NBG2105

Wireless Mini Travel Router

Version 1.00
Edition 1, 11/2012

User's Guide

Default Login Details	
LAN IP Address	192.168.1.1 (Router Mode) 192.168.1.2 (Other Modes)
Password	1234

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the NBG2105 and access the Web Configurator. It contains information on setting up your wireless network.

Contents Overview

Table of Contents

PART I
User's Guide

1

Introduction

1.1 Overview

This chapter introduces the main features and applications of the NBG2105.

The NBG2105 extends the range of your existing wired network without additional wiring, providing easy network access to mobile users. You can set up a wireless network with other IEEE 802.11b/g/n compatible devices.

A range of services such as a firewall and content filtering are also available for secure Internet computing.

1.2 Applications

Your can have the following networks using the NBG2105:

- **Wired**. You can connect network devices via the Ethernet ports of the NBG2105 so that they can communicate with each other and access the Internet.
- **Wireless**. Wireless clients can connect to the NBG2105 to access network resources. You can use WPS (WiFi Protected Setup) to create an instant network connection with another WPS-compatible device.
- **WAN**. Connect to a broadband modem/router for Internet access.

1.3 Ways to Manage the NBG2105

Use any of the following methods to manage the NBG2105.

- WPS (Wi-Fi Protected Setup). You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your ZyXEL Device.
- Web Configurator. This is recommended for everyday management of the NBG2105 using a (supported) web browser.

1.4 Good Habits for Managing the NBG2105

Do the following things regularly to make the NBG2105 more secure and to manage the NBG2105 more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the NBG2105 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG2105. You could simply restore your last configuration.

1.5 Resetting the NBG2105

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **RESET** button on the underside of the NBG2105 to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password and the IP address will be reset to the defaults shown on the cover of this user's guide.

1.5.1 How to Use the RESET Button

1. Make sure the power LED is on.
2. Press the **RESET** button for longer than five seconds (when the power LED begins to blink) and release it to set the NBG2105 back to its factory-default configurations.

1.6 The WPS Button

Your NBG2105 supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

You can use the WPS button to activate WPS in order to quickly set up a wireless network with strong security.

1. Make sure the power LED is on (not blinking).
2. Press the WPS button for less than two seconds and release it. Press the WPS button on another WPS-enabled device within range of the NBG2105.

Note: You must activate WPS in the NBG2105 and in another wireless device within two minutes of each other.

For more information on using WPS, see Section 8.2 on page 59.

1.7 The Clone MAC Button

Your NBG2105 can clone the MAC address of the computer connected to the NBG2105. It is recommended that you clone the MAC address prior to hooking up the WAN port or connecting to an AP or wireless router with Internet access.

Note: MAC cloning is supported only when the NBG2105 is in Router mode.

1.7.1 Cloning a computer's MAC address

1. Make sure the power LED is on (not blinking).
2. To copy and use the MAC address of a currently connected computer through a wired Ethernet or wireless LAN connection, press the **Clone MAC** button for two to five seconds and release it.
3. The WPS/MAC Clone LED turns on when the clone was successful.
4. The NBG2105 restarts automatically ten seconds after you press the **Clone MAC** button.

1.7.2 Restoring the default MAC address

1. Make sure the power LED is on (not blinking).
2. Press and hold the **Clone MAC** button for more than five seconds to reset the NBG2105 back to the factory default MAC address. The **Clone MAC Address** in the WAN screen shows 000000000000 to indicate the NBG2105 is using the factory default MAC address.
3. The NBG2105 restarts after you press the **Clone MAC** button.

1.8 General Hardware Features

Figure 1 General Hardware Features

The following table describes the LEDs.

Note: WPS is only available with WPA2-PSK security protocol.

Table 1 General Hardware Features

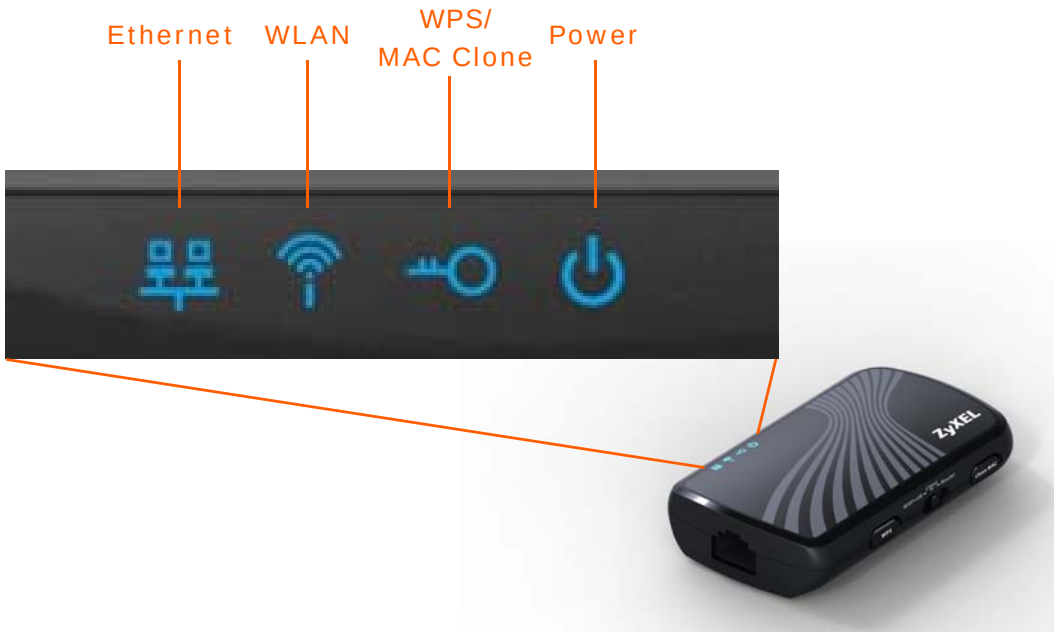
FEATURE	DESCRIPTION
Ethernet	Connect this to your Ethernet network.
LEDs	These show the status of your NBG2105.
WPS	In Router/AP or WISP+UR mode, push this for less than 2 seconds to connect to a wireless client via WPS. In Client mode, push this for less than 2 seconds to connect to an upstream AP via WPS.

Table 1 General Hardware Features (continued)

FEATURE	DESCRIPTION
Operation Mode Switch	Slide this to **Router** to put the NBG2105 into router or AP mode. Slide this to **Client** to put the NBG2105 into WLAN client mode. Slide this to **WISP+UR** to put the NBG2105 into WISP+UR mode.
Clone MAC	Push this for 2 to 5 seconds to clone the first client's MAC address. Push this for more than 5 seconds to reset the NBG2105's MAC address to the factory default. Note: This only works in Router mode.
Micro USB	Connect this to a power supply or computer. Connect to a computer to use as an Ethernet interface.
Reset (on the underside of the NBG2105)	Push this for more than 5 seconds to reset all NBG2105 settings to factory defaults.

1.8.1 LEDs

Figure 2 Top Panel LEDs



The following table describes the LEDs.

Table 2 Top Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
Ethernet	Blue	On	The NBG2105's Ethernet connection is ready.
		Blinking	The NBG2105 is sending/receiving data through the Ethernet port.
	Off		The Ethernet connection is not ready, or has failed.

Table 2 Top Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
WLAN	Blue	On	The NBG2105 is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The NBG2105 is sending/receiving data through the wireless LAN.
	Off		The wireless LAN is not ready, has failed, or is disabled.
WPS/MAC Clone	Blue	On	WPS/MAC clone is ready.
		Blinking	The NBG2105 is negotiating a WPS connection with a wireless client or cloning a MAC address.
	Off		WPS is disabled or has failed. This LED is off for ten seconds and then the NBG2105 automatically restarts when MAC cloning has failed.
Power	Blue	On	The NBG2105 is receiving power and functioning properly.
		Blinking	Boot up process. The NBG2105 is resetting to factory default settings.
	Off		The NBG2105 is not receiving power.

2

Introducing the Web Configurator

2.1 Overview

This chapter describes how to access the NBG2105 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the NBG2105 via Internet browser. Use Internet Explorer 6.0 and later versions, Mozilla Firefox 3 and later versions, or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter (Chapter 17 on page 121) to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

The Ethernet port is a WAN port when the NBG2105 is set to Router or AP mode. It is a LAN port when the NBG2105 is set to WISP+UR or Client mode.

In either mode, users can connect the NBG2105's micro USB port to a computer and install the USB driver in the computer to access the Web Configurator through a USB-to-Ethernet connection (refer to the Quick Start Guide).

Table 3 Accessing the NBG2105

OPERATION MODE	THROUGH THE ETHERNET LAN PORT	VIA WIRELESS LAN CONNECTIONS	THROUGH THE MICRO USB PORT
Router Mode		V	V
AP Mode		V	V
Client Mode	V		V
WISP + UR Mode	V	V	V

1 Make sure your NBG2105 hardware is properly connected and prepare your computer or computer network to connect to the NBG2105 (refer to the Quick Start Guide).

2 Launch your web browser.

3 The NBG2105 is in Router mode by default. Type "http://192.168.1.1" as the website address.

If the NBG2105 isn't in Router mode, the IP address is 192.168.1.2. See Chapter 3 on page 21 for more information about the modes of the NBG2105.

Your computer must be in the same subnet in order to access this website address.

2.2.1 Login Screen

The Web Configurator initially displays the following login screen.

Figure 3 Login screen

The following table describes the labels in this screen.

Table 4 Login screen

LABEL	DESCRIPTION
User Name	Type "admin" (default) as the user name.
Password	Type "1234" (default) as the password.
Language	Select the language you want to use to configure the Web Configurator. Click **Login**.
Login	Click this to login.
Reset	Click this to begin configuring this screen afresh.

3

Operation Modes

3.1 Overview

This chapter introduces the operation modes available on your NBG2105 and how to configure them. The operation mode is a pre-defined combination of routing, access point (AP) and wireless client functions to match your network topology and requirements. Use the Operation Mode switch on the right-side panel (see Section 1.8 on page 16) of the NBG2105 to select the operation mode. Use the Router Operation Mode screen to configure the selected mode.

3.2 What You Can Do

- **Router** mode connects the local network to another network, like the Internet. See Section 3.3 on page 21 for details of this mode.
- **Access Point** mode extends your network by allowing network devices to connect to the NBG2105 wirelessly. See Section 3.4 on page 24 for details of this mode.
- **Client** mode enables the NBG2105 to be a wireless client to an upstream AP. See Section 3.5 on page 27 for details of this mode.
- **WISP + UR** mode enables the NBG2105 to connect your local network to the Internet through an ISP's access point. UR provides Wi-Fi functionality to clients on the LAN side. See Section 3.6 on page 29 for details of this mode.

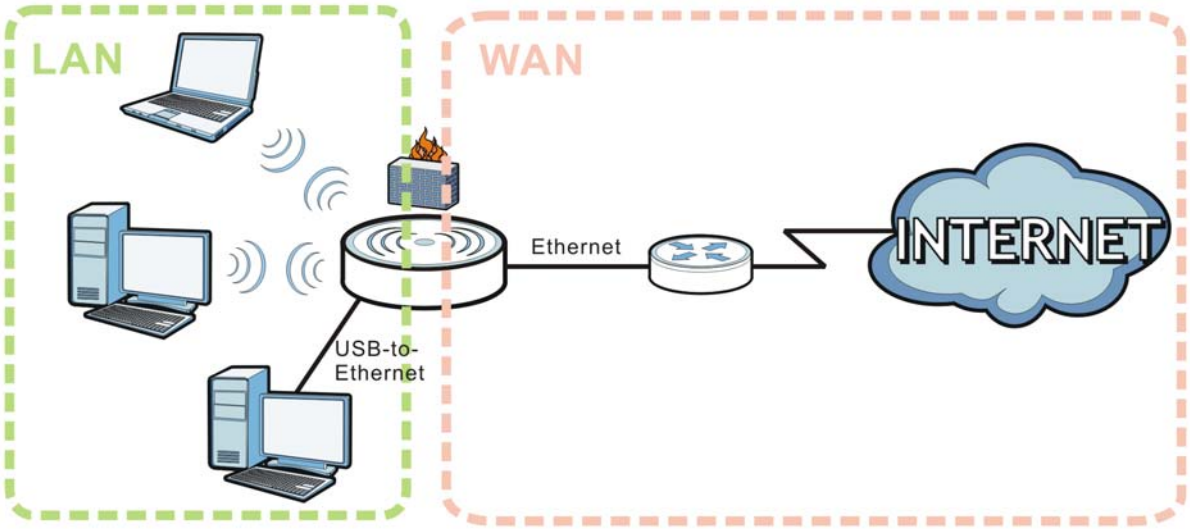
Note: Choose your operation mode carefully to avoid having to change it later. If you select the incorrect operation mode you may not be able to connect to the Internet. When changing to another mode, the IP address of the NBG2105 changes. The running applications and services of the network devices connected to the NBG2105 can be interrupted.

Note: In **WISP + UR** and **Client** modes, you should know the SSID and wireless security details of the access point to which you want to connect.

3.3 Router Mode

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. This mode offers services such as a firewall, QoS or DDNS.

Figure 4 Router Mode Application



3.3.1 Setting Router Mode

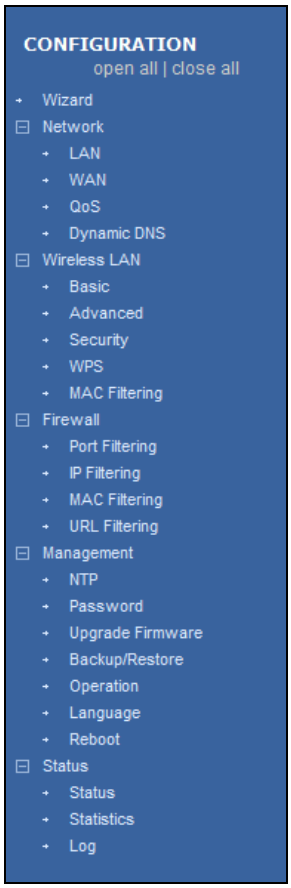
Select Router mode if your device routes traffic between a local network and another network such as the Internet. To set Router mode:

1. Make sure the power LED is on (not blinking).
2. Slide the Operation Mode Switch to **Router**. See Section 1.8 on page 16.
3. The NBG2105 restarts after you slide the Operation Mode Switch.

3.3.2 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG2105 features.

Figure 5 Navigation Panel: Router Mode



The following table describes the sub-menus.

Table 5 Navigation Panel: Router Mode

MENU	FUNCTION
Wizard	The Web Configurator's wizard setup helps you configure your device in router mode for the first time.
Network	
LAN	Use this to configure LAN IP address and subnet mask and DHCP server settings.
WAN	Use this allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.
QoS	Use this to reserve bandwidth for certain traffic based on the IP address or MAC address.
Dynamic DNS	Use this to configure a domain name with a dynamic IP address.
Wireless LAN	
Basic	Use this to turn the wireless connection on or off and make other basic configuration changes.
Advanced	Use this to configure the output power and set the RTS/CTS Threshold.
Security	Use this to configure no, WEP, WPA-PSK, WPA2-PSK or WPA2-PSK Mixed wireless encryption.
WPS	Use this to quickly set up a wireless network with strong security, without having to configure security settings manually.

Table 5 Navigation Panel: Router Mode (continued)

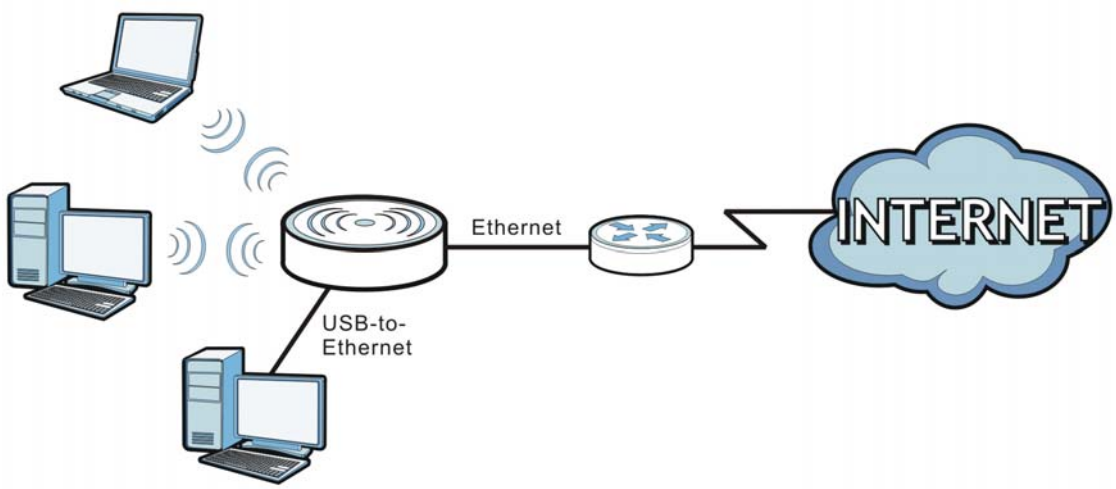
MENU	FUNCTION
MAC Filtering	Use this to allow or deny wireless stations based on their MAC addresses from connecting to the NBG2105.
Firewall	
Port Filtering	Use this to apply filtering based on UDP or TCP port numbers.
IP Filtering	Use this to apply filtering based on IP addresses.
MAC Filtering	Use this to apply filtering based on MAC addresses.
URL Filtering	Use this to apply filtering based on URLs.
Management	
NTP	Use this to change your NBG2105's time and date.
Password	Use this to change your NBG2105's system password.
Upgrade Firmware	Use this to upload firmware to your NBG2105.
Backup/ Restore	Use this to view information related to factory defaults, backup configuration, and restoring configuration.
Operation	Use this to change between access point mode and router mode.
Language	Use this to select the language you prefer.
Reboot	Use this to restart the NBG2105 without turning the power off.
Status	
Status	Use this to view system, wireless, local and WAN network information, as well as general information about the NBG2105.
Statistics	Use this to show the number of packets sent and received on the Wireless LAN and Ethernet WAN interfaces.
Log	Use this to look at all of the NBG2105's logs in one location.

3.4 Access Point Mode

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. In Access Point Mode:

- All clients belong to the same subnet.
- All clients of the device are LAN clients. There is no WAN connection.
- The DHCP server is disabled.
- The IP address of the device on the local network is set to 192.168.1.2.

Figure 6 Access Point Mode Application



3.4.1 Setting Access Point Mode

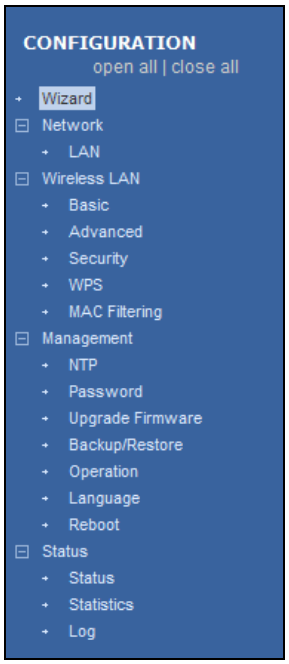
Select Access Point Mode if your device bridges traffic between clients on the same network. To set Access Point mode:

1. Make sure the power LED is on (not blinking).
2. Slide the Operation Mode Switch to **Router**. See Section 1.8 on page 16.
3. The NBG2105 restarts after you slide the Operation Mode Switch.
4. In the Web Configuator, click **Management > Operation**, select **AP** and then click **Apply Changes**.

3.4.2 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG2105 features.

Figure 7 Navigation Panel: Access Point Mode



The following table describes the sub-menus.

Table 6 Navigation Panel: Access Point Mode

MENU	FUNCTION
Wizard	The Web Configurator's wizard setup helps you configure your device in AP mode for the first time.
Network	
LAN	Use this to configure LAN IP address and subnet mask and DHCP server settings.
Wireless LAN	
Basic	Use this to turn the wireless connection on or off and make other basic configuration changes.
Advanced	Use this to configure the output power and set the RTS/CTS Threshold.
Security	Use this to configure no, WEP, WPA-PSK, WPA2-PSK or WPA2-PSK Mixed wireless encryption.
WPS	Use this to quickly set up a wireless network with strong security, without having to configure security settings manually.
MAC Filtering	Use this to allow or deny wireless stations based on their MAC addresses from connecting to the NBG2105.
Management	
NTP	Use this to change your NBG2105's time and date.
Password	Use this to change your NBG2105's system password.
Upgrade Firmware	Use this to upload firmware to your NBG2105.
Backup/ Restore	Use this to view information related to factory defaults, backup configuration, and restoring configuration.
Operation	Use this to change between access point mode and router mode.
Language	Use this to select the language you prefer.
Reboot	Use this to restart the NBG2105 without turning the power off.

Table 6 Navigation Panel: Access Point Mode (continued)

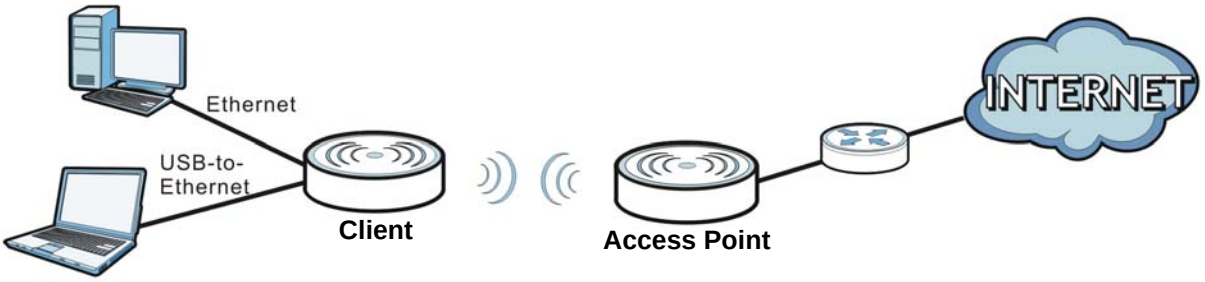
MENU	FUNCTION
Status	
Status	Use this to view system, wireless, local and WAN network information, as well as general information about the NBG2105.
Statistics	Use this to show the number of packets sent and received on the Wireless LAN and Ethernet WAN interfaces.
Log	Use this to look at all of the NBG2105's logs in one location.

3.5 Client Mode

In Client mode, the NBG2105 acts as a wireless client to connect to an existing access point wirelessly. It acts just like a wireless client in notebooks/computers. In Client mode:

- The IP address of the device on the local network is set to 192.168.1.2.

Figure 8 Client Mode Application



3.5.1 Setting Client Mode

Select Client Mode if your device needs a wireless client to connect to an existing access point. To set Client mode:

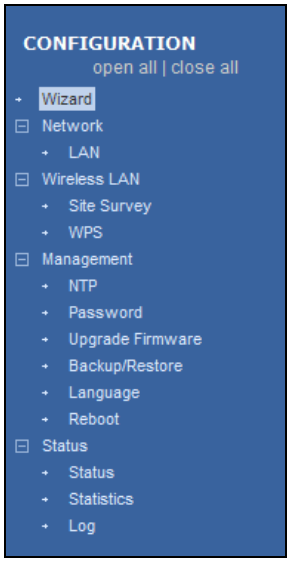
1. Make sure the power LED is on (not blinking).
2. Slide the Operation Mode Switch to **Client**. See Section 1.8 on page 16.
3. The NBG2105 restarts after you slide the Operation Mode Switch.

To allow NBG2105 clients access to the Internet, the NBG2105 must be routed to the access point.

3.5.2 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG2105 features.

Figure 9 Navigation Panel: Client Mode



The following table describes the sub-menus.

Table 7 Navigation Panel: Client Mode

MENU	FUNCTION
Wizard	The Web Configurator's wizard setup helps you configure your device in client mode for the first time.
Network	
LAN	Use this to configure LAN IP address and subnet mask.
Wireless LAN	
Site Survey	Use this to scan for and connect to a wireless network automatically.
WPS	Use this to quickly set up a wireless network with strong security, without having to configure security settings manually.
Management	
NTP	Use this to change your NBG2105's time and date.
Password	Use this to change your NBG2105's system password.
Upgrade Firmware	Use this to upload firmware to your NBG2105.
Backup/ Restore	Use this to view information related to factory defaults, backup configuration, and restoring configuration.
Language	Use this to select the language you prefer.
Reboot	Use this to restart the NBG2105 without turning the power off.
Status	
Status	Use this to view system, wireless, local and WAN network information, as well as general information about the NBG2105.
Statistics	Use this to show the number of packets sent and received on the Wireless LAN and Ethernet WAN interfaces.
Log	Use this to look at all of the NBG2105's logs in one location.

3.6 WISP + UR Mode

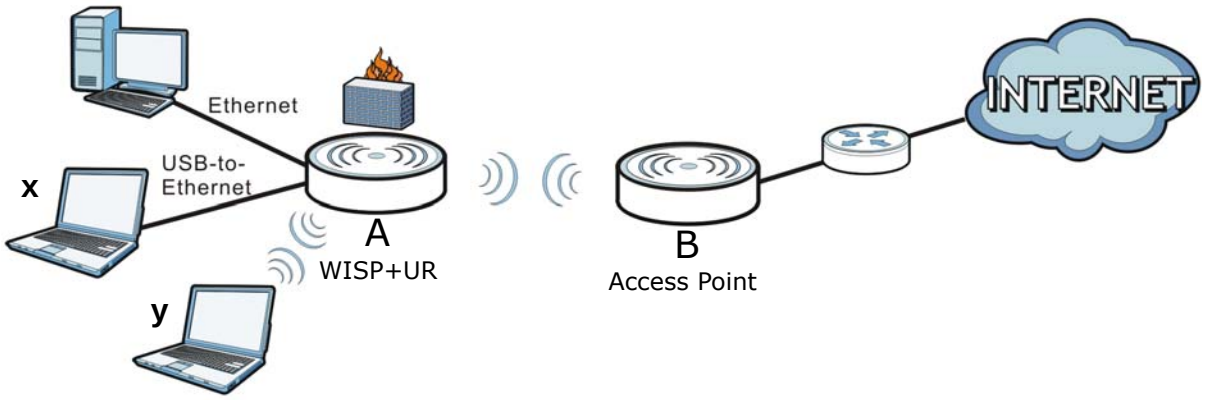
In WISP (Wireless ISP) + UR (Universal Repeater) mode, your NBG2105 can act as a wireless client to wirelessly connect to the Internet or an existing network via an access point. In addition, it can provide Wi-Fi function to the clients on the LAN side. Use this mode if you want to wirelessly connect to the Internet or have an access point or wireless router in your network. In WISP + UR mode, the IP address of the device on the local network is 192.168.1.2.

Note: Make sure your network and the remote network are NOT in the same subnet. If the access point or wireless router is using 192.168.1.x, the NBG2105 in WISP + UR mode needs to use something else, say 192.168.2.x.

Note: When the NBG2105 is in WISP + UR mode, you still need to enter your ISP information in the WAN screen in order to access the Internet.

In the example below, one NBG2105 is configured as WISP +UR mode (**A**) and another is used as an access point (**B**). The NBG2105 (**A**) wirelessly connects to the available access point (**B**), and can allow the clients (**x** and **y**) to access the network through it using a wireless connection.

Figure 10 WISP + UR Mode Application



3.6.1 Setting WISP + UR Mode

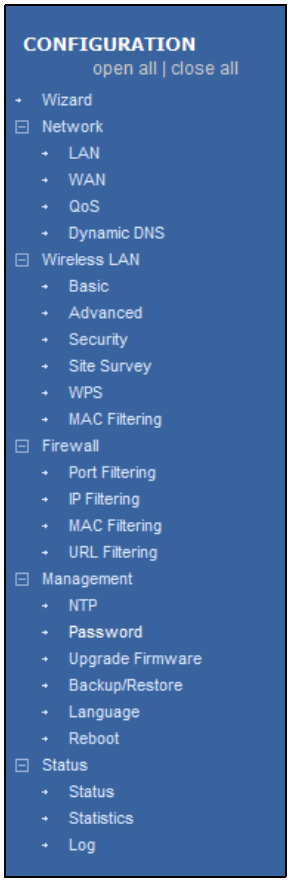
Select WISP + UR Mode if your NBG2105 needs a wireless client to connect to an existing access point, still have router functions, and also allow wireless clients to associate with the NBG2105. To set WISP + UR mode:

1. Make sure the power LED is on (not blinking).
2. Slide the Operation Mode Switch to **WISP + UR**. See Section 1.8 on page 16.
3. The NBG2105 restarts after you slide the Operation Mode Switch.

3.6.2 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG2105 features.

Figure 11 Navigation Panel: WISP+UR Mode



The following table describes the sub-menus.

Table 8 Navigation Panel: WISP+UR Mode

MENU	FUNCTION
Wizard	The Web Configurator's wizard setup helps you configure your device in WISP+UR mode for the first time.
Network	
LAN	Use this to configure LAN IP address and subnet mask.
WAN	Use this allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.
QoS	Use this to reserve bandwidth for certain traffic based on the IP address or MAC address.
Dynamic DNS	Use this to configure a domain name with a dynamic IP address.
Wireless LAN	
Basic	Use this to turn the wireless connection on or off and make other basic configuration changes.
Advanced	Use this to configure the output power and set the RTS/CTS Threshold.
Security	Use this to configure no, WEP, WPA-PSK, WPA2-PSK or WPA2-PSK Mixed wireless encryption.
Site Survey	Use this to scan for and connect to a wireless network automatically.
WPS	Use this to quickly set up a wireless network with strong security, without having to configure security settings manually.

Table 8 Navigation Panel: WISP+UR Mode (continued)

MENU	FUNCTION
MAC Filtering	Use this to allow or deny wireless stations based on their MAC addresses from connecting to the NBG2105.
Firewall	
Port Filtering	Use this to apply filtering based on UDP or TCP port numbers.
IP Filtering	Use this to apply filtering based on IP addresses.
MAC Filtering	Use this to apply filtering based on MAC addresses.
URL Filtering	Use this to apply filtering based on URLs.
Management	
NTP	Use this to change your NBG2105's time and date.
Password	Use this to change your NBG2105's system password.
Upgrade Firmware	Use this to upload firmware to your NBG2105.
Backup/ Restore	Use this to view information related to factory defaults, backup configuration, and restoring configuration.
Language	Use this to select the language you prefer.
Reboot	Use this to restart the NBG2105 without turning the power off.
Status	
Status	Use this to view system, wireless, local and WAN network information, as well as general information about the NBG2105.
Statistics	Use this to show the number of packets sent and received on the Wireless LAN and Ethernet WAN interfaces.
System Log	Use this to look at all of the NBG2105's logs in one location.

4

Router Setup Wizard

4.1 Overview

This chapter provides information on the wizard setup screens in the Web Configurator.

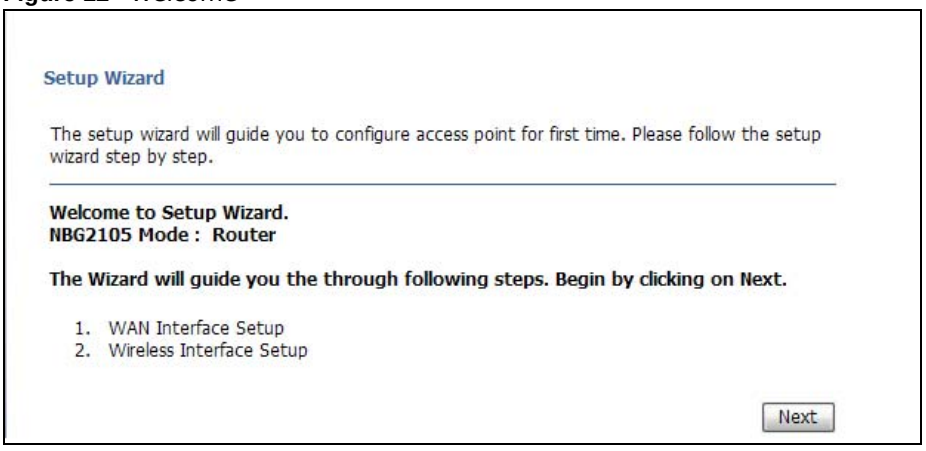
The Web Configurator's wizard setup helps you configure your device in router mode for the first time.

4.2 Welcome Screen

Launch your web browser and type "http://192.168.1.1" as the website address. Type "admin" (default) as the user name and "1234" (default) as the password. Click **Login**.

Click **Wizard** in router mode to open the Welcome screen. Click **Next** after reading the instructions on this screen.

Figure 12 Welcome



4.3 WAN Interface Setup

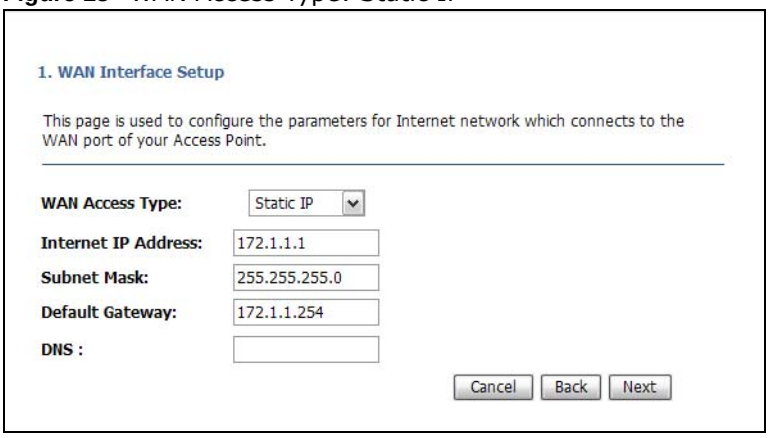
The NBG2105 offers three WAN access types. They are **Static IP**, **DHCP Client** or **PPPoE**.

The following screen depends on your WAN access type. Enter the details provided by your Internet Service Provider (ISP) in the fields (if any).

4.3.1 WAN Access Type: Static IP

Select **Static IP** as the **WAN Access Type** to setup a static IP Configuration on the WAN port. Complete the fields described. Click **Next** to proceed with the **Wireless Network Name (SSID)** screen.

Figure 13 WAN Access Type: Static IP



The following table describes the labels in this screen.

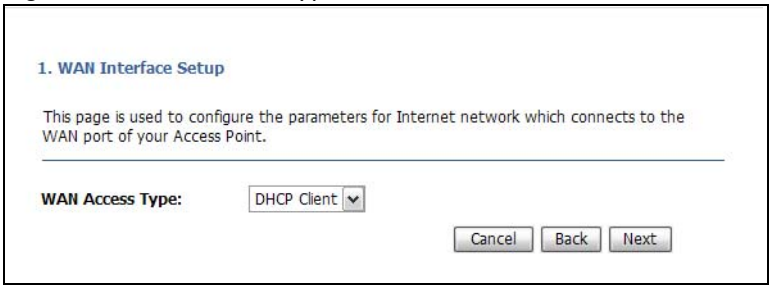
Table 9 WAN Access Type: Static IP

LABEL	DESCRIPTION
WAN Access Type	Select **Static IP** to enable manual configuration of all NBG2105 IP settings.
Internet IP Address	Enter the Internet-facing IP address.
Subnet Mask	Enter the subnet mask of the NBG2105 WAN interface.
Default Gateway	Enter the IP address of a default gateway to the Internet.
DNS	Enter the IP address of the DNS server.
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Next	Click this to go to the next step in the wizard.

4.3.2 WAN Access Type: DHCP Client

Select **DHCP Client** as the **WAN Access Type** to make the WAN port setup its IP configuration via DHCP. Click **Next** to proceed with the **Wireless Network Name (SSID)** screen.

Figure 14 WAN Access Type: DHCP Client



The following table describes the labels in this screen.

Table 10 WAN Access Type: DHCP Client

LABEL	DESCRIPTION
WAN Access Type	Select **DHCP Client** to make the NBG2105 get its IP configuration from a DHCP server.
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Next	Click this to go to the next step in the wizard.

4.3.3 WAN Access Type: PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

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

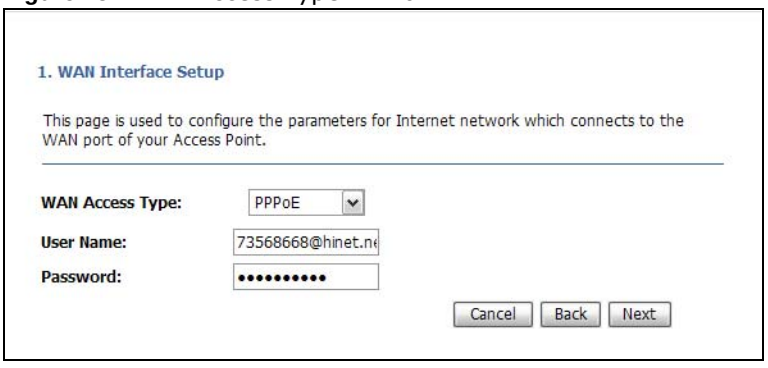
One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

By implementing PPPoE directly on the NBG2105 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG2105 does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Select **PPPoE** as the **WAN Access Type** to make the WAN port setup its IP configuration via PPPoE. Complete the fields described. Click **Next** to proceed with the **Wireless Network Name (SSID)** screen.

Figure 15 WAN Access Type: PPPoE



The following table describes the labels in this screen.

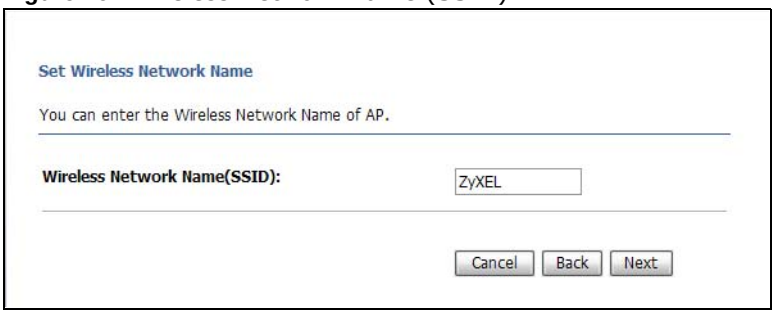
Table 11 WAN Access Type: PPPoE

LABEL	DESCRIPTION
WAN Access Type	Select **PPPoE** to make the NBG2105 get its IP configuration via PPPoE.
User Name	Enter the user name provided by your ISP.
Password	Enter the password provided by your ISP.
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Next	Click this to go to the next step in the wizard.

4.4 Wireless Network Name (SSID) Setup

Name your wireless network by entering an SSID. Click **Next** to proceed with the **Wireless Security Mode** screen.

Figure 16 Wireless Network Name (SSID)



The following table describes the labels in this screen.

Table 12 Wireless Network Name (SSID)

LABEL	DESCRIPTION
Wireless Network Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the NBG2105, make sure all wireless stations use the same SSID in order to access the network.
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Next	Click this to go to the next step in the wizard.

4.5 Wireless Security

Configure the wireless security settings on your NBG2105 in the following screen. The fields that show up depend on the kind of security you select.

4.5.1 Encryption: None

Choose **None** in the **Encryption** field to let wireless devices within range access your wireless network. Complete the fields described. Click **Finished** to save the configuration end exit the wizard.

Figure 17 Encryption: None

The following table describes the labels in this screen.

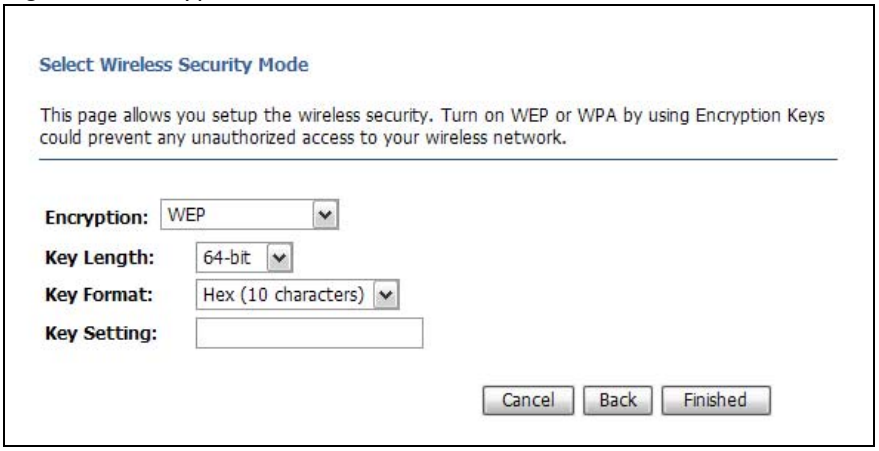
Table 13 Encryption: None

LABEL	DESCRIPTION
Encryption	Select **None** to have no wireless LAN security configured. If you do not enable any wireless security on your NBG2105, your network is accessible to any wireless networking device that is within range.
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Finished	Click this to finish the wizard.

4.5.2 Encryption: WEP

Choose **WEP** in the **Encryption** field to protect your wireless network with Wired Equivalent Privacy. Complete the fields described. Click **Finished** to save the configuration end exit the wizard.

Figure 18 Encryption: WEP



The following table describes the labels in this screen.

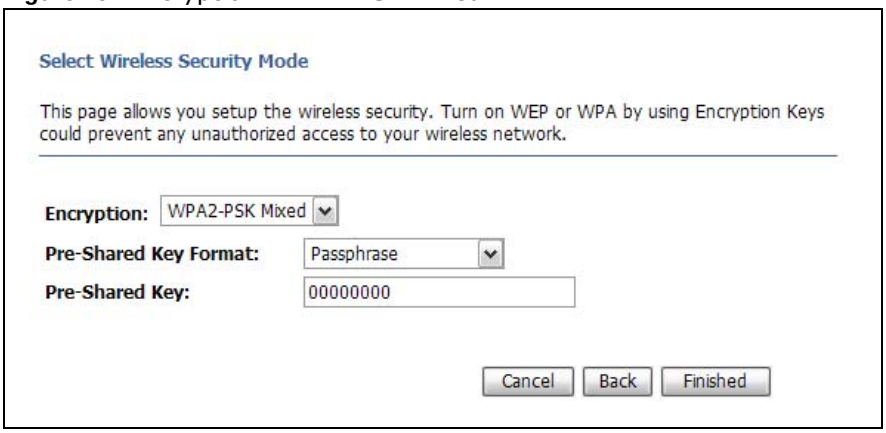
Table 14 Encryption: WEP

LABEL	DESCRIPTION
Encryption	Select **WEP** to allow clients to associate this network with WEP authentication.
Key Length	Select **64-bit** or **128-bit**. This dictates the length of the security key that the network is going to use.
Key Format	Select **Hex** to enter hexadecimal characters as a WEP key. Select **ASCII** to enter ASCII characters as WEP key.
Key Setting	The WEP keys are used to encrypt data. Both the NBG2105 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit** in the **Key Format** field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit** in the **Key Format** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Finished	Click this to finish the wizard.

4.5.3 Encryption: WPA-PSK, WPA2-PSK or WPA2-PSK Mixed

Choose **WPS-PSK**, **WPA2-PSK** or **WPA2-PSK Mixed** in the **Encryption** field to protect your wireless network with WPA-PSK, WPA2-PSK or both at the same time. Complete the fields described. Click **Finished** to save the configuration end exit the wizard.

Figure 19 Encryption: WPA2-PSK Mixed



Note: Although only the **WPA2-PSK Mixed** screen is shown, all fields are the same for **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK Mixed** screens.

The following table describes the labels in this screen.

Table 15 Encryption: WPA-PSK, WPA2-PSK or WPA2-PSK Mixed

LABEL	DESCRIPTION
Encryption	Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK Mixed** to allow clients to associate this network with WPA-PSK, WPA2-PSK or either WPA-PSK or WPA2-PSK authentication.
Pre-Shared Key Format	Select **Passphrase** to make the NBG2105 generate a key from a phrase typed into the **Pre-Shared Key** field. Select **Hex** to configure the NBG2105 to accept a key in hexadecimal format in the **Pre-Shared Key** field.
Pre-Shared Key	If **Passphrase** was selected in the **Pre-Shared Key Format** field, type a pre-shared key from 8 to 63 case-sensitive keyboard characters. If **Hex** was selected in the **Pre-Shared Key Format** field, type a pre-shared key using hexadecimal characters ("0-9", "A-F").
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Finished	Click this to finish the wizard.

5

AP Setup Wizard

5.1 Overview

This chapter provides information on the wizard setup screens in the Web Configurator.

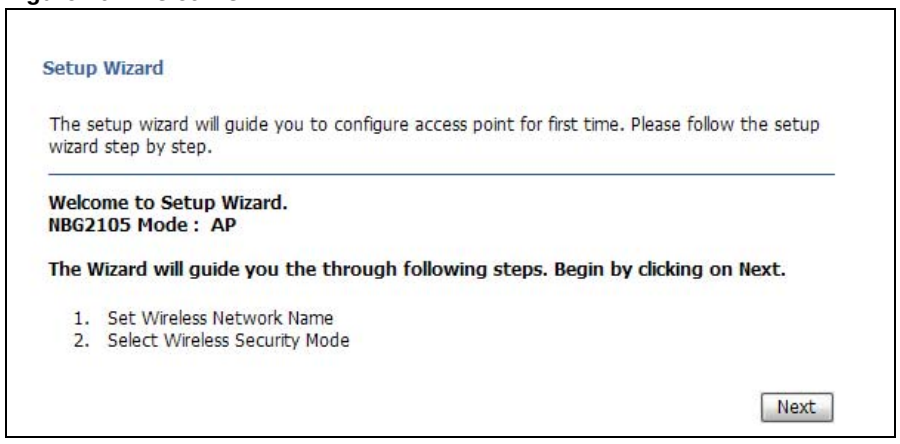
The Web Configurator's wizard setup helps you configure your device in AP mode for the first time.

5.2 Welcome Screen

Launch your web browser and type "http://192.168.1.2" as the website address. Type "admin" (default) as the user name and "1234" (default) as the password. Click **Login**.

Click **Wizard** in router mode to open the Welcome screen. Click **Next** after reading the instructions on this screen.

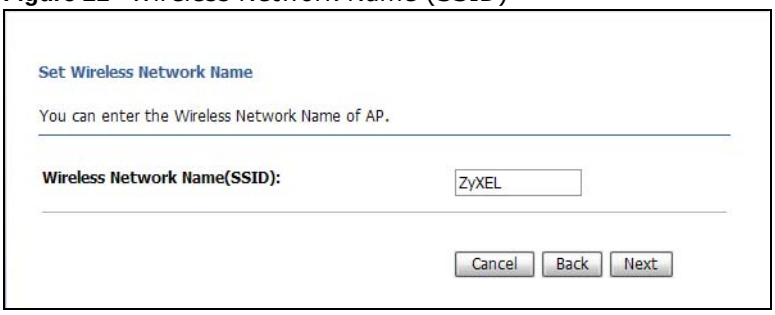
Figure 20 Welcome



5.3 Wireless Network Name (SSID) Setup

Name your wireless network by entering an SSID. Click **Next** to proceed with the **Wireless Security Mode** screen.

Figure 21 Wireless Network Name (SSID)



The following table describes the labels in this screen.

Table 16 Wireless Network Name (SSID)

LABEL	DESCRIPTION
Wireless Network Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the NBG2105, make sure all wireless stations use the same SSID in order to access the network.
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Next	Click this to go to the next step in the wizard.

5.4 Wireless Security

Configure the wireless security settings on your NBG2105 in the following screen. The fields that show up depend on the kind of security you select.

5.4.1 Encryption: None

Choose **None** in the **Encryption** field to let wireless devices within range access your wireless network. Complete the fields described. Click **Finished** to save the configuration end exit the wizard.

Figure 22 Encryption: None

The following table describes the labels in this screen.

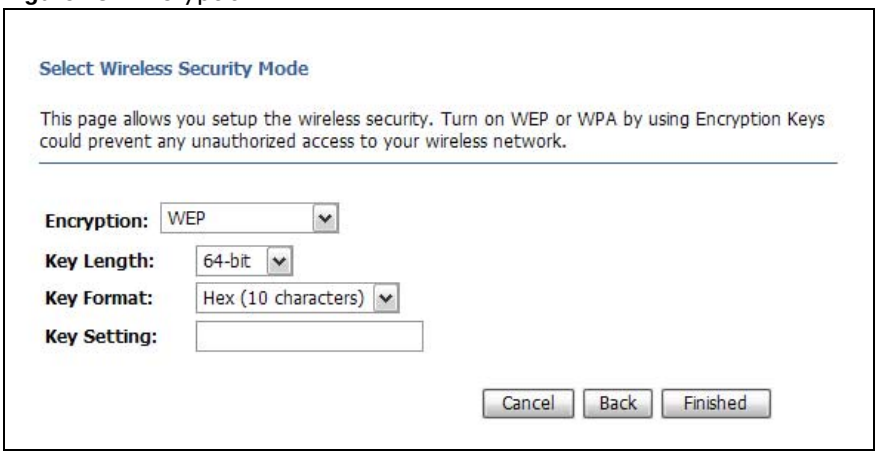
Table 17 Encryption: None

LABEL	DESCRIPTION
Encryption	Select **None** to have no wireless LAN security configured. If you do not enable any wireless security on your NBG2105, your network is accessible to any wireless networking device that is within range.
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Finished	Click this to finish the wizard.

5.4.2 Encryption: WEP

Choose **WEP** in the **Encryption** field to protect your wireless network with Wired Equivalent Privacy. Complete the fields described. Click **Finished** to save the configuration end exit the wizard.

Figure 23 Encryption: WEP



The following table describes the labels in this screen.

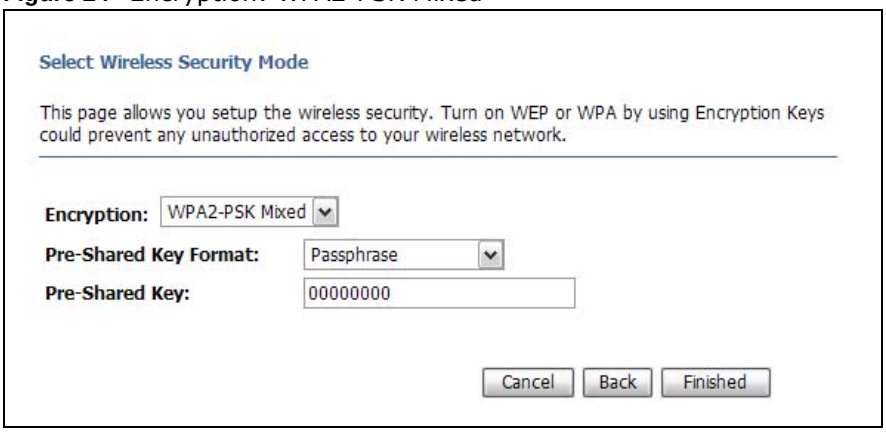
Table 18 Encryption: WEP

LABEL	DESCRIPTION
Encryption	Select **WEP** to allow clients to associate this network with WEP authentication.
Key Length	Select **64-bit** or **128-bit**. This dictates the length of the security key that the network is going to use.
Key Format	Select **Hex** to enter hexadecimal characters as a WEP key. Select **ASCII** to enter ASCII characters as WEP key.
Key Setting	The WEP keys are used to encrypt data. Both the NBG2105 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit** in the **Key Format** field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit** in the **Key Format** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Finished	Click this to finish the wizard.

5.4.3 Encryption: WPA-PSK, WPA2-PSK or WPA2-PSK Mixed

Choose **WPS-PSK**, **WPA2-PSK** or **WPA2-PSK Mixed** in the **Encryption** field to protect your wireless network with WPA-PSK, WPA2-PSK or both at the same time. Complete the fields described. Click **Finished** to save the configuration end exit the wizard.

Figure 24 Encryption: WPA2-PSK Mixed



Note: Although only the **WPA2-PSK Mixed** screen is shown, all fields are the same for **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK Mixed** screens.

The following table describes the labels in this screen.

Table 19 Encryption: WPA-PSK, WPA2-PSK or WPA2-PSK Mixed

LABEL	DESCRIPTION
Encryption	Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK Mixed** to allow clients to associate this network with WPA-PSK, WPA2-PSK or either WPA-PSK or WPA2-PSK authentication.
Pre-Shared Key Format	Select **Passphrase** to make the NBG2105 generate a key from a phrase typed into the **Pre-Shared Key** field. Select **Hex** to configure the NBG2105 to accept a key in hexadecimal format in the **Pre-Shared Key** field.
Pre-Shared Key	If **Passphrase** was selected in the **Pre-Shared Key Format** field, type a pre-shared key from 8 to 63 case-sensitive keyboard characters. If **Hex** was selected in the **Pre-Shared Key Format** field, type a pre-shared key using hexadecimal characters ("0-9", "A-F").
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Finished	Click this to finish the wizard.

6

Client Setup Wizard

6.1 Overview

This chapter provides information on the wizard setup screens in the Web Configurator.

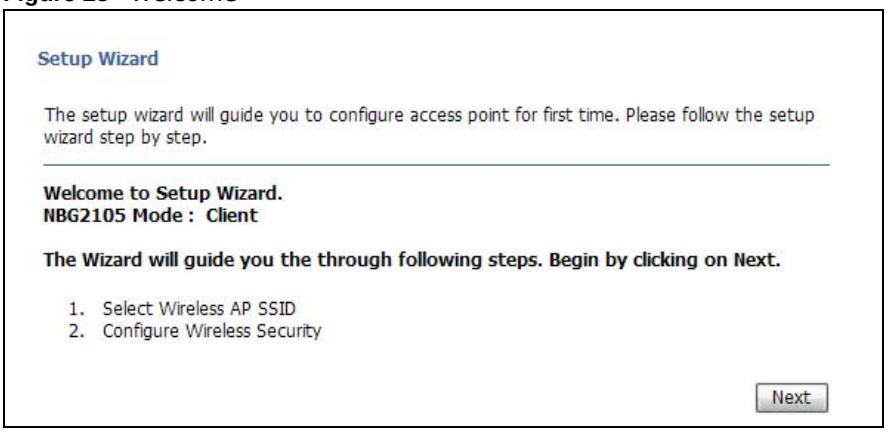
The Web Configurator's wizard setup helps you configure your device in Client mode for the first time.

6.2 Welcome Screen

Launch your web browser and type "http://192.168.1.2" as the website address. Type "admin" (default) as the user name and "1234" (default) as the password. Click **Login**.

Click **Wizard** in client mode to open the Welcome screen. Click **Next** after reading the instructions on this screen.

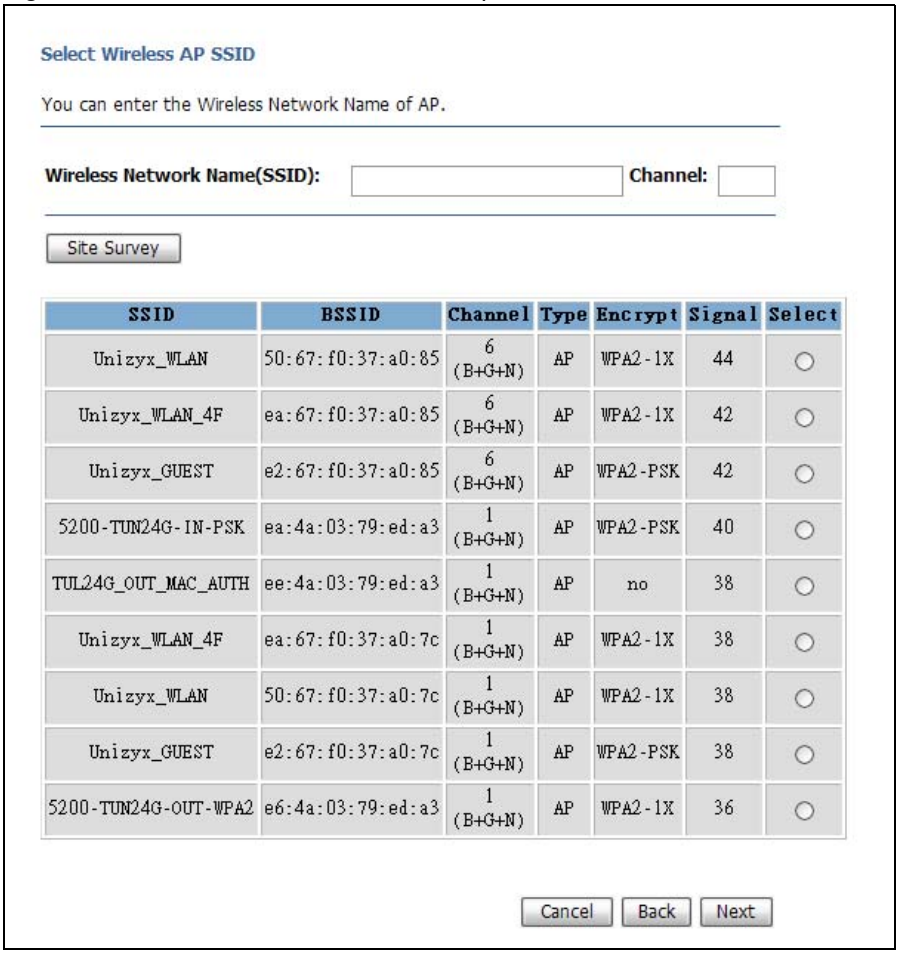
Figure 25 Welcome



6.3 Wireless Network Name Setup

Name your wireless network by entering an SSID or by clicking **Site Survey** and selecting one of the detected devices. Click **Next** to proceed with the **Wireless Security Mode** screen.

Figure 26 Wireless Network Name Setup



The following table describes the labels in this screen.

Table 20 Wireless Network Name Setup

LABEL	DESCRIPTION
Wireless Network Name (SSID)	Enter the SSID of the AP to which you want the NBG2105 in client mode to connect.
Channel	Enter the channel number used by the wireless device to which the NBG2105 is connecting. This is optional if the AP does not broadcast and hides the SSID.
Site Survey	Click this to search for available wireless devices within transmission range and update this table.
SSID	This shows the SSID of the wireless device.
BSSID	This shows the MAC address of the wireless device.
Channel	This shows the channel number and wireless standard used by this wireless device.
Type	This shows the type of device found in the survey.
Encrypt	This displays the data encryption and authentication method used by this wireless device.
Signal	This displays the strength of the wireless signal. The signal strength mainly depends on the antenna output power and the distance between your NBG2105 and this device.
Select	Click this to select a device.
Cancel	Click this to cancel the wizard.

Table 20 Wireless Network Name Setup (continued)

LABEL	DESCRIPTION
Back	Click this to go back to the previous step in the wizard.
Next	Click this to open a screen to configure wireless security options.

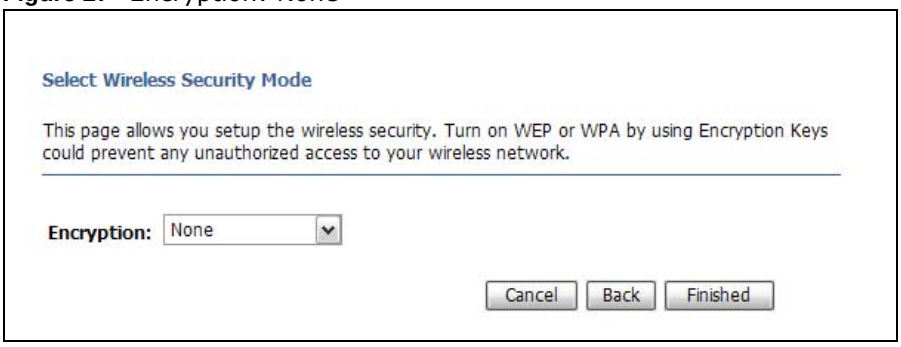
6.4 Wireless Security

Configure the wireless security settings on your NBG2105 in the following screen. The fields that show up depend on the kind of security you select.

6.4.1 Encryption: None

Choose **None** in the **Encryption** field to let wireless devices within range access your wireless network. Complete the fields described. Click **Finished** to save the configuration end exit the wizard.

Figure 27 Encryption: None



The following table describes the labels in this screen.

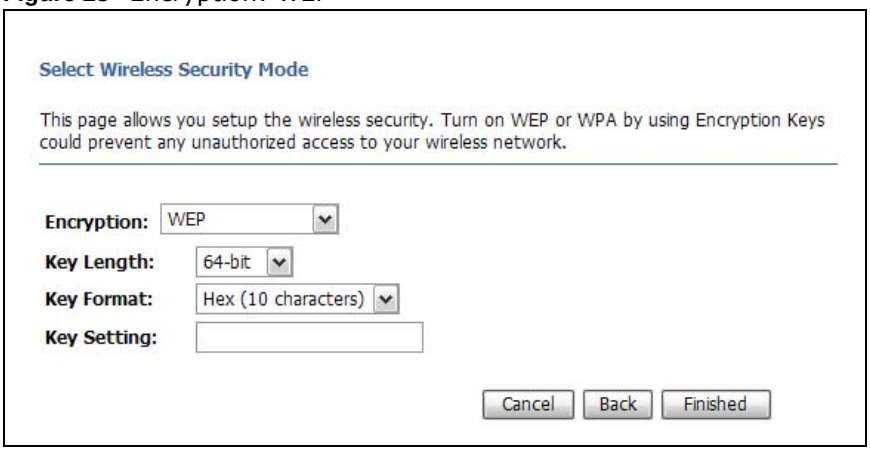
Table 21 Encryption: None

LABEL	DESCRIPTION
Encryption	Select **None** to have no wireless LAN security configured. If you do not enable any wireless security on your NBG2105, your network is accessible to any wireless networking device that is within range.
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Finished	Click this to finish the wizard.

6.4.2 Encryption: WEP

Choose **WEP** in the **Encryption** field to protect your wireless network with Wired Equivalent Privacy. Complete the fields described. Click **Finished** to save the configuration end exit the wizard.

Figure 28 Encryption: WEP



The following table describes the labels in this screen.

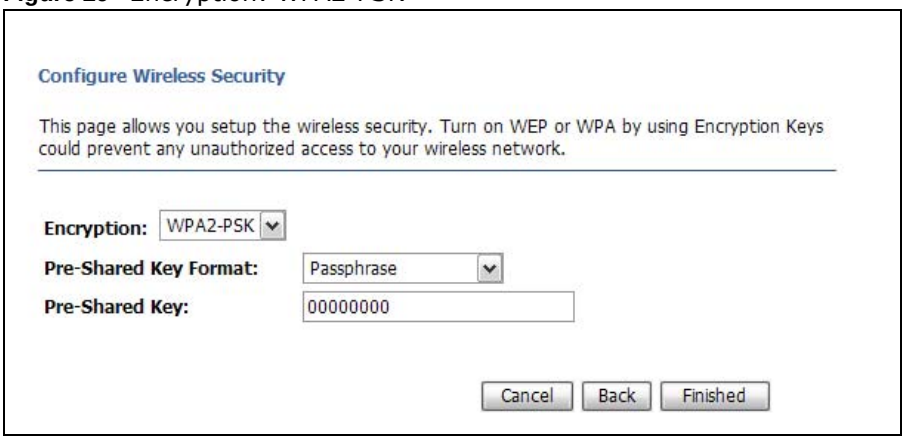
Table 22 Encryption: WEP

LABEL	DESCRIPTION
Encryption	Select **WEP** to allow clients to associate this network with WEP authentication.
Key Length	Select **64-bit** or **128-bit**. This dictates the length of the security key that the network is going to use.
Key Format	Select **Hex** to enter hexadecimal characters as a WEP key. Select **ASCII** to enter ASCII characters as WEP key.
Key Setting	The WEP keys are used to encrypt data. Both the NBG2105 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit** in the **Key Format** field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit** in the **Key Format** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Finished	Click this to finish the wizard.

6.4.3 Encryption: WPA-PSK or WPA2-PSK

Choose **WPA-PSK or WPA2-PSK** in the **Encryption** field to protect your wireless network with WPA-PSK or WPA2-PSK encryption. Complete the fields described. Click **Finished** to save the configuration end exit the wizard.

Figure 29 Encryption: WPA2-PSK



Note: Although only the **WPA2-PSK** screen is shown, all fields are the same for the **WPA-PSK** screen.

The following table describes the labels in this screen.

Table 23 Encryption: WPA-PSK or WPA2-PSK

LABEL	DESCRIPTION
Encryption	Select **WPA-PSK** or **WPA2-PSK** to allow clients to associate this network with WPA or WPA2 authentication.
Pre-Shared Key Format	Select **Passphrase** to make the NBG2105 generate a key from a phrase typed into the **Pre-Shared Key** field. Select **HEX** to configure the NBG2105 to accept a key in hexadecimal format in the **Pre-Shared Key** field.
Pre-Shared Key	If **Passphrase** was selected in the **Pre-Shared Key Format** field, type a pre-shared key from 8 to 63 case-sensitive keyboard characters. If **HEX** was selected in the **Pre-Shared Key Format** field, type a pre-shared key using hexadecimal characters ("0-9", "A-F").
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Finished	Click this to finish the wizard.

7

WISP+UR Setup Wizard

7.1 Overview

This chapter provides information on the wizard setup screens in the Web Configurator.

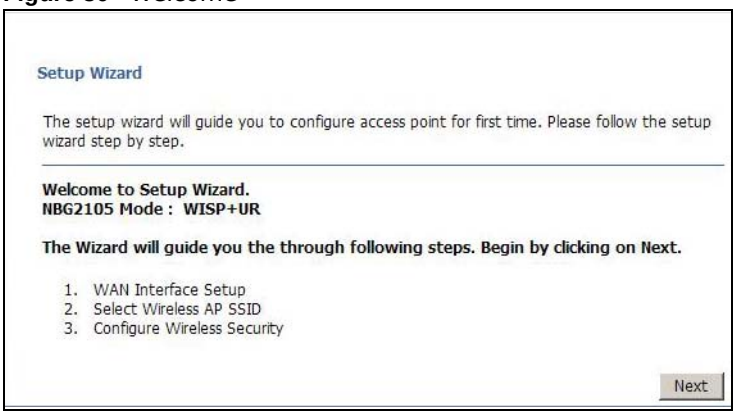
The Web Configurator's wizard setup helps you configure the wireless network name and wireless network security in WISP+UR mode for the first time.

7.2 Welcome Screen

Launch your web browser and type "http://192.168.1.2" as the website address. Type "admin" (default) as the user name and "1234" (default) as the password. Click **Login**.

Click **Wizard** in WISP+UR mode to open the Welcome screen. Click **Next** after reading the instructions on this screen.

Figure 30 Welcome



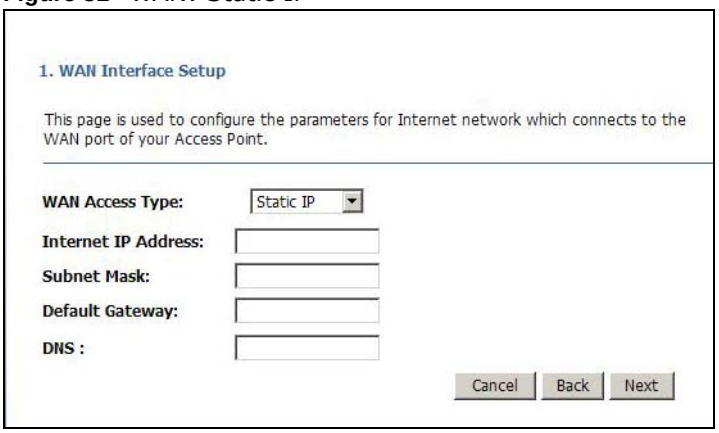
7.3 WAN Interface Setup

Click **Network** > **WAN** to change how your NBG2105's WAN interface accesses your ISP. The screen differs according to the **WAN Access Type** you choose.

7.3.1 Static IP

Select **Static IP** from **WAN Access Type** to configure all NBG2105 WAN IP configuration settings manually.

Figure 31 WAN: Static IP



The following table describes the labels in this screen.

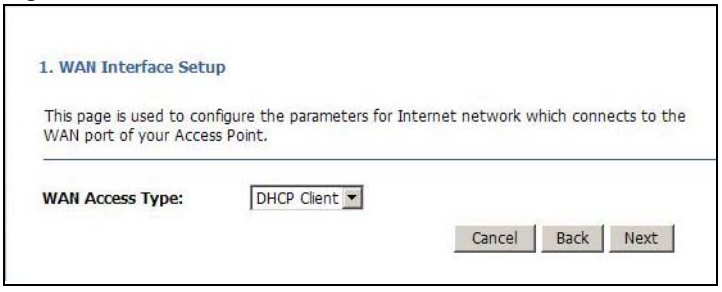
Table 24 WAN: Static IP

LABEL	DESCRIPTION
WAN Access Type	Select **Static IP** to enable manual configuration of all NBG2105 IP settings.
Internet IP Address	Enter the Internet-facing IP address.
Subnet Mask	Enter the subnet mask of the NBG2105 WAN interface.
Default Gateway	Enter the IP address of a default gateway to the Internet.
DNS	Enter the IP address of the DNS server.
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Next	Click this to open a screen to configure wireless security options.

7.3.2 DHCP Client

Select **DHCP Client** from **WAN Access Type** to make the NBG2105 get its IP configuration from a DHCP server.

Figure 32 WAN: DHCP Client



The following table describes the labels in this screen.

Table 25 WAN: DHCP Client

LABEL	DESCRIPTION
WAN Access Type	Select **DHCP Client** to make the NBG2105 get its IP configuration from a DHCP server.
Cancel	Click this to cancel the wizard.

Table 25 WAN: DHCP Client (continued)

LABEL	DESCRIPTION
Back	Click this to go back to the previous step in the wizard.
Next	Click this to open a screen to configure wireless security options.

7.3.3 PPPoE

The NBG2105 supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

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

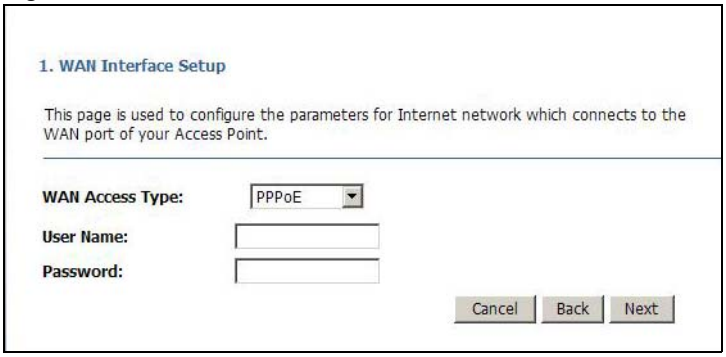
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

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

By implementing PPPoE directly on the NBG2105 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG2105 does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

Select **PPPoE** from **WAN Access Type** to make the NBG2105 get its IP configuration via PPPoE.

Figure 33 WAN: PPPoE



The following table describes the labels in this screen.

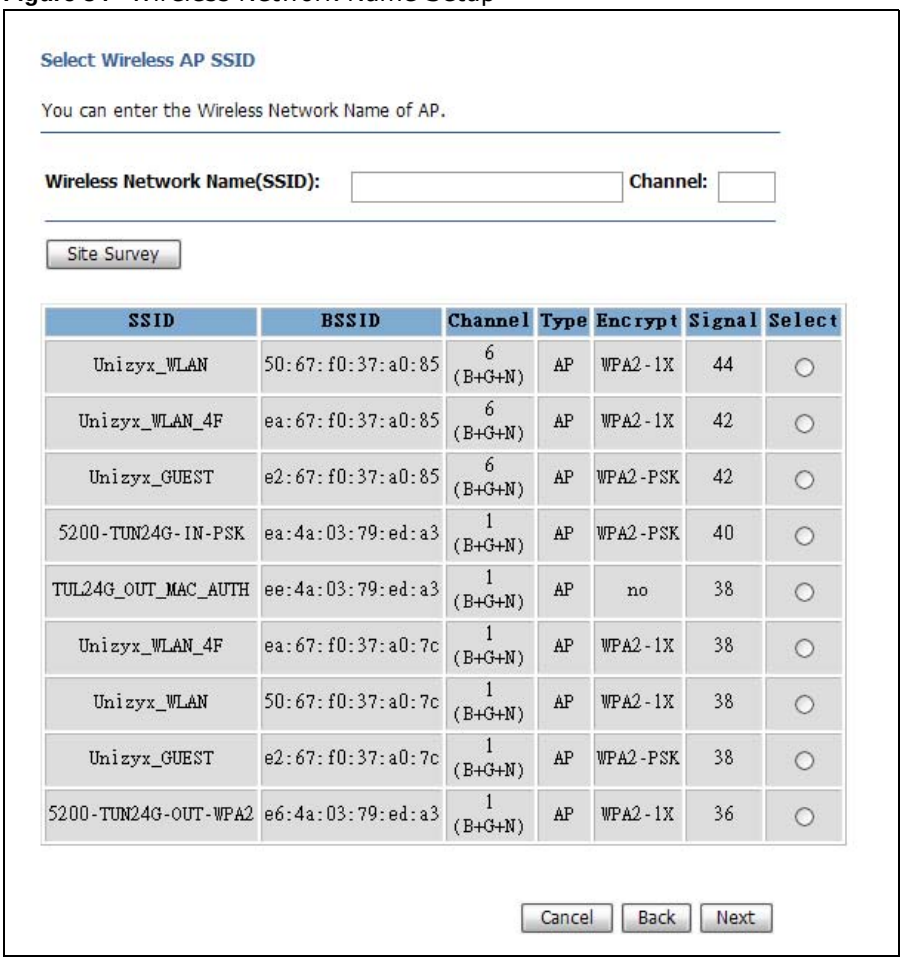
Table 26 WAN: PPPoE

LABEL	DESCRIPTION
WAN Access Type	Select **PPPoE** to make the NBG2105 get its IP configuration via PPPoE.
User Name	Enter the user name provided by your ISP.
Password	Enter the password provided by your ISP.
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Next	Click this to open a screen to configure wireless security options.

7.4 Wireless Network Name Setup

Name your wireless network by entering an SSID or by clicking **Site Survey** and selecting one of the detected devices. Click **Next** to proceed with the **Wireless Security Mode** screen.

Figure 34 Wireless Network Name Setup



The following table describes the labels in this screen.

Table 27 Wireless Network Name Setup

LABEL	DESCRIPTION
Wireless Network Name (SSID)	Enter the SSID of the AP to which you want the NBG2105 in WISP+UR mode to connect.
Channel	Enter the channel number used by the wireless device to which the NBG2105 is connecting. This is optional if the AP does not broadcast and hides the SSID.
Site Survey	Click this to search for available wireless devices within transmission range and update this table.
SSID	This shows the SSID of the wireless device.
BSSID	This shows the MAC address of the wireless device.
Channel	This shows the channel number and wireless standard used by this wireless device.
Type	This shows the type of device found in the survey.

Table 27 Wireless Network Name Setup (continued)

LABEL	DESCRIPTION
Encrypt	This displays the data encryption and authentication method used by this wireless device.
Signal	This displays the strength of the wireless signal. The signal strength mainly depends on the antenna output power and the distance between your NBG2105 and this device.
Select	Click this to select a device.
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Next	Click this to open a screen to configure wireless security options.

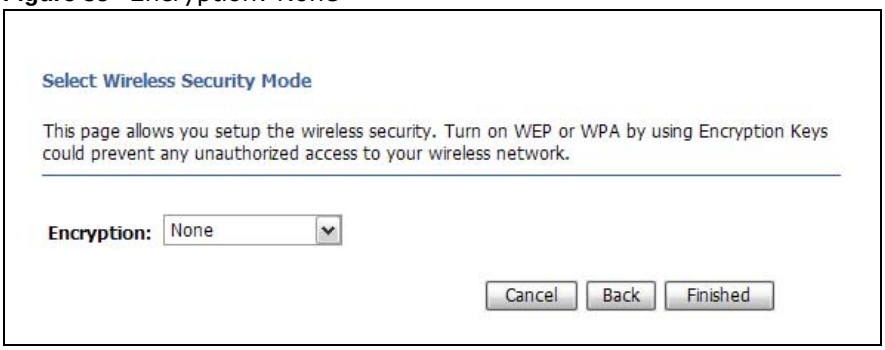
7.5 Wireless Security

Configure the wireless security settings on your NBG2105 in the following screen. The fields that show up depend on the kind of security you select.

7.5.1 Encryption: None

Choose **None** in the **Encryption** field to let wireless devices within range access your wireless network. Complete the fields described. Click **Finished** to save the configuration end exit the wizard.

Figure 35 Encryption: None



The following table describes the labels in this screen.

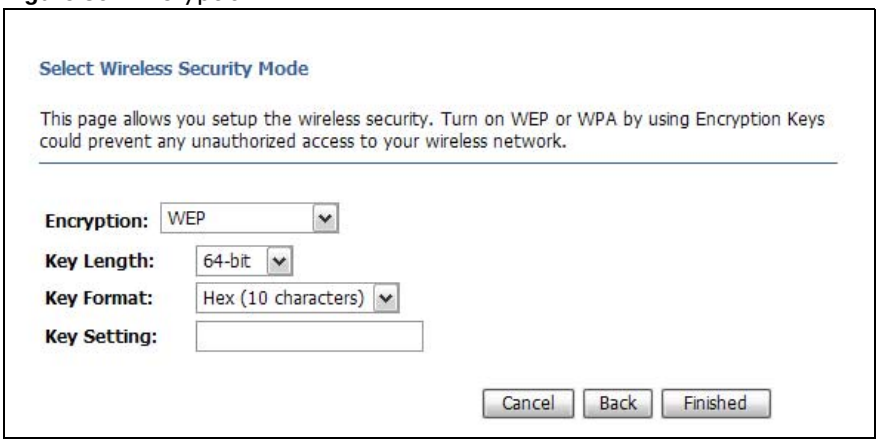
Table 28 Encryption: None

LABEL	DESCRIPTION
Encryption	Select **None** to have no wireless LAN security configured. If you do not enable any wireless security on your NBG2105, your network is accessible to any wireless networking device that is within range.
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Finished	Click this to finish the wizard.

7.5.2 Encryption: WEP

Choose **WEP** in the **Encryption** field to protect your wireless network with Wired Equivalent Privacy. Complete the fields described. Click **Finished** to save the configuration end exit the wizard.

Figure 36 Encryption: WEP



The following table describes the labels in this screen.

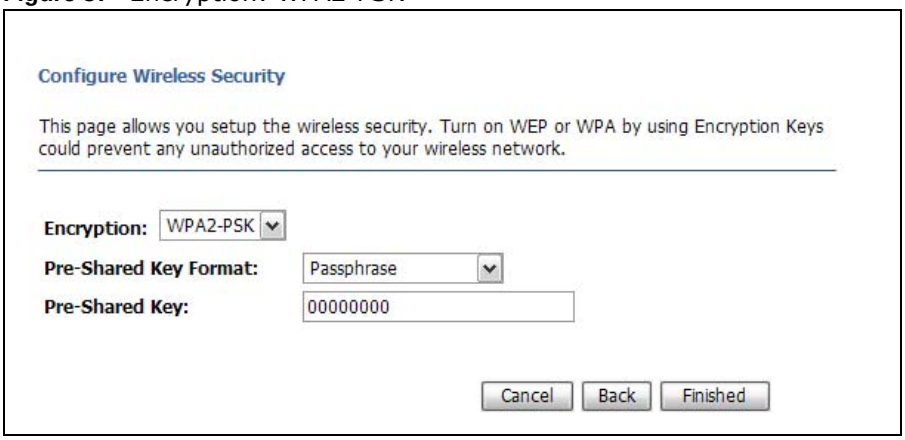
Table 29 Encryption: WEP

LABEL	DESCRIPTION
Encryption	Select **WEP** to allow clients to associate this network with WEP authentication.
Key Length	Select **64-bit** or **128-bit**. This dictates the length of the security key that the network is going to use.
Key Format	Select **Hex** to enter hexadecimal characters as a WEP key. Select **ASCII** to enter ASCII characters as WEP key.
Key Setting	The WEP keys are used to encrypt data. Both the NBG2105 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit** in the **Key Format** field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit** in the **Key Format** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Finished	Click this to finish the wizard.

7.5.3 Encryption: WPA-PSK or WPA2-PSK

Choose **WPA-PSK or WPA2-PSK** in the **Encryption** field to protect your wireless network with WPA-PSK or WPA2-PSK encryption. Complete the fields described. Click **Finished** to save the configuration end exit the wizard.

Figure 37 Encryption: WPA2-PSK



Note: Although only the **WPA2-PSK** screen is shown, all fields are the same for the **WPA-PSK** screen.

The following table describes the labels in this screen.

Table 30 Encryption: WPA-PSK or WPA2-PSK

LABEL	DESCRIPTION
Encryption	Select **WPA-PSK** or **WPA2-PSK** to allow clients to associate this network with WPA or WPA2 authentication.
Pre-Shared Key Format	Select **Passphrase** to make the NBG2105 generate a key from a phrase typed into the **Pre-Shared Key** field. Select **HEX** to configure the NBG2105 to accept a key in hexadecimal format in the **Pre-Shared Key** field.
Pre-Shared Key	If **Passphrase** was selected in the **Pre-Shared Key Format** field, type a pre-shared key from 8 to 63 case-sensitive keyboard characters. If **HEX** was selected in the **Pre-Shared Key Format** field, type a pre-shared key using hexadecimal characters ("0-9", "A-F").
Cancel	Click this to cancel the wizard.
Back	Click this to go back to the previous step in the wizard.
Finished	Click this to finish the wizard.

8

Tutorials

8.1 Overview

This chapter provides tutorials for setting up your NBG2105.

- Set Up a Wireless Network with WPS
- Configure Wireless Security without WPS

8.2 Set Up a Wireless Network with WPS

This section gives you an example of how to set up wireless network using WPS. This example uses the NBG2105 as the AP and NWD210N as the wireless client which connects to a notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCI card).

There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section 8.2.1 on page 59.This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the NBG2105's interface. See Section 8.2.2 on page 60. This is the more secure method, since one device can authenticate the other.

8.2.1 Push Button Configuration (PBC)

1. Make sure that your NBG2105 is turned on and working as an AP or wireless router. Make sure that the device is placed within range of your notebook.
2. Make sure that you have installed the wireless client (this example uses the NWD210N) driver and utility in your notebook.
3. In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button)
4. Log into NBG2105's Web Configurator and press the **Start PBC** button in the **Wireless LAN** > **WPS** screen.

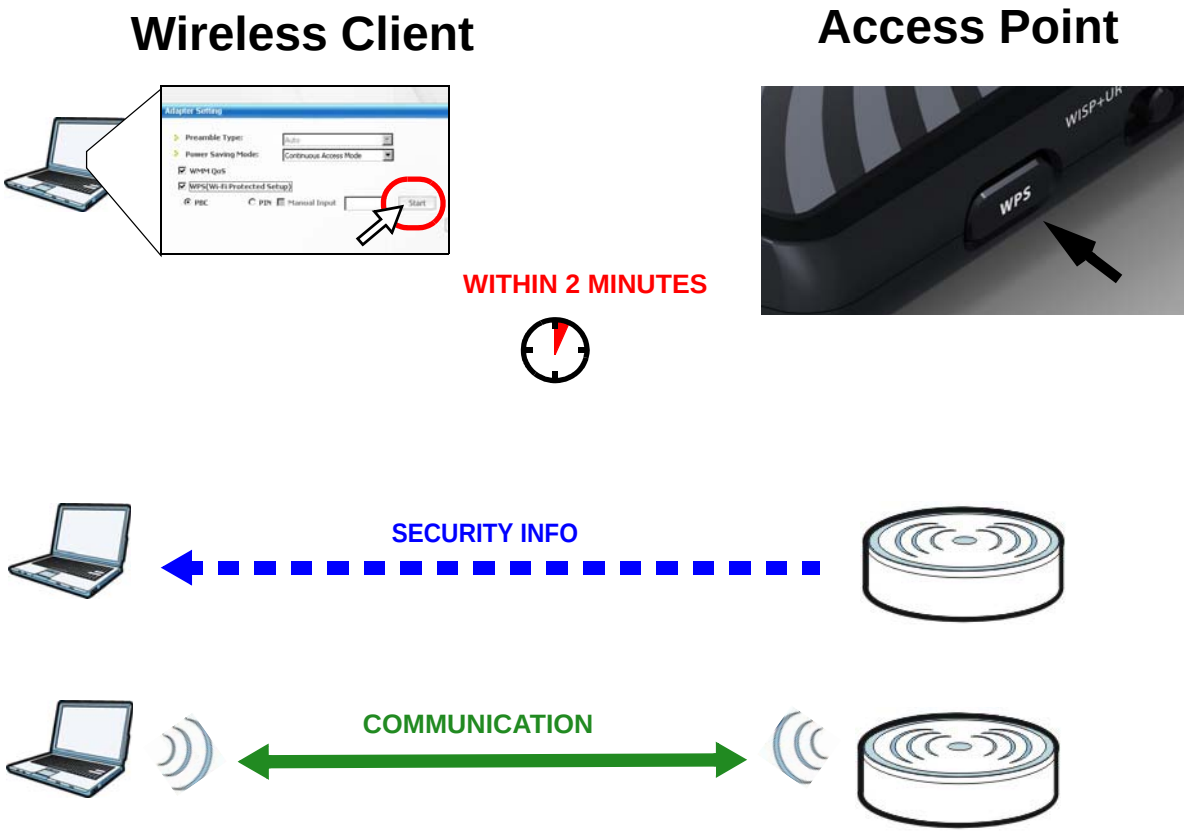
Note: Your NBG2105 has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The NBG2105 sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the NBG2105 securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both NBG2105 and wireless client (the NWD210N in this example).

Figure 38 Example WPS Process: PBC Method



8.2.2 PIN Configuration

When you use the PIN configuration method, you need to use both NBG2105's configuration interface and the client's utilities.

1 Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.

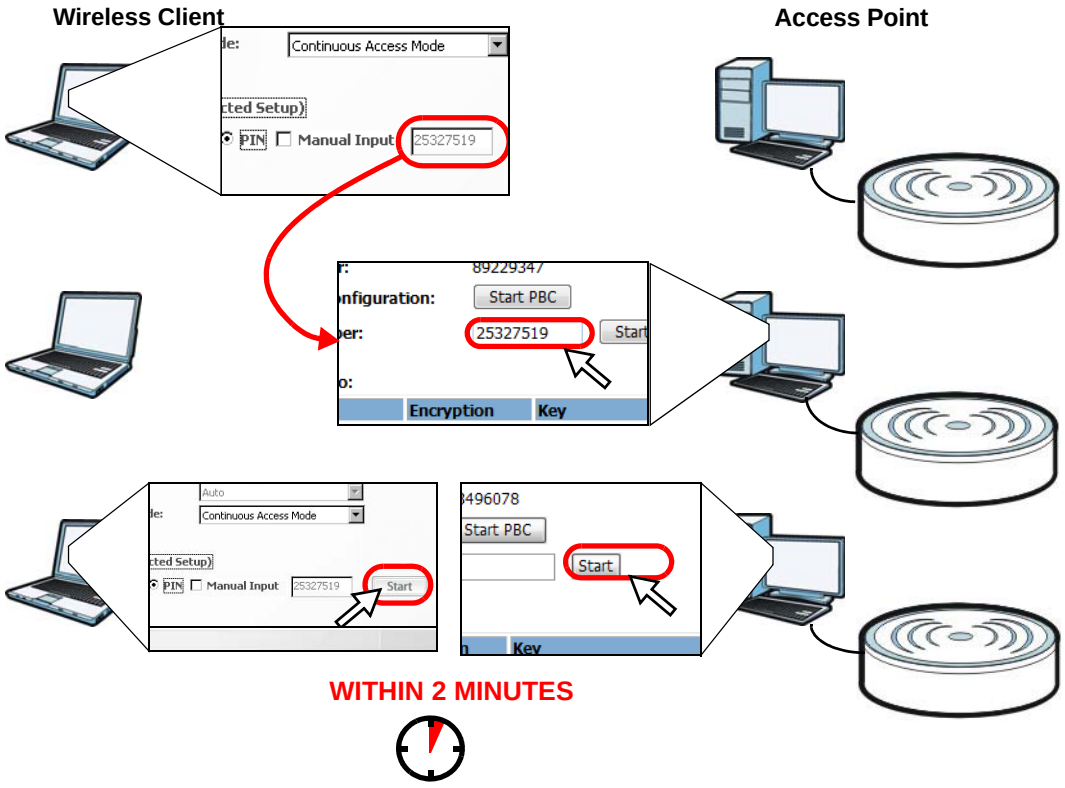
2 Enter the PIN number into the **Station PIN Number** field in the **Wireless LAN** > **WPS** screen on the NBG2105.

3 Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the NBG2105's **Wireless LAN** > **WPS** screen within two minutes.

The NBG2105 authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the NBG2105 securely.

The following figure shows you the example to set up wireless network and security on NBG2105 and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 39 Example WPS Process: PIN Method



8.3 Configure Wireless Security without WPS

This example shows you how to configure wireless security settings with the following parameters on your NBG2105. This section does not apply to Client mode.

SSID	SSID_Example3
Channel	6
Security	WPA2-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your NBG2105.

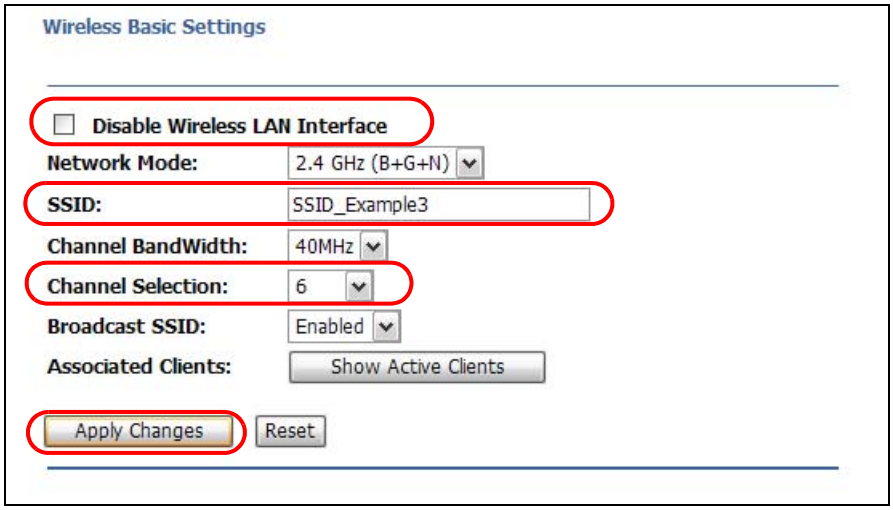
The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection (see Section 2.2 on page 19).

1 Make sure your NBG2105 is turned on and working as an AP or wireless router.

2 Open the **Wireless LAN > Basic** screen in the NBG2105's Web Configurator.

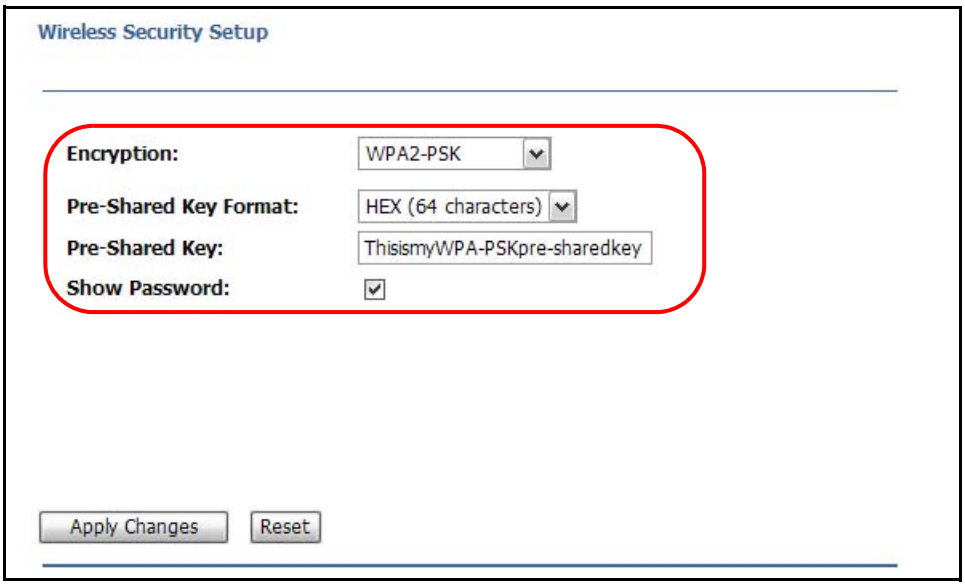
3 Confirm that **Disable Wireless LAN Interface** is not selected.

4 Enter **SSID_Example3** as the SSID and select **6** as the channel. Click **Apply Changes**.

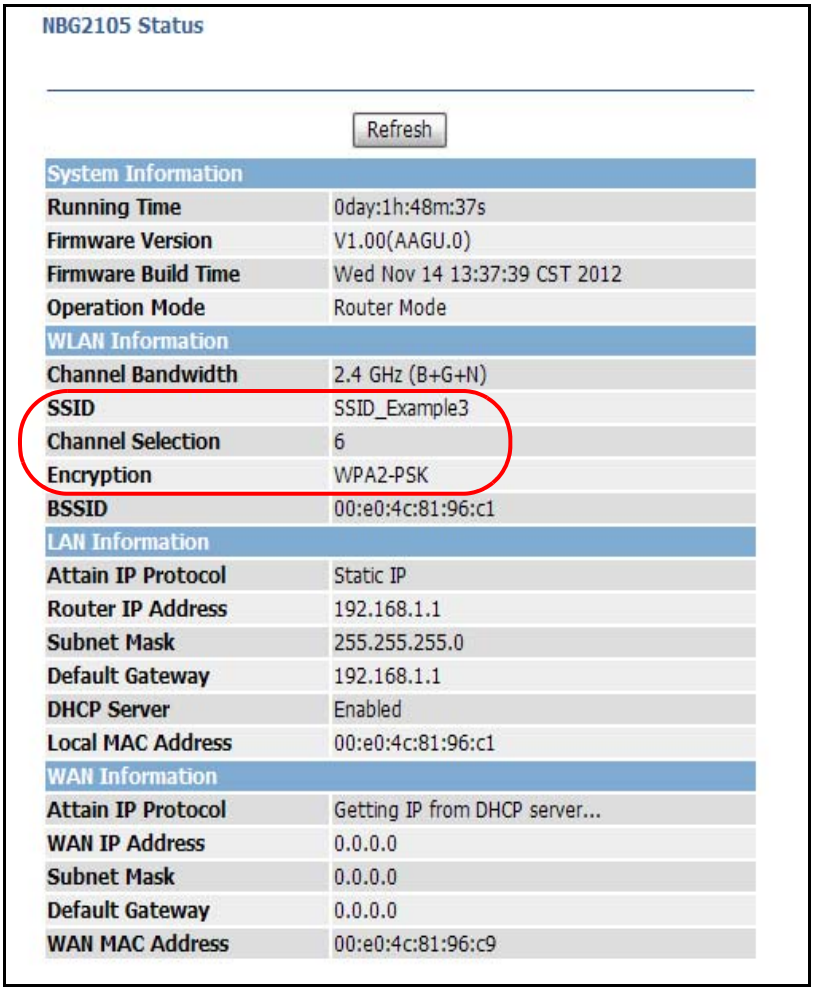


5 Open the **Wireless LAN > Security** screen in the NBG2105's Web Configurator.

6 Set **Encryption** to **WPA2-PSK**, set **Pre-Shared Key Format** to **HEX** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field.



7 Open the **Status** screen. Verify your wireless and wireless security settings under **Wireless Network**.



8.3.1 Configure Your Notebook

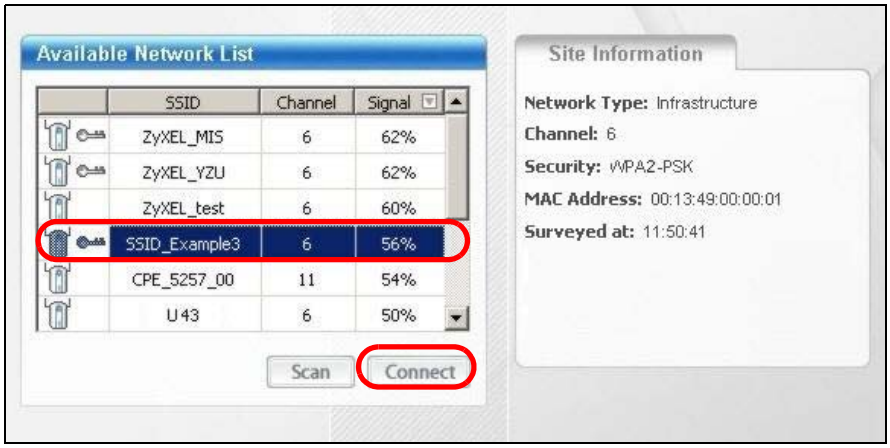
Note: We use the ZyXEL NWD2205 wireless adapter utility screens as an example for the wireless client. The screens may vary for different models.

1 The NBG2105 supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

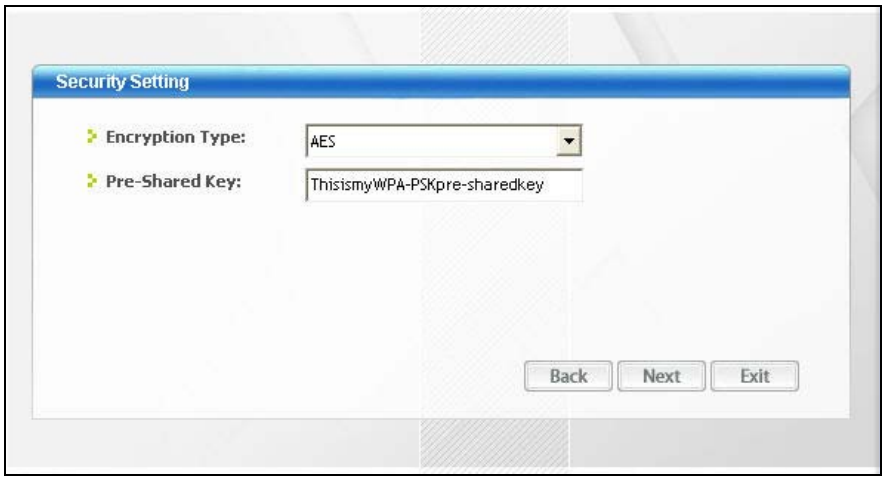
2 Wireless adapters come with software sometimes called a "utility" that you install on your computer. See your wireless adapter's User's Guide for information on how to do that.

3 After you've installed the utility, open it. If you cannot see your utility's icon on your screen, go to **Start > Programs** and click on your utility in the list of programs that appears. The utility displays a list of APs within range, as shown in the example screen below.

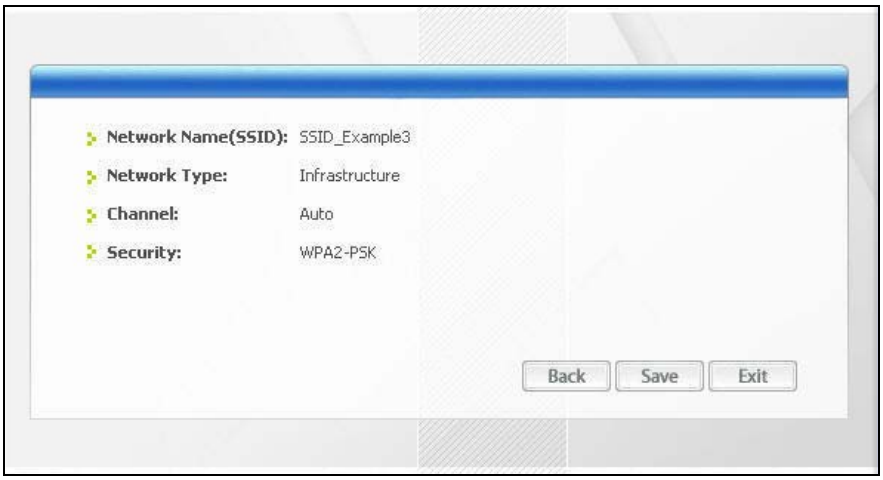
4 Select SSID_Example3 and click **Connect**.



5 Select **AES** and type the security key in the following screen. Click **Next**.



6 The **Confirm Save** window appears. Check your settings and click **Save** to continue.



7 Check the status of your wireless connection in the screen below. If your wireless connection is weak or you have no connection, see the Troubleshooting section of this User's Guide.

If your connection is successful, open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

PART II
Technical Reference

9

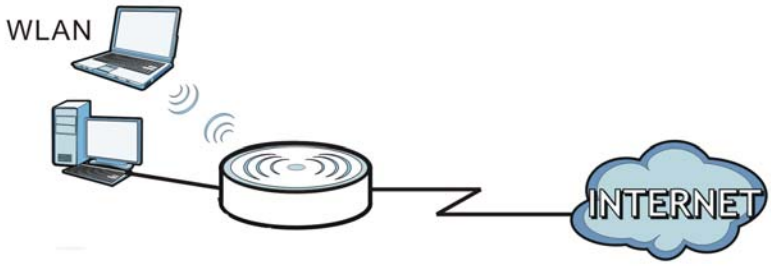
LAN

9.1 Overview

This chapter describes how to configure LAN settings.

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

Figure 40 LAN Example



9.2 What You Can Do

- Use the **LAN Interface Setup** screen to change the IP address for your NBG2105 (Section 9.4 on page 70).
- Use the **Active DHCP Client** screen to see which DHCP clients have accepted their IP configuration from the NBG2105 (Section 9.4.1 on page 71).

9.3 What You Need To Know

The LAN parameters of the NBG2105 are preset in the factory with the following values:

- IP address of 192.168.1.1 (Router mode) or 192.168.1.2 (non-router modes) with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled (Router mode or WISP+UR mode) with client IP addresses starting from 192.168.1.100 and ending with 192.168.1.200.

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

9.3.1 IP Pool Setup

The NBG2105 is pre-configured with a pool of IP addresses starting from 192.168.1.100 to 192.168.1.200. This configuration leaves 98 IP addresses (excluding the NBG2105 itself) under 192.168.1.99 for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

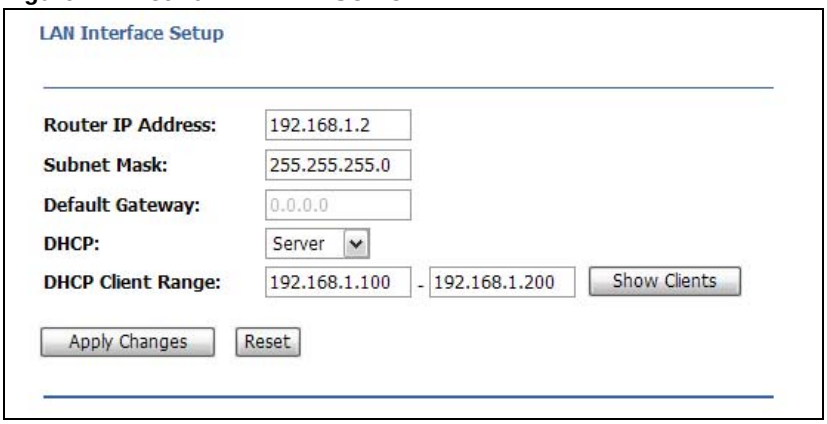
9.3.2 LAN TCP/IP

The NBG2105 has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

9.4 LAN Interface Setup Screen

Use this screen to change the IP address for your NBG2105 and configure the DHCP server. Click **Network > LAN**.

Figure 41 Network > LAN: Server



The following table describes the labels in this screen.

Table 31 Network > LAN

LABEL	DESCRIPTION
Router IP Address	Enter the IP address of the NBG2105 management interface.
Subnet Mask	Enter the subnet mask of the NBG2105 management interface.
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. DHCP server is disabled by default when the NBG2105 is in AP or Client mode. Select **Server** to enable the DHCP server of the NBG2105. When configured as a server, the NBG2105 provides TCP/IP configuration for the clients. Select **Disable** to stop the NBG2105 acting as a DHCP server. If disabled, you must have another DHCP server on your LAN, or else the computers must be manually configured.
DHCP Client Range	Enter the range of IP addresses that can be issued by the DHCP server. This field is not configurable when DHCP server is disabled.

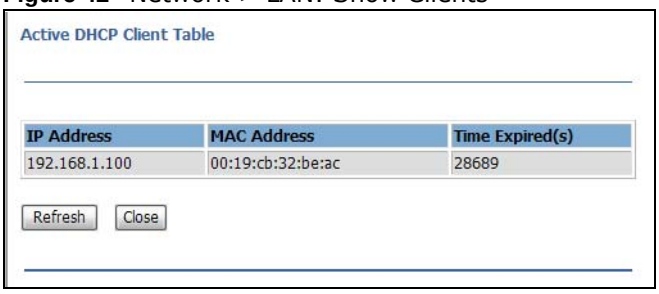
Table 31 Network > LAN (continued)

LABEL	DESCRIPTION
Show Clients	Click this to show the IP addresses that have been issued by the DHCP server. This field is not configurable when DHCP server is disabled.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.

9.4.1 Active DHCP Client Screen

Use this screen to view which DHCP clients have accepted their IP configuration from the NBG2105. Click **Network > LAN**, and then **Show Clients**.

Figure 42 Network > LAN: Show Clients



The following table describes the labels in this screen.

Table 32 Network > LAN: Show Clients

LABEL	DESCRIPTION
IP Address	This shows the IP address leased to a DHCP client.
MAC Address	This shows the MAC address of the client that leased the IP address.
Time Expired (s)	This shows how many seconds remain on the DHCP lease.
Refresh	Click this to update the screen.
Close	Click this to close this screen.

10 WAN

10.1 Overview

This chapter discusses the NBG2105's **WAN** screens. Use these screens to configure your NBG2105 for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

10.2 What You Can Do

You can configure your WAN interface to access your ISP in the following ways.

- **Static IP** allows you to configure all NBG2105 WAN IP configuration settings manually (Section 10.4.1 on page 74).
- **DHCP Client** allows the NBG2105 to get its IP configuration from a DHCP server (Section 10.4.2 on page 75).
- **PPPoE** allows the NBG2105 to connect via the Point-to-Point Protocol over Ethernet (Section 10.4.3 on page 76).

10.3 What You Need To Know

The information in this section can help you configure the screens for your WAN connection.

10.3.1 Configuring Your Internet Connection

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the NBG2105, which makes it accessible from an outside network. It is used by the NBG2105 to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the NBG2105 tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The NBG2105 can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the NBG2105's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

WAN MAC Address

The WAN port's MAC address can be configured by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Clear Mac Clone** to select the factory assigned default MAC Address.

Otherwise, press the Clone MAC address button on the side of the NBG2105 to clone the MAC address of the computer connected to the NBG2105. Once it is successfully configured, the address will be copied to configuration file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

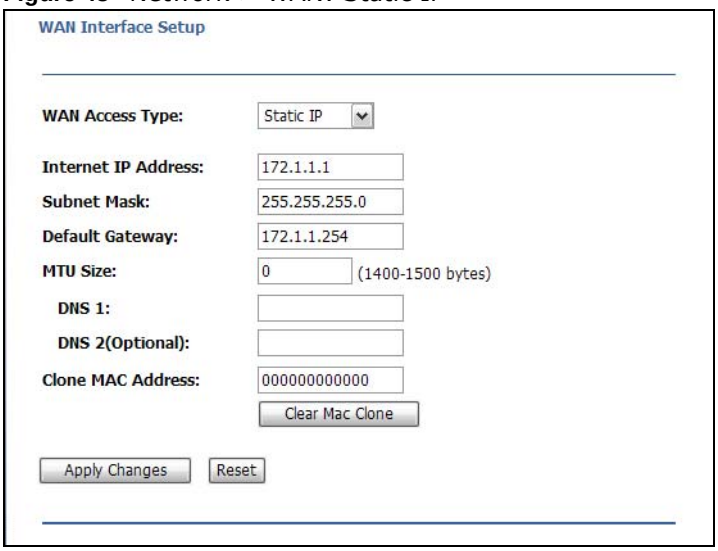
10.4 WAN Interface Setup

Click **Network** > **WAN** to change how your NBG2105's WAN interface accesses your ISP. The screen differs according to the **WAN Access Type** you choose.

10.4.1 Static IP

Select **Static IP** from **WAN Access Type** to configure all NBG2105 WAN IP configuration settings manually.

Figure 43 Network > WAN: Static IP



The following table describes the labels in this screen.

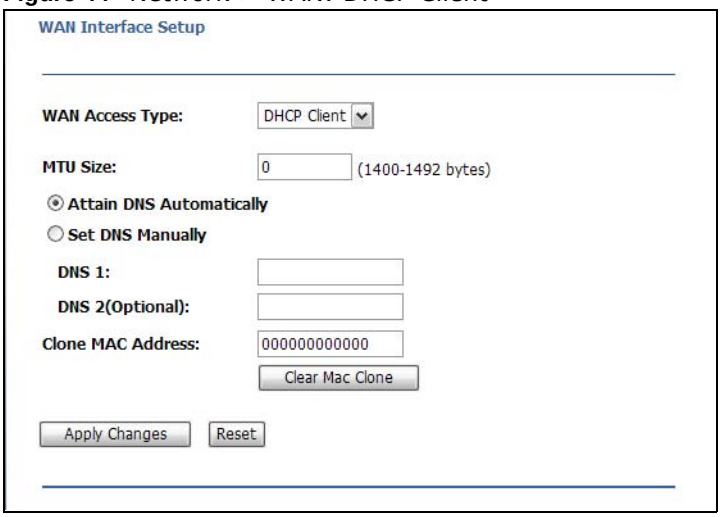
Table 33 Network > WAN: Static IP

LABEL	DESCRIPTION
WAN Access Type	Select **Static IP** to enable manual configuration of all NBG2105 IP settings.
Internet IP Address	Enter the Internet-facing IP address.
Subnet Mask	Enter the subnet mask of the NBG2105 WAN interface.
Default Gateway	Enter the IP address of a default gateway to the Internet.
MTU Size	Enter the MTU (Maximum Transmission Unit) size for each packet. If a larger packet arrives, the NBG2105 divides it into smaller fragments.
DNS 1	Enter the IP address of the primary DNS server.
DNS 2 (Optional)	Enter the IP address of the secondary DNS server.
Clone MAC Address	Enter the MAC address of the WAN interface. This field is available only when the NBG2105 is in router mode.
Clear Mac Clone	Click this to reset the MAC address of the WAN interface to factory defaults. This field is available only when the NBG2105 is in router mode.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.

10.4.2 DHCP Client

Select **DHCP Client** from **WAN Access Type** to make the NBG2105 get its IP configuration from a DHCP server.

Figure 44 Network > WAN: DHCP Client



The following table describes the labels in this screen.

Table 34 Network > WAN: DHCP Client

LABEL	DESCRIPTION
WAN Access Type	Select **DHCP Client** to make the NBG2105 get its IP configuration from a DHCP server.
MTU Size	Enter the MTU (Maximum Transmission Unit) size for each packet. If a larger packet arrives, the NBG2105 divides it into smaller fragments.
Attain DNS Automatically	Select this to configure the NBG2105 to get addresses of DNS servers via DHCP.
Set DNS Manually	Select this to configure the NBG2105 to use DNS server addresses manually.
DNS 1	Enter the IP address of the primary DNS server.
DNS 2 (Optional)	Enter the IP address of the secondary DNS server.
Clone MAC Address	Enter the MAC address of the WAN interface. This field is available only when the NBG2105 is in router mode.
Clear Mac Clone	Click this to reset the MAC address of the WAN interface to factory defaults. This field is available only when the NBG2105 is in router mode.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.

10.4.3 PPPoE

The NBG2105 supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

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

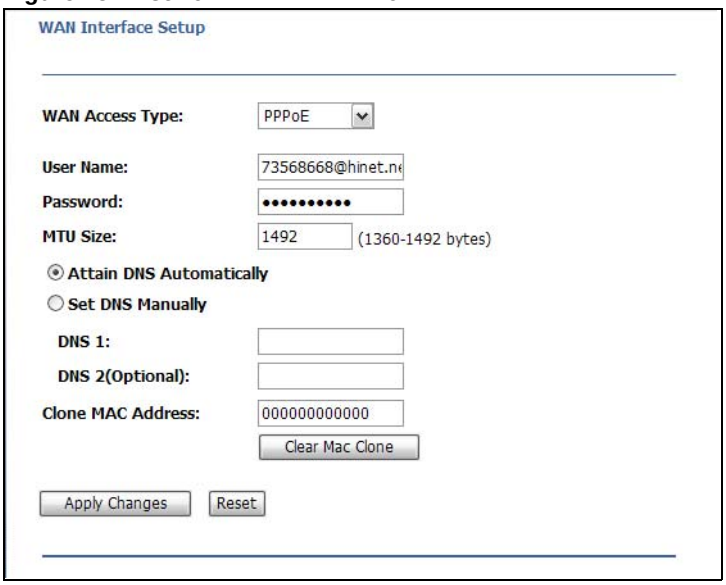
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

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

By implementing PPPoE directly on the NBG2105 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG2105 does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

Select **PPPoE** from **WAN Access Type** to make the NBG2105 get its IP configuration via PPPoE.

Figure 45 Network > WAN: PPPoE



The following table describes the labels in this screen.

Table 35 Network > WAN: PPPoE

LABEL	DESCRIPTION
WAN Access Type	Select **PPPoE** to make the NBG2105 get its IP configuration via PPPoE.
User Name	Enter the user name provided by your ISP.
Password	Enter the password provided by your ISP.
MTU Size	Enter the MTU (Maximum Transmission Unit) size for each packet. If a larger packet arrives, the NBG2105 divides it into smaller fragments.
Attain DNS Automatically	Select this to configure the NBG2105 to get addresses of DNS servers via DHCP.
Set DNS Manually	Select this to configure the NBG2105 to use DNS server addresses manually.
DNS 1	Enter the IP address of the primary DNS server.
DNS 2 (Optional)	Enter the IP address of the secondary DNS server.
Clone MAC Address	Enter the MAC address of the WAN interface. This field is available only when the NBG2105 is in router mode.
Clear Mac Clone	Click this to reset the MAC address of the WAN interface to factory defaults. This field is available only when the NBG2105 is in router mode.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.

11

Quality of Service (QoS)

11.1 Overview

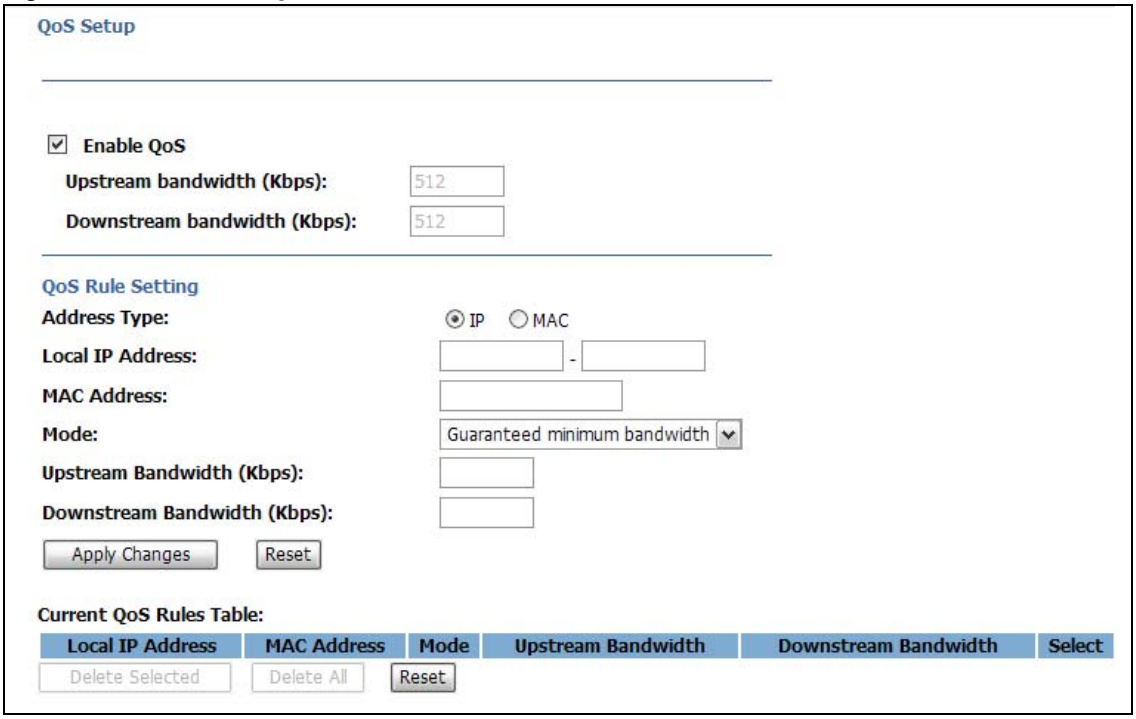
Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

Configure QoS on the NBG2105 to reserve bandwidth for certain traffic based on the IP address or MAC address.

11.2 QoS Setup Screen

Click **Network > QoS** to show the **QoS Setup** screen.

Figure 46 Network > QoS



The following table describes the labels in this screen.

Table 36 Network > QoS

LABEL	DESCRIPTION
QoS Setup	
Enable QoS	Select this to enable QoS.
Upstream bandwidth (Kbps)	This shows the amount of upstream bandwidth for the WAN interface that you can allocate using QoS. The NBG2105 automatically sets this number to the WAN interface's actual upstream transmission speed.
Downstream bandwidth (Kbps)	This shows the amount of downstream bandwidth for the WAN interface that you can allocate using QoS. The NBG2105 automatically sets this number to the WAN interface's actual downstream transmission speed.
QoS Rule Setting	
Address Type	Select **IP** to configure a QoS rule to match the source IP address of outgoing packets or the destination IP address of incoming packets. Select **MAC** to configure a QoS rule to match the source MAC address of outgoing frames or the destination MAC address of incoming frames.
Local IP Address	Enter the source IP address of outgoing packets or the destination IP address of incoming packets that this QoS rule matches.
MAC Address	Enter the source MAC address of outgoing packets or the destination MAC address of incoming packets that this QoS rule matches.
Mode	Select the mode for this rule: **Guaranteed minimum bandwidth** or **restricted maximum bandwith**.
Upstream Bandwidth (Kbps)	Enter the maximum/guaranteed minimum bandwidth (according to the mode you select) allowed for outgoing traffic that matches the IP address or MAC address you specified.
Downstream Bandwidth (Kbps)	Enter the maximum/guaranteed minimum bandwidth (according to the mode you select) allowed for incoming traffic that matches the IP address or MAC address you specified.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.
Current QoS Rules Table	
Local IP Address	This shows the source IP address of outgoing packets or the destination IP address of incoming packets that this QoS rule matches.
MAC Address	This shows the source MAC address of outgoing packets or the destination MAC address of incoming packets that this QoS rule matches.
Mode	This shows the mode of this rule.
Upstream Bandwidth	This shows the uplink bandwidth that this rule enforces according to the **Mode**.
Downstream Bandwidth	This shows the downlink bandwidth that this rule enforces according to the **Mode**.
Select	Click this to select this rule.
Delete Selected	Click this to delete the selected rules.
Delete All	Click this to delete all rules.
Reset	Click this to reset all selections.

12

Dynamic DNS (DDNS)

12.1 Overview

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

12.2 What You Need To Know

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

What is DDNS?

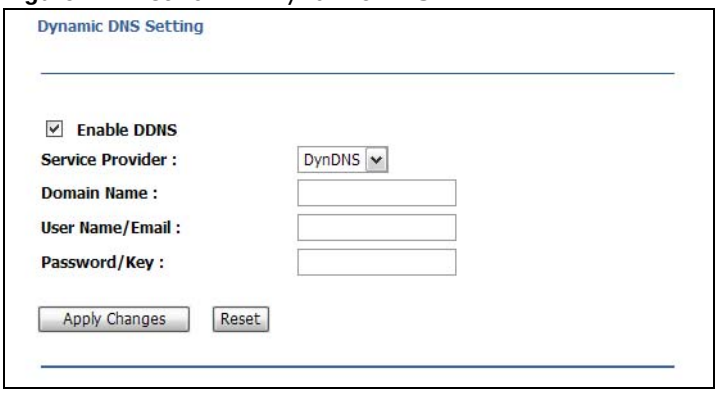
Dynamic Domain Name Service (DDNS) services let you use a fixed domain name with a dynamic IP address. Users can always use the same domain name instead of a different dynamic IP address that changes each time to connect to the NBG2105 or a server in your network.

Note: The NBG2105 must have a public global IP address and you should have your registered DDNS account information on hand.

12.3 Dynamic DNS

To change your NBG2105's DDNS, click **Network > Dynamic DNS**.

Figure 47 Network > Dynamic DNS



The following table describes the labels in this screen.

Table 37 Network > Dynamic DNS

LABEL	DESCRIPTION
Enable DDNS	Click this to enable dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Domain Name	Enter the domain name assigned by your service provider to your NBG2105.
Username/Email	Enter the user name assigned by your service provider to your NBG2105. If you've selected **TZO** in the **Service Provider** field, enter the user name you registered with the service provider.
Password/Key	Enter the password assigned by your service provider to your NBG2105. If you've selected **TZO** in the **Service Provider** field, enter the key you registered with the service provider.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.

13

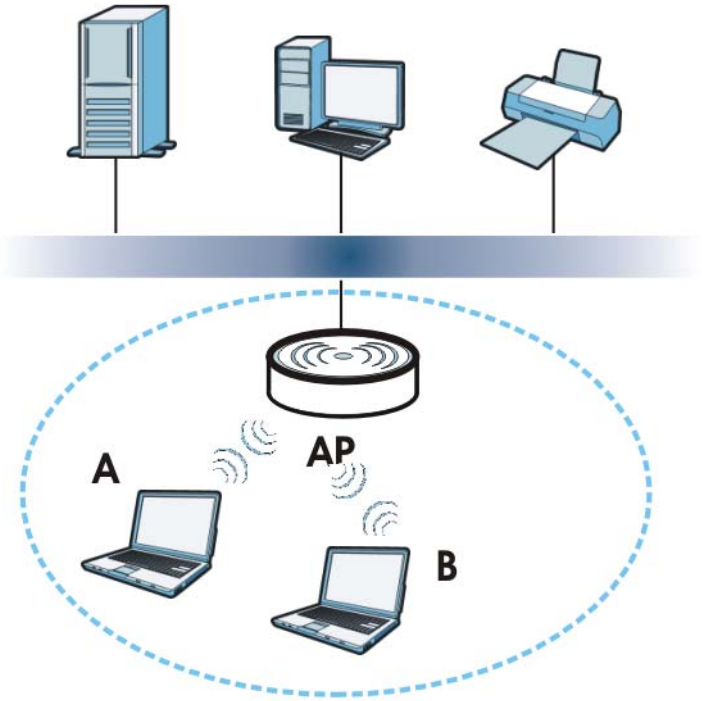
Wireless LAN

13.1 Overview

This chapter discusses how to configure the wireless network settings in your NBG2105. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 48 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your NBG2105 is the AP.

13.1.1 What You Can Do

- Use the **Basic** screen to turn the wireless connection on or off and make other basic configuration changes (Section 13.2 on page 86).
- Use the **Advanced** screen to configure wireless advanced features, such as the output power and set the RTS/CTS Threshold (Section 13.4 on page 88).
- Use the **Security** screen to set up wireless security between the NBG2105 and the wireless clients (Section 13.5 on page 89).

- Use the **Site Survey** screen to scan for and connect to a wireless network automatically. (Section 13.6 on page 92)
- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually (Section 13.8 on page 95).
- Use the **MAC Filtering** screen to allow or deny wireless stations based on their MAC addresses from connecting to the NBG2105 (Section 13.9 on page 97).

13.1.2 What You Should Know

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

Authentication

Authentication is the process of confirming a client's user name and password when they connect to a network. Turning off authentication means allowing anyone to connect to the network.

Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. It is the process of taking data and encoding it, usually using a secret code, so that it becomes unreadable unless decrypted with the proper code or pass phrase. If you do not know the secret code, you cannot understand the message.

WEP

Data Encryption

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the NBG2105 and the AP or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

Authentication Type

The IEEE 802.11b/g/n standard describes a simple authentication method between the wireless stations and AP. Three authentication types are defined: **Both**, **Open** and **Shared**.

- **Open** mode is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.
- **Shared** mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.
- **Both** authentication mode allows the NBG2105 to switch between the open system and shared key modes automatically. Use this mode if you do not know the authentication mode of the other wireless stations.

WPA-PSK and WPA2-PSK

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

If both an AP and the wireless clients support WPA2-PSK, use WPA2-PSK for stronger data encryption. If the AP or the wireless clients do not support WPA2-PSK, just use WPA-PSK. Select WEP only when the AP and/or wireless clients do not support WPA-PSK or WPA2-PSK. WEP is less secure than WPA-PSK or WPA2-PSK.

MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

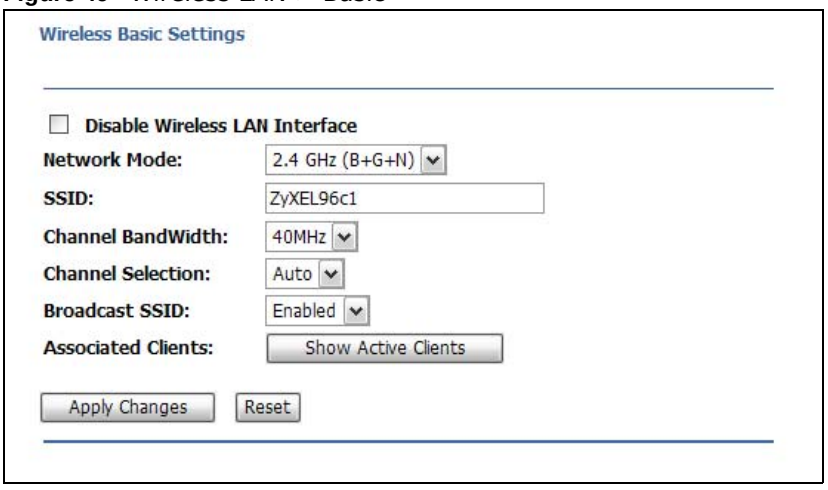
WPS

WiFi Protected Setup (WPS) is an industry standard specification, defined by the WiFi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the Section 8.2 on page 59.

13.2 Wireless Basic Screen

Click **Wireless LAN** > **Basic** to make basic wireless configuration changes.

Figure 49 Wireless LAN > Basic



1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

The following table describes the labels in this screen.

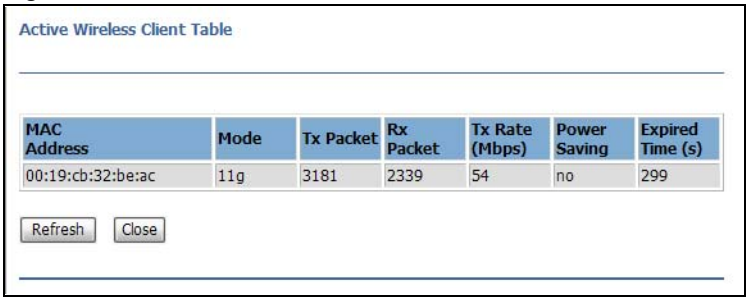
Table 38 Wireless LAN > Basic

LABEL	DESCRIPTION
Disable Wireless LAN Interface	Select this to disable the wireless LAN interface.
Network Mode	Select the frequency band and wireless network mode for your network.
SSID	Enter the SSID (Service Set IDentity) to identify the service set with which wireless clients are associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Channel Bandwidth	Select the wireless channel width used by NBG2105. A standard 20 MHz channel offers transfer speeds of up to 150 Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.
Channel Selection	Select a channel number. The channels you can select depend on the frequency band and the country you are in.
Broadcast SSID	Select **Enabled** to broadcast the SSID or **Disabled** to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Show Active Clients	Click this to show the clients connected to the NBG2105.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.

13.3 Active Wireless Clients Screen

Click **Show Active Clients** in **Wireless LAN** > **Basic** to show the clients connected to the NBG2105.

Figure 50 Wireless LAN > Basic: Show Active Clients



The following table describes the labels in this screen.

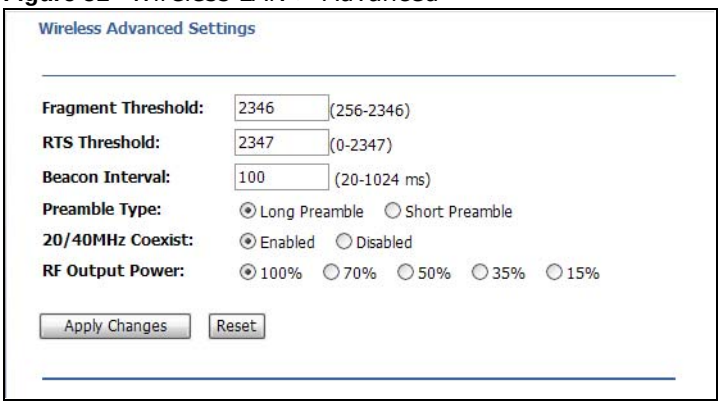
Table 39 Wireless LAN > Basic: Show Active Clients

LABEL	DESCRIPTION
MAC Address	This shows the MAC addresses of wireless clients associated with the NBG2105.
Mode	This shows which wireless standard a wireless client is using to connect to the NBG2105.
Tx Packet	This shows how many packets have been transmitted by the NBG2105 since association.
Rx Packet	This shows how many packets have been received by the NBG2105 since association.
Tx Rate (Mbps)	This shows the rate at which packets are being sent by the NBG2105 to this client.
Power Saving	This shows whether power saving is turned on for this wireless client.
Expired Time (s)	This shows when the association with this client6 will expire.
Refresh	Click this to update the screen.
Close	Click this to close this screen.

13.4 Advanced Wireless Settings Screen

Click **Wireless LAN** > **Advanced** to make advanced wireless configuration changes.

Figure 51 Wireless LAN > Advanced



The following table describes the labels in this screen.

Table 40 Wireless LAN > Advanced

LABEL	DESCRIPTION
Fragment Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. This field is not configurable and the NBG2105 automatically changes to use the maximum value if you select **2.4 GHz (N)**, **2.4 GHz (G + N)** or **2.4 GHz (B + G + N)** in the **Wireless LAN > Basic** screen.
RTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/ CTS (Clear To Send) handshake. This field is not configurable and the NBG2105 automatically changes to use the maximum value if you select **2.4 GHz (N)**, **2.4 GHz (G + N)** or **2.4 GHz (B + G + N)** in the **Wireless LAN > Basic** screen.

Table 40 Wireless LAN > Advanced (continued)

LABEL	DESCRIPTION
Beacon Interval	Enter a value to configure how often beacon frames are broadcast.
Preamble Type	Select **Short Preamble** for better performance or **Long Preamble** for better compatibility.
20/40MHz Coexist	Select **Enabled** to allow the NBG2105 to adjust the channel bandwidth automatically.
RF Output Power	Set the output power of the NBG2105 in this field. If there is a high density of APs in an area, decrease the output power of the NBG2105 to reduce interference with other APs. Select one of the following **100%**, **70%**, **50%**, **35%** or **15%**.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.

13.5 Wireless Security

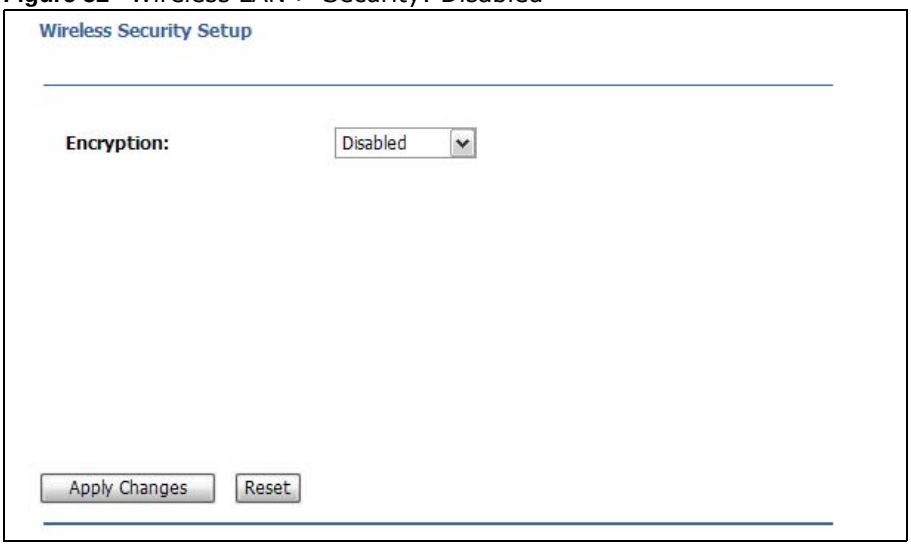
The screen varies depending on what you select in the **Encryption** field. Click **Wireless LAN** > **Security**. This screen is not available when the NBG2105 is in Client mode.

13.5.1 Disabled

Select **Disabled** to allow wireless clients to communicate with the access points without any data encryption.

Note: If you do not enable any wireless security on your NBG2105, your network is accessible to any wireless networking device that is within range.

Figure 52 Wireless LAN > Security: Disabled



The following table describes the labels in this screen.

Table 41 Wireless LAN > Security: Disabled

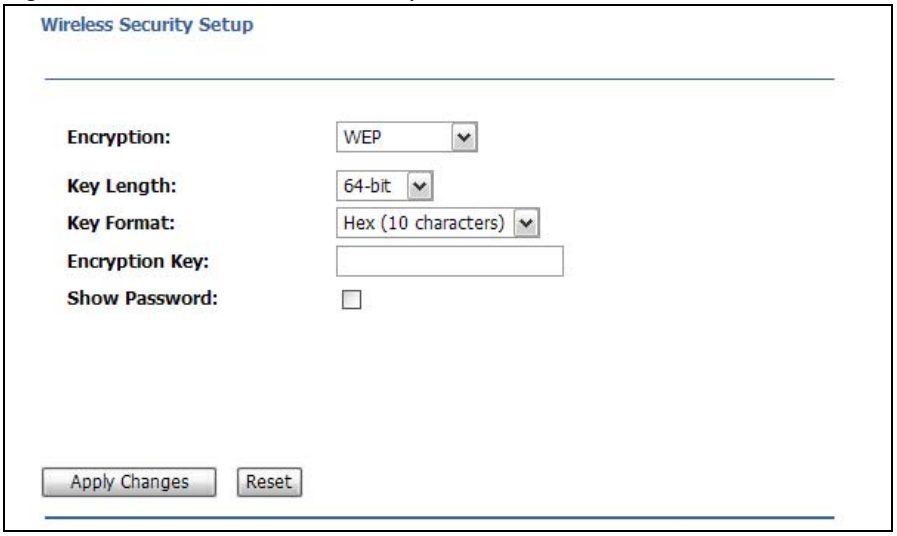
LABEL	DESCRIPTION
Encryption	Select **Disabled** to allow any client to associate this network without authentication.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.

13.5.2 WEP Encryption

Your NBG2105 allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

Select **WEP** from the **Encryption** list.

Figure 53 Wireless LAN > Security: WEP



The following table describes the labels in this screen.

Table 42 Wireless LAN > Security: WEP

LABEL	DESCRIPTION
Encryption	Select **WEP** to allow clients to associate this network with WEP authentication.
Key Length	Select **64-bit** or **128-bit**. This dictates the length of the security key that the network is going to use.
Key Format	Select **Hex** to enter hexadecimal characters as a WEP key. Select **ASCII** to enter ASCII characters as WEP key.
Encryption Key	The WEP keys are used to encrypt data. Both the NBG2105 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit** in the **Key Format** field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit** in the **Key Format** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
Show Password	Select this to show the encryption key on the screen.

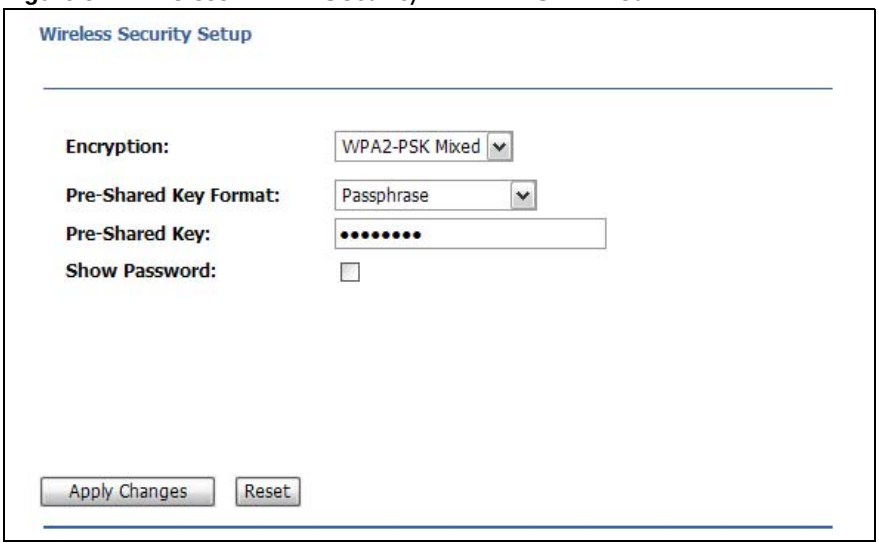
Table 42 Wireless LAN > Security: WEP (continued)

LABEL	DESCRIPTION
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.

13.5.3 WPA-PSK/WPA2-PSK/WPA2-PSK Mixed

Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK Mixed** from the **Encryption** list.

Figure 54 Wireless LAN > Security: WPA2-PSK Mixed



The following table describes the labels in this screen.

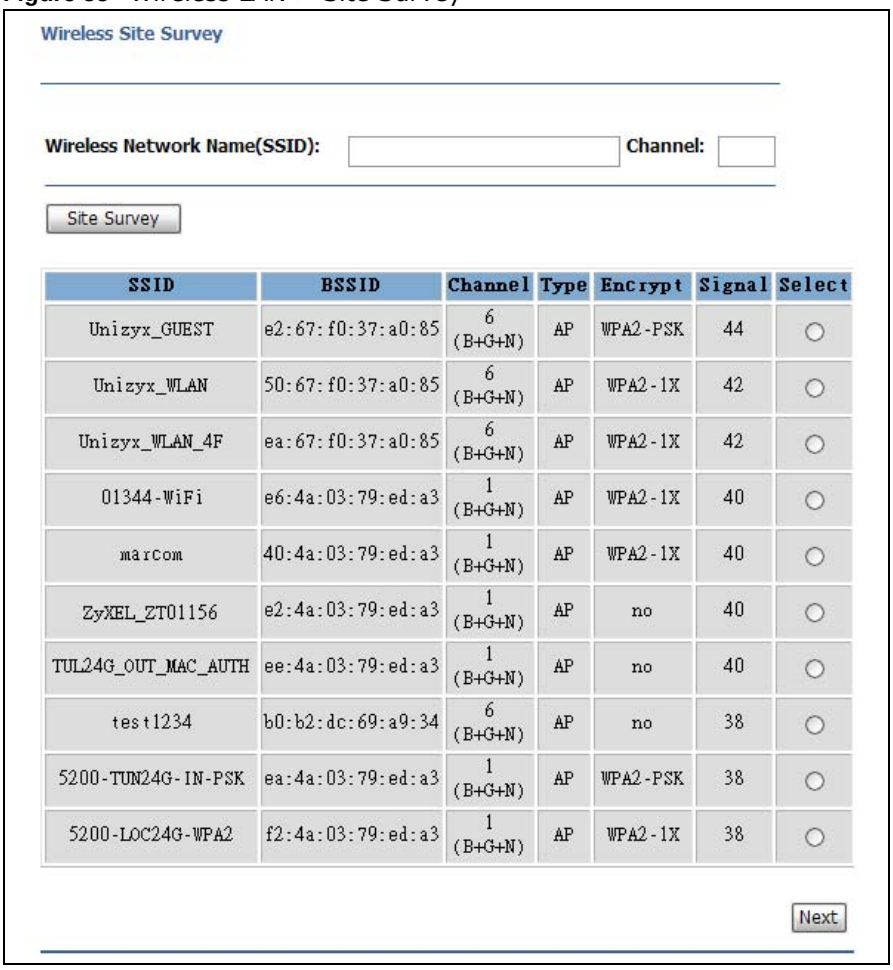
Table 43 Wireless LAN > Security: WPA-PSK, WPA2-PSK or WPA2-PSK Mixed

LABEL	DESCRIPTION
Encryption	Select **WPA-PSK**, **WPA2-PSK** or **WPA2-Mixed** to allow clients to associate this network with WPA-PSK, WPA2-PSK or either WPA-PSK or WPA2-PSK authentication.
Pre-Shared Key Format	Select **Passphrase** to make the NBG2105 generate a key from a phrase typed into the **Pre-Shared Key** field. Select **HEX** to configure the NBG2105 to accept a key in hexadecimal format in the **Pre-Shared Key** field.
Pre-Shared Key	If **Passphrase** was selected in the **Pre-Shared Key Format** field, type a pre-shared key from 8 to 63 case-sensitive keyboard characters. If **HEX** was selected in the **Pre-Shared Key Format** field, type a pre-shared key using hexadecimal characters ("0-9", "A-F").
Show Password	Select this to show the pre-shared key on the screen.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.

13.6 Site Survey Screen

Use this screen to scan for and connect to a wireless network automatically. Go to **Wireless LAN > Site Survey** to open the following screen. This screen is available only when the NBG2105 is in WISP+UR or Client mode.

Figure 55 Wireless LAN > Site Survey



The following table describes the labels in this screen.

Table 44 Wireless LAN > Site Survey

LABEL	DESCRIPTION
Wireless Network Name (SSID)	Enter the SSID of the AP to which you want the NBG2105 in WISP+UR mode or client mode to connect.
Channel	Enter the channel number used by the wireless device to which the NBG2105 is connecting.
Site Survey	Click this to search for available wireless devices within transmission range and update this table.
SSID	This shows the SSID of the wireless device.
BSSID	This shows the MAC address of the wireless device.
Channel	This shows the channel number and wireless standard used by this wireless device.
Type	This shows the type of device found in the survey.

Table 44 Wireless LAN > Site Survey (continued)

LABEL	DESCRIPTION
Encrypt	This displays the data encryption and authentication method used by this wireless device.
Signal	This displays the strength of the wireless signal. The signal strength mainly depends on the antenna output power and the distance between your NBG2105 and this device.
Select	Click this to select a device.
Next	Click this to open a screen to configure wireless security options.

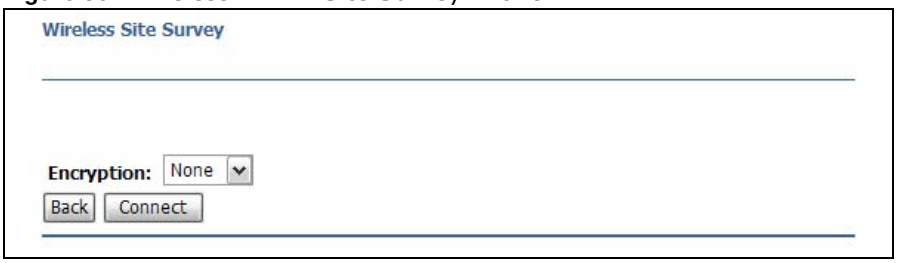
13.7 Site Survey: Wireless Security

The screen varies depending on what you select in the **Encryption** field.

13.7.1 None

Select **None** if the NBG2105 can communicate with the selected access point without any data encryption.

Figure 56 Wireless LAN > Site Survey: None



The following table describes the labels in this screen.

Table 45 Wireless LAN > Site Survey: None

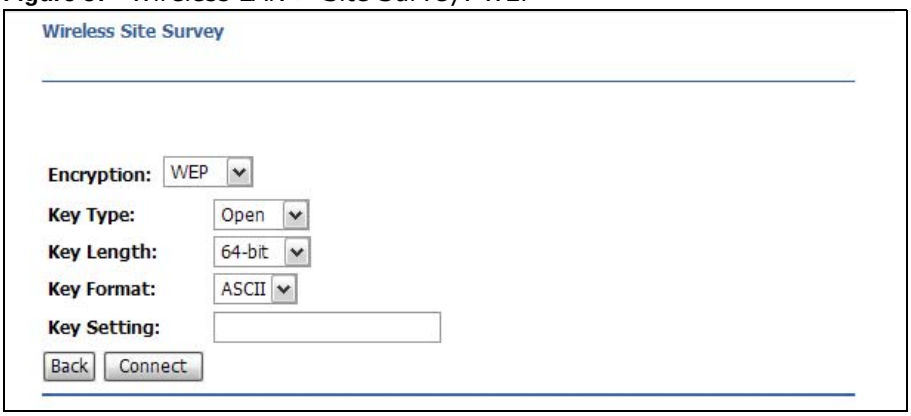
LABEL	DESCRIPTION
Encryption	Select **None** if the NBG2105 can communicate with the selected access point without any data encryption.
Back	Click this to go back to the initial site survey screen.
Connect	Click this to associate the NBG2105 with the selected access point.

13.7.2 WEP Encryption

Your NBG2105 can associate with APs that use 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

Select **WEP** from the **Encryption** list.

Figure 57 Wireless LAN > Site Survey: WEP



The following table describes the labels in this screen.

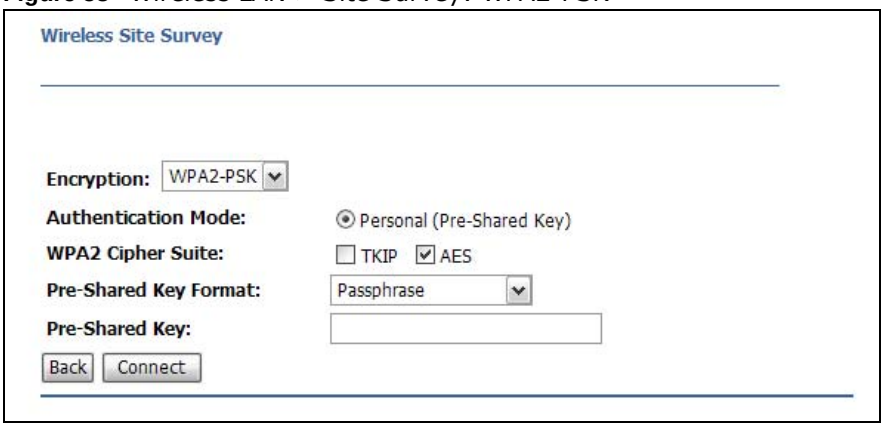
Table 46 Wireless LAN > Site Survey: WEP

LABEL	DESCRIPTION
Encryption	Select **WEP** to associate with the selected AP using WEP authentication.
Key Type	Select **Open**, **Shared** or **Both**. This field specifies whether the NBG2105 must provide a WEP key to login to the selected access point.
Key Length	Select **64-bit** or **128-bit**. This dictates the length of the security key that selected access point is using.
Key Format	Select **ASCII** to enter ASCII characters as a WEP key. Select **Hex** to enter hexadecimal characters as a WEP key.
Key Setting	The WEP keys are used to encrypt data. Both the NBG2105 and the access point must use the same WEP key for data transmission. If you chose **64-bit** in the **Key Format** field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit** in the **Key Format** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
Back	Click this to go back to the initial site survey screen.
Connect	Click this to associate the NBG2105 with the selected access point.

13.7.3 WPA-PSK/WPA2-PSK Encryption

Select **WPA-PSK** or **WPA2-PSK** from the **Encryption** list.

Figure 58 Wireless LAN > Site Survey: WPA2-PSK



The following table describes the labels in this screen.

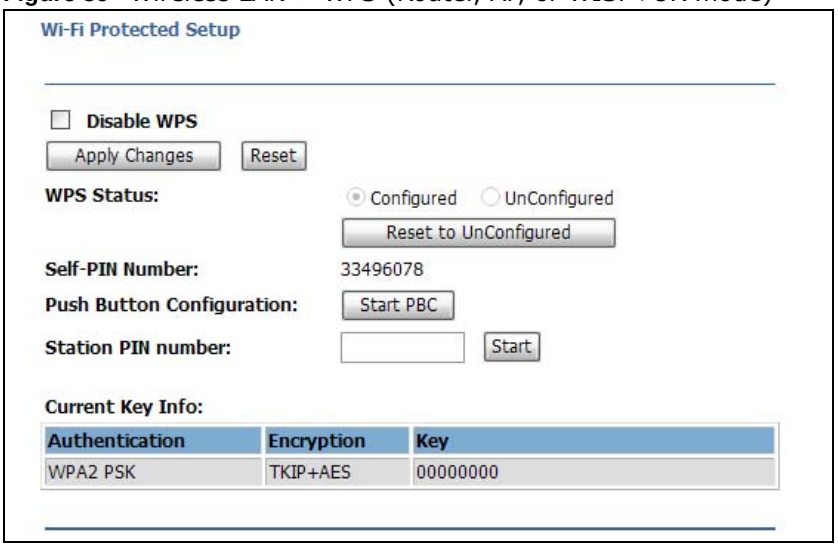
Table 47 Wireless LAN > Site Survey: WPA-PSK or WPA2-PSK

LABEL	DESCRIPTION
Encryption	Select **WPA-PSK** or **WPA2-PSK** to associate with the selected AP using WPA-PSK or WPA2-PSK.
Authentication Mode	**Personal (Pre-Shared Key)** is selected to use a simple common password for authentication.
WPA Cipher Suite	Select **TKIP** and/or **AES** to configure which encryption options the NBG2105 uses to connect to the selected access point. This appears when **WPA** encryption is selected.
WPA2 Cipher Suite	Select **TKIP** and/or **AES** to configure which encryption options the NBG2105 uses to connect to the selected access point. This appears when **WPA2** encryption is selected.
Pre-Shared Key Format	Select **Passphrase** to make the NBG2105 generate a key from a phrase typed into the **Pre-Shared Key** field. Select **HEX** to configure the NBG2105 to accept a key in hexadecimal format in the **Pre-Shared Key** field.
Pre-Shared Key	If **Passphrase** was selected in the **Pre-Shared Key Format** field, type a pre-shared key from 8 to 63 case-sensitive keyboard characters. If **HEX** was selected in the **Pre-Shared Key Format** field, type a pre-shared key using hexadecimal characters ("0-9", "A-F").
Back	Click this to go back to the initial site survey screen.
Connect	Click this to associate the NBG2105 with the selected access point.

13.8 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Wireless LAN** > **WPS**. The screen varies depending on the operation mode in which the NBG2105 is working.

Figure 59 Wireless LAN > WPS (Router, AP, or WISP+UR mode)



The following table describes the labels in this screen.

Table 48 Wireless LAN > WPS (Router, AP, or WISP+UR mode)

LABEL	DESCRIPTION
Disable WPS	Select this to turn off the WPS feature.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.
WPS Status	This displays **Configured** when the NBG2105 has connected to a wireless network using WPS or when WPS is enabled and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there are no wireless or wireless security changes on the NBG2105 or you click **Release Configuration** to remove the configured wireless and wireless security settings.
Reset to UnConfigured	This button is only available when the WPS status displays **Configured**. Click this button to remove all configured wireless and wireless security settings for WPS connections on the NBG2105.
Self PIN Number	This is the WPS PIN (Personal Identification Number) of the NBG2105. Enter this PIN in the configuration utility of the device you want to connect to the NBG2105 using WPS. The PIN is not necessary when you use WPS push-button method.
Start PBC	Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
Station PIN number	Type the same PIN number generated in the wireless station's utility. Then click **Start** to associate to each other and perform the wireless security information synchronization.
Start	Use this button when you use the PIN Configuration method to configure wireless station's wireless settings.
Current Key Info.	
Authentication	This shows the current authentication method being used by WPS.
Encryption	This shows the current encryption method being used by WPS.
Key	This shows the current encryption key being used by WPS.

Figure 60 Wireless LAN > WPS (Client mode)

The following table describes the labels in this screen.

Table 49 Wireless LAN > WPS (Client mode)

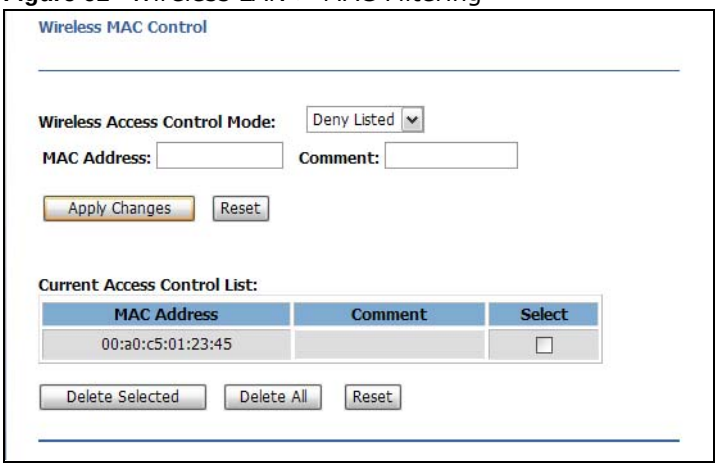
LABEL	DESCRIPTION
Disable WPS	Select this to turn off the WPS feature.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.
Self PIN Number	This is the WPS PIN (Personal Identification Number) of the NBG2105. Enter this PIN in the configuration utility of the device you want to connect to the NBG2105 using WPS. The PIN is not necessary when you use WPS push-button method.
Start	Use this button when the AP to which the NBG2105 is connecting uses the PIN Configuration method to configure wireless station's wireless settings. Click **Start** to associate to each other and perform the wireless security information synchronization.
Start PBC	Use this button when the AP to which the NBG2105 is connecting uses the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. Click **Start PBC** to start WPS-aware wireless station scanning and the wireless security information synchronization.

13.9 MAC Filtering Screen

The MAC filter screen allows you to configure the NBG2105 to give exclusive access to devices (**Allow Listed**) or exclude devices from accessing the NBG2105 (**Deny Listed**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your NBG2105's MAC filter settings, click **Wireless LAN** > **MAC Filtering**.

Figure 61 Wireless LAN > MAC Filtering



The following table describes the labels in this screen.

Table 50 Wireless LAN > MAC Filtering

LABEL	DESCRIPTION
Wireless Access Control Mode	Select **Disable** to turn off MAC address filtering, or define the filter action for the list of MAC addresses in the **Current Access Control List**. Select **Allow Listed** to permit access to the NBG2105, MAC addresses not listed will be denied access to the NBG2105. Select **Deny Listed** to block access to the NBG2105, MAC addresses not listed will be allowed to access the NBG2105.
MAC Address	Enter the MAC address for this access control entry.
Comment	Enter a description of this access control entry.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.
Current Access Control List	
MAC Address	This shows the MAC address of the wireless station that is allowed or denied access to the NBG2105.
Comment	This shows a description of this access control entry.
Select	Click this to select this rule.
Delete Selected	Click this to delete the selected rules.
Delete All	Click this to delete all rules.
Reset	Click this to reset all selections.

14

Firewall

14.1 Overview

This chapter shows you how to enable and configure the NBG2105 firewall settings.

The NBG2105 firewall is a packet filtering firewall and restricts access based on the source/ destination computer network address of a packet and the type of application.

14.2 What You Can Do

- Use the **Port Filtering** screen to apply filtering based on UDP or TCP port numbers (Section 14.4 on page 100).
- Use the **IP Filtering** screen to apply filtering based on IP addresses (Section 14.5 on page 101).
- Use the **MAC Filtering** to apply filtering based on MAC addresses (Section 14.6 on page 101).
- Use the **URL Filtering** to apply filtering based on URLs (Section 14.7 on page 102).

14.3 What You Need To Know

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

What is a Firewall?

A "firewall" is a system or group of systems that enforces an access-control policy between two networks. Of course, firewalls cannot solve every security problem.

Guidelines For Enhancing Security

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.

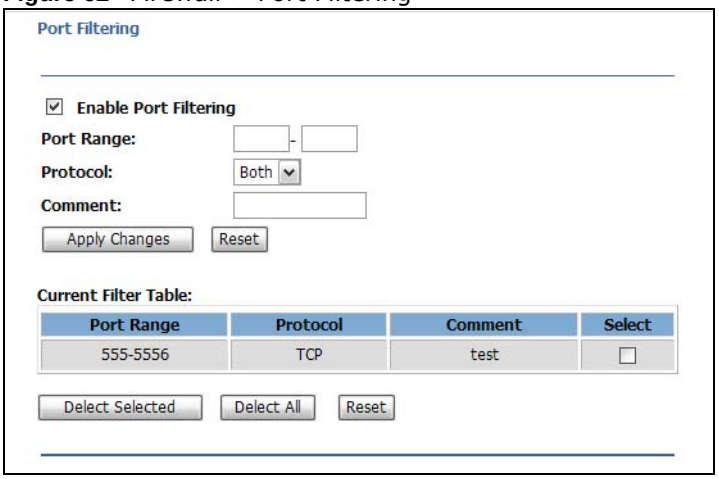
5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.

6 Keep the NBG2105 in a secured (locked) room.

14.4 Port Filtering Screen

Click **Firewall** > **Port Filtering** to apply filtering based on UDP or TCP port numbers.

Figure 62 Firewall > Port Filtering



The following table describes the labels in this screen.

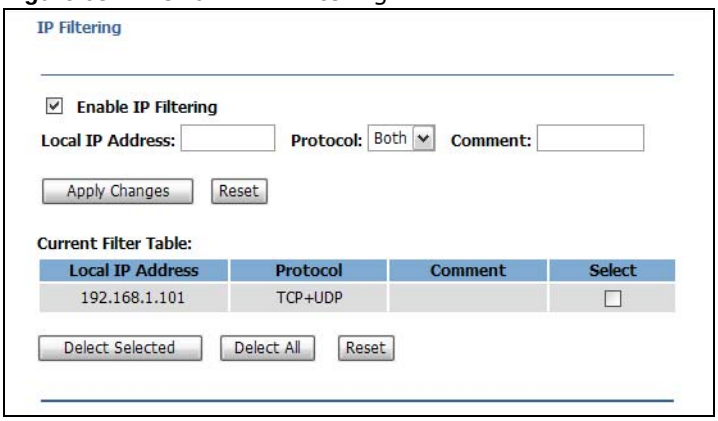
Table 51 Firewall > Port Filtering

LABEL	DESCRIPTION
Enable Port Filtering	Click this to apply filtering based on UDP or TCP port numbers.
Port Range	Enter the port number or range of ports that define the traffic type. For example TCP port 80 defines web traffic.
Protocol	Select **TCP** to filter on TCP ports, **UDP** to filter on UDP ports or **Both** to filter on both TCP and UDP ports.
Comment	Enter a description of this rule.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.
Current Filter Table	
Port Range	This shows the port number or range of ports that define the traffic type. For example TCP port 80 defines web traffic.
Protocol	This shows **TCP** for TCP port filtering, **UDP** for UDP port filtering or **Both** for TCP and UDP port filtering.
Comment	Enter a description of this rule.
Select	Click this to select this rule.
Delete Selected	Click this to delete the selected rules.
Delete All	Click this to delete all rules.
Reset	Click this to reset all selections.

14.5 IP Filtering Screen

Click **Firewall** > **IP Filtering** to apply filtering based on IP addresses.

Figure 63 Firewall > IP Filtering



The following table describes the labels in this screen.

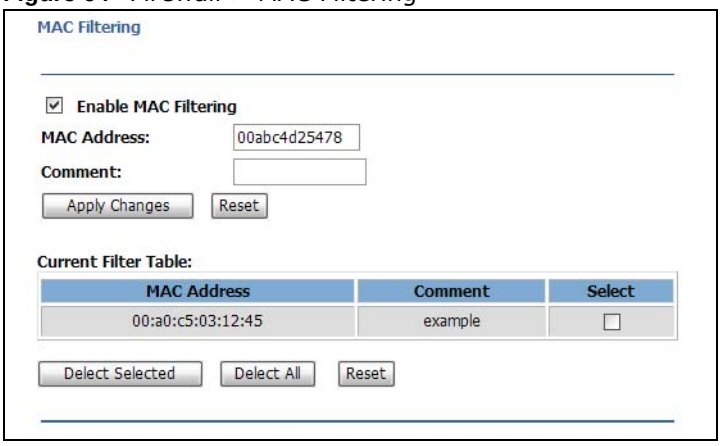
Table 52 Firewall > IP Filtering

LABEL	DESCRIPTION
Enable IP Filtering	Click this to apply filtering based on IP addresses.
Local IP Address	Enter the source IP address of outgoing packets or the destination IP address of incoming packets that this rule matches.
Protocol	Select **TCP** to filter on TCP packets, **UDP** to filter on UDP packets or **Both** to filter on both TCP and UDP packets.
Comment	Enter a description of this rule.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.
Current Filter Table	
Local IP Address	This shows the source IP address of outgoing packets or the destination IP address of incoming packets that this rule matches.
Protocol	This shows **TCP** for TCP port filtering, **UDP** for UDP port filtering or **Both** for TCP and UDP port filtering.
Comment	Enter a description of this rule.
Select	Click this to select this rule.
Delete Selected	Click this to delete the selected rules.
Delete All	Click this to delete all rules.
Reset	Click this to reset all selections.

14.6 MAC Filtering Screen

Click **Firewall** > **MAC Filtering** to apply filtering based on MAC addresses.

Figure 64 Firewall > MAC Filtering



The following table describes the labels in this screen.

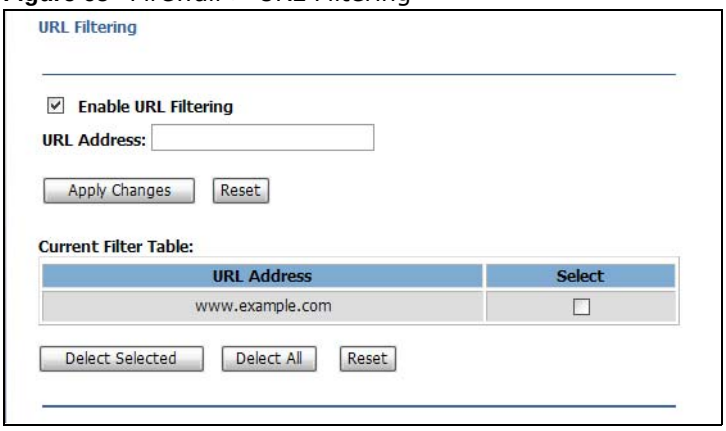
Table 53 Firewall > MAC Filtering

LABEL	DESCRIPTION
Enable MAC Filtering	Click this to apply filtering based on MAC addresses.
MAC Address	Enter the source MAC address of outgoing packets or the destination MAC address of incoming packets that this rule matches.
Comment	Enter a description of this rule.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.
Current Filter Table	
MAC Address	This shows the source MAC address of outgoing packets or the destination MAC address of incoming packets that this rule matches.
Comment	Enter a description of this rule.
Select	Click this to select this rule.
Delete Selected	Click this to delete the selected rules.
Delete All	Click this to delete all rules.
Reset	Click this to reset all selections.

14.7 URL Filtering Screen

Click **Firewall** > **URL Filtering** to apply filtering based on URLs.

Figure 65 Firewall > URL Filtering



The following table describes the labels in this screen.

Table 54 Firewall > URL Filtering

LABEL	DESCRIPTION
Enable URL Filtering	Click this to apply filtering based on URLs.
URL Address	Enter the URL that this rule matches.
Comment	Enter a description of this rule.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.
Current Filter Table	
URL Address	This shows the source URL that this rule matches.
Select	Click this to select this rule.
Delete Selected	Click this to delete the selected rules.
Delete All	Click this to delete all rules.
Reset	Click this to reset all selections.

15

Management

15.1 Overview

This chapter describes the **Management** screens.

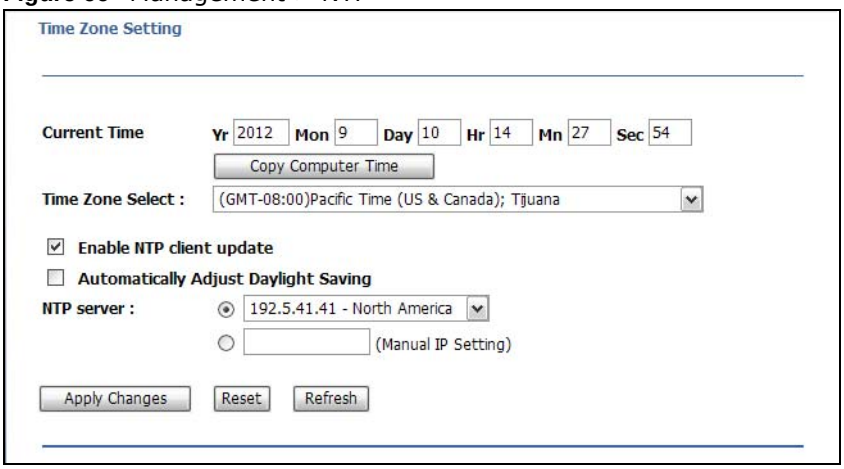
15.2 What You Can Do

- Use the **NTP** screen to change your NBG2105's time and date (Section 15.3 on page 105).
- Use the **Password** screen to change your NBG2105's system password (Section 15.4 on page 106).
- Use the **Upgrade Firmware** screen to upload firmware to your NBG2105 (Section 15.5 on page 107).
- Use the **Backup / Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration (Section 15.6 on page 108).
- Use the **Operation** screen to select how you want to use your NBG2105 (Section 15.7 on page 109).
- Use the **Language** screen to change the language for the Web Configurator (Section 15.8 on page 109).
- Use the **Reboot** screen to reboot the NBG2105 without turning the power off (Section 15.9 on page 110).

15.3 NTP Screen

Use this screen to configure the NBG2105's time based on your local time zone. To change your NBG2105's time and date, click **Management** > **NTP**.

Figure 66 Management > NTP



The following table describes the labels in this screen.

Table 55 Management > NTP

LABEL	DESCRIPTION
Current Time	Enter the current time, or click **Copy Computer Time** to use your computer to set the time.
Copy Computer Time	Click this to use your computer to set the time.
Time Zone Select	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable NTP client update	Select this to configure the NBG2105 to update its time from an NTP server automatically.
Automatically Adjust Daylight Saving	Select this to configure the NBG2105 to automatically change the time according to daylight saving conventions in your time zone. 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.
NTP Server	Select an NTP server, closest to you, or manually enter the IP address of an NTP server.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.
Refresh	Click this to update the screen.

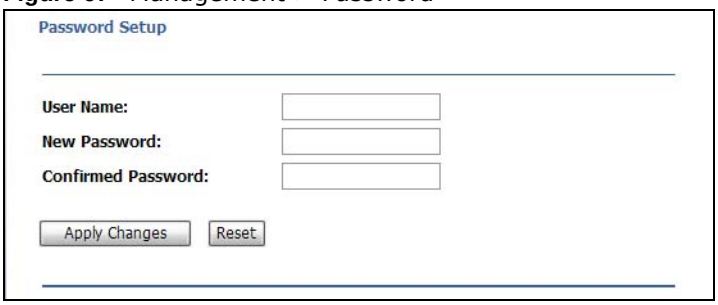
15.4 Password Screen

It is strongly recommended that you change your NBG2105's password.

Note: If you forget your NBG2105's password (or IP address), you will need to reset the device. See Section 1.5.1 on page 14 for details.

Click **Management** > **Password**.

Figure 67 Management > Password



The following table describes the labels in this screen.

Table 56 Management > Password

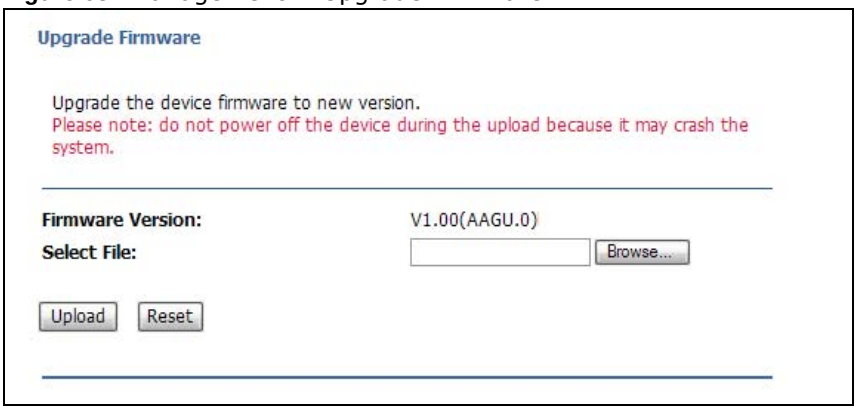
LABEL	DESCRIPTION
User Name	Enter your new user name.
New Password	Enter your new system password. Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Confirmed Password	Enter the new password again in this field.
Apply Changes	Click this to save changes back to the NBG2105.
Reset	Click this to begin configuring this screen afresh.

15.5 Upgrade Firmware 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(AAAGU.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 **Management** > **Upgrade Firmware**. Follow the instructions in this screen to upload firmware to your NBG2105.

Figure 68 Management > Upgrade Firmware



The following table describes the labels in this screen.

Table 57 Management > Upgrade Firmware

LABEL	DESCRIPTION
Firmware Version	This shows the current firmware version installed on the NBG2105.
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.
Reset	Click this to begin configuring this screen afresh.

Note: Do not turn off the NBG2105 while firmware upload is in progress!

The NBG2105 automatically restarts in this time causing a temporary network disconnect.

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

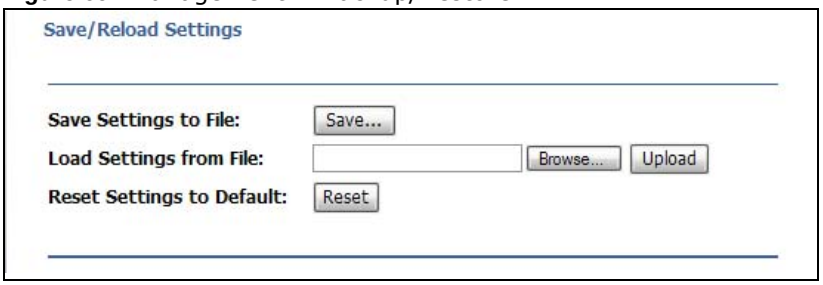
15.6 Backup/Restore Screen

Backup configuration allows you to back up (save) the NBG2105's current configuration to a file on your computer. Once your NBG2105 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 NBG2105.

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

Figure 69 Management > Backup/Restore



The following table describes the labels in this screen.

Table 58 Management > Backup/Restore

LABEL	DESCRIPTION
Save Settings to File	Click **Save...** to save the NBG2105's current configuration to your computer.
Load Settings from File	
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 58 Management > Backup/Restore (continued)

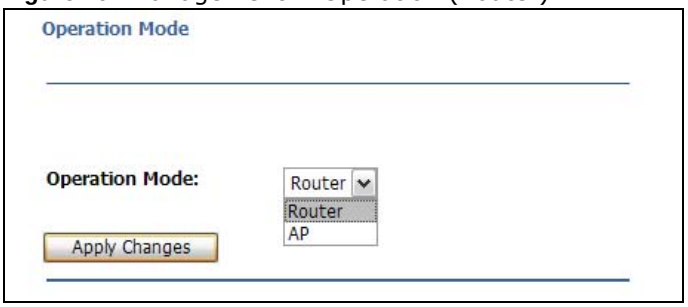
LABEL	DESCRIPTION
Upload	Click this to begin the upload process. Note: Do not turn off the NBG2105 while configuration file upload is in progress. After you see a "configuration upload successful" screen, you must then wait one minute before logging into the NBG2105 again. The NBG2105 automatically restarts in this time causing a temporary network disconnect. If you see an error screen, click Back to return to the Backup/Restore screen.
Reset Settings to Default	
Reset	Click this to clear all user-entered configuration information and return the NBG2105 to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your NBG2105. 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 NBG2105 IP address.

15.7 Router Operation Mode Screen

The NBG2105 can be configured as a wireless router or just an AP when in router mode. Click **Management > Operation**.

Figure 70 Management > Operation (Router)



The following table describes the labels in this screen.

Table 59 Management > Operation (Router)

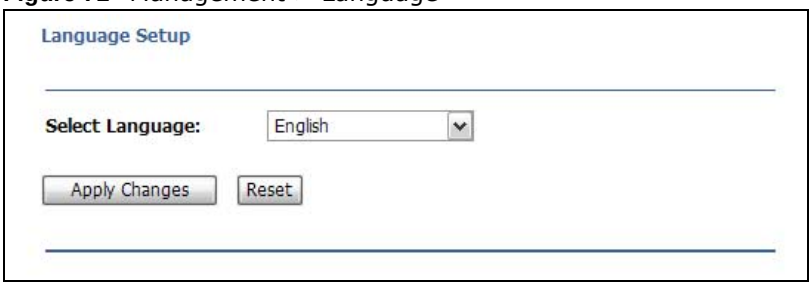
LABEL	DESCRIPTION
Operation Mode	Select **Router** to configure the NBG2105 as a wireless router or **AP** to configure the NBG2105 as an AP only.
Apply Changes	Click this to save changes back to the NBG2105.

15.8 Language Screen

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

Select the language you prefer and click **Apply Changes**. The Web Configurator language changes after a while without restarting the NBG2105.

Figure 71 Management > Language

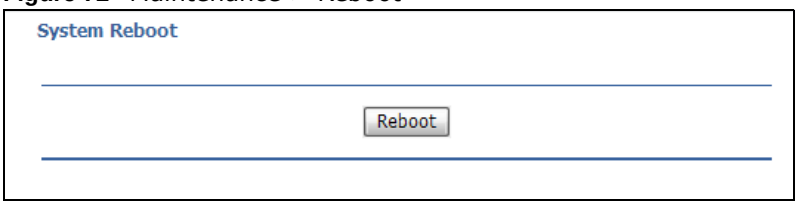


15.9 Restart Screen

System restart allows you to reboot the NBG2105 without turning the power off.

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

Figure 72 Maintenance > Reboot



Click **Reboot** to have the NBG2105 restart. This does not affect the NBG2105's configuration.

16

Status

16.1 Overview

This chapter describes how to show the general status of the NBG2105 as well as statistics and logs collected by the NBG2105.

16.2 What You Can Do

- Use the **Status** screen to view system, wireless, local and WAN network information, as well as general information about the NBG2105.
- Use the **Statistics** screen to show the number of packets sent and received on the Wireless LAN and Ethernet WAN interfaces.
- Use the **Log** screen to look at all of the NBG2105's logs in one location.

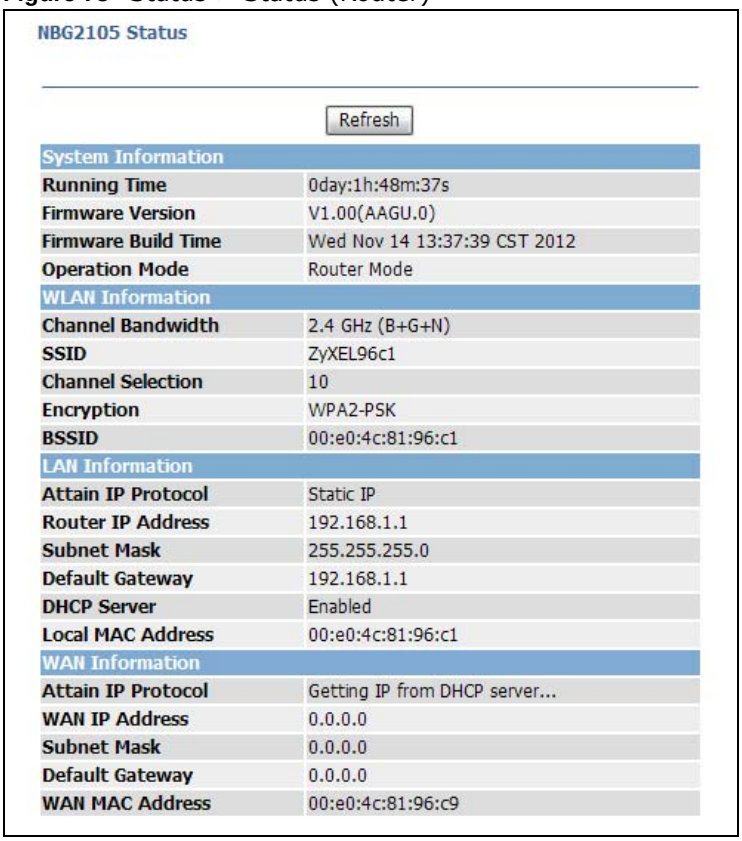
16.3 Status Screen

Click **Status** > **Status**. The screen that appears depends on which mode the NBG2105 is in.

16.3.1 Router Mode

The combination of fields on the following screen appear only in router mode.

Figure 73 Status > Status (Router)



The following table describes the labels in this screen.

Table 60 Status > Status (Router)

LABEL	DESCRIPTION
System Information	
Running Time	This shows how long the NBG2105 has been running.
Firmware Version	This shows the currently running firmware version.
Firmware Build Time	This shows when the currently running firmware was compiled.
Operation Mode	This shows which mode the NBG2105 is in.
WLAN Information	
Channel Bandwidth	This shows which frequency band and wireless mode your network uses.
SSID	This shows a descriptive name used to identify the NBG2105 in the wireless LAN.
Channel Selection	This shows the channel number.
Encryption	This shows the type of wireless encryption the NBG2105 is using.
BSSID	This shows the wireless adapter MAC Address of your device.
LAN Information	
Attain IP Protocol	This shows how the LAN interface gets its IP configuration.
Router IP Address	This shows the LAN interface’s IP address.
Subnet Mask	This shows the LAN interface’s subnet mask.
Default Gateway	This shows the IP address of the LAN interface’s default gateway.
DHCP Server	This shows whether the DHCP server is enabled or not.

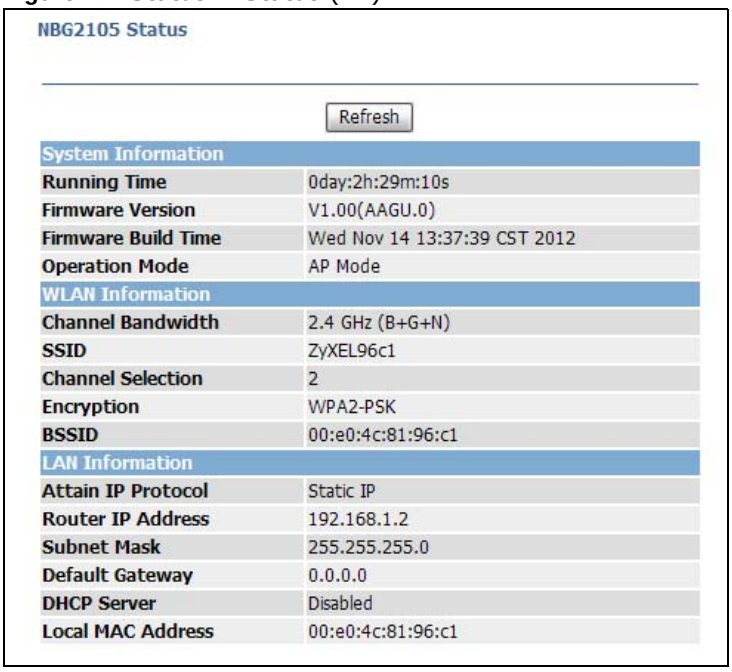
Table 60 Status > Status (Router) (continued)

LABEL	DESCRIPTION
Local MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
WAN Information	
Attain IP Protocol	This shows how the WAN interface gets its IP configuration.
WAN IP Address	This shows the WAN interface's IP address.
Subnet Mask	This shows the WAN interface's subnet mask.
Default Gateway	This shows the WAN interface's gateway IP address.
WAN MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.

16.3.2 AP Mode

The combination of fields on the following screen appear only in AP mode.

Figure 74 Status > Status (AP)



The following table describes the labels in this screen.

Table 61 Status > Status (AP)

LABEL	DESCRIPTION
System Information	
Running Time	This shows how long the NBG2105 has been running.
Firmware Version	This shows the currently running firmware version.
Firmware Build Time	This shows when the currently running firmware was compiled.
Operation Mode	This shows which mode the NBG2105 is in.
WLAN Information	
Channel Bandwidth	This shows which frequency band and wireless mode your network uses.
SSID	This shows a descriptive name used to identify the NBG2105 in the wireless LAN.

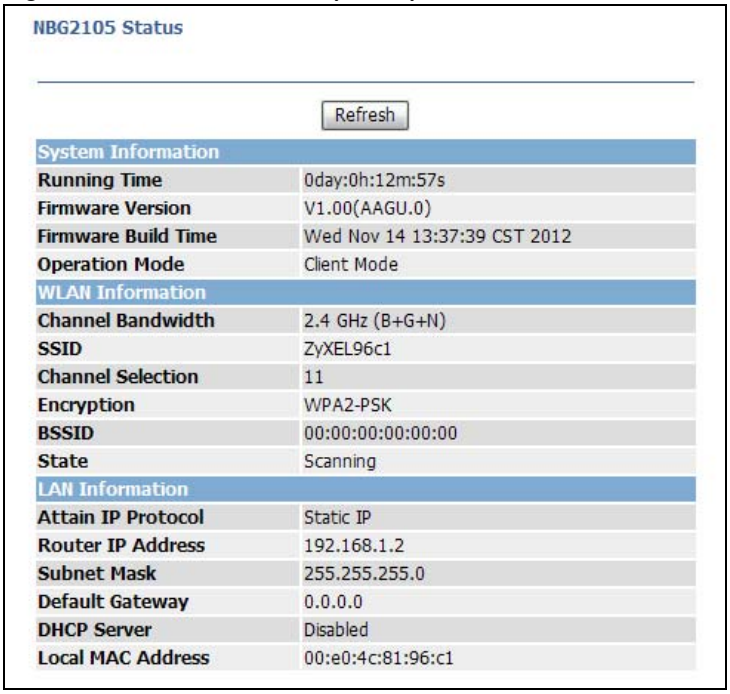
Table 61 Status > Status (AP) (continued)

LABEL	DESCRIPTION
Channel Selection	This shows the channel number.
Encryption	This shows the type of wireless encryption the NBG2105 is using.
BSSID	This shows the wireless adapter MAC Address of your device.
LAN Information	
Attain IP Protocol	This shows how the LAN interface gets its IP configuration.
Router IP Address	This shows the LAN interface's IP address.
Subnet Mask	This shows the LAN interface's subnet mask.
Default Gateway	This shows the IP address of the LAN interface's default gateway.
DHCP Server	This shows whether the DHCP server is enabled or not.
Local MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.

16.3.3 Client Mode

The combination of fields on the following screen appear only in Client mode.

Figure 75 Status > Status (Client)



The following table describes the labels in this screen.

Table 62 Status > Status (Client)

LABEL	DESCRIPTION
System Information	
Running Time	This shows how long the NBG2105 has been running.
Firmware Version	This shows the currently running firmware version.
Firmware Build Time	This shows when the currently running firmware was compiled.

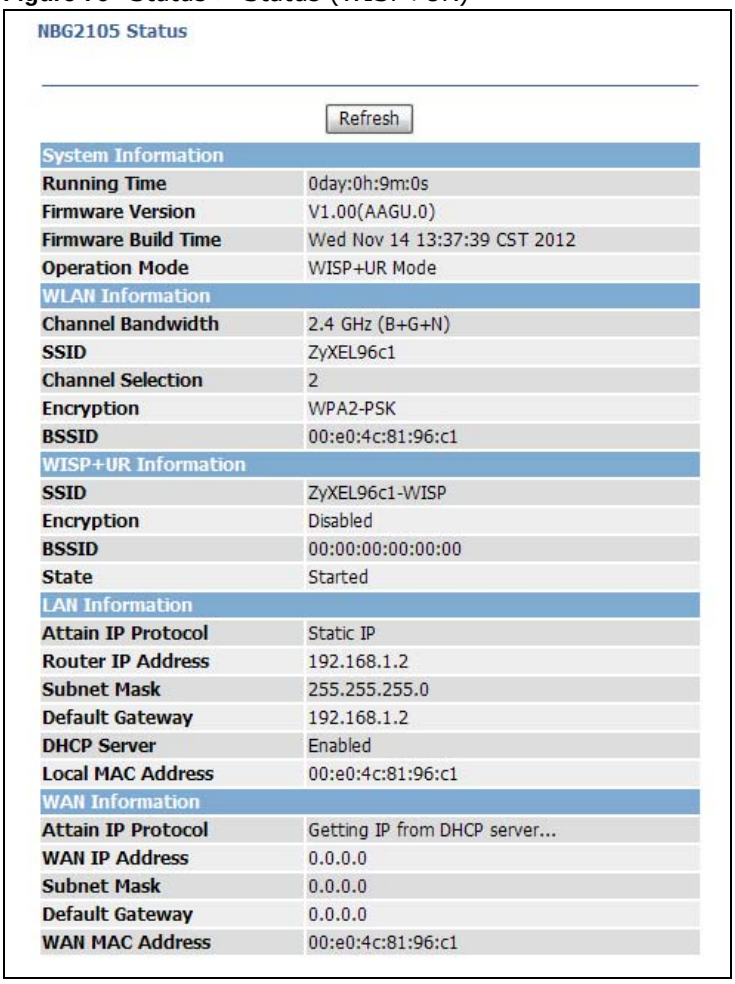
Table 62 Status > Status (Client) (continued)

LABEL	DESCRIPTION
Operation Mode	This shows which mode the NBG2105 is in.
WLAN Information	
Channel Bandwidth	This shows which frequency band and wireless mode your network uses.
SSID	This shows the wireless network name of the AP to which the NBG2105 is connecting.
Channel Selection	This shows the channel number.
Encryption	This shows the type of wireless encryption the NBG2105 is using.
BSSID	This shows the wireless adapter MAC Address of your device.
State	This shows the whether the NBG2105 is scanning the network or not.
LAN Information	
Attain IP Protocol	This shows how the LAN interface gets its IP configuration.
Router IP Address	This shows the LAN interface's IP address.
Subnet Mask	This shows the LAN interface's subnet mask.
Default Gateway	This shows the IP address of the LAN interface's default gateway.
DHCP Server	This shows whether the DHCP server is enabled or not.
Local MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.

16.3.4 WISP+UR Mode

The combination of fields on the following screen appear only in WISP+UR mode.

Figure 76 Status > Status (WISP+UR)



The following table describes the labels in this screen.

Table 63 Status > Status (WISP+UR)

LABEL	DESCRIPTION
System Information	
Running Time	This shows how long the NBG2105 has been running.
Firmware Version	This shows the currently running firmware version.
Firmware Build Time	This shows when the currently running firmware was compiled.
Operation Mode	This shows which mode the NBG2105 is in.
WLAN Information	
Channel Bandwidth	This shows which frequency your network uses.
SSID	This shows the wireless network name of the AP to which the NBG2105 is connecting.
Channel Selection	This shows the channel number.
Encryption	This shows the type of wireless encryption the NBG2105 is using.
BSSID	This shows the wireless adapter MAC Address of your device.
WISP+UR Information	
SSID	This shows the wireless network name of the AP to which the NBG2105 is connecting.
Encryption	This shows the type of wireless encryption the NBG2105 is using.

Table 63 Status > Status (WISP+UR) (continued)

LABEL	DESCRIPTION
BSSID	This shows the wireless adapter MAC Address of your device.
State	This shows what stage the NBG2105 is at with respect to connecting to access points.
LAN Information	
Attain IP Protocol	This shows how the LAN interface gets its IP configuration.
Router IP Address	This shows the LAN interface's IP address.
Subnet Mask	This shows the LAN interface's subnet mask.
Default Gateway	This shows the IP address of the LAN interface's default gateway.
DHCP Server	This shows whether the DHCP server is enabled or not.
Local MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
WAN Information	
Attain IP Protocol	This shows how the WAN interface gets its IP configuration.
WAN IP Address	This shows the WAN interface's IP address.
Subnet Mask	This shows the WAN interface's subnet mask.
Default Gateway	This shows the WAN interface's gateway IP address.
WAN MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.

16.4 Statistics Screen

This screen shows the number of packets sent and received on the Wireless LAN and Ethernet WAN interfaces. Click **Status** > **Statistics**. The screen that appears depends on which mode the NBG2105 is in.

Figure 77 Status > Statistics (Router)

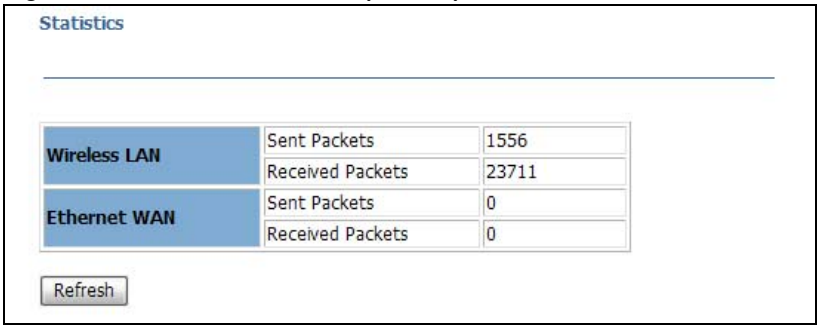


Figure 78 Status > Statistics (AP or Client)

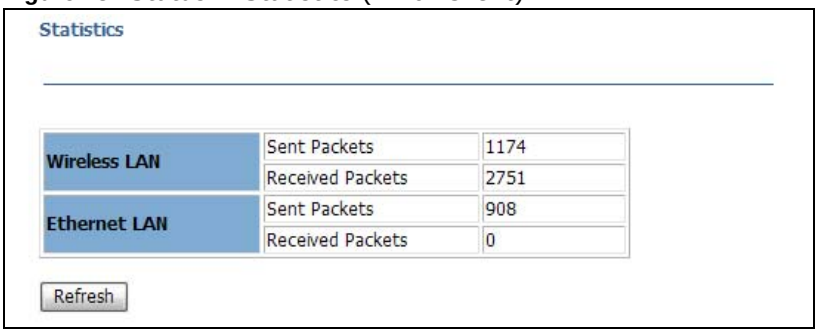


Figure 79 Status > Statistics (WISP+UR)

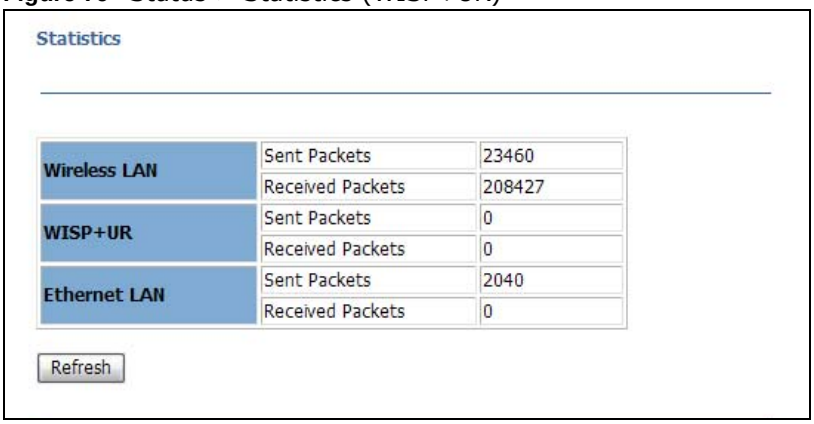


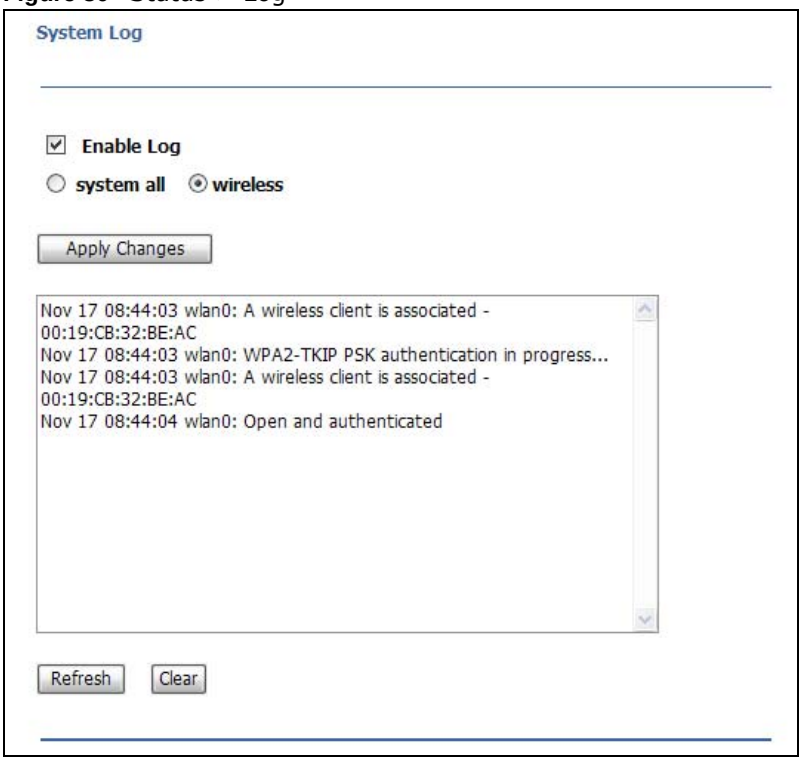
Table 64 Status > Statistics

LABEL	DESCRIPTION
Wireless LAN	
Sent Packets	This shows the number of packets sent through the wireless LAN interface.
Received Packets	This shows the number of packets received on the wireless LAN interface.
Ethernet WAN	
Sent Packets	This shows the number of packets sent through the Ethernet WAN interface.
Received Packets	This shows the number of packets received on the Ethernet WAN interface.
WISP+UR	
Sent Packets	This shows the number of packets sent through the wireless WAN interface.
Received Packets	This shows the number of packets received on the wireless WAN interface.
Ethernet LAN	
Sent Packets	This shows the number of packets sent through the Ethernet LAN interface.
Received Packets	This shows the number of packets received on the Ethernet LAN interface.

16.5 System Log Screen

The Web Configurator allows you to look at all of the NBG2105's logs in one location. Click **Status** > **Log**.

Figure 80 Status > Log



The following table describes the labels in this screen.

Table 65 Status > Log

LABEL	DESCRIPTION
Enable Log	Select this to enable logging.
system all	Select this to log all events, including wireless events.
wireless	Select this to log only wireless events.
Apply Changes	Click this to save changes back to the NBG2105.
Refresh	Click this to update the screen.
Clear	Click this to delete the log.

17

Troubleshooting

17.1 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
- NBG2105 Access and Login
- Internet Access
- Resetting the NBG2105 to Its Factory Defaults
- Wireless LAN Connections

17.2 Power, Hardware Connections, and LEDs

The NBG2105 does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor included with the NBG2105 or have connected the NBG2105 to a computer using a USB cable.
2. Make sure the power adaptor is connected to the NBG2105 and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor to the NBG2105.
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 1.8.1 on page 17.
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 NBG2105.
5. If the problem continues, contact the vendor.

17.3 NBG2105 Access and Login

I don't know the IP address of my NBG2105.

1. The default IP address of the NBG2105 in **Router** mode is **192.168.1.1**. The default IP address of the NBG2105 in other modes is **192.168.1.2**.
2. If you changed the IP address and have forgotten it, you might get the IP address of the NBG2105 (in Router or WISP+UR 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 NBG2105 (it depends on the network), so enter this IP address in your Internet browser.
3. If your NBG2105 (in Router, AP or WISP+UR mode) is a DHCP client and obtains a dynamic IP address from a DHCP server, use the domain name "zyxelsetup.com" to access the NBG2105.
4. Reset your NBG2105 to change all settings back to their default. This means your current settings are lost. See Section 17.5 on page 124 in the **Troubleshooting** for information on resetting your NBG2105.

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 17.5 on page 124.

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 NBG2105 in **Router** mode is **192.168.1.1**. The default IP address of the NBG2105 in other modes is **192.168.1.2**.
   - If you changed the IP address, 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 NBG2105.
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 127.
4. Make sure your computer is in the same subnet as the NBG2105.

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 9.4 on page 70.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG2105. See Section 9.4 on page 70.

5 Reset the device to its factory defaults, and try to access the NBG2105 with the default IP address. See Section 1.5 on page 14.

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

I can see the **Login** screen, but I cannot log in to the NBG2105.

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 USB cable to restart the NBG2105.

4 If this does not work, you have to reset the device to its factory defaults. See Section 1.5.1 on page 14.

17.4 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 Check your Operation Mode setting.

- If the NBG2105 is in **Router** mode make sure the WAN port is connected to a broadband modem or router with Internet access. Your computer and the NBG2105 should be in the same subnet.
- If the NBG2105 is in **Access Point** mode, make sure the Ethernet port is connected to a broadband modem or router with Internet access and your computer is set to obtain an dynamic IP address.
- If the NBG2105 is in **Client** mode, make sure the NBG2105 is wirelessly connected to an access point or wireless router with Internet access. Your computer should be set to obtain an dynamic IP address.
- If the NBG2105 is in **WISP + UR** mode, make sure the NBG2105 is wirelessly connected to an access point or wireless router with Internet access.

3 If the NBG2105 is in **Router** or **WISP+UR** 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 NBG2105), 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 1.8.1 on page 17.

2 Reboot the NBG2105.

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 1.8.1 on page 17. If the NBG2105 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 NBG2105 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 NBG2105.

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.

17.5 Resetting the NBG2105 to Its Factory Defaults

If you reset the NBG2105, you lose all of the changes you have made. The NBG2105 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 NBG2105:

1. Make sure the power LED is on.
2. Press the **RESET** button for longer than five seconds to set the NBG2105 back to its factory-default configurations.

   If the NBG2105 restarts automatically, wait for the NBG2105 to finish restarting, and log in to the Web Configurator. The password is "1234".

   If the NBG2105 does not restart automatically, disconnect and reconnect the NBG2105's power. Then, follow the directions above again.

17.6 Wireless LAN Connections

I cannot access the NBG2105 or ping any computer from the WLAN.

1. Make sure the wireless LAN is enabled on the NBG2105 and the NBG2105 is working in Router, AP or WISP+UR mode.
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 NBG2105.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG2105.
5. Check that both the NBG2105 and the wireless adapter on your computer are using the same wireless and wireless security settings.

I cannot access the Web Configurator after I switched from router mode to another mode.

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

The management IP address of the NBG2105 in other modes is 192.168.1.2.

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.

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

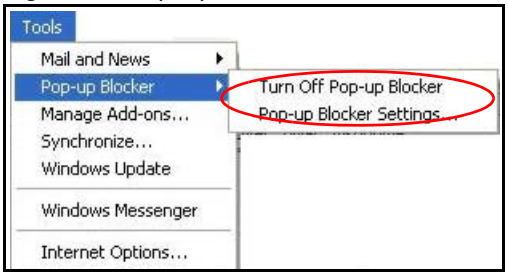
You may have to disable pop-up blocking to log into your device.

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 81 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 82 Internet Options: Privacy

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

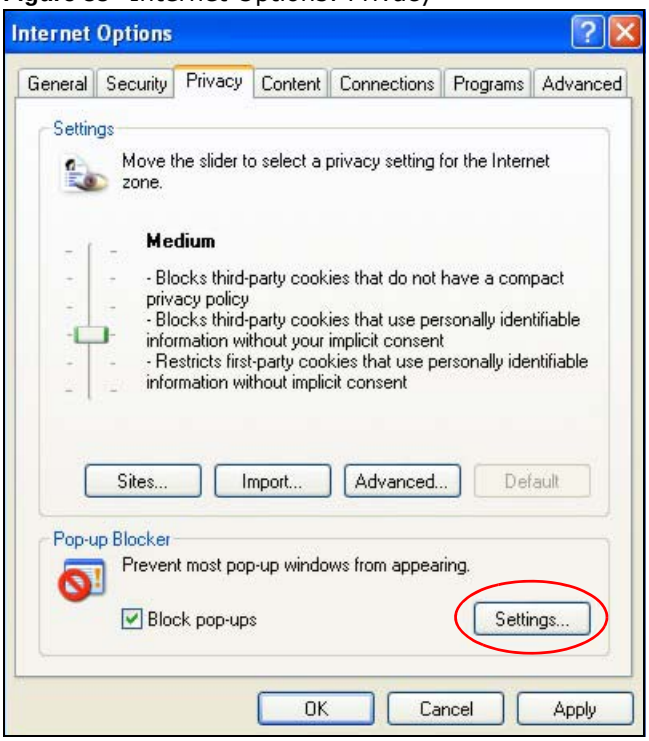
Enable Pop-up Blockers with Exceptions

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.

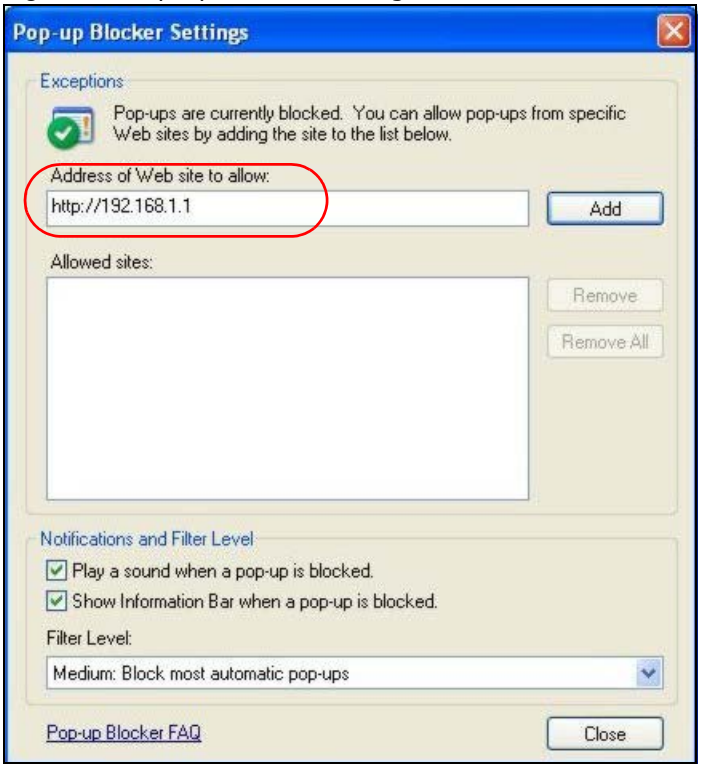
Figure 83 Internet Options: Privacy



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 84 Pop-up Blocker Settings



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

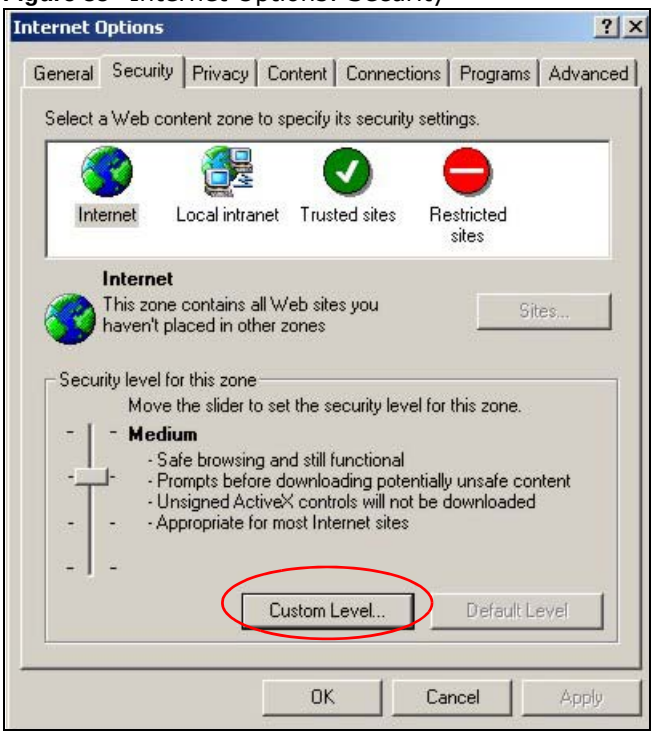
6 Click **Apply** to save this setting.

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 85 Internet Options: Security



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

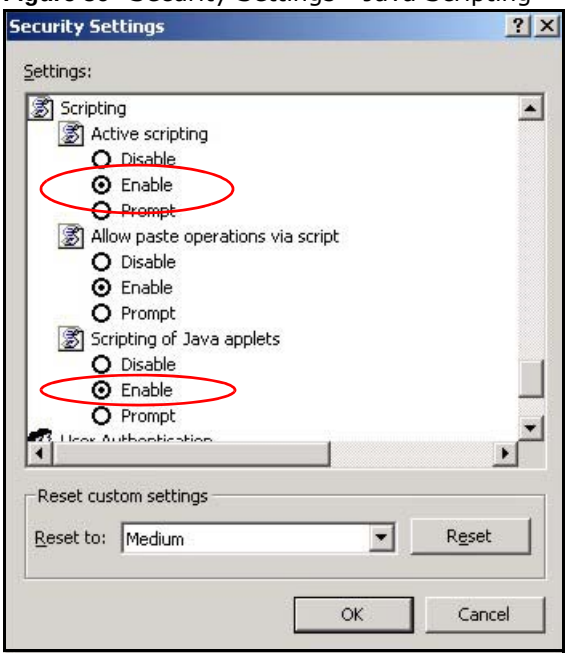
3 Scroll down to **Scripting**.

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 86 Security Settings - Java Scripting



Java Permissions

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

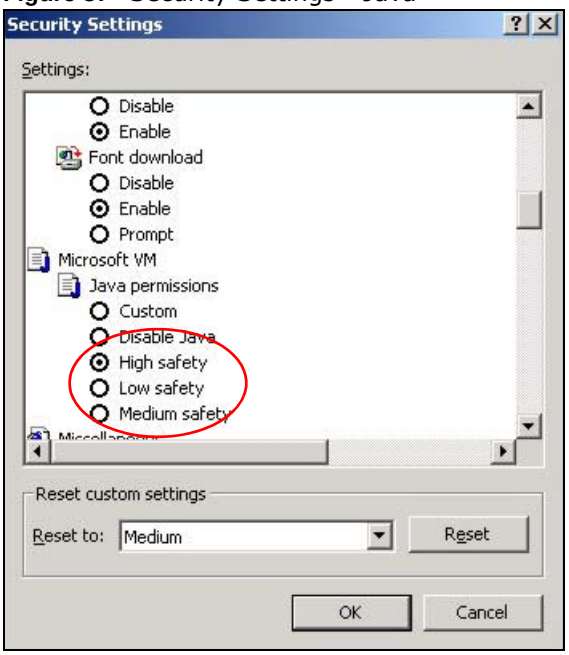
2 Click the **Custom Level...** button.

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 87 Security Settings - Java



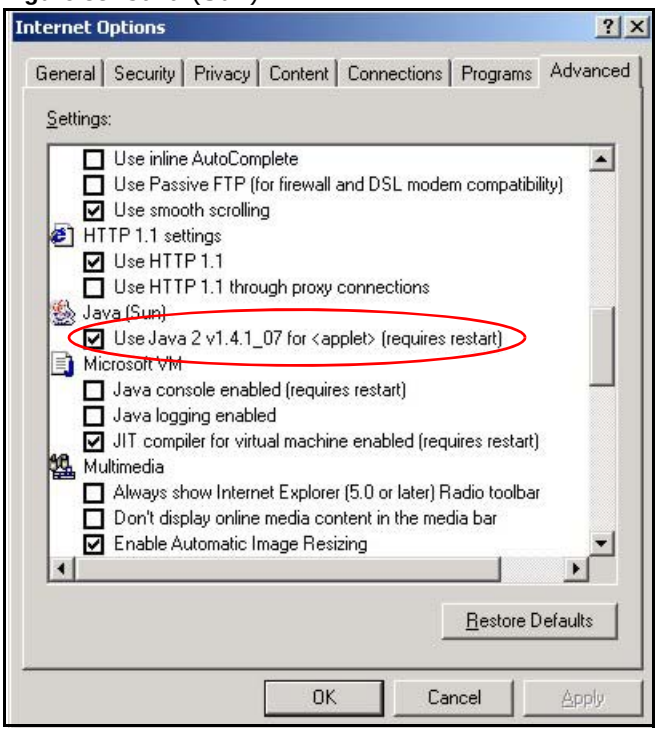
JAVA (Sun)

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 88 Java (Sun)

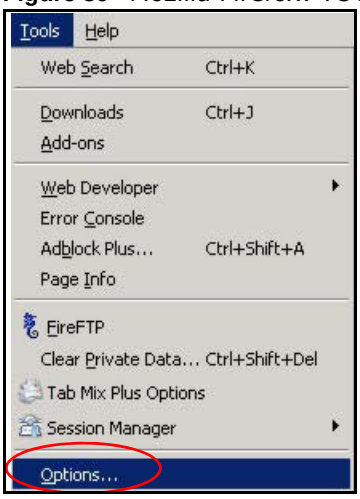


Mozilla Firefox

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.

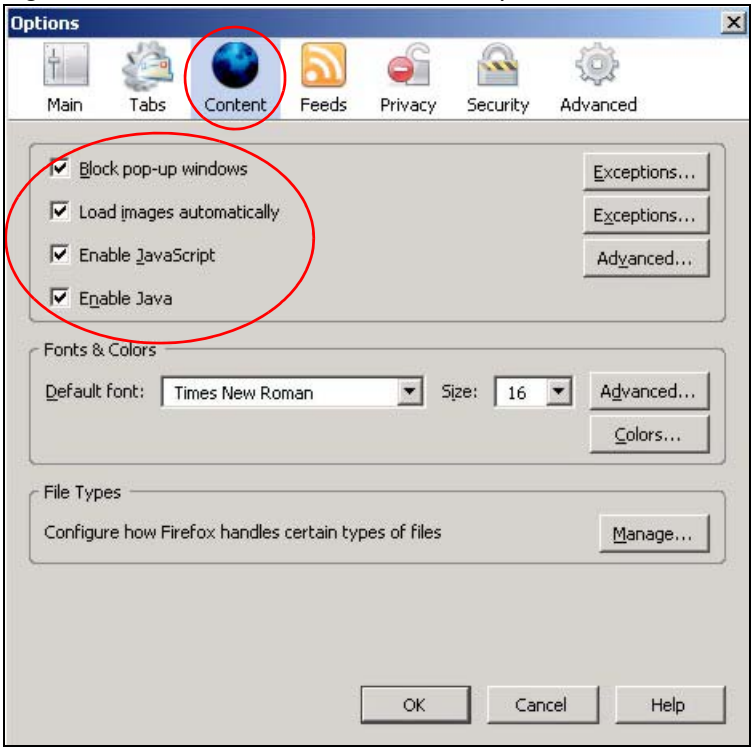
You can enable Java, Javascript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 89 Mozilla Firefox: TOOLS > Options



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

Figure 90 Mozilla Firefox Content Security



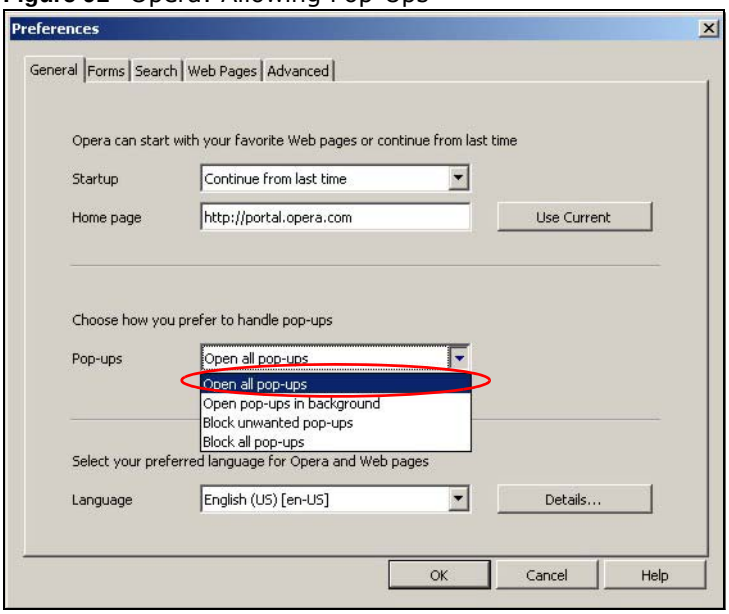
Opera

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**.

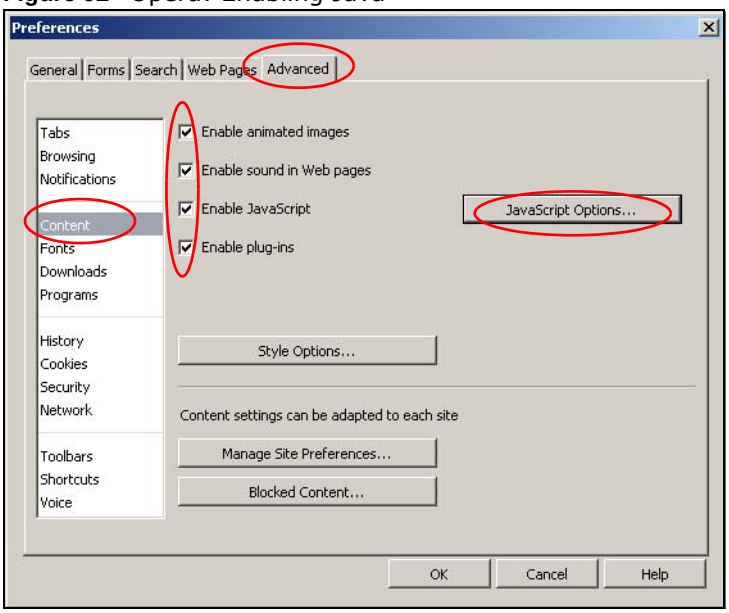
Figure 91 Opera: Allowing Pop-Ups



Enabling Java

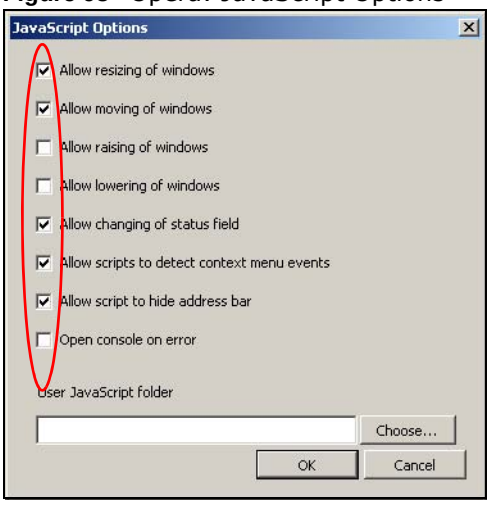
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 92 Opera: Enabling Java



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

Figure 93 Opera: JavaScript Options



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

B

Legal Information

Copyright

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

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。

Notices

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

This device is designed for the WLAN 2.4 GHz and/or 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 GHz et/ou 5 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l'ARCEP, la puissance d'émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d'une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

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.

France

For 2.4 GHz, the output power is restricted to 10 mW EIRP when the product is used outdoors in the band 2454 - 2483.5 MHz. There are no restrictions when used indoors or in other parts of the 2.4 GHz band. Check http://www.arcep.fr/ for more details.

Pour la bande 2.4 GHz, la puissance est limitée à 10 mW en p.i.r.e. pour les équipements utilisés en extérieur dans la bande 2454 - 2483.5 MHz. Il n'y a pas de restrictions pour des utilisations en intérieur ou dans d'autres parties de la bande 2.4 GHz. Consultez http://www.arcep.fr/ pour de plus amples détails.

R&TTE 1999/5/EC		
WLAN 2.4 – 2.4835 GHz		
IEEE 802.11 b/g/n		
Location	Frequency Range (GHz)	Power (EIRP)
Indoor (No restrictions)	2.4 – 2.4835	100mW (20dBm)
Outdoor	2.4 – 2.454	100mW (20dBm)
	2.454 – 2.4835	10mW (10dBm)

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

L

M

O

P

Q

R

S

T

U

W