save the firewall rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Service Name	This is a name that identifies or describes the firewall rule.
MAC address	This is the MAC address of the computer for which the firewall rule applies.
Dest IP	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP	This is the IP address of the computer from which traffic for the application or service is initialized.
Protocol	This is the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Action	**DROP** - Traffic matching the conditions of the firewall rule are stopped.
Delete	Click **Delete** to remove the firewall rule.
Cancel	Click **Cancel** to start configuring this screen again.

See Appendix C on page 249 for commonly used services and port numbers.

19

Content Filtering

19.1 Overview

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

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.

19.1.1 What You Need To Know

The following terms and concepts may help as you read through this chapter.

Content Filtering Profiles

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages.

A content filtering profile conveniently stores your custom settings for the following features.

Keyword Blocking URL Checking

The NBG5615 checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the domain name is www.zyxel.com.tw.

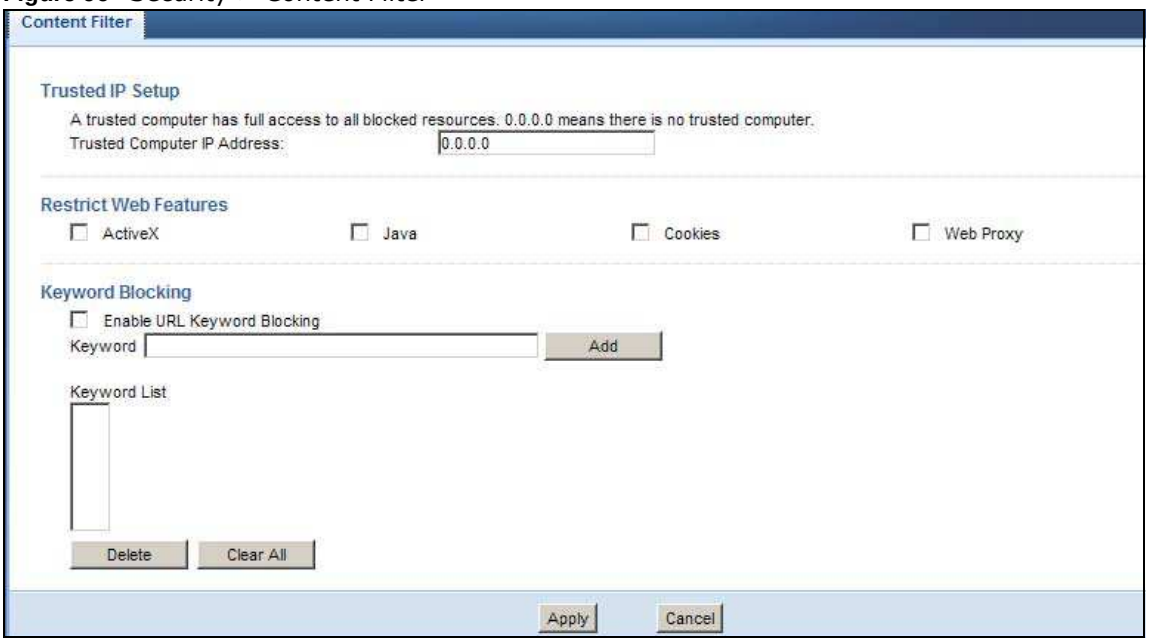
The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

Since the NBG5615 checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the NBG5615 would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

19.2 Content Filter

Use this screen to restrict web features, add keywords for blocking and designate a trusted computer. Click **Security** > **Content Filter** to open the **Content Filter** screen.

Figure 96 Security > Content Filter



The following table describes the labels in this screen.

Table 65 Security > Content Filter

LABEL	DESCRIPTION
Trusted IP Setup	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.
Enable URL Keyword Blocking	The NBG5615 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.
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.
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.

Table 65 Security > Content Filter (continued)

LABEL	DESCRIPTION
Keyword List	This list displays the keywords already added.
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.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh

19.3 Technical Reference

The following section contains additional technical information about the NBG5615 features described in this chapter.

19.3.1 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.

Domain Name or IP Address URL Checking

By default, the NBG5615 checks the URL's domain name or IP address when performing keyword blocking.

This means that the NBG5615 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.

Full Path URL Checking

Full path URL checking has the NBG5615 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.

File Name URL Checking

Filename URL checking has the NBG5615 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.

20

Bandwidth Management

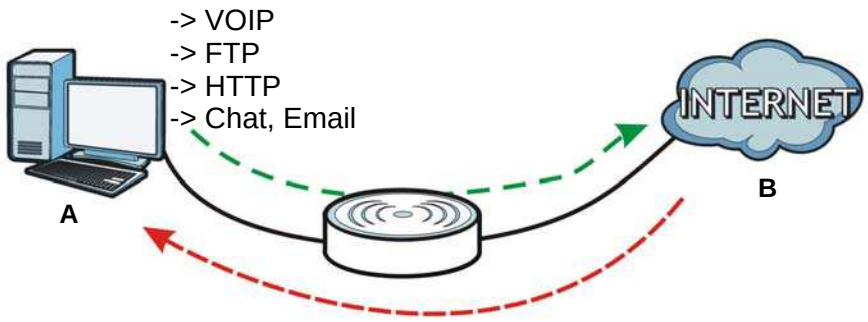
20.1 Overview

This chapter contains information about configuring bandwidth management and editing rules.

ZyXEL's Bandwidth Management allows you to specify bandwidth management rules based on an application.

In the figure below, uplink traffic goes from the LAN device (**A**) to the WAN device (**B**). Bandwidth management is applied before sending the packets out to the WAN. Downlink traffic comes back from the WAN device (**B**) to the LAN device (**A**). Bandwidth management is applied before sending the traffic out to LAN.

Figure 97 Bandwidth Management Example



You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to individual applications (like VoIP, Web, FTP, and E-mail for example).

20.2 What You Can Do

- Use the **General** screen to enable bandwidth management and assign bandwidth values (Section 20.4 on page 166).
- Use the **Advanced** screen to configure bandwidth managements rule for the pre-defined services and applications (Section 20.5 on page 166).

20.3 What You Need To Know

The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WLAN to WAN) must be less than or equal to the **Upstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen (Section 20.5 on page 166).

The sum of the bandwidth allotments that apply to the LAN interface (WAN to LAN, WAN to WLAN) must be less than or equal to the **Downstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen Section 20.5 on page 166.

20.4 General Screen

Use this screen to have the NBG5615 apply bandwidth management.

Click **Management > Bandwidth MGMT** to open the bandwidth management **General** screen.

Figure 98 Management > Bandwidth Management > General

The following table describes the labels in this screen.

Table 66 Management > Bandwidth Management > General

LABEL	DESCRIPTION
Enable Bandwidth Management	This field allows you to have NBG5615 apply bandwidth management. Enable bandwidth management to give traffic that matches a bandwidth rule priority over traffic that does not match a bandwidth rule. Enabling bandwidth management also allows you to control the maximum or minimum amounts of bandwidth that can be used by traffic that matches a bandwidth rule.
Apply	Click **Apply** to save your customized settings.
Cancel	Click **Cancel** to begin configuring this screen afresh.

20.5 Advanced Screen

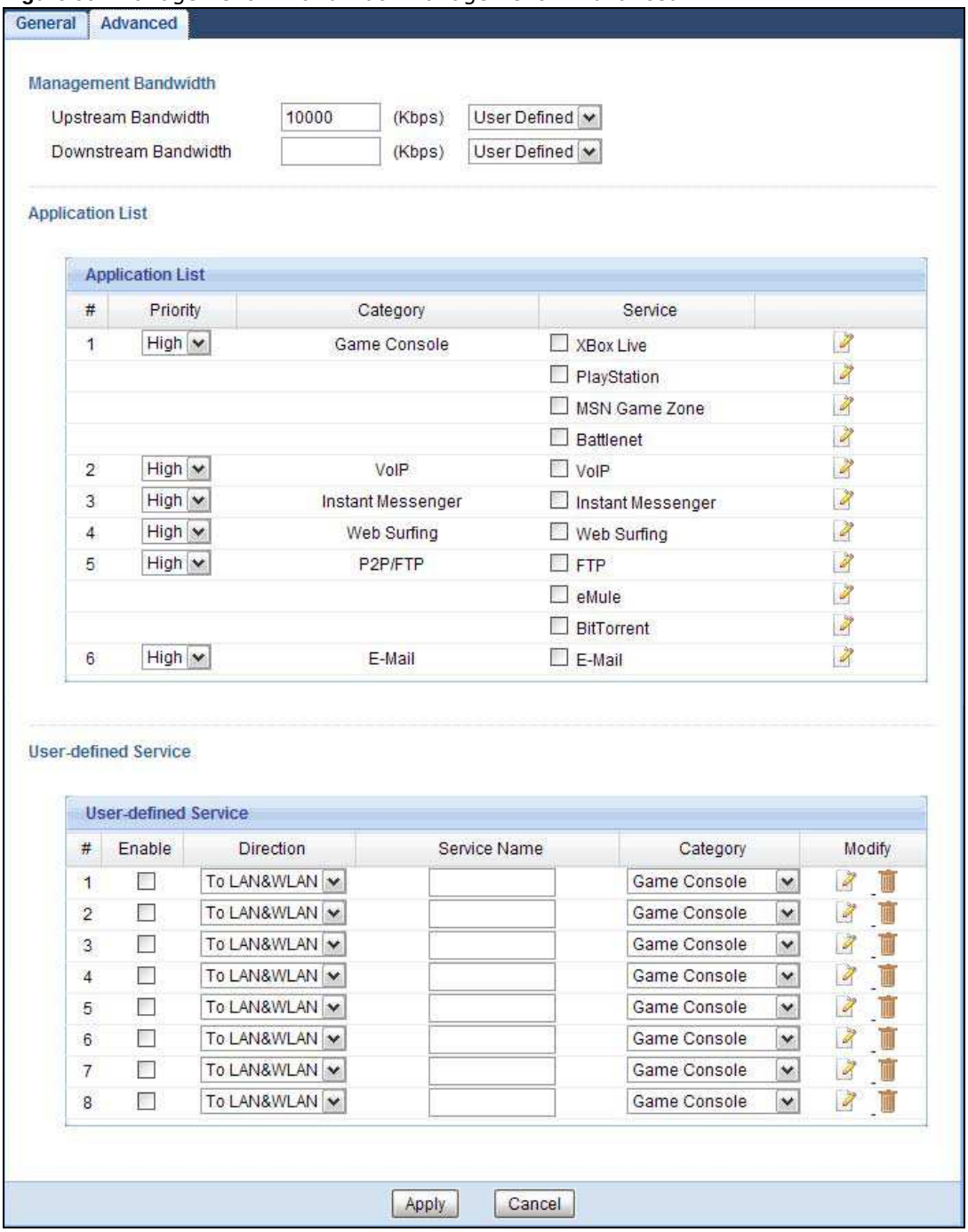
Use this screen to configure bandwidth management rules for the pre-defined services or applications.

You can also use this screen to configure bandwidth management rule for other services or applications that are not on the pre-defined list of NBG5615. Additionally, you can define the source and destination IP addresses and port for a service or application.

Note: The two tables shown in this screen can be configured and applied at the same time.

Click **Management** > **Bandwidth MGMT** > **Advanced** to open the bandwidth management **Advanced** screen.

Figure 99 Management > Bandwidth Management > Advanced



The following table describes the labels in this screen.

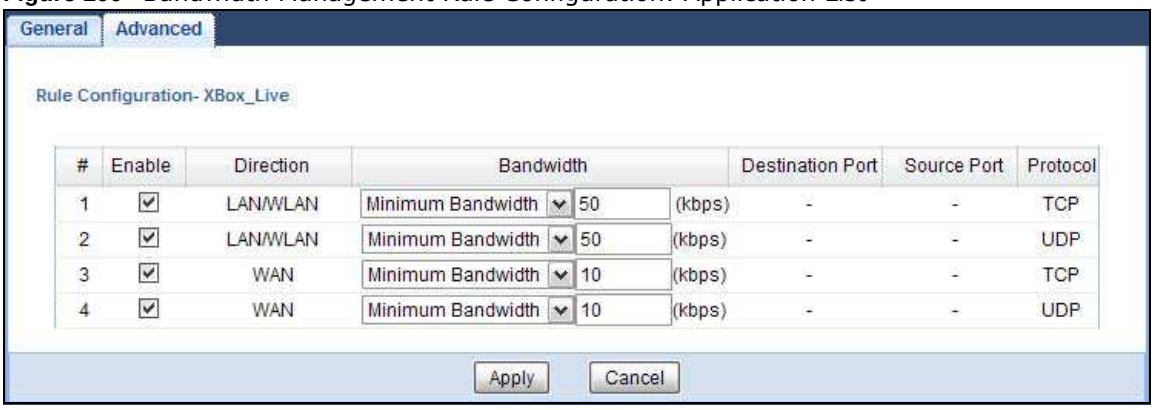
Table 67 Management > Bandwidth Management > Advanced

LABEL	DESCRIPTION
Management Bandwidth	
Upstream Bandwidth	Select the total amount of bandwidth from a drop-down list box that you want to dedicate to uplink traffic. Otherwise, select **User Defined** and manually specify the amount of bandwidth in kilobits per second. This is traffic from LAN/WLAN to WAN.
Downstream Bandwidth	Select the total amount of bandwidth from a drop-down list box that you want to dedicate to uplink traffic. Otherwise, select **User Defined** and manually specify the amount of bandwidth in kilobits per second. This is traffic from WAN to LAN/WLAN.
Application List	Use this table to allocate specific amounts of bandwidth based on a pre-defined service.
#	This is the number of an individual bandwidth management rule.
Priority	Select a priority from the drop down list box. Choose **High**, **Mid** or **Low**. • **High** - Select this for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay). • **Mid** - Select this for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay. • **Low** - Select this for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Category	This is the category where a service belongs.
Service	This is the name of the service. Select the check box to have the NBG5615 apply this bandwidth management rule.
	Click the **Edit** icon to open the **Rule Configuration** screen where you can modify the rule.
User-defined Service	Use this table to allocate specific amounts of bandwidth to specific applications or services you specify.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the NBG5615 apply this bandwidth management rule.
Direction	Select **To LAN&WLAN** to apply bandwidth management to traffic from WAN to LAN and WLAN. Select **To WAN** to apply bandwidth management to traffic from LAN/WLAN to WAN.
Service Name	Enter a descriptive name for the bandwidth management rule.
Category	This is the category where a service belongs.
Modify	Click the **Edit** icon to open the **Rule Configuration** screen. Modify an existing rule or create a new rule in the **Rule Configuration** screen. See Section 20.5.2 on page 169 for more information. Click the **Remove** icon to delete a rule.
Apply	Click **Apply** to save your customized settings.
Cancel	Click **Cancel** to begin configuring this screen afresh.

20.5.1 Rule Configuration: Application Rule Configuration

If you want to edit a bandwidth management rule for a pre-defined service or application, click the **Edit** icon in the **Application List** table of the **Advanced** screen. The following screen displays.

Figure 100 Bandwidth Management Rule Configuration: Application List



The following table describes the labels in this screen.

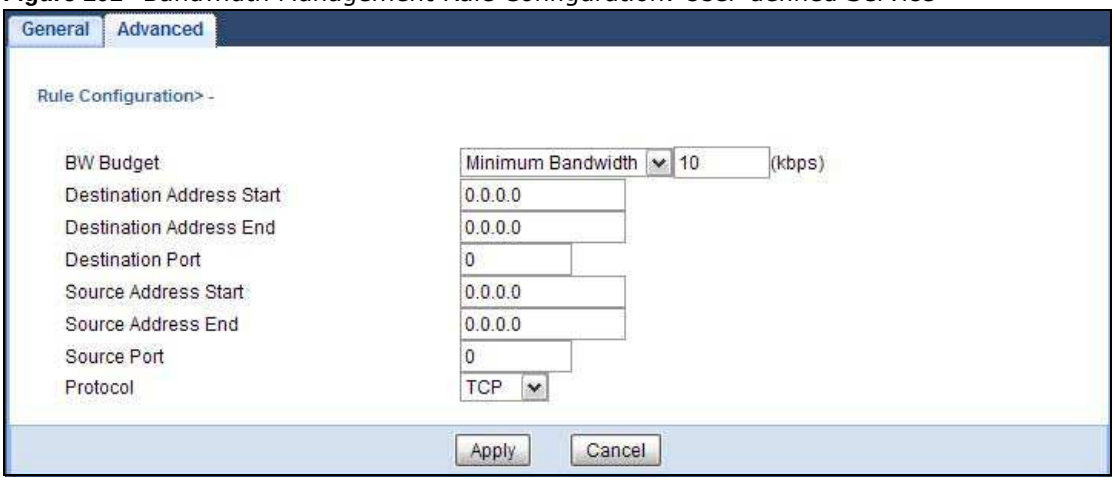
Table 68 Bandwidth Management Rule Configuration: Application List

LABEL	DESCRIPTION
#	This is the number of an individual bandwidth management rule.
Enable	Select an interface's check box to enable bandwidth management on that interface.
Direction	These read-only labels represent the physical interfaces. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the NBG5615 and be managed by bandwidth management.
Bandwidth	Select **Maximum Bandwidth** or **Minimum Bandwidth** and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second.
Destination Port	This is the port number of the destination that define the traffic type, for example TCP port 80 defines web traffic. See Appendix C on page 249 for some common services and port numbers.
Source Port	This is the port number of the source that define the traffic type, for example TCP port 80 defines web traffic. See Appendix C on page 249 for some common services and port numbers.
Protocol	This is the protocol (**TCP**, **UDP** or **user-defined**) used for the service.
Apply	Click **Apply** to save your customized settings.
Cancel	Click **Cancel** to exit this screen without saving.

20.5.2 Rule Configuration: User Defined Service Rule Configuration

If you want to edit a bandwidth management rule for other applications or services, click the **Edit** icon in the **User-defined Service** table of the **Advanced** screen. The following screen displays.

Figure 101 Bandwidth Management Rule Configuration: User-defined Service



The following table describes the labels in this screen.

Table 69 Bandwidth Management Rule Configuration: User-defined Service

LABEL	DESCRIPTION
BW Budget	Select **Maximum Bandwidth** or **Minimum Bandwidth** and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second.
Destination Address Start	Enter the starting IP address of the destination computer. The NBG5615 applies bandwidth management to the service or application that is entering this computer.
Destination Address End	Enter the ending IP address of the destination computer. The NBG5615 applies bandwidth management to the service or application that is entering this computer.
Destination Port	This is the port number of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Address Start	Enter the starting IP address of the computer that initializes traffic for the application or service. The NBG5615 applies bandwidth management to traffic initiating from this computer.
Source Address End	Enter the ending IP address of the computer that initializes traffic for the application or service. The NBG5615 applies bandwidth management to traffic initiating from this computer.
Source Port	This is the port number of the source that define the traffic type, for example TCP port 80 defines web traffic.
Protocol	Select the protocol (**TCP**, **UDP**, **BOTH**) for which the bandwidth management rule applies. If you select **BOTH**, enter the protocol for which the bandwidth management rule applies. For example, ICMP for ping traffic.
Apply	Click **Apply** to save your customized settings.
Cancel	Click **Cancel** to exit this screen without saving.

See Appendix C on page 249 for commonly used services and port numbers.

20.5.3 Predefined Bandwidth Management Services

The following is a description of some services that you can select and to which you can apply media bandwidth management in the **Management** > **Bandwidth MGMT** > **Advanced** screen.

Table 70 Media Bandwidth Management Setup: Services

SERVICE	DESCRIPTION
FTP	File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail.
WWW	The World Wide Web (WWW) 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.
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:
VoIP (SIP)	Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is transported primarily over UDP but can also be transported over TCP.
BitTorrent	BitTorrent is a free P2P (peer-to-peer) sharing tool allowing you to distribute large software and media files. BitTorrent requires you to search for a file with a searching engine yourself. It distributes files by corporation and trading, that is, the client downloads the file in small pieces and share the pieces with other peers to get other half of the file.
Gaming	Online gaming services lets you play multiplayer games on the Internet via broadband technology. As of this writing, your NBG5615 supports Xbox, Playstation, Battlenet and MSN Game Zone.

21

Remote Management

21.1 Overview

This chapter provides information on the Remote Management screens.

Remote Management allows you to manage your NBG5615 from a remote location through the following interfaces:

- LAN and WAN
- LAN only
- WAN only

Note: The NBG5615 is managed using the Web Configurator.

21.2 What You Can Do in this Chapter

- Use the **WWW** screen to define the interface/s from which the NBG5615 can be managed remotely using the web and specify a secure client that can manage the NBG5615 (Section 21.4 on page 174).
- Use the **Telnet** screen to define the interface/s from which the NBG5615 can be managed remotely using Telnet service and specify a secure client that can manage the NBG5615 (Section 21.5 on page 175).
- Use the **Wake On LAN** screen to enable Wake on LAN and remotely turn on a device on the local network (Section 21.6 on page 175).

21.3 What You Need to Know

Remote management over LAN or WAN will not work when:

1. The IP address in the **Secured Client IP Address** field (Section 21.4 on page 174) does not match the client IP address. If it does not match, the NBG5615 will disconnect the session immediately.
2. There is already another remote management session. You may only have one remote management session running at one time.
3. There is a firewall rule that blocks it.

21.3.1 Remote Management and NAT

When NAT is enabled:

- Use the NBG5615's WAN IP address when configuring from the WAN.
- Use the NBG5615's LAN IP address when configuring from the LAN.

21.3.2 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The NBG5615 automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **Maintenance > General** screen

21.4 WWW Screen

To change your NBG5615's remote management settings, click **Management > Remote MGMT > WWW**.

Figure 102 Management > Remote Management > WWW

The following table describes the labels in this screen.

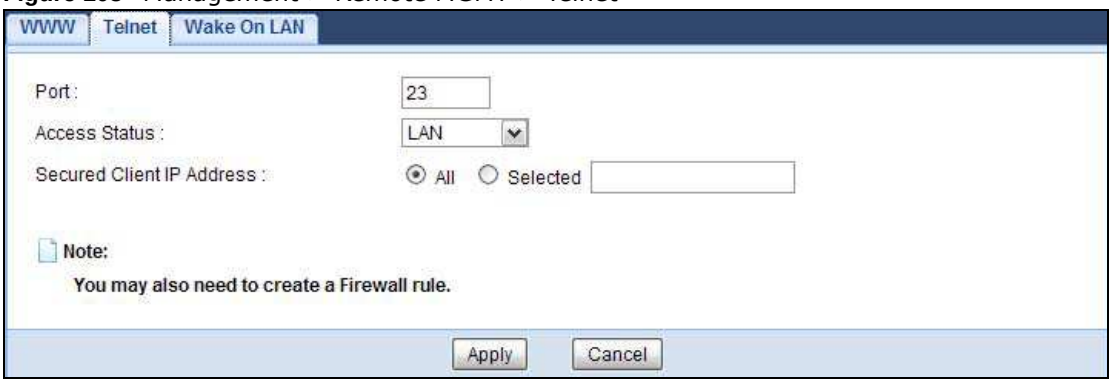
Table 71 Management > Remote Management > WWW

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the NBG5615 using this service.
Secured Client IP Address	Select **All** to allow all computes to access the NBG5615. Otherwise, check **Selected** and specify the IP address of the computer that can access the NBG5615.
Apply	Click **Apply** to save your customized settings.
Cancel	Click **Cancel** to begin configuring this screen afresh.

21.5 Telnet Screen

To change your NBG5615's remote management settings, click **Management > Remote MGMT > Telnet** to open the **Telnet** screen.

Figure 103 Management > Remote MGMT > Telnet



The following table describes the labels in this screen.

Table 72 Management > Remote MGMT > Telnet

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the NBG5615 using this service.
Secured Client IP Address	Select **All** to allow all computes to access the NBG5615. Otherwise, check **Selected** and specify the IP address of the computer that can access the NBG5615.
Apply	Click **Apply** to save your customized settings.
Cancel	Click **Cancel** to begin configuring this screen afresh.

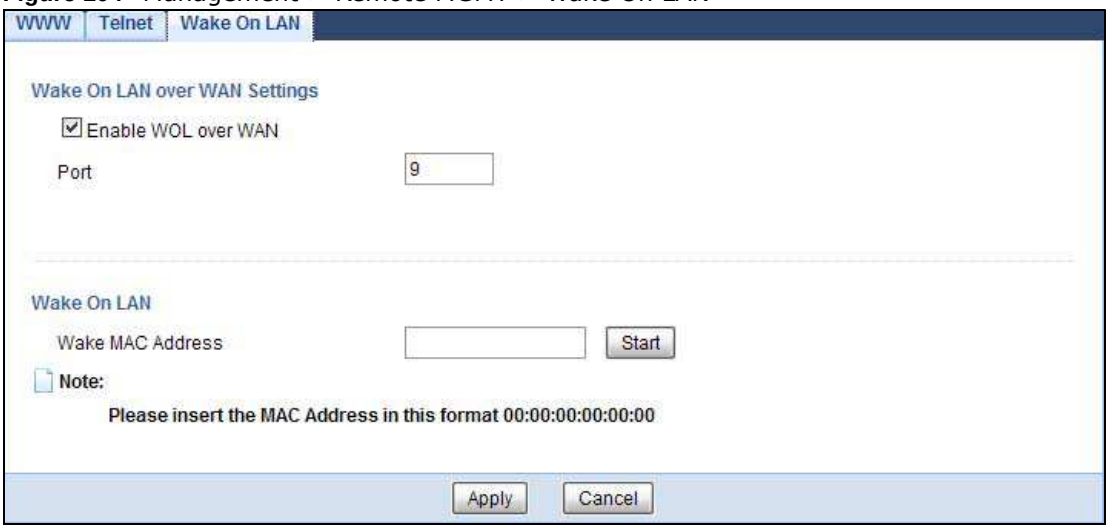
21.6 Wake On LAN Screen

Wake On LAN (WoL) allows you to remotely turn on a device on the network, such as a computer, storage device or media server. To use this feature the remote hardware (for example the network adapter on a computer) must support Wake On LAN using the "Magic Packet" method.

You need to know the MAC address of the remote device. It may be on a label on the device.

Use this screen to remotely turn on a device on the network. Click the **Management > Remote MGMT > Wake On LAN** to open the following screen.

Figure 104 Management > Remote MGMT > Wake On LAN



The following table describes the labels in this screen.

Table 73 Management > Remote MGMT > Wake On LAN

LABEL	DESCRIPTION
Wake On LAN over WAN Settings	
Enable WOL over WAN	Select this option to have the NBG5615 forward a WoL "Magic Packet" to all devices on the LAN if the packet comes from the WAN or remote network and uses the port number specified in the **Port** field. A LAN device whose hardware supports Wake on LAN then will be powered on if it is turned off previously.
Port	Type a port number from which a WoL packet is forwarded to the LAN.
Wake On LAN	
Wake MAC Address	Enter the MAC Address of the device on the network that will be turned on. A MAC address consists of six hexadecimal character pairs.
Start	Click this to have the NBG5615 generate a WoL packet and forward it to turn the specified device on. A screen pops up displaying MAC address error if you input the MAC address incorrectly.
Apply	Click **Apply** to save the setting to the NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

22

Universal Plug-and-Play (UPnP)

22.1 Overview

This chapter introduces the UPnP feature in the web configurator.

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

22.2 What You Need to Know

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

22.2.1 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

22.2.2 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the NBG5615 allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

22.3 UPnP Screen

Use this screen to enable UPnP on your NBG5615.

Click **Management > UPnP** to display the screen shown next.

Figure 105 Management > UPnP

The following table describes the fields in this screen.

Table 74 Management > UPnP

LABEL	DESCRIPTION
UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the NBG5615's IP address (although you must still enter the password to access the web configurator).
Apply	Click **Apply** to save the setting to the NBG5615.
Cancel	Click **Cancel** to return to the previously saved settings.

22.4 Technical Reference

The sections show examples of using UPnP.

22.4.1 Using UPnP in Windows XP Example

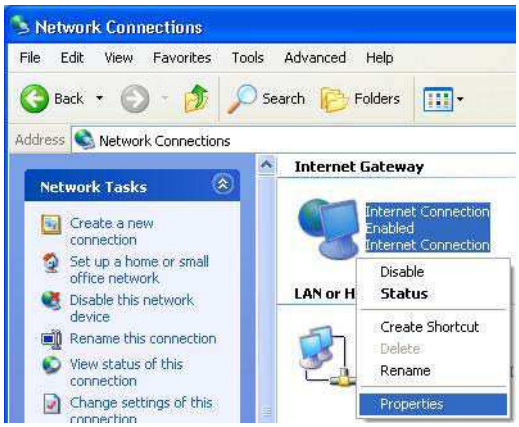
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the NBG5615.

Make sure the computer is connected to a LAN port of the NBG5615. Turn on your computer and the NBG5615.

22.4.1.1 Auto-discover Your UPnP-enabled Network Device

1. Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
2. Right-click the icon and select **Properties**.

Figure 106 Network Connections



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 107 Internet Connection Properties

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 108 Internet Connection Properties: Advanced Settings

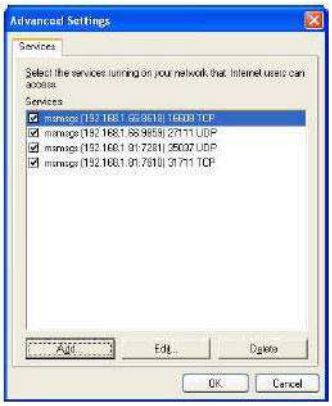
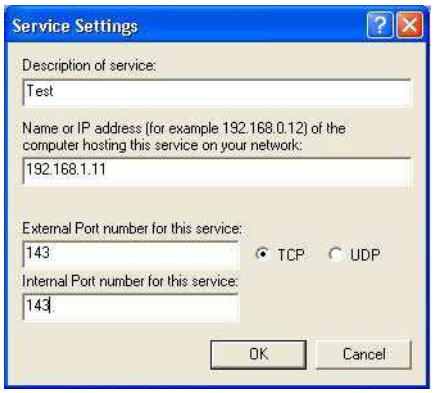


Figure 109 Internet Connection Properties: Advanced Settings: Add



Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

5 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 110 System Tray Icon

6 Double-click on the icon to display your current Internet connection status.

Figure 111 Internet Connection Status

22.4.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the NBG5615 without finding out the IP address of the NBG5615 first. This comes helpful if you do not know the IP address of the NBG5615.

Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

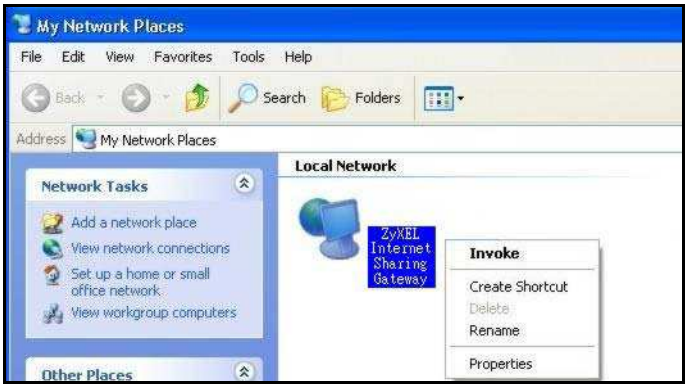
3 Select **My Network Places** under **Other Places**.

Figure 112 Network Connections

4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your NBG5615 and select **Invoke**. The web configurator login screen displays.

Figure 113 Network Connections: My Network Places



6 Right-click on the icon for your NBG5615 and select **Properties**. A properties window displays with basic information about the NBG5615.

Figure 114 Network Connections: My Network Places: Properties: Example

23

USB Media Sharing

23.1 Overview

This chapter describes how to configure the media sharing settings on the NBG5615.

Note: The read and write performance may be affected by amount of file-sharing traffic on your network, type of connected USB device and your USB version (1.1 or 2.0).

Media Server

You can set up your NBG5615 to act as a media server to provide media (like video) to DLNA-compliant players, such as Windows Media Player, ZyXEL DMAs (Digital Media Adapters), Xboxes or PS3s. The media server and clients must have IP addresses in the same subnet.

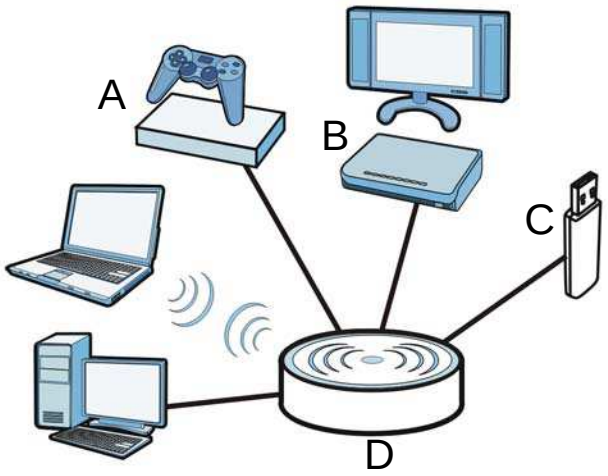
The NBG5615 media server enables you to:

- Publish all folders for everyone to play media files in the USB storage device connected to the NBG5615.
- Use hardware-based media clients like the DMA-2500 to play the files.

Note: Anyone on your network can play the media files in the published folders. No user name and password nor other form of security is required.

The following figure is an overview of the NBG5615's media server feature. DLNA devices **A** and **B** can access and play files on a USB device (**C**) which is connected to the NBG5615 (**D**).

Figure 115 Media Server Overview

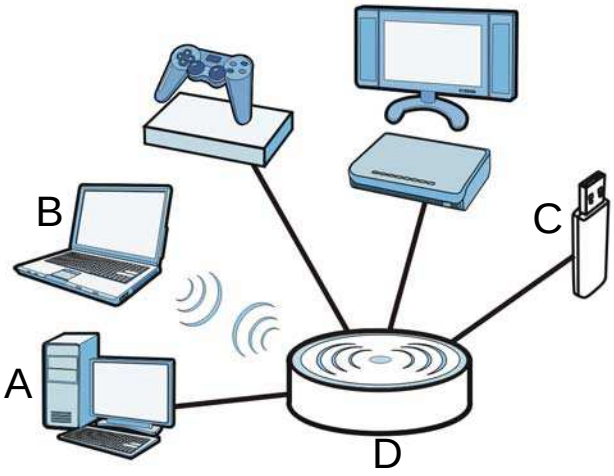


File-Sharing Server

You can also share files on a USB memory stick or hard drive connected to your NBG5615 with users on your network.

The following figure is an overview of the NBG5615's file-sharing server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the NBG5615 (**D**).

Figure 116 File Sharing Overview



23.2 What You Can Do

- Use the **DLNA** screen to use the NBG5615 as a media server and allow DLNA-compliant devices to play media files stored in the attached USB device (Section 23.5 on page 186).
- Use the **SAMBA** screen to enable file-sharing via the NBG5615 using Windows Explorer or the workgroup name. This screen also allow you to configure the workgroup name and create user accounts (Section 23.6 on page 186).
- Use the **FTP** screen to allow file sharing via the NBG5615 using FTP and create user accounts (Section 23.7 on page 188).

23.3 What You Need To Know

DLNA

The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network. DLNA clients play files stored on DLNA servers. The NBG5615 can function as a DLNA-compliant media server and stream files to DLNA-compliant media clients without any configuration.

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file-sharing feature on your NBG5615 supports New Technology File System (NTFS), File Allocation Table (FAT) and FAT32 file systems.

Windows/CIFS

Common Internet File System (CIFS) is a standard protocol supported by most operating systems in order to share files across the network.

CIFS runs over TCP/IP but uses the SMB (Server Message Block) protocol found in Microsoft Windows for file and printer access; therefore, CIFS will allow all applications, not just Web browsers, to open and share files across the Internet.

The NBG5615 uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the NBG5615. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

Samba

SMB is a client-server protocol used by Microsoft Windows systems for sharing files, printers, and so on.

Samba is a free SMB server that runs on most Unix and Unix-like systems. It provides an implementation of an SMB client and server for use with non-Microsoft operating systems.

File Transfer Protocol

This is a method of transferring data from one computer to another over a network such as the Internet.

23.4 Before You Begin

Make sure the NBG5615 is connected to your network and turned on.

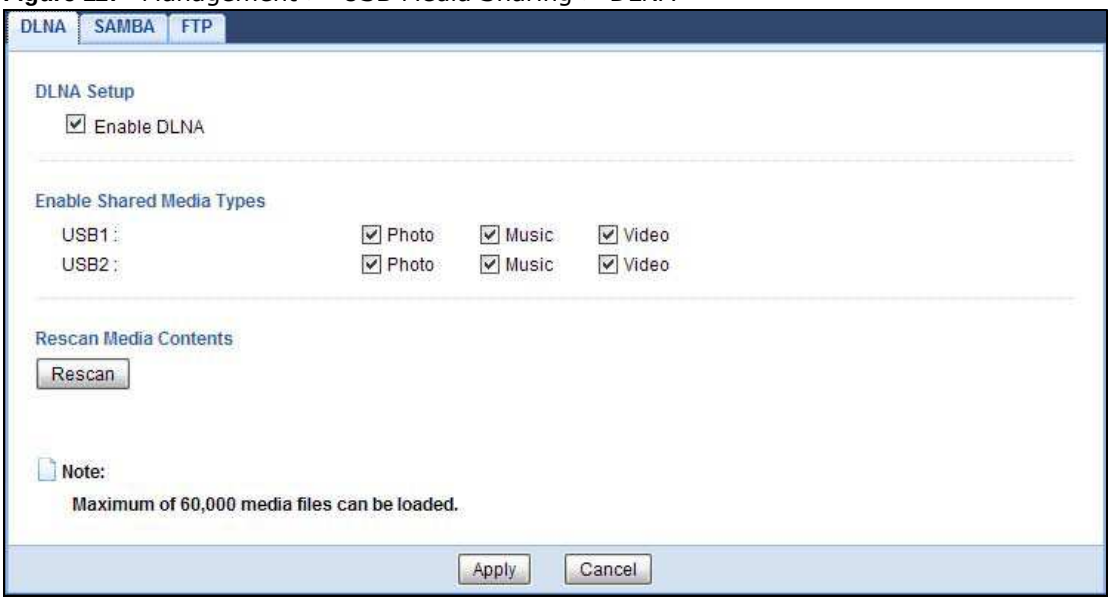
1. Connect the USB device to one of the NBG5615's USB ports.
2. The NBG5615 detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the NBG5615, see the troubleshooting for suggestions.

23.5 DLNA Screen

Use this screen to have the NBG5615 act as a DLNA-compliant media server that lets DLNA-compliant media clients on your network play video, music, and photos from the NBG5615 (without having to copy them to another computer). Click **Management > USB Media Sharing > DLNA**.

Figure 117 Management > USB Media Sharing > DLNA



The following table describes the labels in this screen.

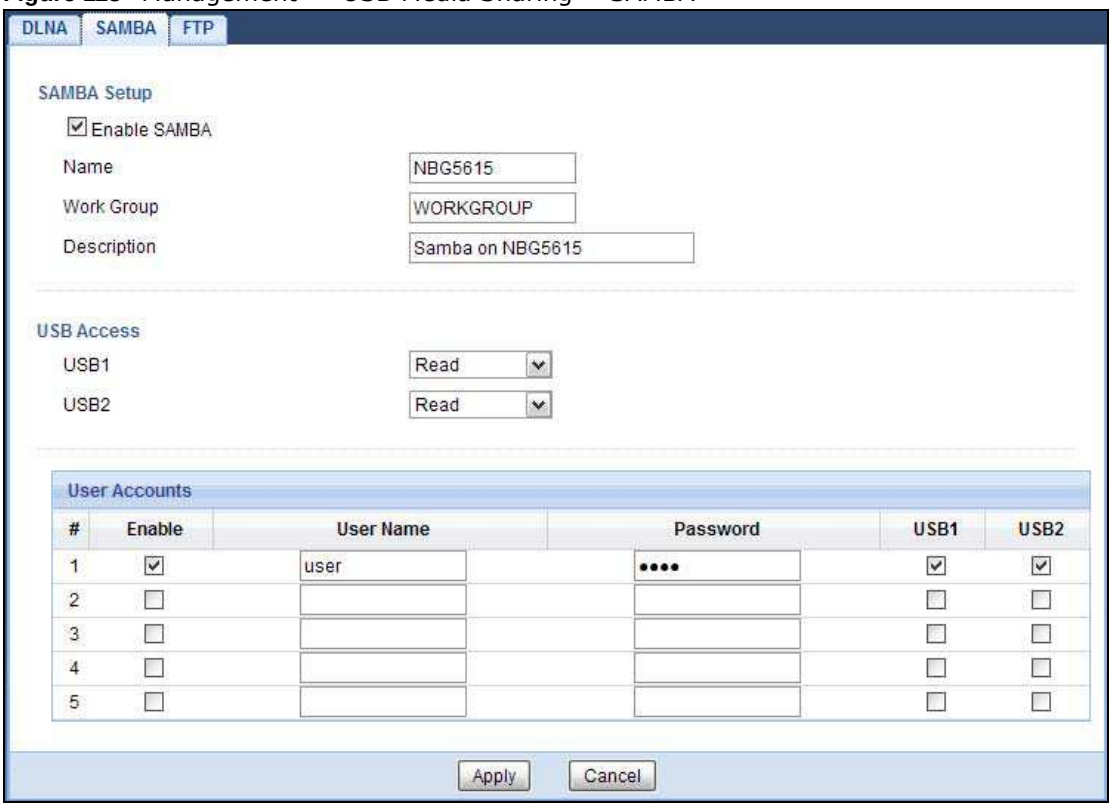
Table 75 Management > USB Media Sharing > DLNA

LABEL	DESCRIPTION
Enable DLNA	Select this to have the NBG5615 function as a DLNA-compliant media server.
USB1/2	Select the media type that you want to share on the USB device connected to the NBG5615's USB port.
Rescan	Click this button to have the NBG5615 scan the media files on the connected USB device and do indexing of the file list again so that DLNA clients can find the new files if any.
Apply	Click **Apply** to save your changes back to the NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.6 SAMBA Screen

Use this screen to set up file-sharing via the NBG5615 using Windows Explorer or the workgroup name. You can also configure the workgroup name and create file-sharing user accounts. Click **Management > USB Media Sharing > SAMBA**.

Figure 118 Management > USB Media Sharing > SAMBA



The following table describes the labels in this screen.

Table 76 Management > USB Media Sharing > SAMBA

LABEL	DESCRIPTION
Enable SAMBA	Select this to enable file sharing through the NBG5615 using Windows Explorer or by browsing to your work group.
Name	Specify the name to identify the NBG5615 in a work group.
Work Group	You can add the NBG5615 to an existing or a new workgroup on your network. Enter the name of the workgroup which your NBG5615 automatically joins. You can set the NBG5615's workgroup name to be exactly the same as the workgroup name to which your computer belongs to. Note: The NBG5615 will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.
Decription	Enter the description of the NBG5615 in a work group.
USB1/2	Specify the user's access rights to the USB storage device which is connected to the NBG5615's USB port. **Read & Write** - The user has read and write rights, meaning that the user can create and edit the files on the connected USB device. **Read** - The user has read rights only and can not create or edit the files on the connected USB device.
User Accounts	Before you can share files you need a user account. Configure the following fields to set up a file-sharing account.
#	This is the index number of the user account.

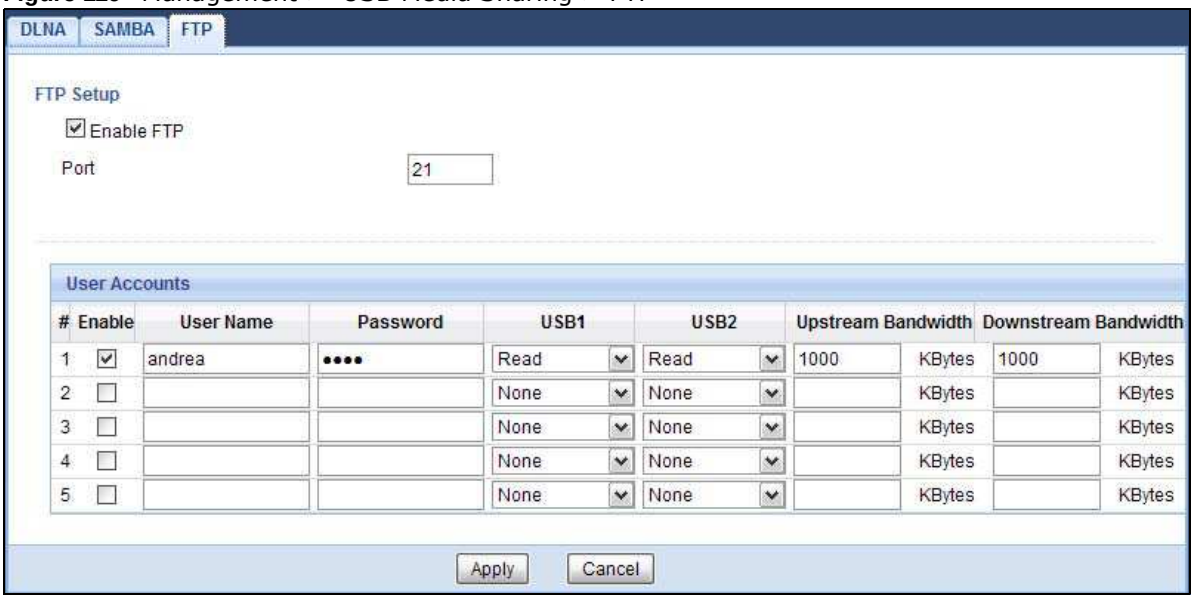
Table 76 Management > USB Media Sharing > SAMBA (continued)

LABEL	DESCRIPTION
Enable	This field displays whether a user account is activated or not. Select the check box to enable the account. Clear the check box to disable the account.
User Name	Enter a user name that will be allowed to access the shared files. You can enter up to 20 characters. Only letters and numbers allowed.
Password	Enter the password used to access the shared files. You can enter up to 20 characters. Only letters and numbers are allowed. The password is case sensitive.
USB1/2	Select the USB port(s) of the NBG5615. The configured user can access the files on the USB device(s) connected to the selected USB port(s) only.
Apply	Click **Apply** to save your changes back to the NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.7 FTP Screen

Use this screen to set up file sharing via the NBG5615 using FTP and create user accounts. Click **Management > USB Media Sharing > FTP**.

Figure 119 Management > USB Media Sharing > FTP



The following table describes the labels in this screen.

Table 77 Management > USB Media Sharing > FTP

LABEL	DESCRIPTION
Enable FTP	Select this to enable the FTP server on the NBG5615 for file sharing using FTP.
Port	You may change the server port number for FTP if needed, however you must use the same port number in order to use that service for file sharing.
User Accounts	Before you can share files you need a user account. Configure the following fields to set up a file-sharing account.
#	This is the index number of the user account.

Table 77 Management > USB Media Sharing > FTP (continued)

LABEL	DESCRIPTION
Enable	This field displays whether a user account is activated or not. Select the check box to enable the account. Clear the check box to disable the account.
User Name	Enter a user name that will be allowed to access the shared files. You can enter up to 20 characters. Only letters and numbers allowed.
Password	Enter the password used to access the shared files. You can enter up to 20 characters. Only letters and numbers are allowed. The password is case sensitive.
USB1/2	Specify the user's access rights to the USB storage device which is connected to the NBG5615's USB port. **Read & Write** - The user has read and write rights, meaning that the user can create and edit the files on the connected USB device. **Read** - The user has read rights only and can not create or edit the files on the connected USB device. **None** - The user cannot access the files on the USB device(s) connected to the USB port.
Upstream Bandwidth	Enter the maximum bandwidth (in Kbps) allowed for incoming FTP traffic.
Downstream Bandwidth	Enter the maximum bandwidth (in Kbps) allowed for outgoing FTP traffic.
Apply	Click **Apply** to save your changes back to the NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.8 Example of Accessing Your Shared Files From a Computer

You can use Windows Explorer or FTP to access the USB storage devices connected to the NBG5615.

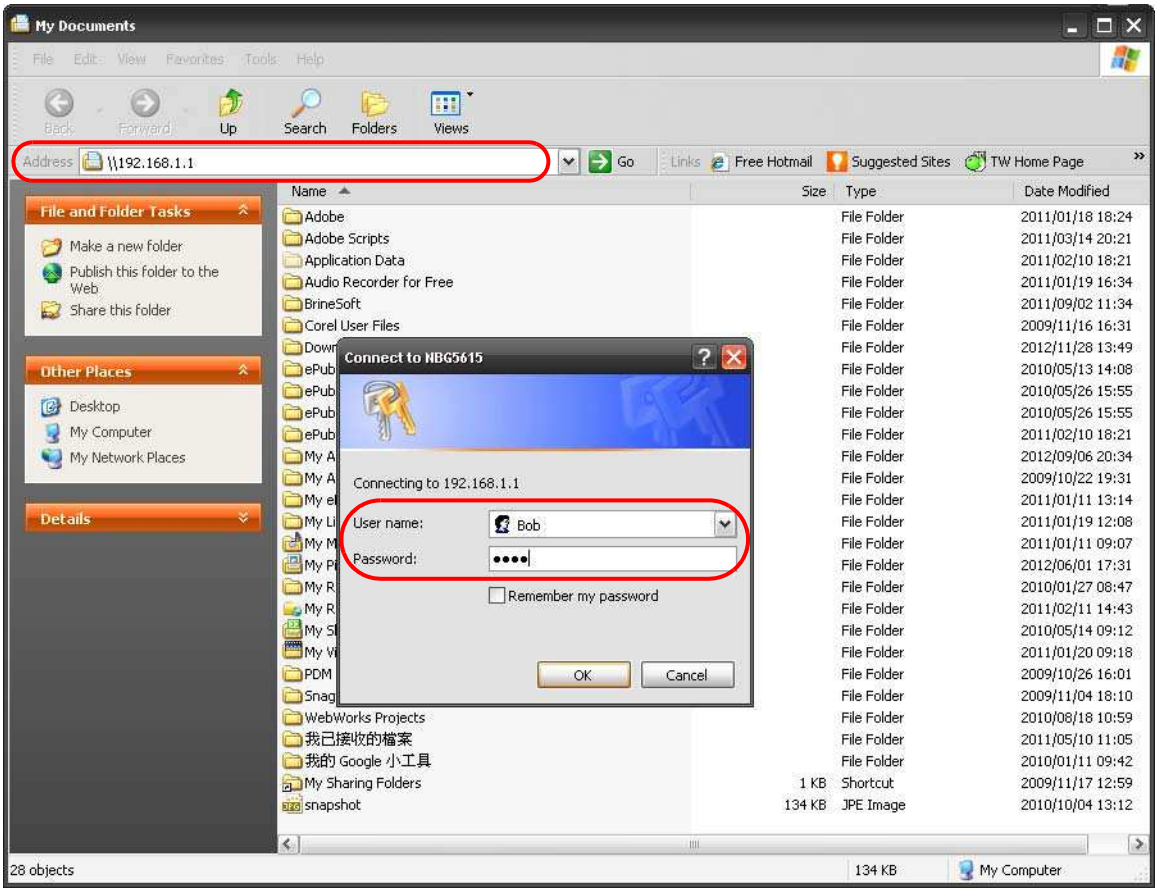
This example shows you how to use Microsoft's Windows XP to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

23.8.1 Use Windows Explorer to Share Files

You should have enabled file sharing and create a user account (Bob/1234 for example) with read and write access to USB 1 in the **USB Media Sharing > SAMBA** screen.

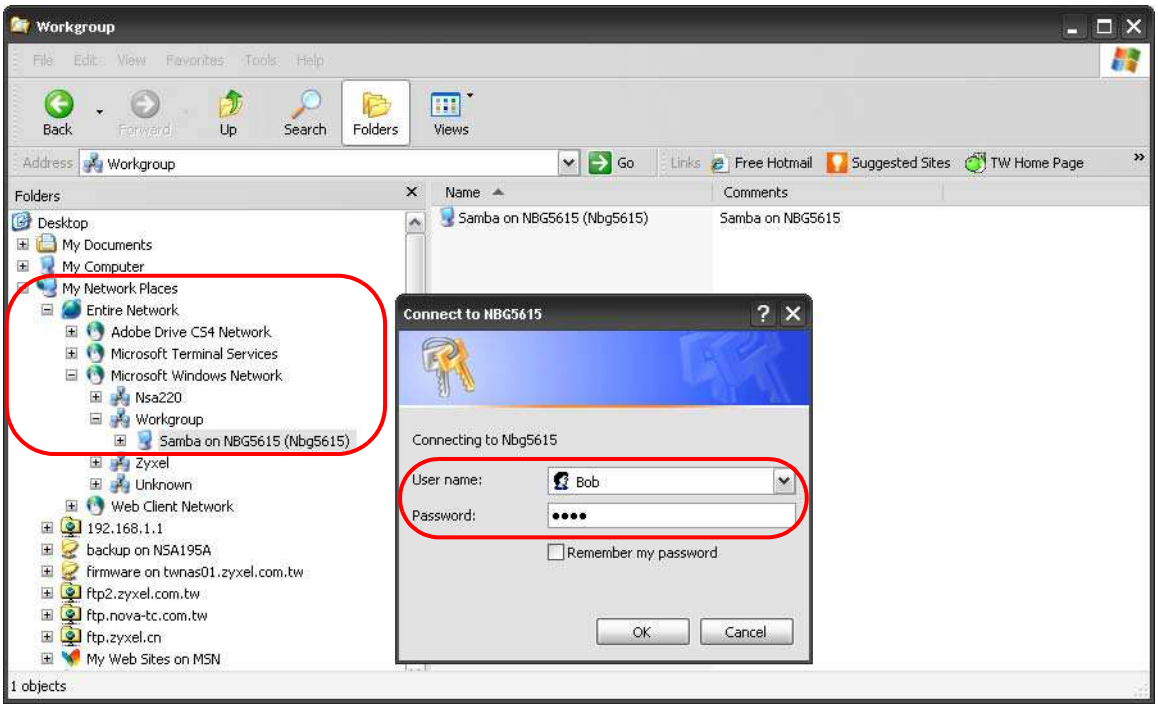
Open Windows Explorer to access the connected USB device using either Windows Explorer browser or by browsing to your workgroup.

1 In Windows Explorer's Address bar type a double backslash "\\" followed by the IP address of the NBG5615 (the default IP address of the NBG5615 in router mode is 192.168.1.1) and press [ENTER]. A screen asking for password authentication appears. Type the user name and password (Bob and 1234 in this example) and click **OK**.



Note: Once you log into the shared folder via your NBG5615, you do not have to relogin unless you restart your computer.

2 You can also use the workgroup name to access files by browsing to the workgroup folder using the folder tree on the left side of the screen. It is located under **My Network Places**. In this example the workgroup name is the default "Workgroup".



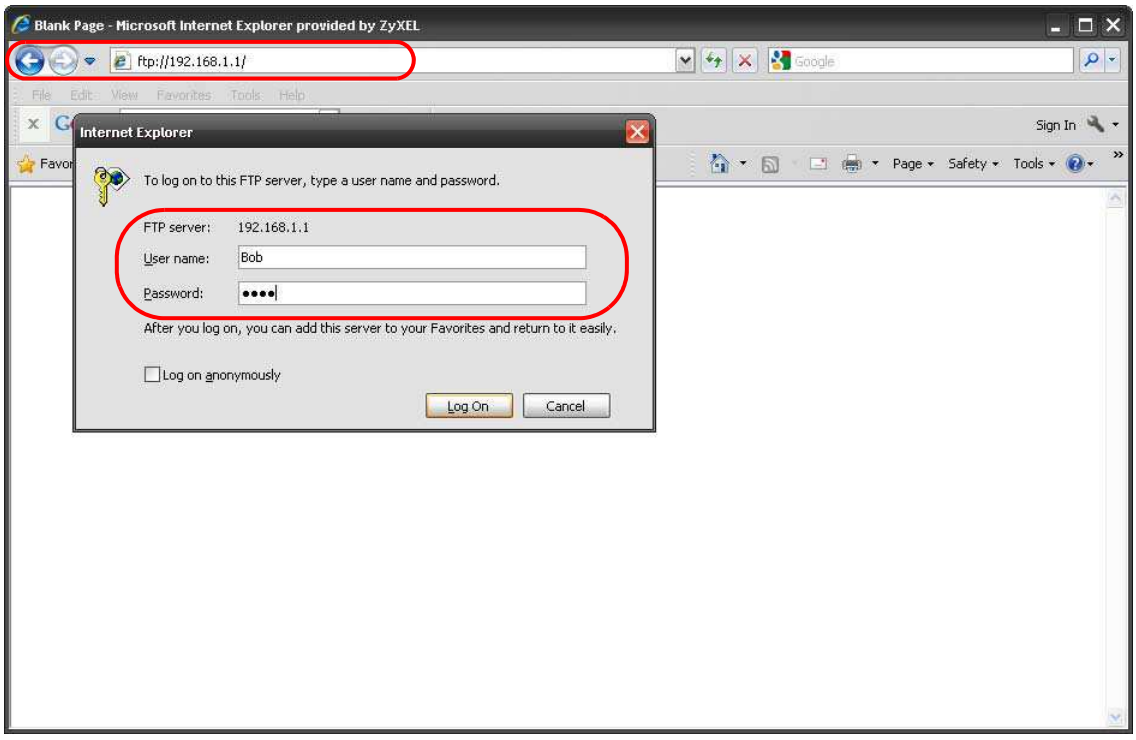
23.8.2 Use FTP to Share Files

You can use FTP to access the USB storage devices connected to the NBG5615. In this example, we use the web browser to share files via FTP from the LAN. The way or screen you log into the FTP server (on the NBG5615) varies depending on your FTP client. See your FTP client documentation for more information.

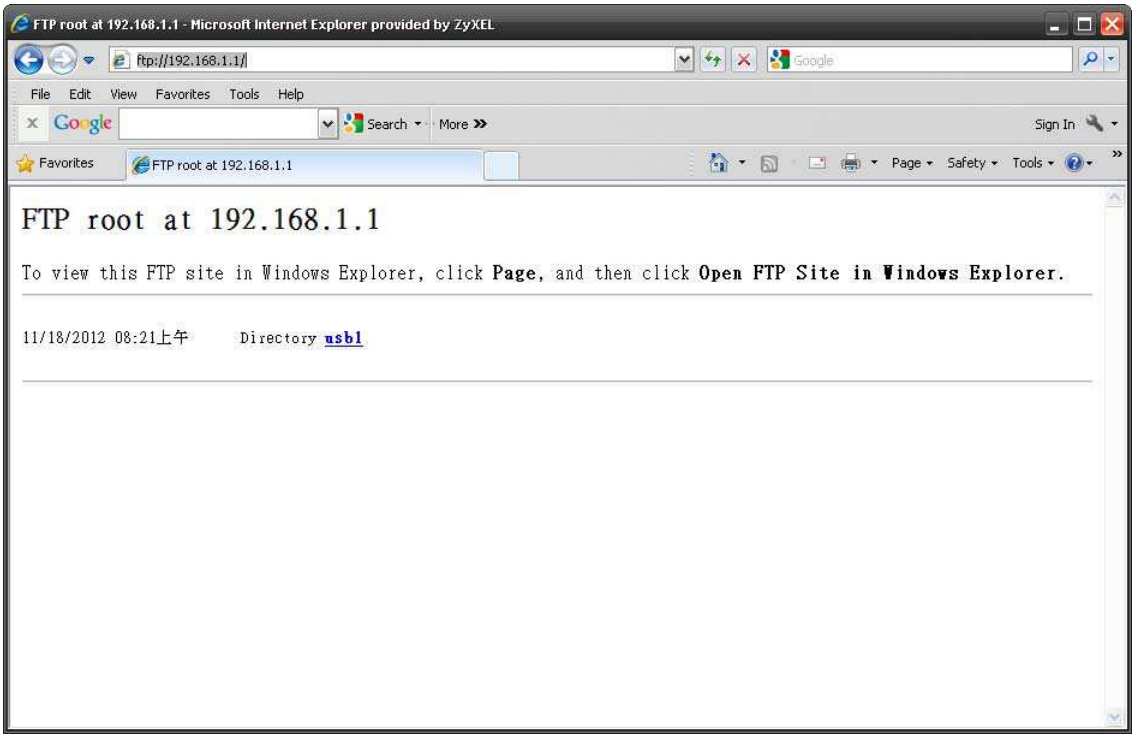
You should have enabled file sharing and create a user account (Bob/1234 for example) with read and write access to USB 1 in the **USB Media Sharing > FTP** screen.

1 In your web browser's address or URL bar type "ftp://" followed by the IP address of the NBG5615 (the default LAN IP address of the NBG5615 in router mode is 192.168.1.1) and click **Go** or press [ENTER].

2 A screen asking for password authentication appears. Enter the user name and password (you configured in the **USB Media Sharing > FTP** screen) and click **Log On**.



3 The screen changes and shows you the folder for the USB storage device connected to your NBG5615. Double-click the folder to display the contents in it.



24

Maintenance

24.1 Overview

This chapter provides information on the **Maintenance** screens.

24.2 What You Can Do

- Use the **General** screen to set the timeout period of the management session (Section 24.3 on page 193).
- Use the **Password** screen to change your NBG5615's system password (Section 24.4 on page 194).
- Use the **Time** screen to change your NBG5615's time and date (Section 24.5 on page 195).
- Use the **Firmware Upgrade** screen to upload firmware to your NBG5615 (Section 24.6 on page 196).
- Use the **Backup/ Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration (Section 24.8 on page 199).
- Use the **Restart** screen to reboot the NBG5615 without turning the power off (Section 24.8 on page 199).
- Use the **Language** screen to change the language for the Web Configurator (Section 24.9 on page 199) .
- Use the **Sys OP Mode** screen to select how you want to use your NBG5615 (Section 24.11 on page 201).

24.3 General Screen

Use this screen to set the management session timeout period. Click **Maintenance** > **General**. The following screen displays.

Figure 120 Maintenance > General

The following table describes the labels in this screen.

Table 78 Maintenance > General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the NBG5615 in an Ethernet network.
Domain Name	Enter the domain name you want to give to the NBG5615.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click **Apply** to save your changes back to the NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

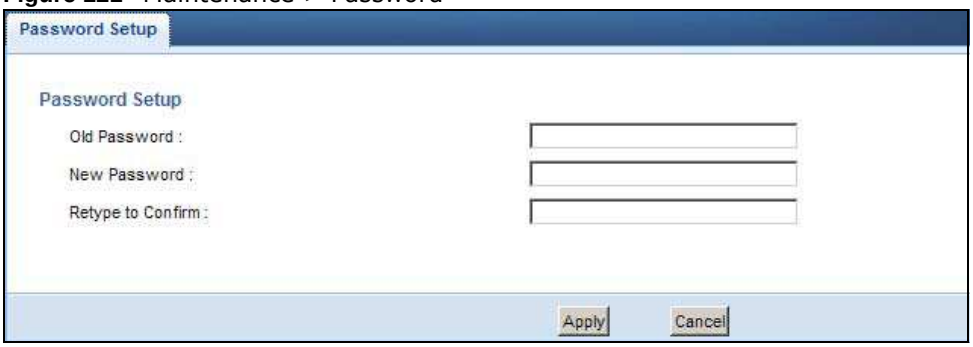
24.4 Password Screen

It is strongly recommended that you change your NBG5615's password.

If you forget your NBG5615's password (or IP address), you will need to reset the device. See Section 24.8 on page 199 for details.

Click **Maintenance** > **Password**. The screen appears as shown.

Figure 121 Maintenance > Password



The following table describes the labels in this screen.

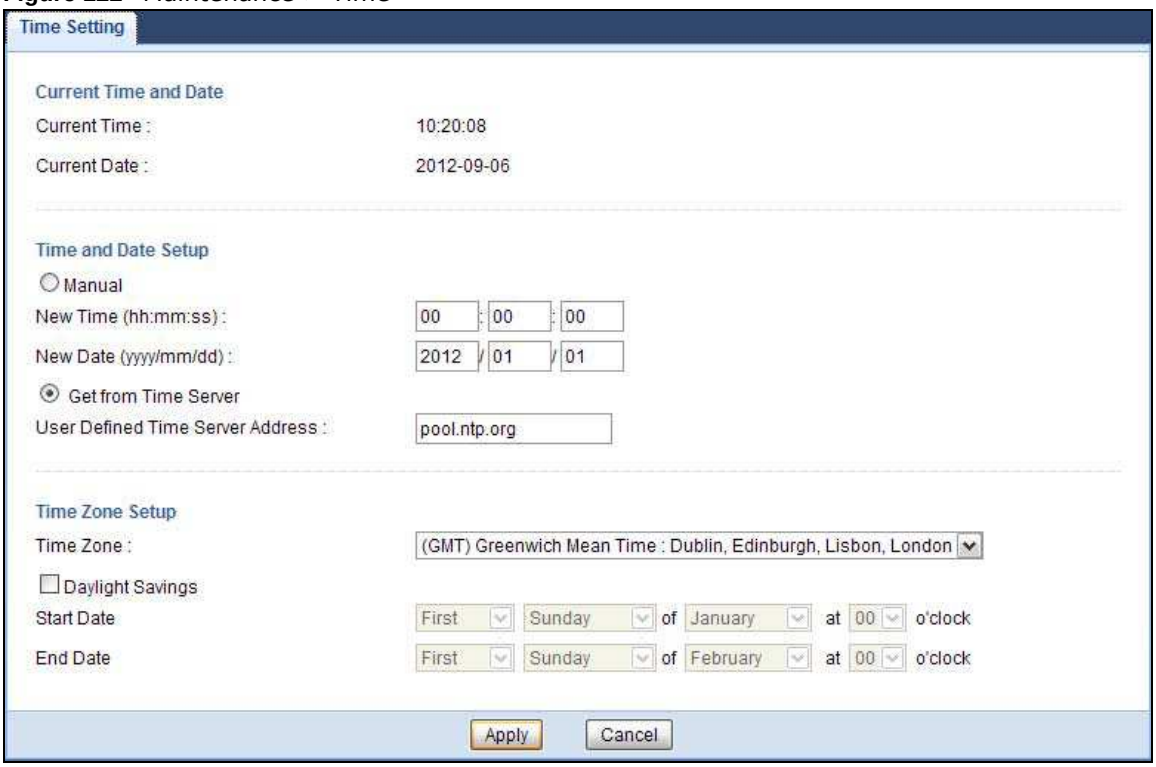
Table 79 Maintenance > Password

LABEL	DESCRIPTION
Password Setup	Change your NBG5615's password (recommended) using the fields as shown.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24.5 Time Setting Screen

Use this screen to configure the NBG5615's time based on your local time zone. To change your NBG5615's time and date, click **Maintenance** > **Time**. The screen appears as shown.

Figure 122 Maintenance > Time



The following table describes the labels in this screen.

Table 80 Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NBG5615. Each time you reload this page, the NBG5615 synchronizes the time with the time server.
Current Date	This field displays the date of your NBG5615. Each time you reload this page, the NBG5615 synchronizes the date with the time server.
Current Time and Date	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you select **Manual**, enter the new time in this field and then click **Apply**.

Table 80 Maintenance > Time (continued)

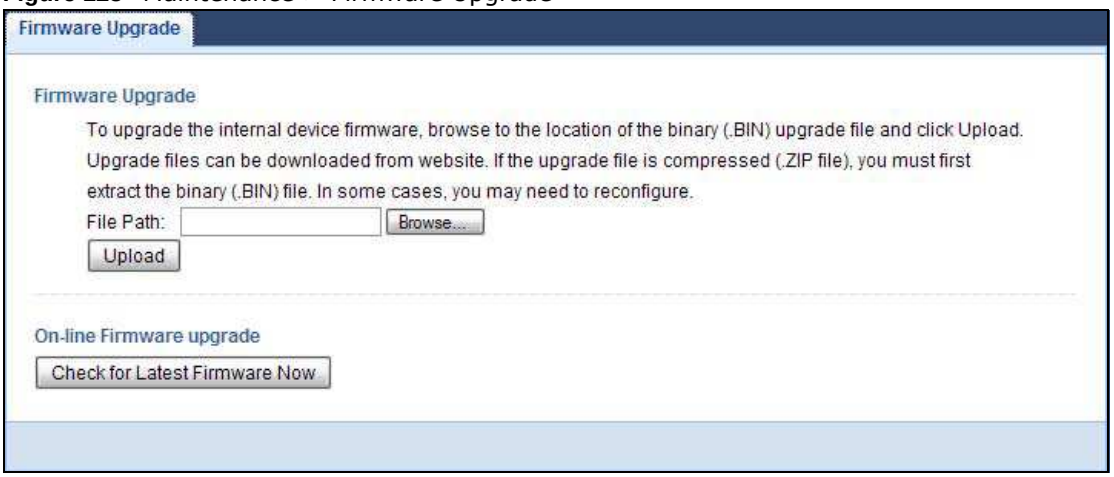
LABEL	DESCRIPTION
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you select **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the NBG5615 get the time and date from the time server you specified below.
User Defined Time Server Address	Select **User Defined Time Server Address** and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and select **2** in the **at** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you select in the **at** field depends on your time zone. In Germany for instance, you would select 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and select 2 in the **at** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you select in the **at** field depends on your time zone. In Germany for instance, you would select 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes back to the NBG5615.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24.6 Firmware Upgrade Screen

Find firmware at www.zyxel.com in a file that uses the version number and project code with a "*.bin" extension, e.g., "V1.00(AAGI.0).bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your NBG5615.

Figure 123 Maintenance > Firmware Upgrade



The following table describes the labels in this screen.

Table 81 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
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 .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.
Check for Latest Firmware Now	Click this to check for the latest updated firmware.

Note: Do not turn off the NBG5615 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the NBG5615 again.

The NBG5615 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 124 Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, an error message appears. Click **Return** to go back to the **Firmware Upgrade** screen.

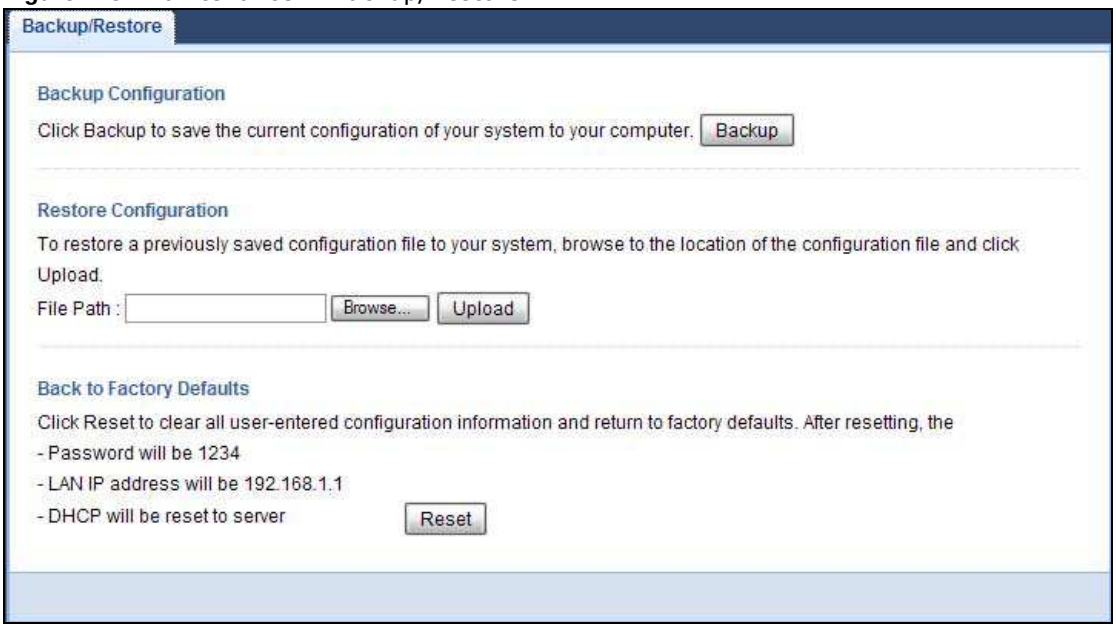
24.7 Configuration Backup/Restore Screen

Backup configuration allows you to back up (save) the NBG5615's current configuration to a file on your computer. Once your NBG5615 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NBG5615.

Click **Maintenance > Backup/ Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 125 Maintenance > Backup/Restore



The following table describes the labels in this screen.

Table 82 Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup	Click **Backup** to save the NBG5615's current configuration to your computer.
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 file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.

Table 82 Maintenance > Backup/Restore (continued)

LABEL	DESCRIPTION
Upload	Click **Upload** to begin the upload process. Note: Do not turn off the NBG5615 while configuration file upload is in progress. After you see a "configuration upload successful" screen, you must then wait one minute before logging into the NBG5615 again. The NBG5615 automatically restarts in this time causing a temporary network disconnect. If you see an error screen, click Back to return to the Backup/Restore screen.
Reset	Pressing the **Reset** button in this section clears all user-entered configuration information and returns the NBG5615 to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your NBG5615. Refer to the chapter about introducing the Web Configurator for more information on the **RESET** button.

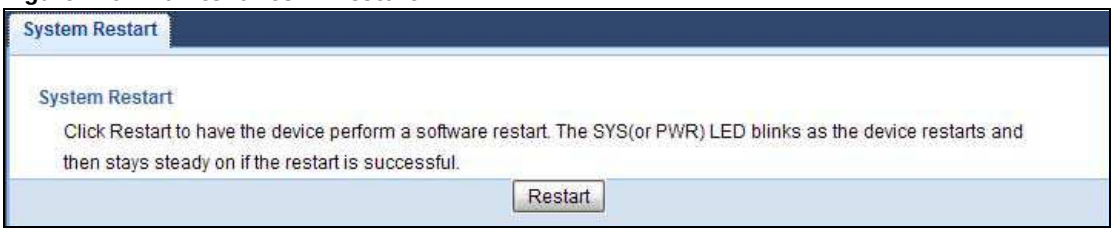
Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default NBG5615 IP address (192.168.1.1). See Appendix B on page 221 for details on how to set up your computer's IP address.

24.8 Restart Screen

System restart allows you to reboot the NBG5615 without turning the power off.

Click **Maintenance > Restart** to open the following screen.

Figure 126 Maintenance > Restart



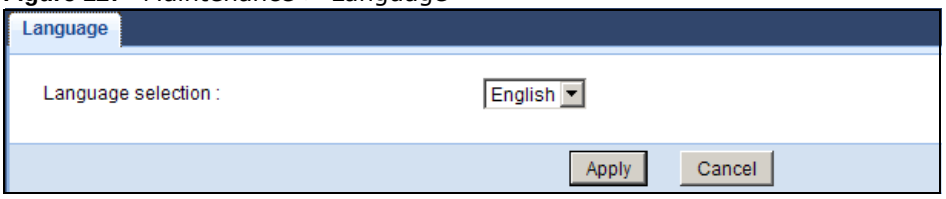
Click **Restart** to have the NBG5615 reboot. This does not affect the NBG5615's configuration.

24.9 Language Screen

Use this screen to change the language for the Web Configurator.

Select the language you prefer and click **Apply**. The Web Configurator language changes after a while without restarting the NBG5615.

Figure 127 Maintenance > Language



24.10 System Operation Mode Overview

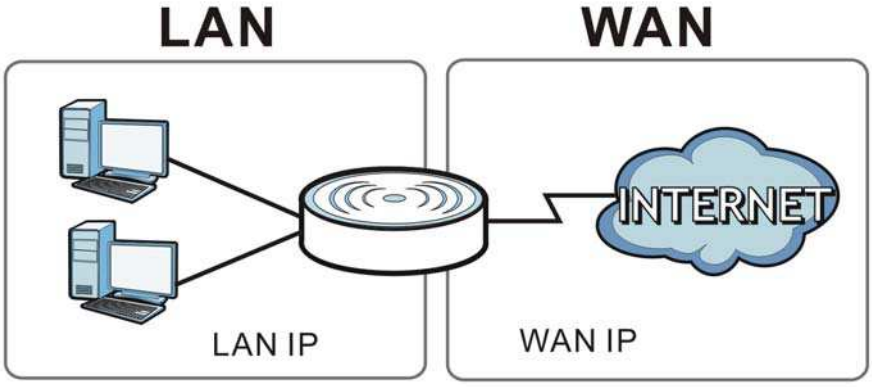
The **Sys OP Mode** (System Operation Mode) function lets you configure your NBG5615 as a router or access point. You can choose between **Router Mode**, and **Access Point Mode** depending on your network topology and the features you require from your device.

The following describes the device modes available in your NBG5615.

Router

A router connects your local network with another network, such as the Internet. The router has two IP addresses, the LAN IP address and the WAN IP address.

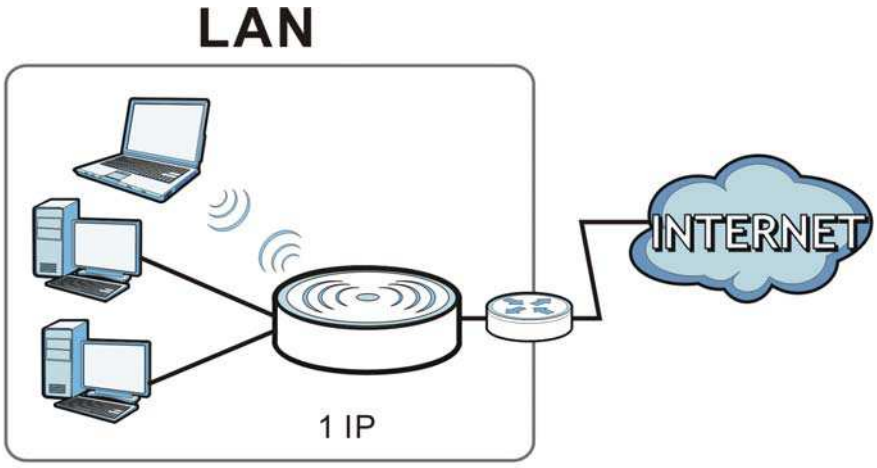
Figure 128 LAN and WAN IP Addresses in Router Mode



Access Point

An access point enabled all ethernet ports to be bridged together and be in the same subnet. To connect to the Internet, another device, such as a router, is required.

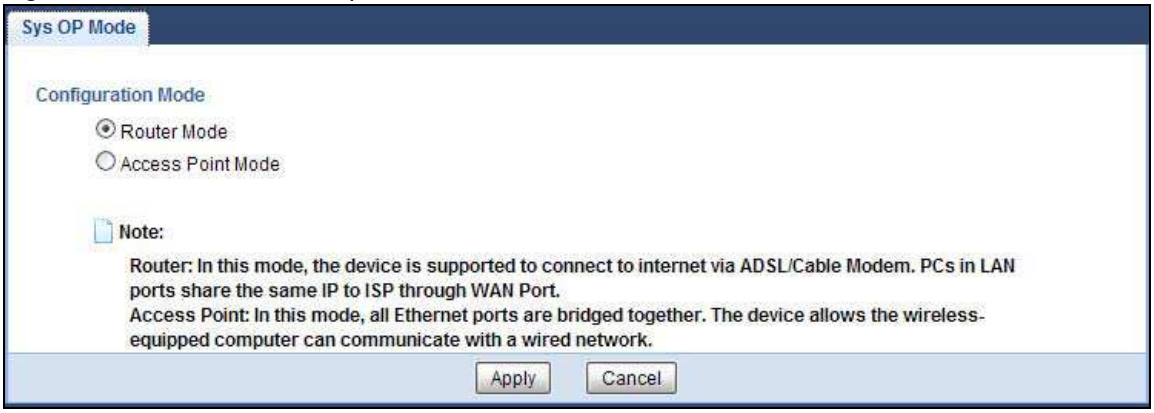
Figure 129 Access Point Mode



24.11 Sys OP Mode Screen

Use this screen to select how you want to use your NBG5615.

Figure 130 Maintenance > Sys OP Mode



The following table describes the labels in the **General** screen.

Table 83 Maintenance > Sys OP Mode

LABEL	DESCRIPTION
Configuration Mode	
Router Mode	Select **Router Mode** if your device routes traffic between a local network and another network such as the Internet. This mode offers services such as a firewall or bandwidth management. You can configure the IP address settings on your WAN port. Contact your ISP or system administrator for more information on appropriate settings.

Table 83 Maintenance > Sys OP Mode (continued)

LABEL	DESCRIPTION
Access Point Mode	Select **Access Point Mode** if your device bridges traffic between clients on the same network. • In **Access Point Mode**, all Ethernet ports have the same IP address. • All ports on the rear panel of the device are LAN ports, including the port labeled WAN. There is no WAN port. • The DHCP server on your device is disabled. • Router functions (such as NAT, bandwidth management, remote management, firewall and so on) are not available when the NBG5615 is in **Access Point Mode**. • The IP address of the device on the local network is set to 192.168.1.2.
Apply	Click **Apply** to save your settings.
Cancel	Click **Cancel** to return your settings to the default (**Router**).

Note: If you select the incorrect system operation Mode you may not be able to connect to the Internet.

25

Troubleshooting

25.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- NBG5615 Access and Login
- Internet Access
- Resetting the NBG5615 to Its Factory Defaults
- Wireless Connections
- USB Device Problems
- ZyXEL Share Center Utility Problems

25.2 Power, Hardware Connections, and LEDs

The NBG5615 does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the NBG5615.
2. Make sure the power adaptor or cord is connected to the NBG5615 and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the NBG5615.
4. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.7 on page 18.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Disconnect and re-connect the power adaptor to the NBG5615.

5 If the problem continues, contact the vendor.

25.3 NBG5615 Access and Login

I don't know the IP address of my NBG5615.

1 The default IP address of the NBG5615 in **Router Mode** is **192.168.1.1**. The default IP address of the NBG5615 in **Access Point Mode** is **192.168.1.2**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the NBG5615 in **Router Mode** by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the NBG5615 (it depends on the network), so enter this IP address in your Internet browser.

3 If your NBG5615 in **Access Point Mode** is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.

4 Reset your NBG5615 to change all settings back to their default. This means your current settings are lost. See Section 25.5 on page 207 in the **Troubleshooting** for information on resetting your NBG5615.

I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 25.5 on page 207.

I cannot see or access the **Login** screen in the Web Configurator.

1 Make sure you are using the correct IP address.

- The default IP address of the NBG5615 in **Router Mode** is **192.168.1.1**. The default IP address of the NBG5615 in **Access Point Mode** is **192.168.1.2**.
- If you changed the IP address (Section 13.4 on page 130), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I don't know the IP address of my NBG5615.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix A on page 211.

4 Make sure your computer is in the same subnet as the NBG5615. (If you know that there are routers between your computer and the NBG5615, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 13.4 on page 130.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG5615. See Section 13.4 on page 130.

5 Reset the device to its factory defaults, and try to access the NBG5615 with the default IP address. See Section 1.5 on page 16.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the NBG5615 using another service, such as Telnet. If you can access the NBG5615, check the remote management settings and firewall rules to find out why the NBG5615 does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN/ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the NBG5615.

1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.

2 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.

3 Disconnect and re-connect the power adaptor or cord to the NBG5615.

4 If this does not work, you have to reset the device to its factory defaults. See Section 25.5 on page 207.

25.4 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
2. Go to **Maintenance > Sys OP Mode**. Check your System Operation Mode setting.
   - If the NBG5615 is in **Router Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access. Your computer and the NBG5615 should be in the same subnet.
   - If the NBG5615 is in **Access Point Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access and your computer is set to obtain an dynamic IP address.
3. If the NBG5615 is in **Router Mode**, make sure you entered your ISP account information correctly in the wizard or the WAN screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.
4. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
5. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
6. If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NBG5615), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.7 on page 18.
2. Reboot the NBG5615.
3. If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.7 on page 18. If the NBG5615 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength. If the signal strength is low, try moving the NBG5615 closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
3. Reboot the NBG5615.
4. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

   Advanced Suggestion

- Check the settings for QoS. If it is disabled, you might consider activating it.

25.5 Resetting the NBG5615 to Its Factory Defaults

If you reset the NBG5615, you lose all of the changes you have made. The NBG5615 re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

To reset the NBG5615:

1. Make sure the power LED is on.
2. Press the **RESET** button for one to four seconds to restart/reboot the NBG5615.
3. Press the **RESET** button for longer than five seconds to set the NBG5615 back to its factory-default configurations.

   If the NBG5615 restarts automatically, wait for the NBG5615 to finish restarting, and log in to the Web Configurator. The password is "1234".

   If the NBG5615 does not restart automatically, disconnect and reconnect the NBG5615's power. Then, follow the directions above again.

25.6 Wireless Connections

I cannot access the NBG5615 or ping any computer from the WLAN.

1. Make sure the wireless LAN is enabled on the NBG5615.
2. Make sure the wireless adapter on your computer is working properly.
3. Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the NBG5615.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG5615.
5. Check that both the NBG5615 and the wireless adapter on your computer are using the same wireless and wireless security settings.
6. Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the NBG5615.

7 Make sure you allow the NBG5615 to be remotely accessed through the WLAN interface. Check your remote management settings.

- See the chapter on Wireless LAN in the User's Guide for more information.

I set up URL keyword blocking, but I can still access a website that should be blocked.

Make sure that you select the **Enable URL Keyword Blocking** check box in the Content Filtering screen. Make sure that the keywords that you type are listed in the **Keyword List**.

If a keyword that is listed in the **Keyword List** is not blocked when it is found in a URL, customize the keyword blocking using commands. See the Customizing Keyword Blocking URL Checking section in the Content Filtering chapter.

I cannot access the Web Configurator after I switched to AP mode.

When you change from router mode to AP mode, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".

Refer to Appendix B on page 221 for instructions on how to change your computer's IP address.

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

- Position the antennas for best reception. If the AP is placed on a table or floor, point the antennas upwards. If the AP is placed at a high position, point the antennas downwards. Try pointing the antennas in different directions and check which provides the strongest signal to the wireless clients.

25.7 USB Device Problems

I cannot access or see a USB device that is connected to the NBG5615.

1. Be sure to install the ZyXEL NetUSB Share Center Utility (for NetUSB functionality) first from the included disc, or download the latest version from the zyxel.com website.
2. Disconnect the problematic USB device, then reconnect it to the NBG5615.
3. Ensure that the USB device has power.
4. Check your cable connections.
5. Restart the NBG5615 by disconnecting the power and then reconnecting it.
6. If the USB device requires a special driver, install the driver from the installation disc that came with the device. After driver installation, reconnect the USB device to the NBG5615 and try to connect to it again with your computer.
7. If the problem persists, contact your vendor.

What kind of USB devices do the NBG5615 support?

1. It is strongly recommended to use version 2.0 or lower USB storage devices (such as memory sticks, USB hard drives) and/or USB devices (such as USB printers). Other USB products are not guaranteed to function properly with the NBG5615.

25.8 ZyXEL Share Center Utility Problems

I cannot access or see a USB device that is connected to the NBG5615.

1. Disconnect the problematic USB device, then reconnect it to the NBG5615.
2. Ensure that the USB device in question has power.

3 Check your cable connections.

4 Restart the NBG5615 by disconnecting the power and then reconnecting it.

5 If the USB device requires a special driver, install the driver from the installation disc that came with the device. After driver installation, reconnect the USB device to the NBG5615 and try to connect to it again with your computer.

6 If the problem persists, contact your vendor.

I cannot install the ZyXEL Share Center Utility.

1 Make sure that the set up program is one required for your operating system.

2 Install the latest patches and updates for your operating system.

3 Check the zyxel.com download site for a newer version of the utility.

A

Pop-up Windows, JavaScript and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: The screens used below belong to Internet Explorer version 6, 7 and 8. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

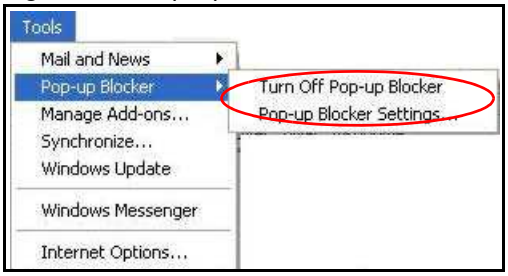
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 131 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 132 Internet Options: Privacy

3 Click **Apply** to save this setting.

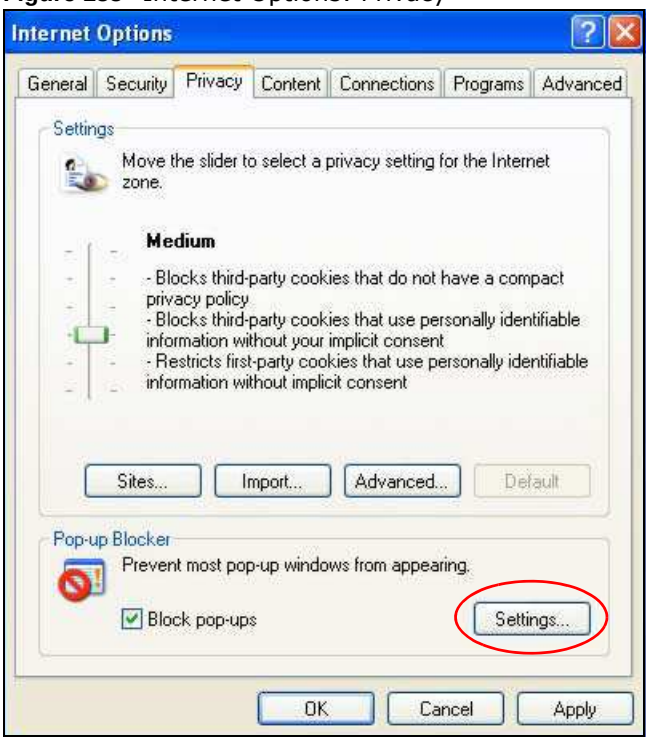
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 133 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 134 Pop-up Blocker Settings

5 Click **Close** to return to the **Privacy** screen.

6 Click **Apply** to save this setting.

JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 135 Internet Options: Security

2 Click the **Custom Level...** button.

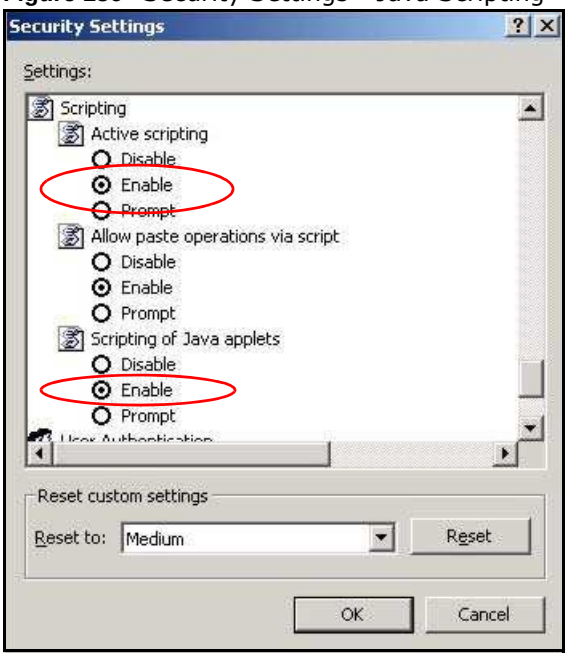
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 136 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

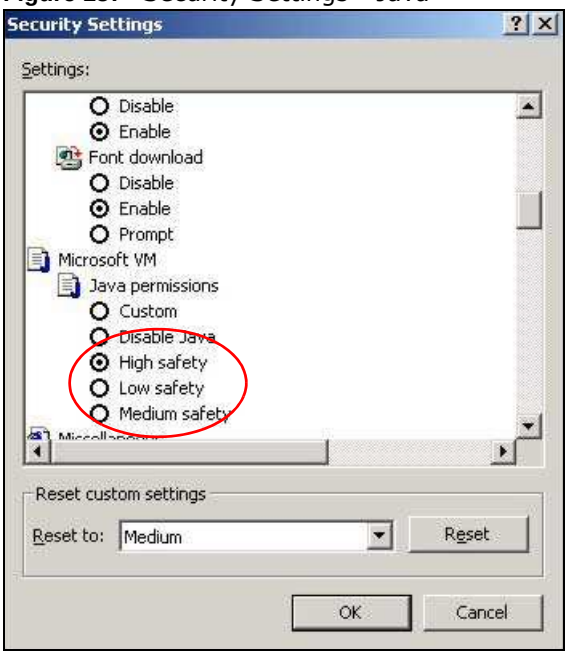
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 137 Security Settings - Java



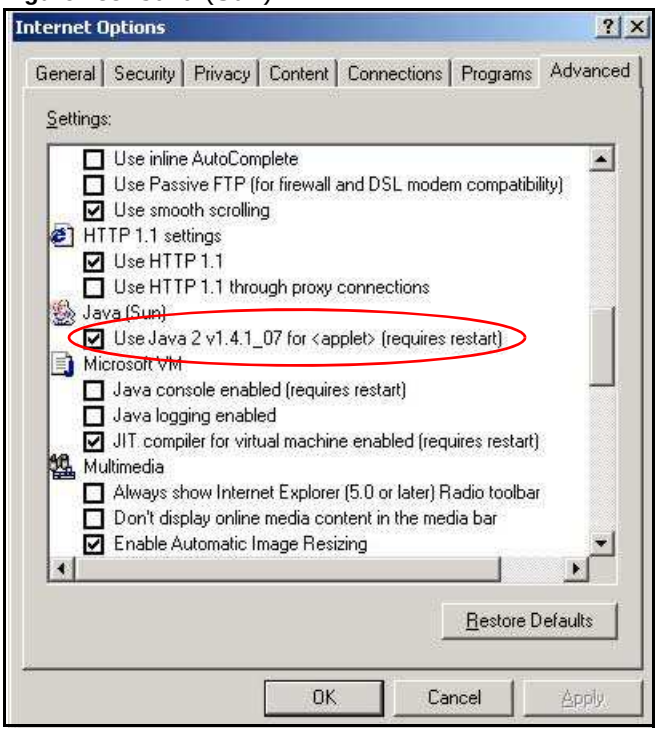
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 138 Java (Sun)

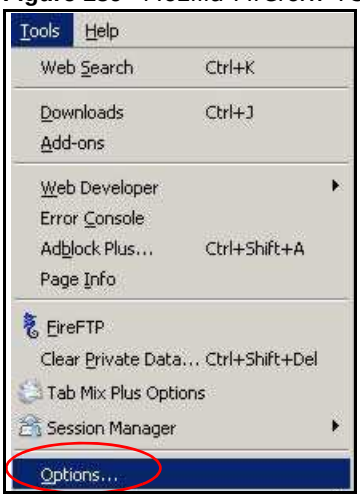


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary slightly. The steps below apply to Mozilla Firefox 3.0 as well.

You can enable Java, Javascript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 139 Mozilla Firefox: TOOLS > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 140 Mozilla Firefox Content Security

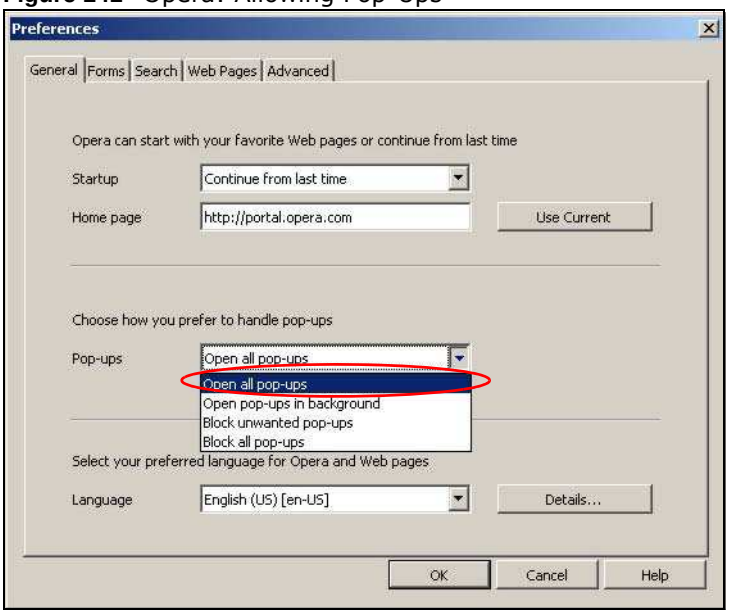
Opera

Opera 10 screens are used here. Screens for other versions may vary slightly.

Allowing Pop-Ups

From Opera, click **Tools**, then **Preferences**. In the **General** tab, go to **Choose how you prefer to handle pop-ups** and select **Open all pop-ups**.

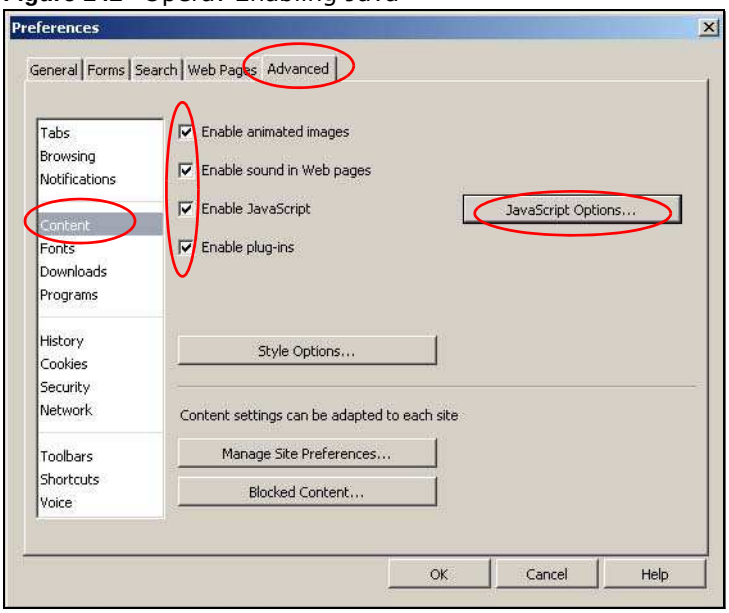
Figure 141 Opera: Allowing Pop-Ups



Enabling Java

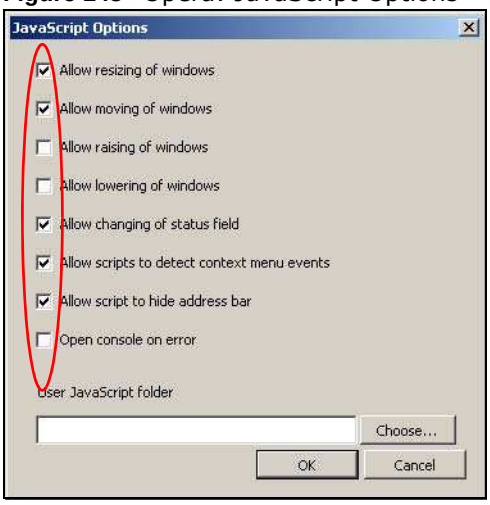
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 142 Opera: Enabling Java



To customize JavaScript behavior in the Opera browser, click **JavaScript Options**.

Figure 143 Opera: JavaScript Options



Select the items you want Opera's JavaScript to apply.

B

Setting Up Your Computer's IP Address

Note: Your specific NBG5615 may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

- Windows XP/NT/2000 on page 221
- Windows Vista on page 225
- Windows 7 on page 229
- Mac OS X: 10.3 and 10.4 on page 233
- Mac OS X: 10.5 and 10.6 on page 236
- Linux: Ubuntu 8 (GNOME) on page 239
- Linux: openSUSE 10.3 (KDE) on page 243

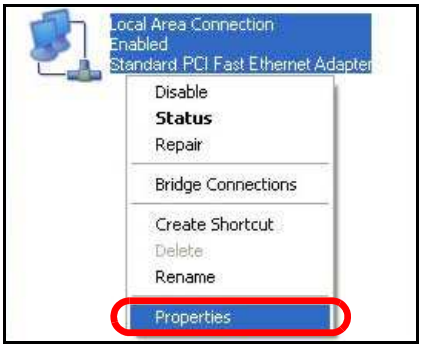
Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

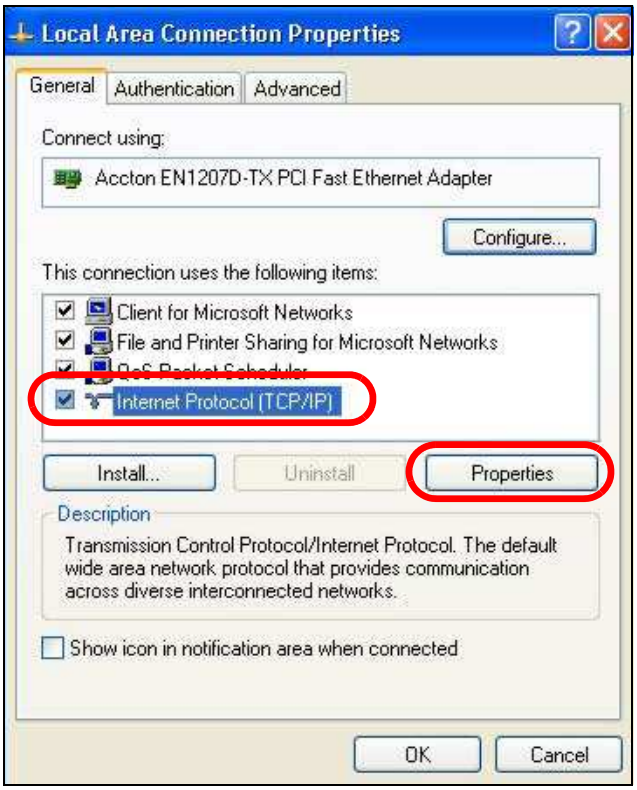
1 Click **Start** > **Control Panel**.

2 In the **Control Panel**, click the **Network Connections** icon.

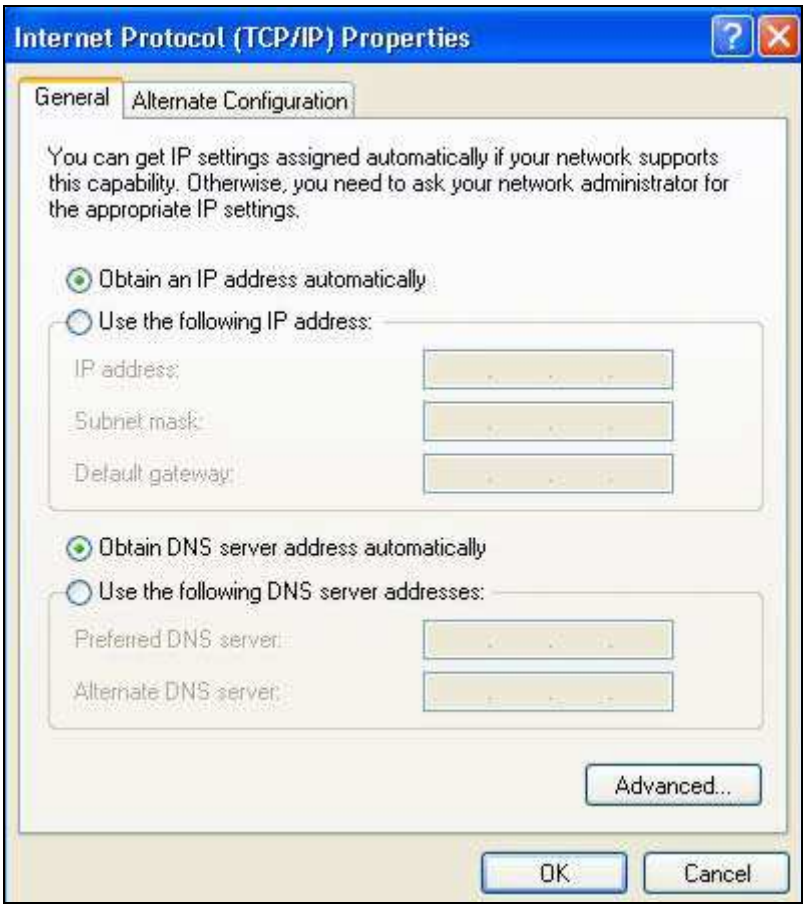
3 Right-click **Local Area Connection** and then select **Properties**.



4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.



5 The **Internet Protocol TCP/ IP Properties** window opens.



6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

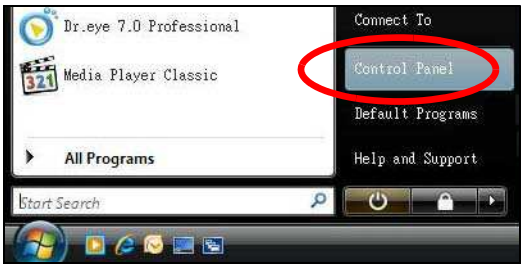
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

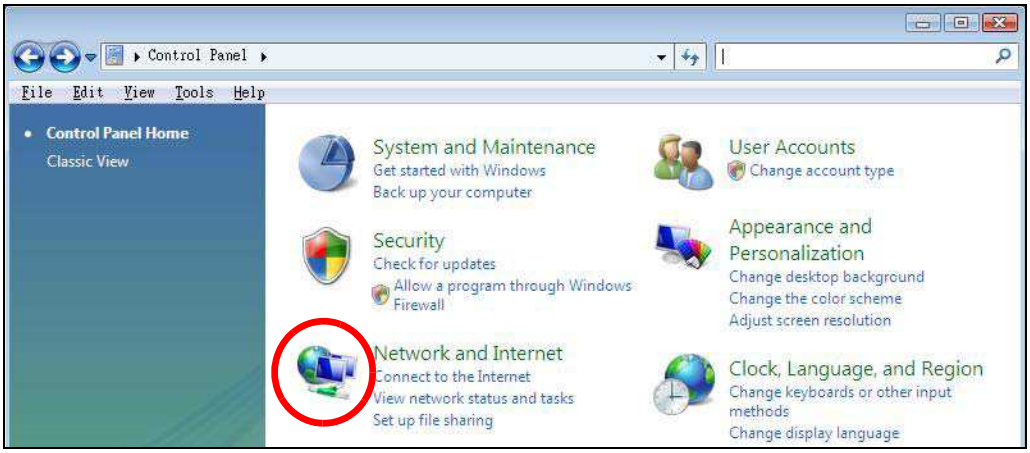
Windows Vista

This section shows screens from Windows Vista Professional.

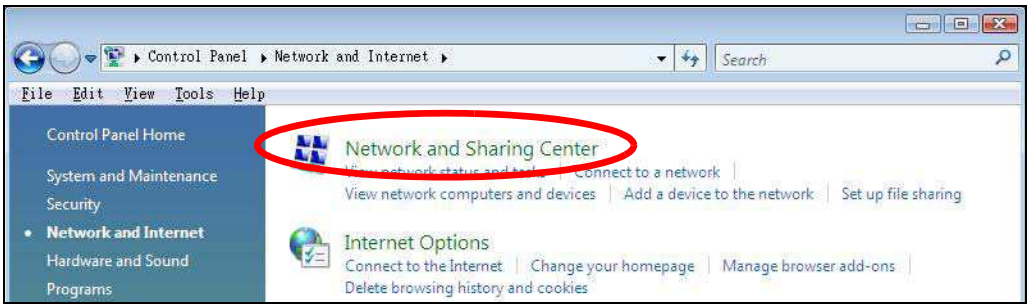
1 Click **Start** > **Control Panel**.



2 In the **Control Panel**, click the **Network and Internet** icon.

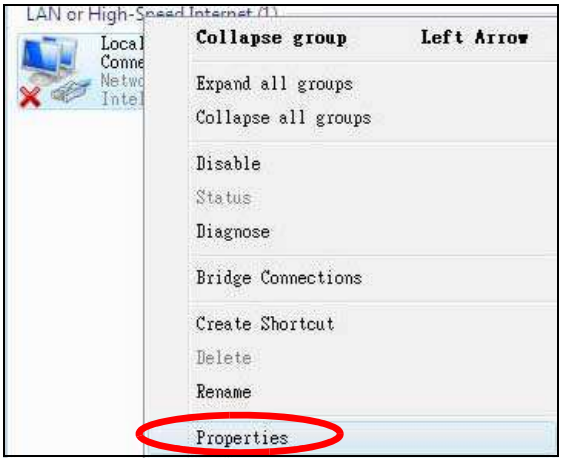


3 Click the **Network and Sharing Center** icon.



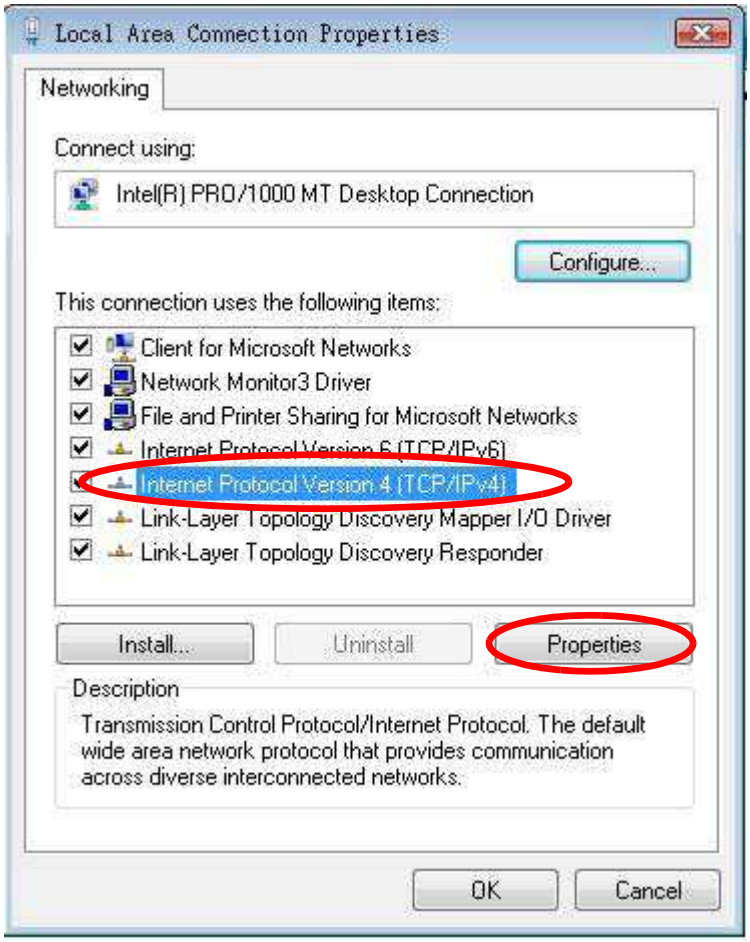
4 Click **Manage network connections**.

5 Right-click **Local Area Connection** and then select **Properties**.

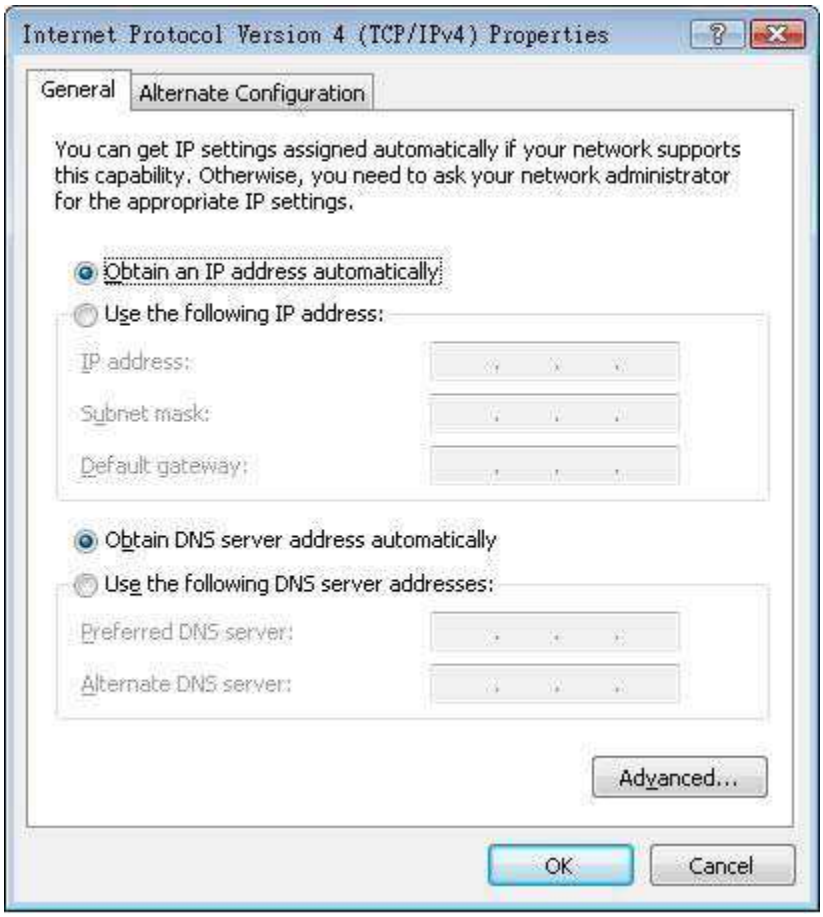


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.



8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

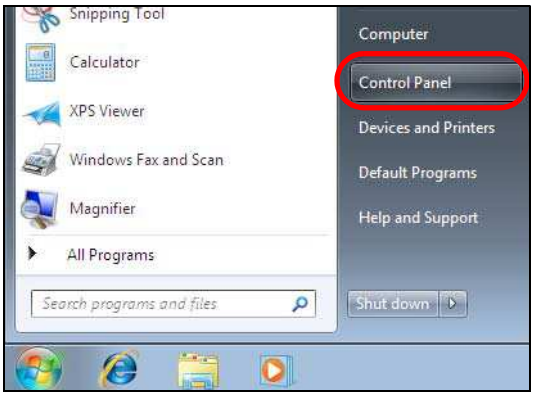
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows 7

This section shows screens from Windows 7 Enterprise.

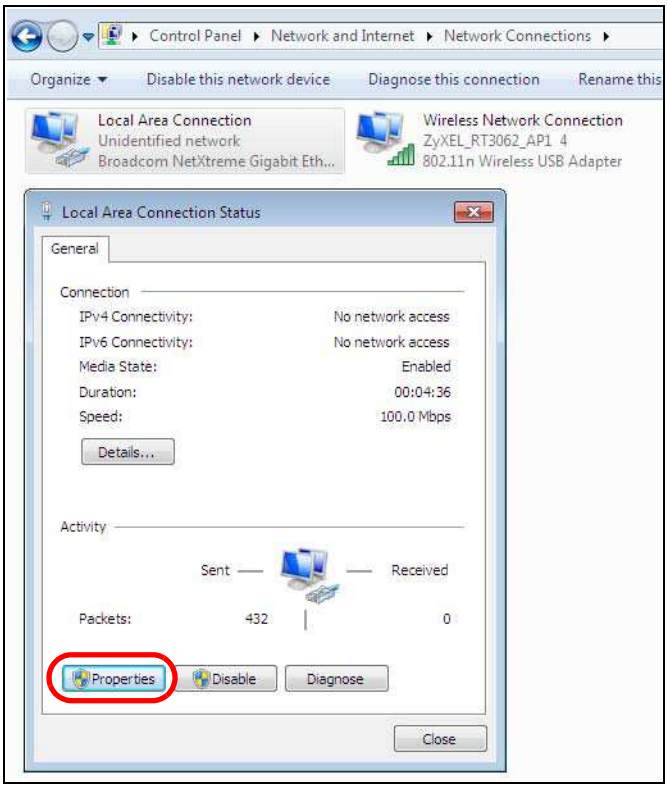
1 Click **Start** > **Control Panel**.



2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

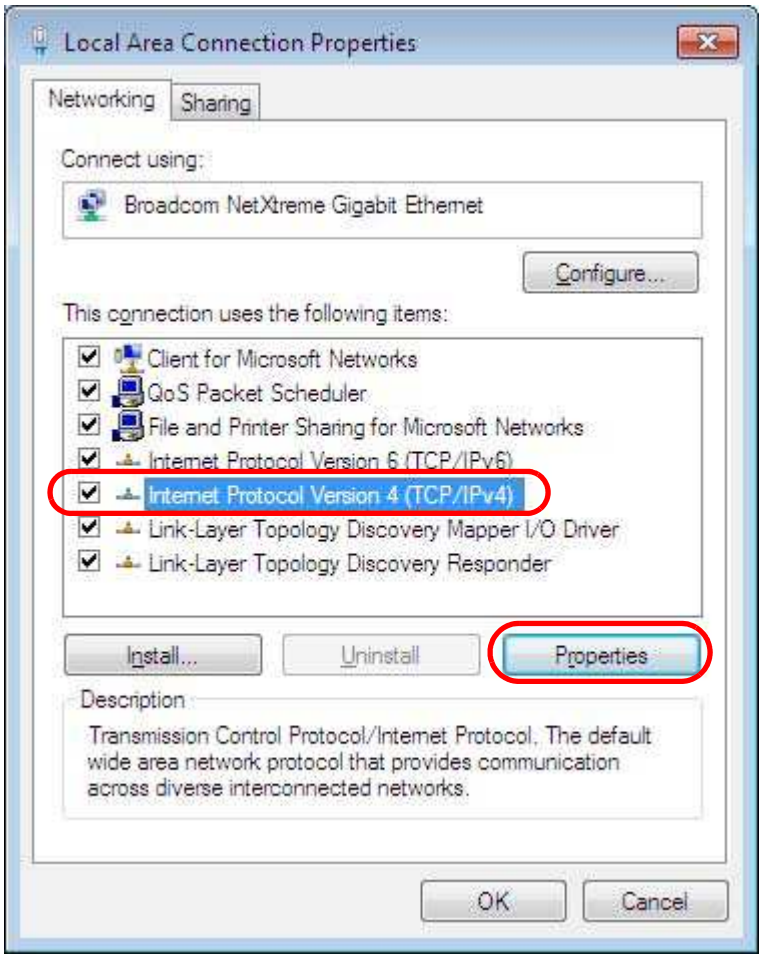
3 Click **Change adapter settings**.

4 Double click **Local Area Connection** and then select **Properties**.

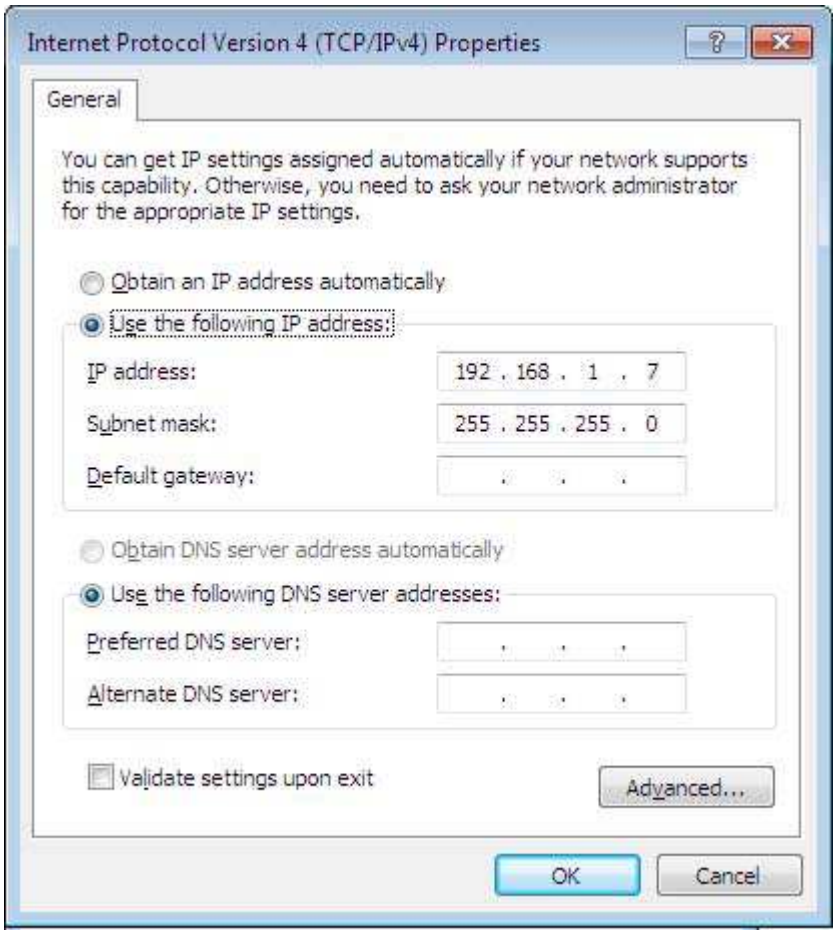


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.



7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

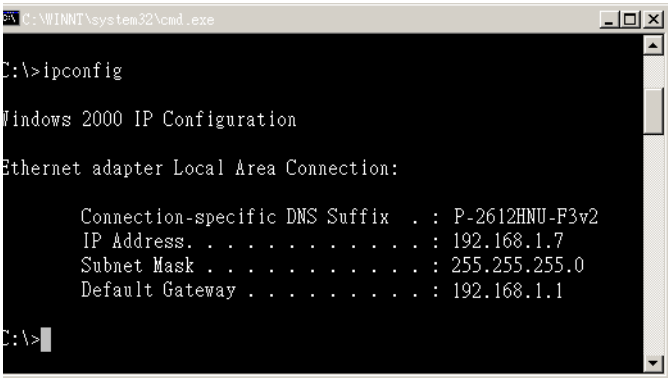
9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

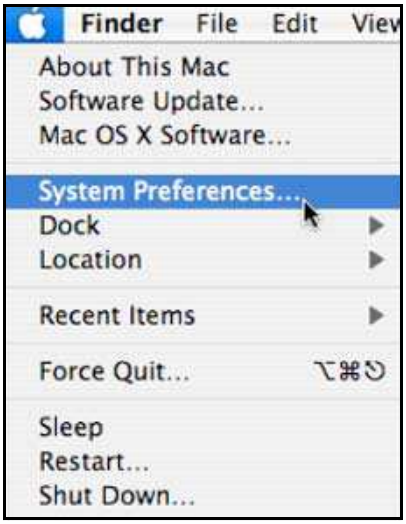
3 The IP settings are displayed as follows.



Mac OS X: 10.3 and 10.4

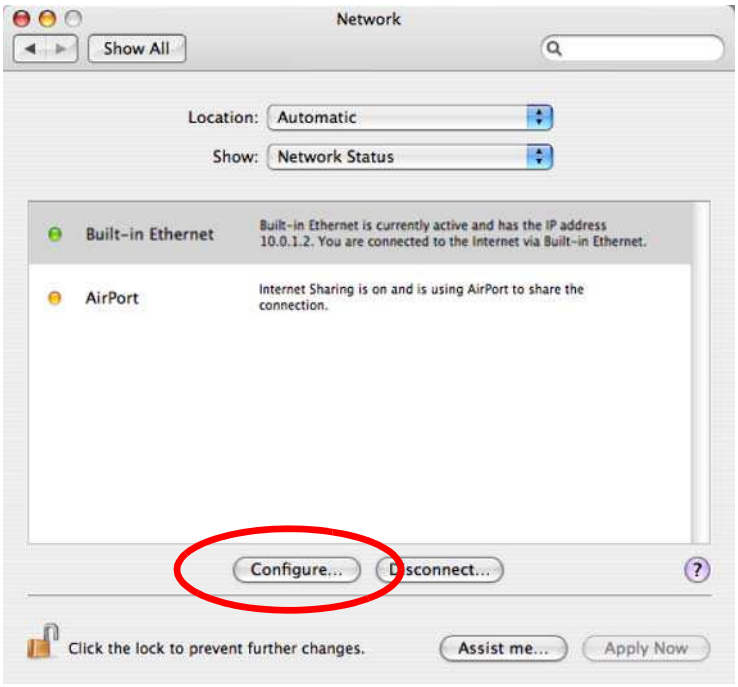
The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

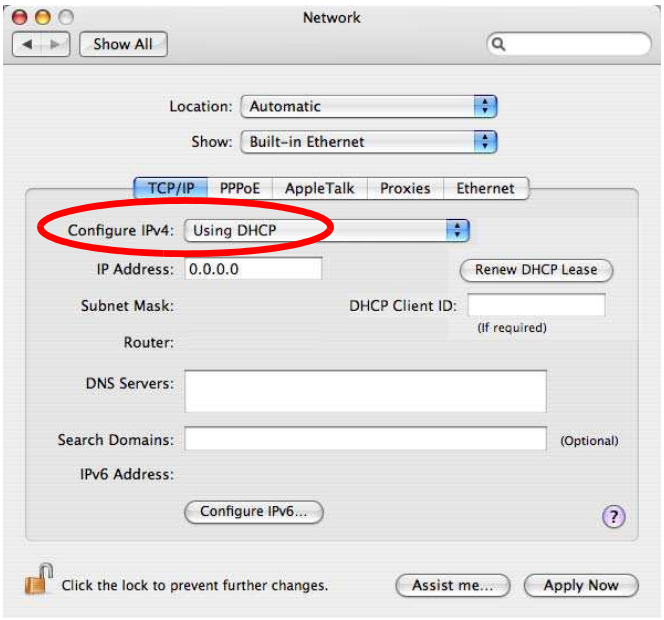


2 In the **System Preferences** window, click the **Network** icon.

3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

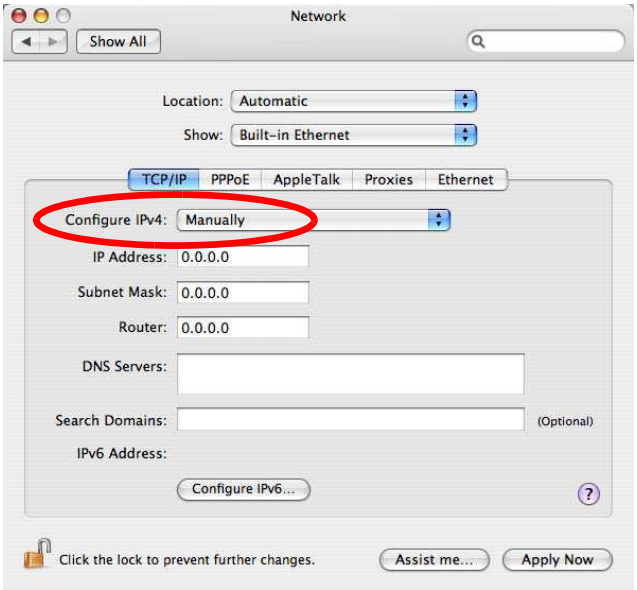


4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.



5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.
- In the **Router** field, type the IP address of your device.

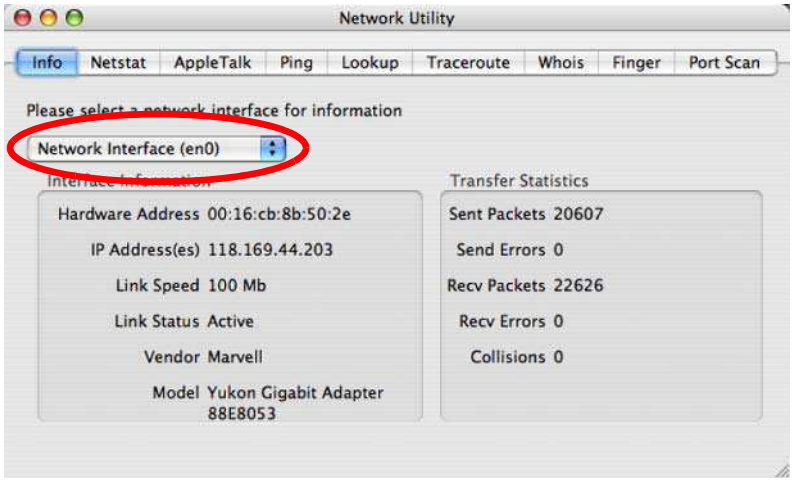


6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

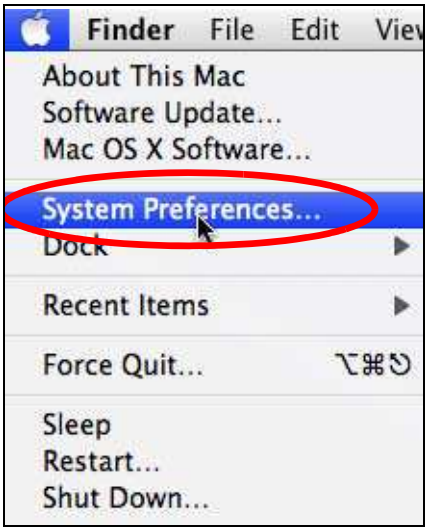
Figure 144 Mac OS X 10.4: Network Utility



Mac OS X: 10.5 and 10.6

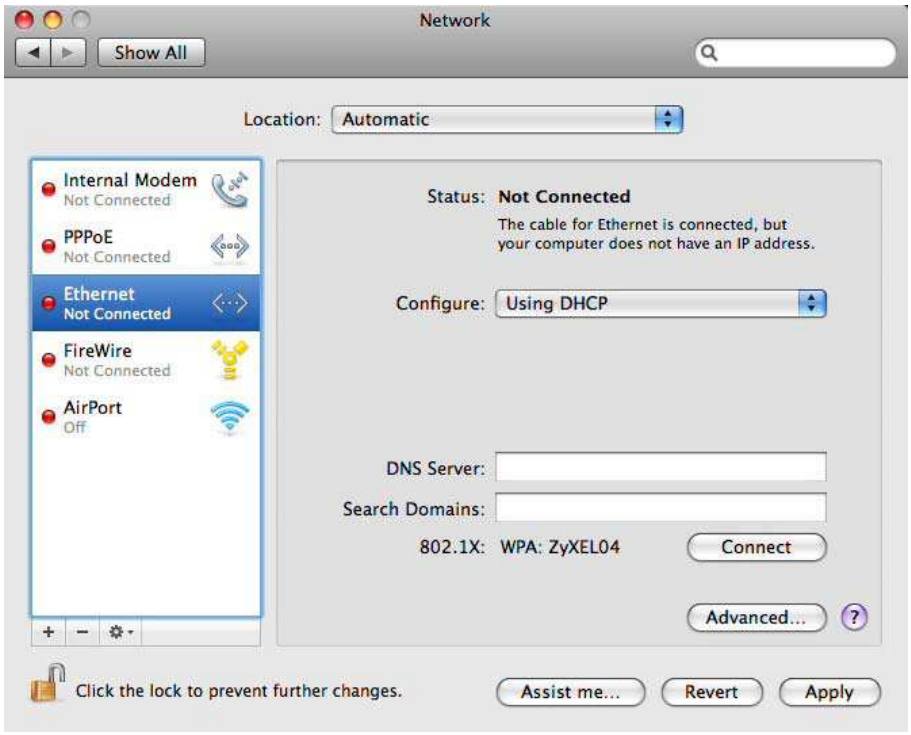
The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

1 Click **Apple** > **System Preferences**.



2 In **System Preferences**, click the **Network** icon.

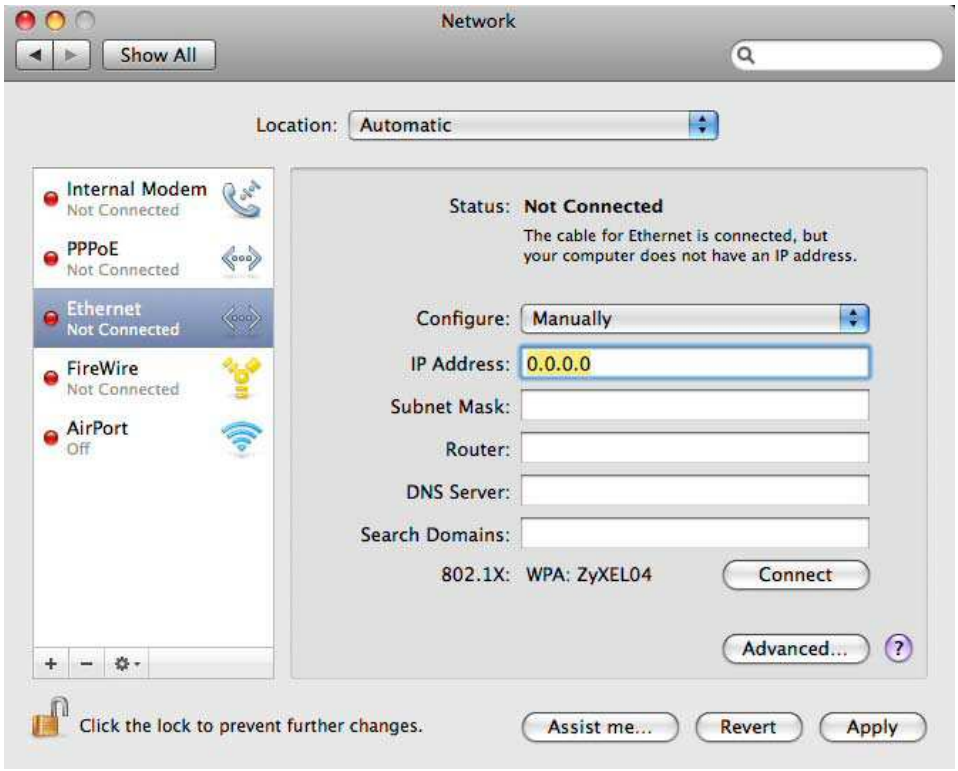
3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.



4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your NBG5615.

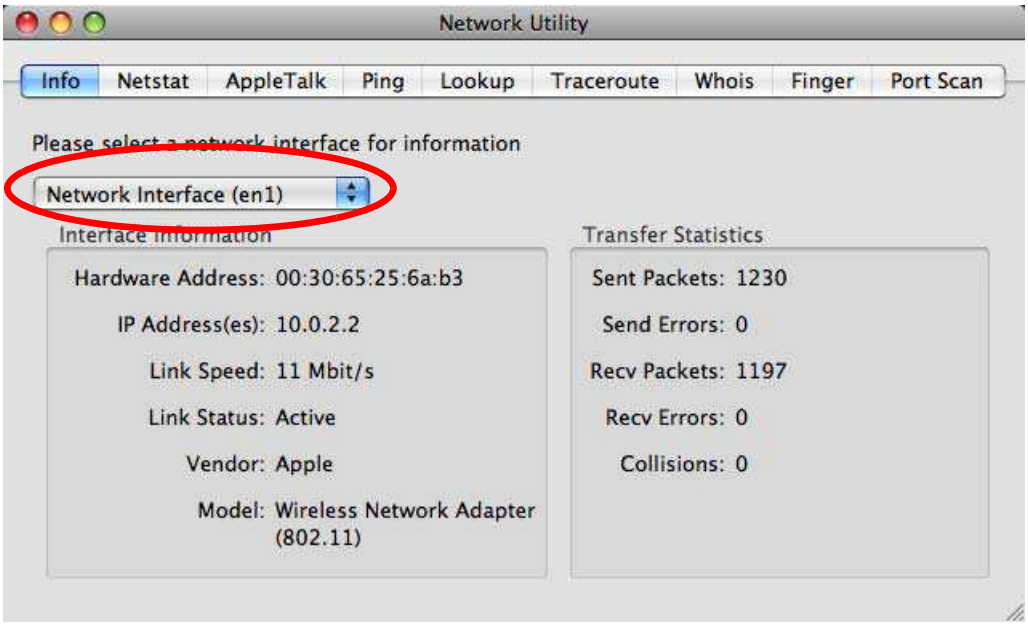


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 145 Mac OS X 10.5: Network Utility



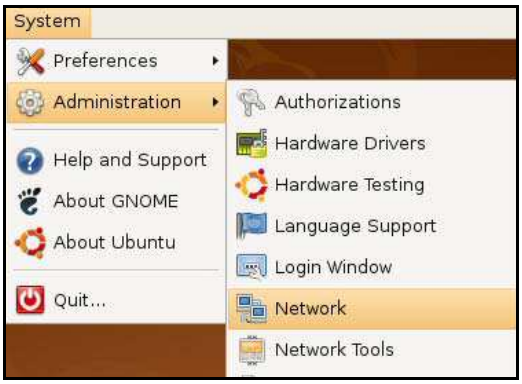
Linux: Ubuntu 8 (GNOME)

This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

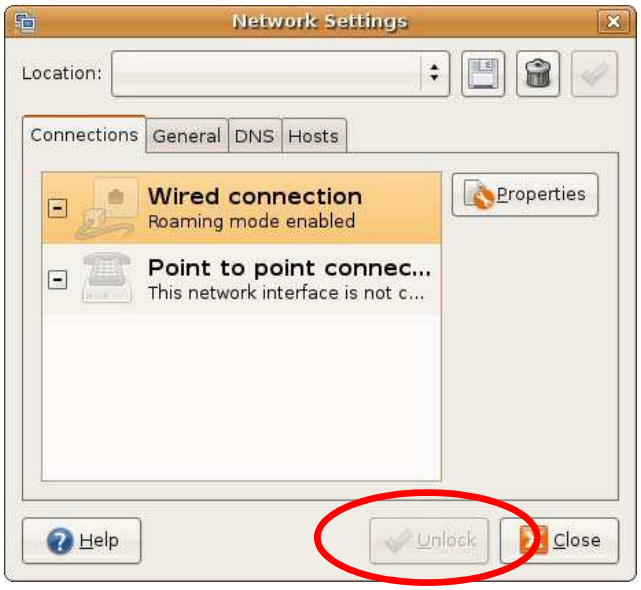
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

1 Click **System > Administration > Network**.



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

5 The **Properties** dialog box opens.

- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

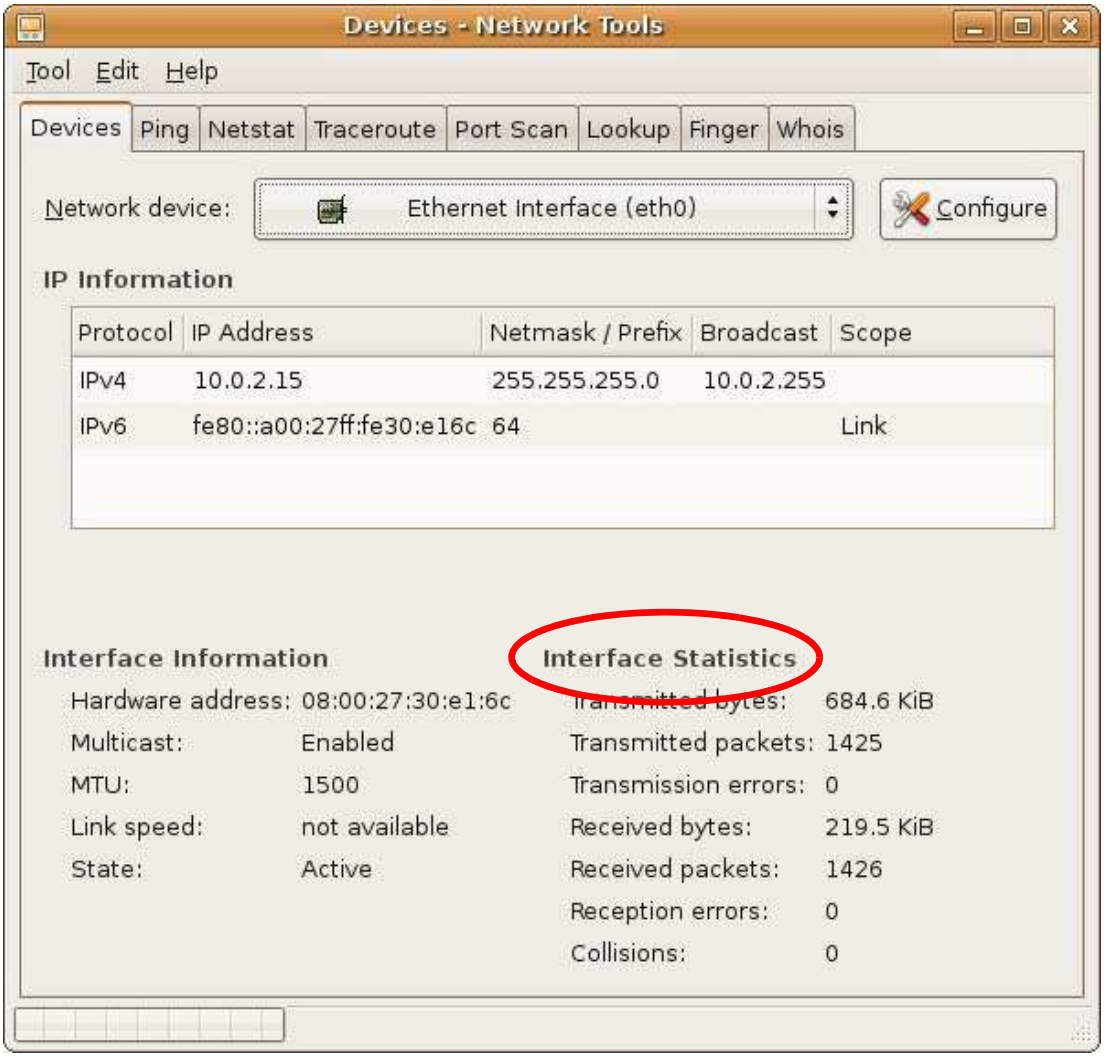
7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 146 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

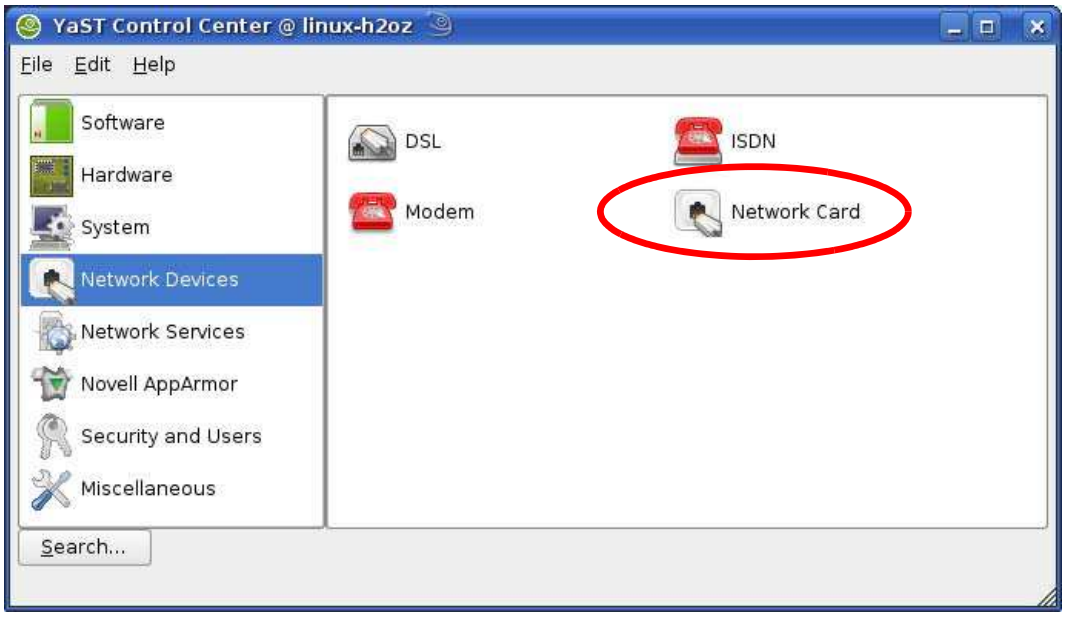
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

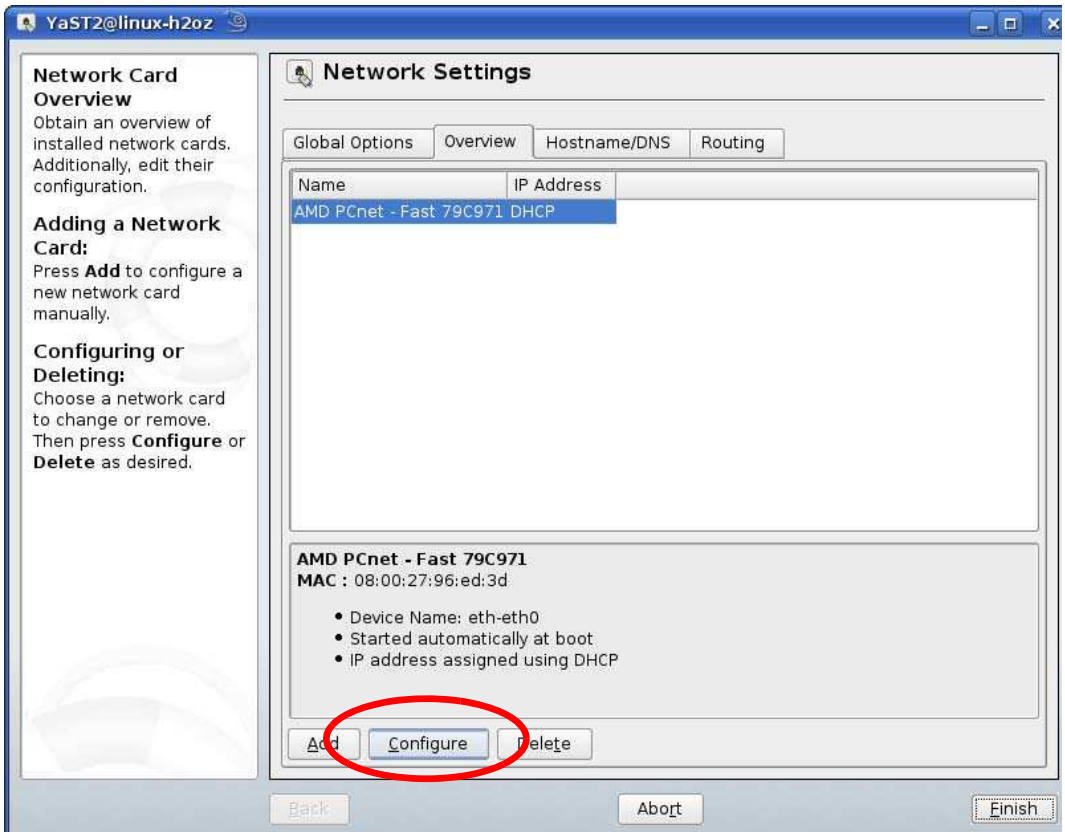
1 Click **K Menu > Computer > Administrator Settings (YaST)**.

2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

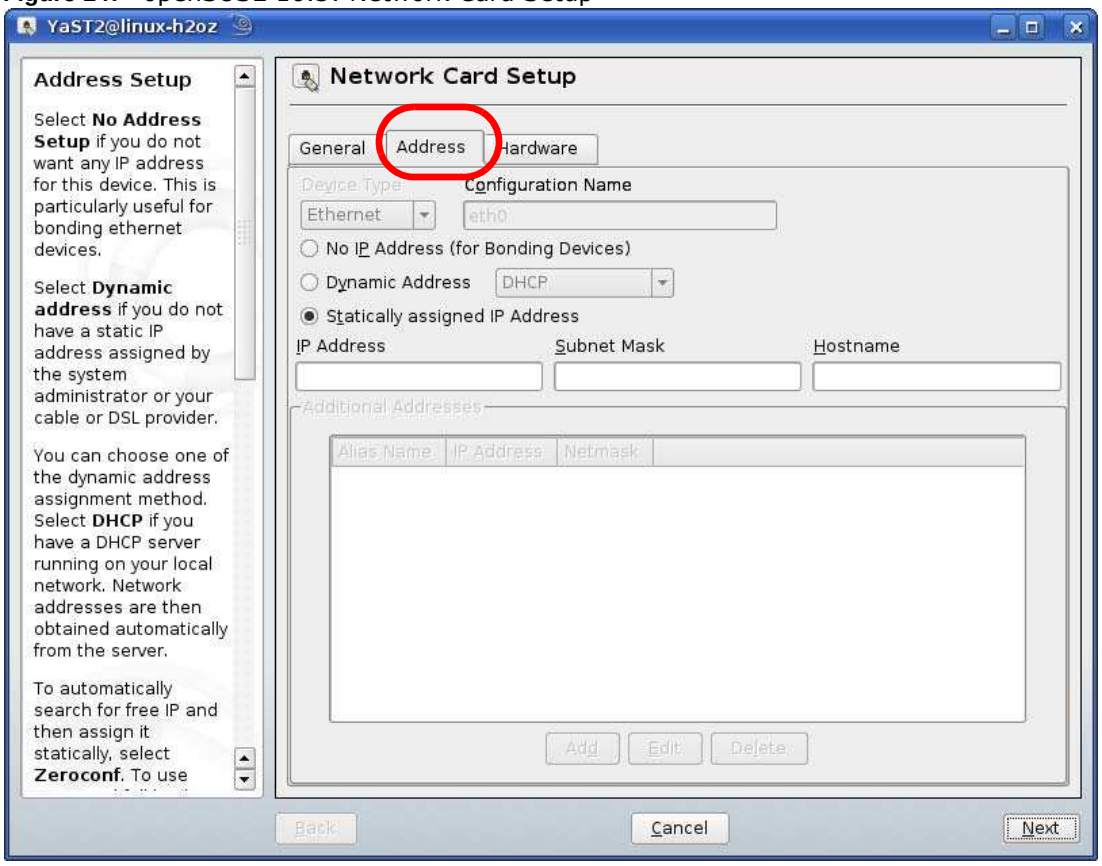


4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 147 openSUSE 10.3: Network Card Setup

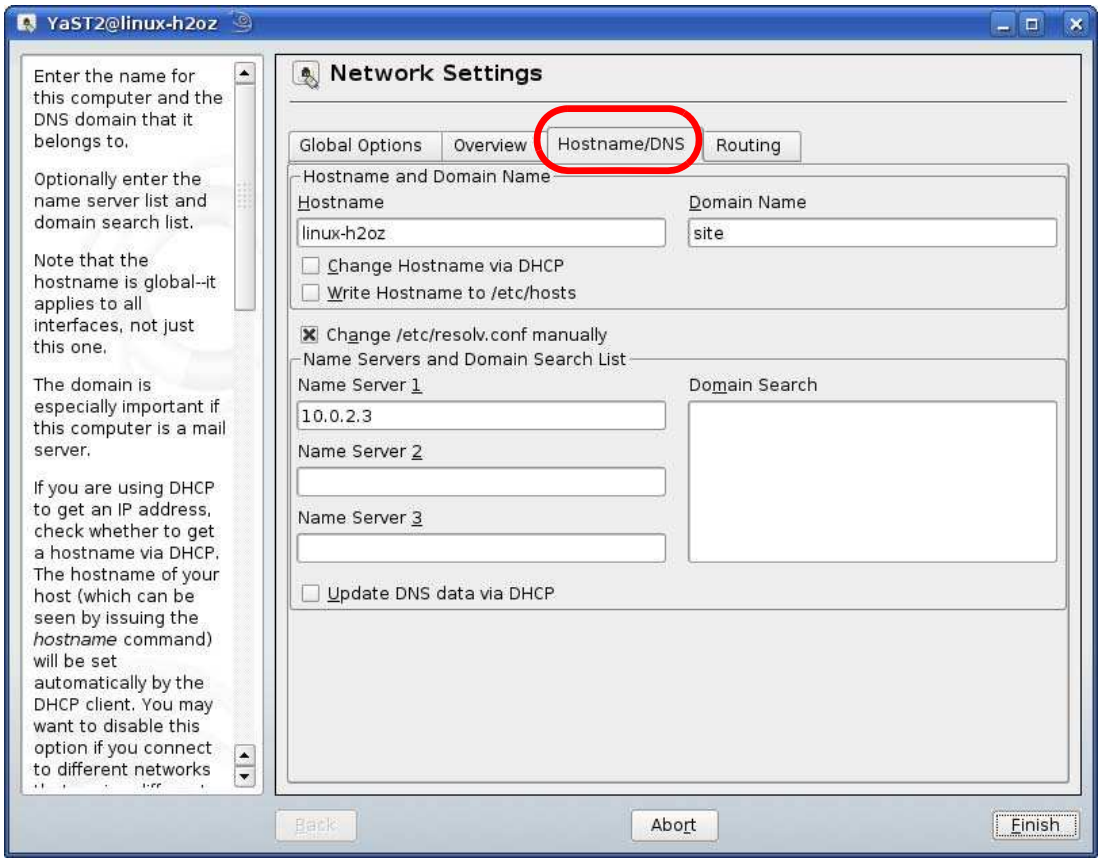


6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/ DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.



9 Click **Finish** to save your settings and close the window.

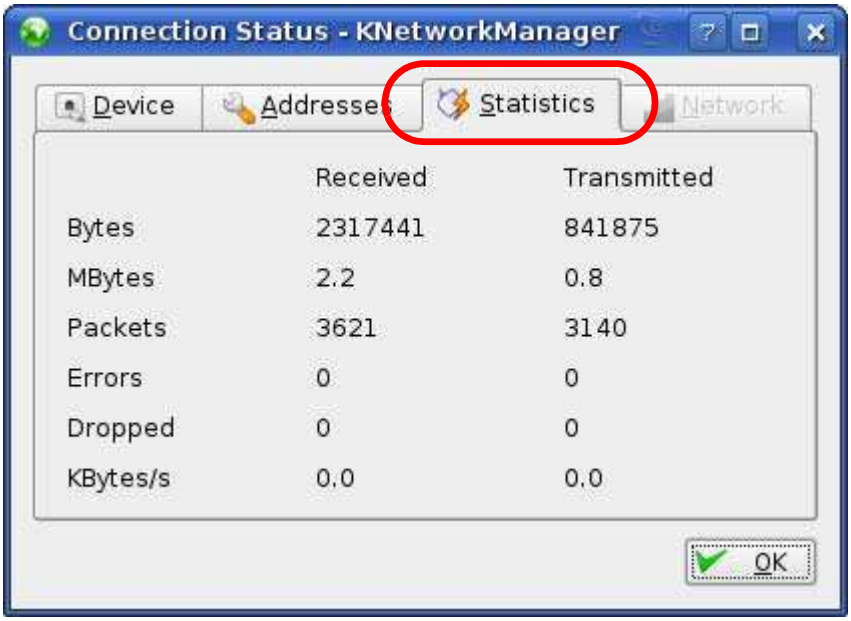
Verifying Settings

Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 148 openSUSE 10.3: KNetwork Manager

When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 149 openSUSE: Connection Status - KNetwork Manager



C

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/ UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/ UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 84 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.

Table 84 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.

Table 84 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

D

Legal Information

Copyright

Copyright © 2012 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

NetUSB is a trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

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

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b, 802.11g or 802.11n (20MHz) operation of this product in the U.S.A. is firmware-limited to channels 1 through 11. IEEE 802.11n (40MHz) operation of this product in the U.S.A. is firmware-limited to channels 3 through 9.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

1) this device may not cause interference and

2) this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IC Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

在 5.25 - 5.35 GHz 頻帶內操作之無線資訊傳輸設備，限於室內使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Regulatory Information

European Union

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance Information for 2.4GHz and 5GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

[Czech]	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
[Danish]	Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[German]	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
[Estonian]	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[Spanish]	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

[Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕC.
[French]	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
[Italian]	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak.
[Polish]	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[Portuguese]	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
[Slovenian]	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
[Slovak]	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
[Finnish]	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[Swedish]	Härmed intygar ZyXEL att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
[Bulgarian]	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/ЕС.
[Icelandic]	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
[Norwegian]	Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 1999/5/EF.
[Romanian]	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC.

CE

National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2, 4- and 5-GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries inwhich additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "*Overview of Regulatory Requirements for Wireless LANs*":.

Overview of Regulatory Requirements for Wireless LANs			
Frequency Band (MHz)	Max Power Level (EIRP)[1] (mW)	Indoor ONLY	Indoor and Outdoor
2400-2483.5	100		V
5150-5350	200	V	
5470-5725	1000		V

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used(specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Malta	MT
Belgium	BE	Netherlands	NL
Cyprus	CY	Poland	PL
Czech Republic	CR	Portugal	PT
Denmark	DK	Slovakia	SK
Estonia	EE	Slovenia	SI
Finland	FI	Spain	ES
France	FR	Sweden	SE
Germany	DE	United Kingdom	GB
Greece	GR	Iceland	IS
Hungary	HU	Liechtenstein	LI
Ireland	IE	Norway	NO
Italy	IT	Switzerland	CH
Latvia	LV	Bulgaria	BG
Lithuania	LT	Romania	RO
Luxembourg	LU	Turkey	TR

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.

- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Index

A

ActiveX 162
Address Assignment 96
AP 15
AP Mode
  menu 69
  status screen 67
AP+Bridge 15

B

Bandwidth management
  overview 165
  priority 167
  services 171
BitTorrent 171
Bridge/Repeater 15

C

certifications 253
  notices 254
  viewing 254
Channel 59, 68
channel 106
CIFS 185
Common Internet File System, see CIFS
Configuration
  restore 198
content filtering 161
  by keyword (in URL) 161
Cookies 162
copyright 253
CPU usage 60, 68

D

Daylight saving 196
DDNS 149
  see also Dynamic DNS
  service providers 149
DHCP 90, 133
  DHCP server
  see also Dynamic Host Configuration Protocol
DHCP server 130, 133
Digital Living Network Alliance 184
disclaimer 253
DLNA 183, 184
  indexing 186
  overview 183
  rescan 186
DLNA-compliant client 184
DNS 135
DNS Server 96
DNS server 135
documentation
  related 2
Domain Name System 135
Domain Name System. See DNS.
duplex setting 60, 69
Dynamic DNS 149
Dynamic Host Configuration Protocol 133
DynDNS 149
DynDNS see also DDNS 149

E

encryption 107
  and local (user) database 108
  key 108
  WPA compatible 108
ESSID 207

F

FCC interference statement 253
file sharing 184
  access right 187, 189
  bandwidth 189
  example 189
  FTP 188
  overview 184
  Samba 186
  user account 187, 188
  Windows Explorer 186
  work group 186
File Transfer Program 171
Firewall 156
  Firewall overview
  guidelines 156
  ICMP packets 157
  network security
  Stateful inspection 156
  ZyXEL device firewall 156
firewall
  stateful inspection 155
Firmware upload 196
  file extension
  using HTTP
firmware version 59, 68
FTP. see also File Transfer Program 171

G

General wireless LAN screen 110
Guest WLAN 108
Guest WLAN Bandwidth 109
Guide
  Quick Start 2

H

HTTP 171
Hyper Text Transfer Protocol 171

I

IGMP 97
  see also Internet Group Multicast Protocol
  version
IGMP version 97
Internet Group Multicast Protocol 97
IP Address 131, 132, 142
IP alias 130
IP Pool 134

J

Java 162

L

LAN 129
  IP pool setup 130
LAN overview 129
LAN setup 129
LAN TCP/IP 130
Language 199
Link type 60, 69
local (user) database 107
  and encryption 108
Local Area Network 129

M

MAC 121
MAC address 96, 107
  cloning 96
MAC address filter 107
MAC address filtering 121
MAC filter 121
managing the device
  good habits 16
  using the web configurator. See web configurator.
  using the WPS. See WPS.
MBSSID 15

Media access control 121
media client 183
media file 183, 186
  type 186
media server 183
  overview 183
meida file play 183
Memory usage 60, 68
mode 15
Multicast 97
  IGMP 97

N

NAT 139, 142
  global 140
  how it works 141
  inside 140
  local 140
  outside 140
  overview 139
  port forwarding 146
  see also Network Address Translation
  server 140
  server sets 146
NAT Traversal 177
Navigation Panel 60, 69
navigation panel 60, 69
Network Address Translation 139, 142

O

operating mode 15
other documentation 2

P

P2P 171
peer-to-peer 171
Point-to-Point Protocol over Ethernet 99
Point-to-Point Tunneling Protocol 101
Pool Size 134
Port forwarding 142, 146
  default server 142, 146
  example 146
  local server 142
  port numbers
  services
port speed 60, 69
PPPoE 99
  dial-up connection
PPTP 101
product registration 254

Q

Quality of Service (QoS) 123
Quick Start Guide 2

R

RADIUS server 107
registration
  product 254
related documentation 2
Remote management
  and NAT 174
  limitations 173
  system timeout 174
Reset button 16
Reset the device 16
Restore configuration 198
Roaming 123
Router Mode
  status screen 57
RTS/CTS Threshold 106, 123

S

Samba 185
Scheduling 126
Server Message Block, see SMB
Service and port numbers 159, 170

Service Set 53, 110, 120
Service Set IDentification 53, 110, 120
Service Set IDentity. See SSID.
Session Initiated Protocol 171
SIP 171
SMB 185
SSID 53, 59, 68, 106, 110, 120
stateful inspection firewall 155
Static DHCP 134
Static Route 151
Status 57
Subnet Mask 131, 132
Summary
  DHCP table 90
  Packet statistics 91
  Wireless station status 92
System General Setup 193
System restart 199

T

TCP/IP configuration 133
Time setting 195
trademarks 253
trigger port 147
Trigger port forwarding 147
  example 147
  process 147

U

Universal Plug and Play 177
  Application 177
  Security issues 177
UPnP 177
URL Keyword Blocking 162
USB media sharing 183
user authentication 107
  local (user) database 107
  RADIUS server 107
User Name 150

V

VoIP 171
VPN 101

W

Wake On LAN 175
WAN (Wide Area Network) 95
WAN MAC address 96
warranty 254
  note 254
Web Configurator
  how to access 39
  Overview 39
web configurator 16
Web Proxy 162
WEP Encryption 114, 116
WEP encryption 113
WEP key 113
windows media player 183
Wireless association list 92
wireless channel 207
wireless LAN 207
wireless LAN scheduling 126
Wireless network
  basic guidelines 106
  channel 106
  encryption 107
  example 105
  MAC address filter 107
  overview 105
  security 106
  SSID 106
Wireless security 106
  overview 106
  type 106
wireless security 207
Wireless tutorial 73
Wizard setup 27
WLAN button 17
WoL 175
work group 185
  name 185

Windows 185
World Wide Web 171
WPA compatible 108
WPS 16
WWW 171

X

Xbox Live 171