

## 16.3 What You Need To Know

You can limit an application's uplink or downlink bandwidth. This limit keeps the traffic from using up too much of the out-going interface's bandwidth. This way you can make sure there is bandwidth for other applications. Use the following guidelines:

- The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WLAN to WAN) must be less than or equal to the **Uplink** value that you configure in the **Bandwidth Management General** screen.
- The sum of the bandwidth allotments that apply to the LAN port (WAN to LAN, WAN to WLAN) must be less than or equal to the **Downlink** value that you configure in the **Bandwidth Management General** screen.

## 16.4 General Configuration

Use this screen to enable bandwidth management and assign uplink/downlink limits. You can use either one of the following types:

- **Priority Queue.** Enable bandwidth management to give uplink traffic that matches a bandwidth rule priority over traffic that does not match a bandwidth rule. (This type does not apply to downlink traffic.)
- **Bandwidth Allocation.** Enabling bandwidth management also allows you to control the maximum or minimum amounts of bandwidth that can be used by traffic that matches a bandwidth rule.

Note: You cannot apply both bandwidth management types at the same time.

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

**Figure 82** Management > Bandwidth MGMT > General

General		Advanced
<b>Service Management</b>		
Bandwidth Management Type	Priority Queue	
<b>Total Bandwidth Setting</b>		
Uplink	30720 Kbps	30M bps
Downlink	30720 Kbps	30M bps
<input type="button" value="Apply"/> <input type="button" value="Reset"/>		

The following table describes the labels in this screen.

**Table 55** Management > Bandwidth MGMT > General

LABEL	DESCRIPTION
Service Management	
Bandwidth Management Type	<p>This field allows you to have NBG4604 apply bandwidth management.</p> <p>Select <b>Priority Queue</b> or <b>Bandwidth Allocation</b> to enable bandwidth management.</p> <ul style="list-style-type: none"> <li>• Select <b>Priority Queue</b> to allocate bandwidth based on the pre-defined priority assigned to an application. Refer to <a href="#">Section 16.5 on page 149</a>.</li> <li>• Select <b>Bandwidth Allocation</b> allocate specific amounts of bandwidth to specific protocols on an IP or IP range. Refer to <a href="#">Section 16.5 on page 149</a>.</li> </ul> <p>Select <b>Disable</b> if you do not want to use this feature.</p>
Total Bandwidth Setting. The fields below appear when you enable Bandwidth Management.	
Uplink	<p>Type or select the total amount of bandwidth (from 64 Kbps to 30 Mbps) that you want to dedicate to uplink traffic.</p> <p>If you type the amount of bandwidth, the selection automatically becomes <b>User Defined</b>. If you select the amount of bandwidth, the field automatically displays the value in Kbps.</p> <p>This is traffic from LAN/WLAN to WAN.</p>
Downlink	<p>Type or select the total amount of bandwidth (from 64 Kbps to 30 Mbps) that you want to dedicate to downlink traffic.</p> <p>If you type the amount of bandwidth, the selection automatically becomes <b>User Defined</b>. If you select the amount of bandwidth, the field automatically displays the value in Kbps.</p> <p>This is traffic from WAN to LAN/WLAN.</p>
Apply	Click <b>Apply</b> to save your customized settings.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 16.5 Advanced Configuration

Use this screen to configure bandwidth managements rule for the pre-defined services or applications.

Use this screen to configure bandwidth managements rule for specific protocols on an IP or IP range.

Note: This screen contains the **Priority Queue** and **Bandwidth Allocation** tables. Though both tables are described in this section, you can only apply the rules in one table. Fill out the table of the **Bandwidth Management Type** you selected in [Section 16.4 on page 148](#).

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

**Figure 83** Management > Bandwidth MGMT > Advanced

The screenshot shows the 'Advanced' configuration page for bandwidth management. It is divided into three main sections:

- Unlimited Priority Queue:** Contains a 'Local IP Address' input field (set to '0.0.0.0') and a note: 'Note: The IP address will not be bounded in the QoS limitation'.
- Priority Queue:** A table with 12 rows. Each row has columns for 'id', 'Enable' (checkbox), 'Service', 'Priority' (dropdown), and 'Specific Port' (dropdowns for Front, Middle, Back). Services listed include FTP, WWW, L2L, L-Mail, VoIP (SIP), SIP, and Gaming.
- Bandwidth Allocation:** A table with 12 rows. Each row has columns for 'id', 'Enable' (checkbox), 'LAN IP Range', 'Direction', 'Port Range', 'Policy', 'Rate', and 'Modify' (edit/delete icons).

At the bottom of the screen are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

**Table 56** Management > Bandwidth MGMT > Advanced

LABEL	DESCRIPTION
Priority Queue	
Local IP Address	Enter the IP address of the computer to which bandwidth management does not apply.
Priority Queue	Use this table to allocate specific amounts of bandwidth based on the pre-defined service.

**Table 56** Management > Bandwidth MGMT > Advanced (continued)

LABEL	DESCRIPTION
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the NBG4604 apply this bandwidth management rule.
Service	This is the name of the service.  You can also enter the name (up to 10 keyboard characters) of a service you want to add in the priority queue (for example, Messenger).
Priority	Select a priority from the drop down list box. Choose <b>High</b> or <b>Low</b> .
Specific Port	This displays the port/s assigned to the service.  You can also specify the port/s to services to which you want to allocate bandwidth. Choose either <b>Both</b> , <b>TCP</b> or <b>UDP</b> in the drop-down menu and enter the port or range of ports in the provided boxes.  Note: If you are entering a specific port and not a range of ports, you can either leave the second port field blank or enter the same port number again.
Bandwidth Allocation	Use this table to allocate specific amounts of bandwidth to specific protocols on an IP or IP range.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the NBG4604 apply this bandwidth management rule.
LAN IP Range	This displays the range of IP addresses for which the bandwidth management rule applies.
Direction	These read-only labels represent uplink or downlink traffic.  <b>To LAN</b> applies bandwidth management to traffic from WAN to LAN/WLAN (i.e., downlink).  <b>To WAN</b> applies bandwidth management to traffic from LAN/WLAN to WAN (i.e., uplink).  <b>Both</b> applies bandwidth management to traffic that the NBG4604 forwards to both the LAN and the WAN.
Port Range	This displays the range of ports for which the bandwidth management rule applies.
Policy	This displays either <b>Max</b> (maximum) or <b>Min</b> (minimum) and refers to the maximum or minimum bandwidth allowed for the rule in kilobits per second in the field below.
Rate	This is the maximum or minimum bandwidth allowed (refer to the field above) for the rule in bits per second.
Modify	Click the <b>Edit</b> icon to open the <b>Rule Configuration</b> screen. Modify an existing rule or create a new rule in the <b>Rule Configuration</b> screen. See <a href="#">Section 16.5.2 on page 152</a> for more information.  Click the <b>Remove</b> icon to delete a rule.
Apply	Click <b>Apply</b> to save your customized settings.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 16.5.1 Priority Levels

Traffic with a higher priority gets through faster while traffic with a lower priority is dropped if the network is congested.

The following describes the priorities that you can apply to traffic that the NBG4604 forwards out through an interface.

- **High** - Typically used for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay).
- **Low** - This is typically used for all other traffic that are not time-sensitive.

## 16.5.2 User Defined Service Rule Configuration

If you want to edit a bandwidth management rule for specific protocols on an IP or IP range, click the **Edit** icon in the **Bandwidth Allocation** table of the **Advanced** screen. The following screen displays.

**Figure 84** Management > Bandwidth MGMT > Advanced: Allocation Setup

The following table describes the labels in this screen.

**Table 57** Management > Bandwidth MGMT > Advanced: Allocation Setup

LABEL	DESCRIPTION
Active	Select this check box to turn on this bandwidth management rule.
Direction	Enter whether you want to apply the rule to uplink or downlink traffic.  <b>To LAN</b> applies bandwidth management to traffic from WAN to LAN/WLAN (i.e., downlink).  <b>To WAN</b> applies bandwidth management to traffic from LAN/WLAN to WAN (i.e., uplink).  Select <b>Both</b> applies bandwidth management to traffic that the NBG4604 forwards to both the LAN and the WAN.
LAN IP Range	Specify the range of IP addresses for which the bandwidth management rule applies.
Protocol	Select the protocol (TCP, UDP, SMTP, HTTP, POP3, FTP or ALL) for which the bandwidth management rule applies.

LABEL	DESCRIPTION
Port Range	Enter the range of ports for which the bandwidth management rule applies.
Policy	Select <b>Max</b> or <b>Min</b> and specify the maximum or minimum bandwidth allowed for the rule in bits per second in the field below.
Rate (bps)	Type or select the maximum or minimum bandwidth allowed (refer to the field above) for the rule in bits per second.  If you type the amount of bandwidth, the selection automatically becomes <b>User Defined</b> . If you select the amount of bandwidth, the field automatically displays the value in Kbps.
Apply	Click <b>Apply</b> to save your customized settings.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 16.5.3 Predefined Bandwidth Management Services

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

**Table 58** Media Bandwidth Management Setup: Services

SERVICE	DESCRIPTION
FTP	File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail. FTP uses port number 21.
WWW	The World Wide Web (WWW) is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser. WWW uses port 80.
Telnet	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. Telnet uses port 23.
E-Mail	Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail:  POP3 - port 110  SMTP - port 25
VoIP (SIP)	Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.  SIP is transported primarily over UDP but can also be transported over TCP, using the default port number 5060.

**Table 58** Media Bandwidth Management Setup: Services (continued)

SERVICE	DESCRIPTION
BitTorrent	BitTorrent is a free P2P (peer-to-peer) sharing tool allowing you to distribute large software and media files using ports 6881 to 6889. BitTorrent requires you to search for a file with a searching engine yourself. It distributes files by corporation and trading, that is, the client downloads the file in small pieces and share the pieces with other peers to get other half of the file.
Gaming	Online gaming services lets you play multiplayer games on the Internet via broadband technology. One example is Microsoft's Xbox Live, which uses port 3074. As of this writing, your NBG4604 supports Xbox, Playstation, Battlenet and MSN Game Zone.

### 16.5.4 Services and Port Numbers

See [Appendix E on page 259](#) for commonly used services and port numbers.

# Remote Management

## 17.1 Overview

This chapter provides information on the Remote Management screens.

Remote management allows you to determine which services/protocols can access which NBG4604 interface (if any) from which computers.

You may manage your NBG4604 from a remote location via:

- LAN only
- LAN and WAN

Note: When you configure remote management to allow management from the LAN and WAN in the options above, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.

## 17.2 What You Can Do

Use the WWW screen ([Section 17.4 on page 157](#)) to change your NBG4604's World Wide Web settings.

## 17.3 What You Need To Know

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field. You may only have one remote management session running at a time.



### 17.3.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 You have disabled that service in one of the remote management screens.
- 2 The IP address in the **Secured Client IP Address** field does not match the client IP address. If it does not match, the NBG4604 will disconnect the session immediately.
- 3 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- 4 There is a firewall rule that blocks it.

### 17.3.2 Remote Management and NAT

When NAT is enabled:

- Use the NBG4604's WAN IP address when configuring from the WAN.
- Use the NBG4604's LAN IP address when configuring from the LAN.

### 17.3.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The NBG4604 automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen

## 17.4 WWW Screen

To change your NBG4604's World Wide Web settings, click **Management > Remote MGMT** to display the **WWW** screen.

**Figure 85** Management > Remote MGMT > WWW

The screenshot shows the 'WWW' configuration page. At the top, there is a breadcrumb trail: 'WWW'. Below that, the page title is 'WWW'. The configuration fields are:
 

- Server Port:** A text box containing '8080' with a note '(Apply for remote WAN site only)' to its right.
- Server Access:** A dropdown menu currently set to 'LAN'.
- Secured Client WAN IP Address:** Radio buttons for 'All' (selected) and 'Selected', followed by a text box containing '0.0.0.0'.

 Below the fields is a 'Note' section with a yellow icon and the text: '1. For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.' At the bottom of the form are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen

**Table 59** Management > Remote MGMT > WWW

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NBG4604 using this service.
Secured Client IP Address	<p>A secured client is a "trusted" computer that is allowed to communicate with the NBG4604 using this service.</p> <p>Select <b>All</b> to allow any computer to access the NBG4604 using this service.</p> <p>Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the NBG4604 using this service.</p> <p>Note: This only applies on WAN IP.</p>
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

Company Confidential

# Universal Plug-and-Play (UPnP)

## 18.1 Overview

This chapter introduces the UPnP feature in the Web Configurator.

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

## 18.2 What You Can Do

Use the UPnP screen ([Section 18.4 on page 160](#)) to enable UPnP on the NBG4604.

## 18.3 What You Need to Know

### How do I know if I'm using UPnP?

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

### NAT Traversal

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

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

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

See the NAT chapter for more information on NAT.

### Cautions with UPnP

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

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the NBG4604 allows multicast messages on the LAN only.

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

## 18.4 UPnP Screen

Use this screen to enable UPnP. Click the **Management > UPnP** to open the following screen.

**Figure 86** Management > UPnP > General



The following table describes the labels in this screen.

**Table 60** Management > UPnP > General

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the NBG4604's IP address (although you must still enter the password to access the Web Configurator).
Allow users to make port forwarding changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the NBG4604 so that they can communicate through the NBG4604, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Apply	Click <b>Apply</b> to save the setting to the NBG4604.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 18.5 Technical Reference

The sections show examples of using UPnP.

### 18.5.1 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the NBG4604.

Make sure the computer is connected to a LAN port of the NBG4604. Turn on your computer and the NBG4604.

#### 18.5.1.1 Auto-discover Your UPnP-enabled Network Device

- 1 Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

- 2 Right-click the icon and select **Properties**.

**Figure 87** Network Connections



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

**Figure 88** Internet Connection Properties



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

**Figure 89** Internet Connection Properties: Advanced Settings



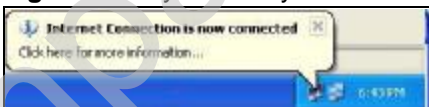
**Figure 90** Internet Connection Properties: Advanced Settings: Add



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

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

**Figure 91** System Tray Icon





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

**Figure 92** Internet Connection Status



## 18.5.2 Web Configurator Easy Access

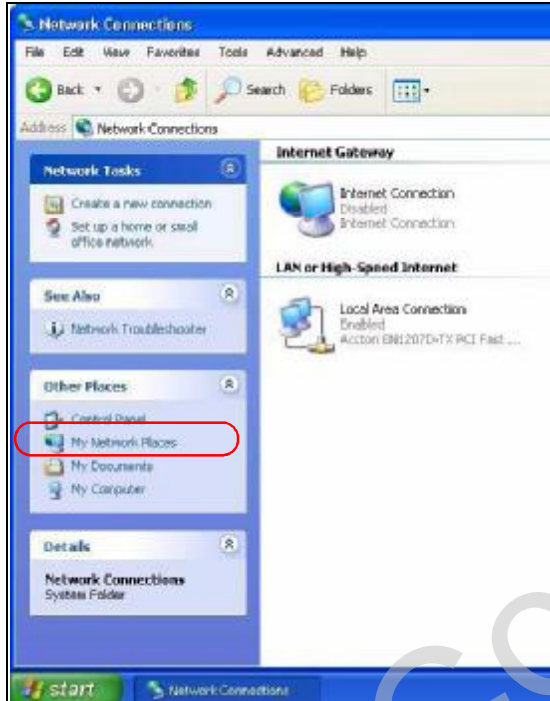
With UPnP, you can access the web-based configurator on the NBG4604 without finding out the IP address of the NBG4604 first. This comes helpful if you do not know the IP address of the NBG4604.

Follow the steps below to access the Web Configurator.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.

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

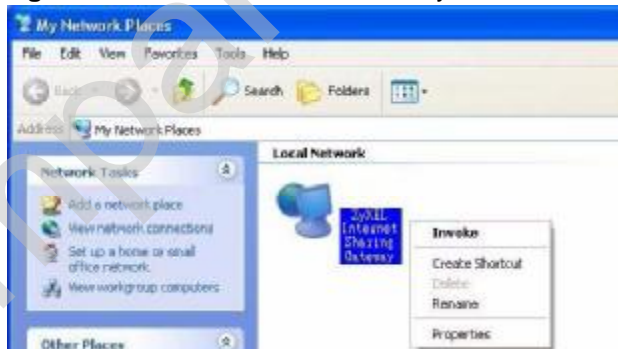
**Figure 93** Network Connections



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

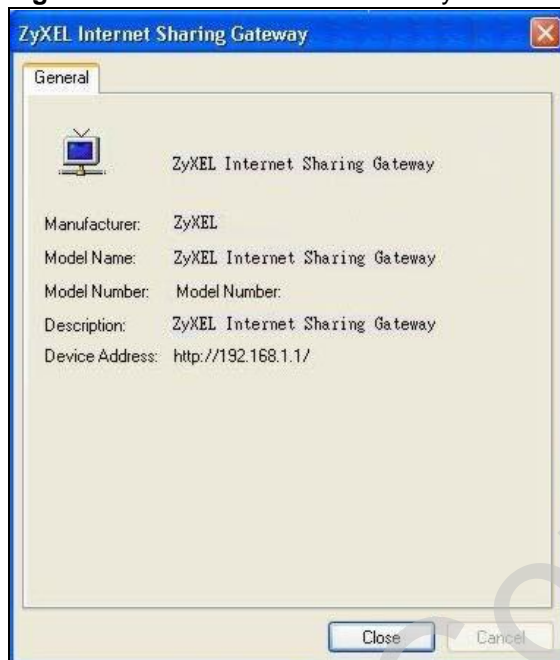
5 Right-click on the icon for your NBG4604 and select **Invoke**. The Web Configurator login screen displays.

**Figure 94** Network Connections: My Network Places



- 6 Right-click on the icon for your NBG4604 and select **Properties**. A properties window displays with basic information about the NBG4604.

**Figure 95** Network Connections: My Network Places: Properties: Example



## 19.1 Overview

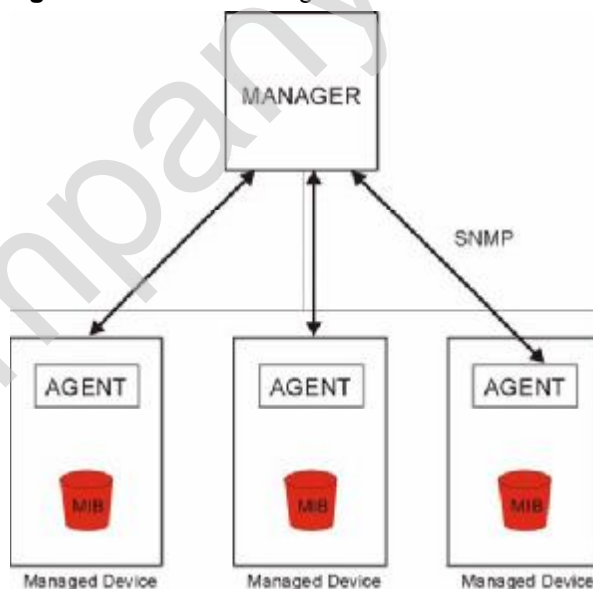
Simple Network Management Protocol (SNMP) is a protocol for collecting and managing information about network devices. Your NBG4604 supports SNMP agent functionality, which allows a manager station to manage and monitor the NBG4604 through the network. The NBG4604 supports SNMP version one (SNMPv1) and version two (SNMPv2c).

Note: Only configure the SNMP feature with settings provided by your ISP.

## 19.2 What You Need to Know

An SNMP managed network consists of two main types of component: agents and a manager.

**Figure 96** SNMP Management Model



An agent is a management software module that resides in a managed device (the NBG4604). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

## 19.3 SNMP Screen

Use this screen to enable SNMP. Click **Management > SNMP** to open the following screen.

**Figure 97** Management > SNMP > General

The screenshot shows a web-based configuration interface for SNMP. The main heading is 'SNMP Settings' under a 'General' tab. The settings are as follows:

Setting	Value
Enable SNMP	<input checked="" type="checkbox"/>
SNMP Version	All
Read Community	public
Set Community	private
System Location	ZyXEL Communications Corp.
System Contact	ZyXEL Communications Corp.

Buttons: Apply, Reset

The following table describes the labels in this screen.

**Table 61** Management > UPnP > General

LABEL	DESCRIPTION
Enable SNMP	Select this to enable SNMP on this device.
SNMP version	Select the SNMP version that corresponds the SNMP used by the server.
Read Community	Enter the SNMP read community information here.
Get Community	Enter the SNMP get community information here.
System Location	Enter the SNMP system location.
System Contact	Enter the SNMP system contact.
Apply	Click <b>Apply</b> to save the setting to the NBG4604.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

Company Confidential

## 20.1 Overview

This chapter shows you to configure the NBG4604's ACS settings so that it can be remotely configured by an Auto-Configuration Server (ACS).

An administrator can use an ACS to remotely set up the NBG4604, modify its settings, perform firmware upgrades, and monitor and diagnose it. In order to do so, you must enable the TR-069 feature on your NBG4604 and then configure it appropriately. (The ACS server which it will use must also be configured by its administrator.)

## 20.2 What You Can Do in this Chapter

- Use the **General** screen ([Section 20.4 on page 172](#)) to configure set up the ACS server information on your NBG4604.
- Use the **Certificate** screen ([Section 20.5 on page 175](#)) to upload encrypted security certificates to your NBG4604.

## 20.3 What You Need to Know

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

### ACS

An Auto-Configuration Server (ACS) centralizes the management and configuration of a variety of networking devices such as routers, set-top boxes, Voice over IP (VoIP) gateways, and other Customer Premises Equipment (CPE). It is based on the TR-069 standard.



### OUI Filter

An Organizationally Unique Identifier (OUI) filter blocks or forwards packets from devices with the specified OUI in the MAC address. The OUI field is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device.

### STUN

STUN allows a device to find the public IP address assigned by a NAT router and/or a firewall between it and the public Internet.

## 20.4 General Screen

The General screen allows you to set up the ACS server information on your NBG4604 so it can be remotely updated. Only use information provided by your network administrator.

### 20.4.1 STUN

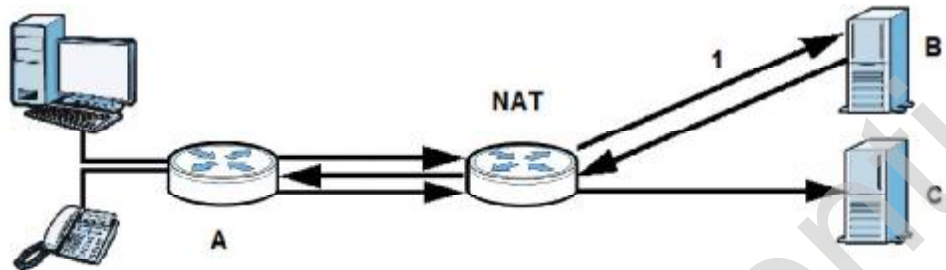
STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the NBG4604 to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the NBG4604 to find the public IP address that NAT assigned, so the NBG4604 can embed it in the SIP data stream. STUN does not work with symmetric NAT routers or firewalls. See RFC 3489 for details on STUN.

The following figure shows how STUN works.

- 1 The NBG4604 (A) sends SIP packets to the STUN server (B).
- 2 The STUN server (B) finds the public IP address and port number that the NAT router used on the NBG4604's SIP packets and sends them to the NBG4604.

- 3 The NBG4604 uses the public IP address and port number in the SIP packets that it sends to the SIP server (C).

**Figure 98** STUN



Click **Management > ACS** to open this screen.

**Figure 99** Management > ACS > General

General		Certificate
<b>ACS Server Setup</b>		
URL	<input type="text" value="http://"/>	
Account Name	<input type="text" value="user"/>	
Password	<input type="password"/>	
Period	<input type="text" value="30"/>	
<b>Device Configuration</b>		
Manufacturer	<input type="text" value="ZyXEL"/>	
Manufacture Oui	<input type="text" value="oui"/>	
Product Class	<input type="text" value="product class"/>	
Model Name	<input type="text" value="NBG4604"/>	
<b>Device Connection Request</b>		
Username	<input type="text"/>	
Password	<input type="password"/>	
<b>Device Connection Request</b>		
STUN Server	<input type="text"/>	
STUN Username	<input type="text"/>	
STUN Password	<input type="password"/>	
<b>Logs</b>		
<input type="button" value="Backup"/> <input type="button" value="Clear Logs"/>		
<input type="button" value="Apply"/> <input type="button" value="Reset"/>		

The following table describes the labels in this screen.

**Table 62** Management > ACS > General

LABEL	DESCRIPTION
ACS Server Setup	
URL	Enter the URL of the ACS server.
Account Name	Enter the login name used by the NBG4604 to log into the ACS server.
Password	Enter the password for the account used to log into the ACS server.
Period	Enter the duration in seconds over which the NBG4604 attempts to log into the ACS server.
Device Configuration	
Manufacturer	This displays the manufacturer name of the NBG4604, 'ZyXEL', and cannot be edited.
Manufacturer Oui	Enter the manufacturer organizational unit identifier. This number must consist of a 3-octet MAC address.
Product Class	Enter the product class if this was provided by the network administrator. Otherwise, leave it at its default setting.
Model Name	This displays the model name. In this case, it is 'NBG4604' and cannot be edited.
Device Connection Request	
Username	Enter the username required for the ACS server to connect directly to the NBG4604.
Password	Enter the password required for the ACS server to connect directly to the NBG4604.
Device Connection Request	
STUN Server	Enter the URL of the STUN server.
STUN Username	Enter the username required to log into the STUN server.
STUN Password	Enter the password of the username used to log into the STUN server.
Logs	
Backup	Click <b>Backup</b> to save a copy of the NBG4604's ACS activity.
Clear Logs	Click <b>Clear Logs</b> to delete the files containing a record of the NBG4604's ACS activity.
Apply	Click <b>Apply</b> to save the setting to the NBG4604.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 20.5 Certificate Screen

This screen allows you to upload security certificates to the NBG4604. Click Management > ACS > Certificates to open this screen.

**Figure 100** Management > ACS > Certificates

The following table describes the labels in this screen.

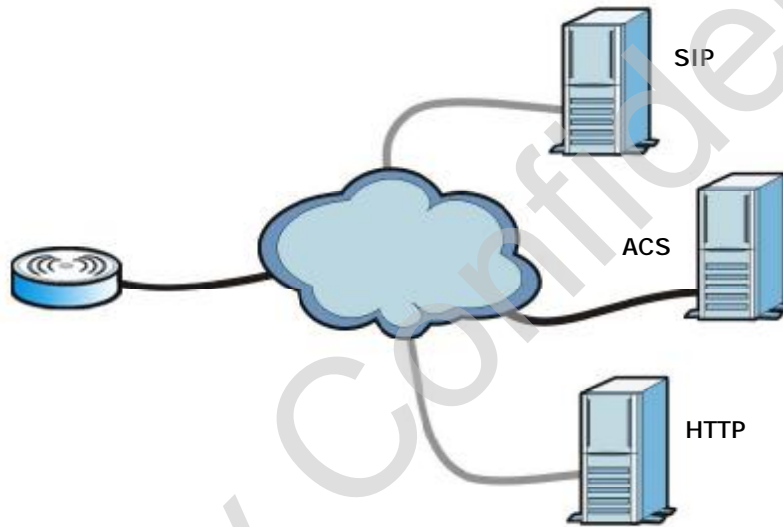
**Table 63** Management > UPnP > General

LABEL	DESCRIPTION
File Path	Enter the path of the certificate file's location on your local computer, or click the <b>Browse</b> button to open a browse dialog box to search for it.
CA Certificate	Click <b>Upload</b> to copy the certicate listed in File Path to the NBG4604. Click <b>Clear</b> to remove the current CA Certificate from the device.
Client Certificate	Click <b>Upload</b> to copy the certicate listed in File Path to the NBG4604. Click <b>Clear</b> to remove the current Client Certificate from the device.
Client Key	Click <b>Upload</b> to copy the certicate listed in File Path to the NBG4604. Click <b>Clear Key</b> to remove the current CA Certificate from the device.

## 20.6 Technical Reference

TR-069 is an abbreviation of "Technical Reference 069", a protocol designed to facilitate the remote management of Customer Premise Equipment (CPE), such as the NBG4604. It can be managed over a WAN by means of an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between the ACS and the client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

**Figure 101** TR-069 Example



In this example, the NBG4604 receives data from at least 3 sources: A SIP server for handling voice calls, an HTTP server for handling web services, and an ACS, for configuring the NBG4604 remotely. All three servers are owned and operated by the client's Internet Service Provider. However, without the configuration settings from the ACS, the NBG4604 cannot access the other two servers. Once the NBG4604 receives its configuration settings and implements them, it can connect to the other servers. If the settings change, it will once again be unable to connect until it receives its updates from the ACS.

The NBG4604 can be configured to periodically check for updates from the auto-configuration server so that the end user need not be worried about it.

## 21.1 Overview

This chapter provides information on the System screens.

See the chapter about wizard setup for more information on the next few screens.

## 21.2 What You Can Do

- Use the General screen (Section 21.3 on page 177) to enter a name to identify the NBG4604 in the network and set the password.
- Use the Time Setting screen (Section 21.4 on page 179) to change your NBG4604's time and date.

## 21.3 System General Screen

Use this screen to enter a name to identify the NBG4604 in the network and set the password. Click Maintenance > System. The following screen displays.

Figure 102 Maintenance > System > General

The screenshot shows a web interface for system configuration. It has two tabs: 'General' (selected) and 'Time Setting'. The 'System Setup' section contains three input fields: 'System Name' with the value 'NMG4604', 'Domain Name' with the value 'zyxel.com', and 'Administrator Inactivity Timer' with the value '30' and a note '(minutes, 0 means no timeout)'. The 'Password Setup' section contains three input fields: 'Old Password', 'New Password', and 'Retype to Confirm', all masked with dots. At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

**Table 64** Maintenance > System > General

LABEL	DESCRIPTION
System Setup	
System Name	<p>System Name is a unique name to identify the NBG4604 in an Ethernet network. It is recommended you enter your computer's "Computer name" in this field (see the chapter about wizard setup for how to find your computer's name).</p> <p>This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.</p>
Domain Name	<p>Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP.</p> <p>The domain name entered by you is given priority over the ISP assigned domain name.</p>
Administrator Inactivity Timer	<p>Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).</p>
Password Setup	<p>Change your NBG4604's password (recommended) using the fields as shown.</p>
Old Password	<p>Type the default password or the existing password you use to access the system in this field.</p>
New Password	<p>Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.</p>
Retype to Confirm	<p>Type the new password again in this field.</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the NBG4604.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

## 21.4 Time Setting Screen

To change your NBG4604's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown. Use this screen to configure the NBG4604's time based on your local time zone.

**Figure 103** Maintenance > System > Time Setting

The following table describes the labels in this screen.

**Table 65** Maintenance > System > Time Setting

LABEL	DESCRIPTION
<b>Current Time and Date</b>	
Current Time	This field displays the time of your NBG4604. Each time you reload this page, the NBG4604 synchronizes the time with the time server.
Current Date	This field displays the date of your NBG4604. Each time you reload this page, the NBG4604 synchronizes the date with the time server.
<b>Time and Date Setup</b>	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.



**Table 65** Maintenance > System > Time Setting

LABEL	DESCRIPTION
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually.  When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new time in this field and then click <b>Apply</b> .
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually.  When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new date in this field and then click <b>Apply</b> .
Get from Time Server	Select this radio button to have the NBG4604 get the time and date from the time server you specified below.
Auto	Select <b>Auto</b> to have the NBG4604 automatically search for an available time server and synchronize the date and time with the time server after you click <b>Apply</b> .
User Defined Time Server Address	Select <b>User Defined Time Server Address</b> and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
<b>Time Zone Setup</b>	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.  Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected <b>Daylight Savings</b> . The o'clock field uses the 24 hour format. Here are a couple of examples:  Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>First, Sunday, April</b> and type <b>2</b> in the o'clock field.  Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, March</b> . The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type <b>2</b> because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

**Table 65** Maintenance > System > Time Setting

LABEL	DESCRIPTION
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected <b>Daylight Savings</b>. The o'clock field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Last, Sunday, October</b> and type 2 in the o'clock field.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, October</b>. The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Apply	Click <b>Apply</b> to save your changes back to the NBG4604.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

Company Confidential

## 22.1 Overview

This chapter contains information about configuring general log settings and viewing the NBG4604's logs.

The Web Configurator allows you to look at all of the NBG4604's logs in one location.

## 22.2 What You Can Do

- Use the **View Log** screen ([Section 22.4 on page 184](#)) to see the logs for the categories such as system maintenance, system errors, access control, allowed or blocked web sites, blocked web features, and so on.
- Use the **Log Settings** screen ([Section 5.8 on page 5](#)) to send copies of the NBG4604 syslog files to a dedicated syslog server.

## 22.3 What You Need to Know

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

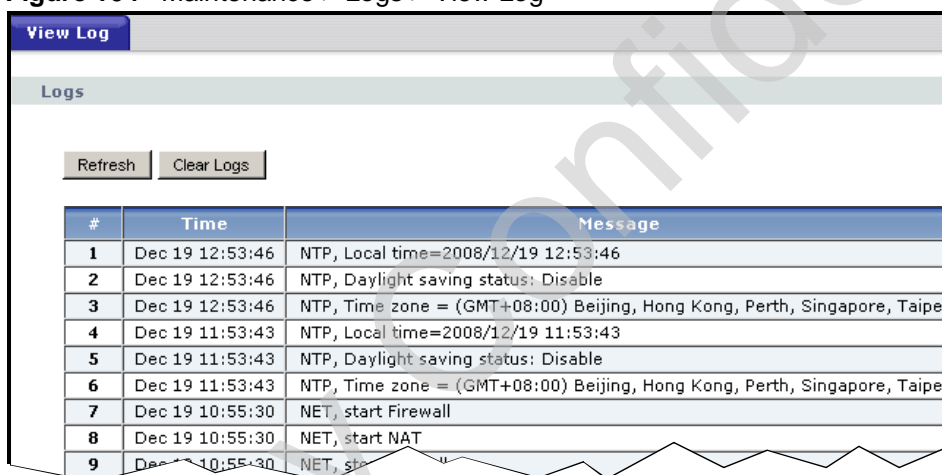
## 22.4 View Log Screen

Use the **View Log** screen to see the logged messages for the NBG4604. Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, Java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Click **Maintenance > Logs** to open the **View Log** screen.

**Figure 104** Maintenance > Logs > View Log



#	Time	Message
1	Dec 19 12:53:46	NTP, Local time=2008/12/19 12:53:46
2	Dec 19 12:53:46	NTP, Daylight saving status: Disable
3	Dec 19 12:53:46	NTP, Time zone = (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei
4	Dec 19 11:53:43	NTP, Local time=2008/12/19 11:53:43
5	Dec 19 11:53:43	NTP, Daylight saving status: Disable
6	Dec 19 11:53:43	NTP, Time zone = (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei
7	Dec 19 10:55:30	NET, start Firewall
8	Dec 19 10:55:30	NET, start NAT
9	Dec 19 10:55:30	NET, start

The following table describes the labels in this screen.

**Table 66** Maintenance > Logs > View Log

LABEL	DESCRIPTION
Refresh	Click <b>Refresh</b> to renew the log screen.
Clear Log	Click <b>Clear Log</b> to delete all the logs.
#	This is the index number of the log entry.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the NBG4604's time and date.
Message	This field states the reason for the log.

## 22.5 Log Settings Screen

Use this screen to send copies of the NBG4604 syslog files to a dedicated syslog server. For information on setting up a syslog server, consult the documentation that came with your syslog server product.

Click **Maintenance > Logs > Log Settings** to open this screen.

**Figure 105** Maintenance > Logs > Log Settings



The following table describes the labels in this screen.

**Table 67** Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Active	Select this to enable syslog logging on this device.
Syslog Server IP Address	Enter the IP address of the syslog server to receive syslogs from this device.
Apply	Click <b>Apply</b> to save the setting to the NBG4604.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

Company Confidential

## 23.1 Overview

This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the NBG4604.

## 23.2 What You Can Do

- Use the **Firmware** screen ([Section 23.3 on page 187](#)) to upload firmware to your NBG4604.
- Use the **Configuration** screen ([Section 23.4 on page 190](#)) to view information related to factory defaults, backup configuration, and restoring configuration.
- Use the **Restart** screen ([Section 23.5 on page 192](#)) to have the NBG4604 reboot.

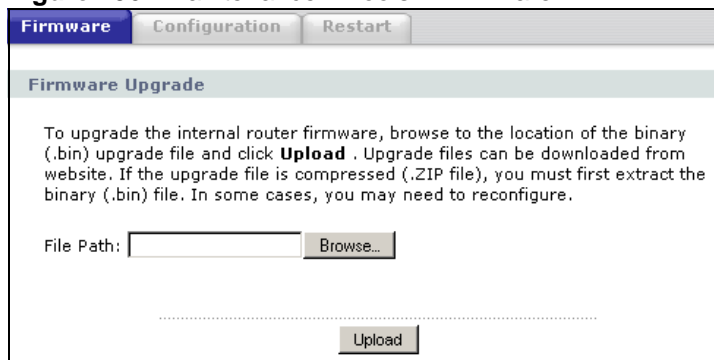
## 23.3 Firmware Upload Screen

Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses the system model name with a ".bin" extension, e.g., "NBG4604.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.



Click **Maintenance > Tools**. Follow the instructions in this screen to upload firmware to your NBG4604.

**Figure 106** Maintenance > Tools > Firmware



The following table describes the labels in this screen.

**Table 68** Maintenance > Tools > Firmware

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.

Note: Do not turn off the NBG4604 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the NBG4604 again.

**Figure 107** Upload Warning



The NBG4604 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 108** Network Temporarily Disconnected



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

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

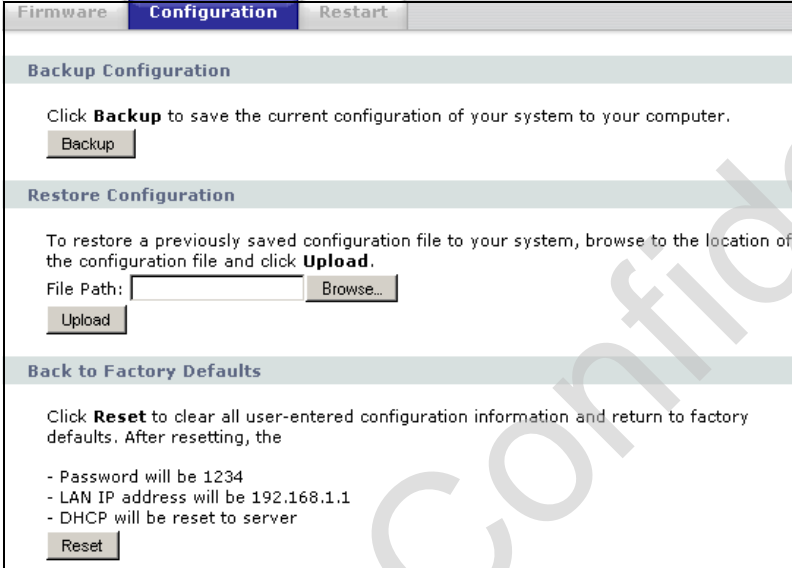
**Figure 109** Upload Error Message



## 23.4 Configuration Screen

Click **Maintenance > Tools > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

**Figure 110** Maintenance > Tools > Configuration



The screenshot shows the Configuration screen with the following content:

- Configuration** (selected tab)
- Backup Configuration**
  - Click **Backup** to save the current configuration of your system to your computer.
  -
- Restore Configuration**
  - To restore a previously saved configuration file to your system, browse to the location of the configuration file and click **Upload**.
  - File Path:
  -
- Back to Factory Defaults**
  - Click **Reset** to clear all user-entered configuration information and return to factory defaults. After resetting, the
    - Password will be 1234
    - LAN IP address will be 192.168.1.1
    - DHCP will be reset to server
  -

### 23.4.1 Backup Configuration

Backup configuration allows you to back up (save) the NBG4604's current configuration to a file on your computer. Once your NBG4604 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.

Click **Backup** to save the NBG4604's current configuration to your computer.

## 23.4.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NBG4604.

**Table 69** Maintenance Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.
Browse...	Click <b>Browse...</b> to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process.

Note: Do not turn off the NBG4604 while configuration file upload is in progress

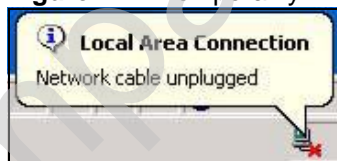
After you see a "configuration upload successful" screen, you must then wait one minute before logging into the NBG4604 again.

**Figure 111** Configuration Restore Successful



The NBG4604 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 112** Temporarily Disconnected



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 NBG4604 IP address (192.168.1.1). See [Appendix C on page 229](#) for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

**Figure 113** Configuration Restore Error



### 23.4.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the NBG4604 to its factory defaults.

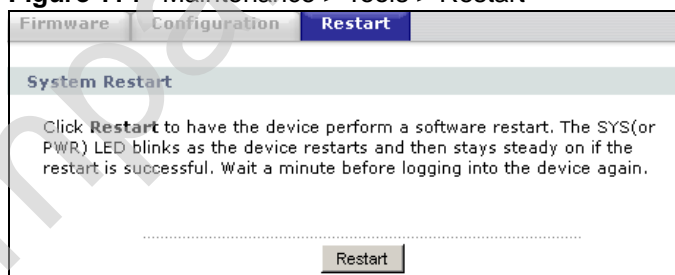
You can also press the **RESET** button on the rear panel to reset the factory defaults of your NBG4604. Refer to the chapter about introducing the Web Configurator for more information on the **RESET** button.

## 23.5 Restart Screen

System restart allows you to reboot the NBG4604 without turning the power off.

Click **Maintenance > Tools > Restart**. Click **Restart** to have the NBG4604 reboot. This does not affect the NBG4604's configuration.

**Figure 114** Maintenance > Tools > Restart



## Sys OP Mode

### 24.1 Overview

The Sys OP Mode (System Operation Mode) function lets you configure whether your NBG4604 is a router or AP.

You can choose between **Router Mode** and **AP Mode** depending on your network topology and the features you require from your device. See [Section 1.1 on page 21](#) for more information on which mode to choose.

### 24.2 What You Can Do

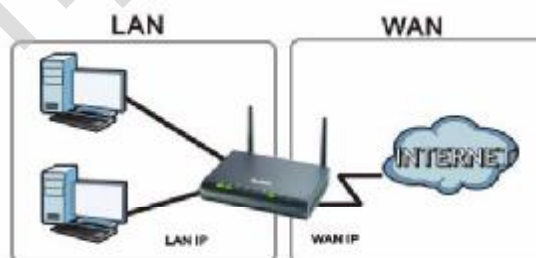
Use the General screen ([Section 24.4 on page 194](#)) to select how you connect to the Internet.

### 24.3 What You Need to Know

#### Router

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

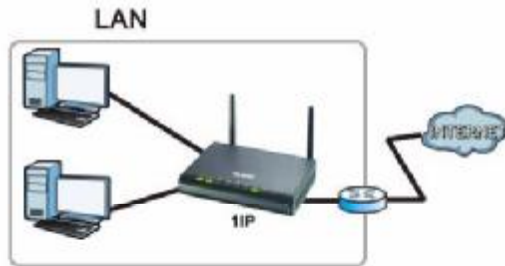
**Figure 115** LAN and WAN IP Addresses in Router Mode



## AP

An AP extends one network and so has just one IP address. All Ethernet ports on the AP have the same IP address. To connect to the Internet, another device, such as a router, is required.

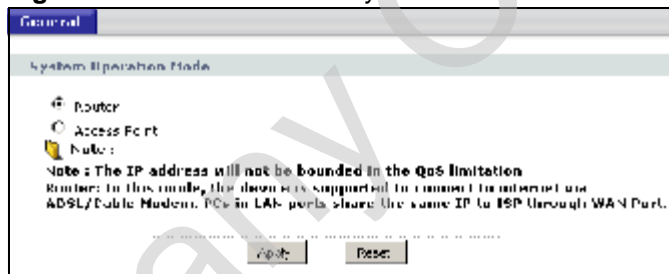
**Figure 116** IP Address in AP Mode



## 24.4 General Screen

Use this screen to select how you connect to the Internet.

**Figure 117** Maintenance > Sys OP Mode > General



If you select Router Mode, the following pop-up message window appears.

**Figure 118** Maintenance > Sys Op Mode > General: Router



- In this mode there are both LAN and WAN ports. The LAN Ethernet and WAN Ethernet ports have different IP addresses.
- The DHCP server on your device is enabled and allocates IP addresses to other devices on your local network.
- The LAN IP address of the device on the local network is set to 192.168.1.1.

- You can configure the IP address settings on your WAN port. Contact your ISP or system administrator for more information on appropriate settings.

If you select Access Point the following pop-up message window appears.

**Figure 119** Maintenance > Sys Op Mode > General: AP



- In AP Mode all Ethernet ports have the same IP address.
- All ports on the rear panel of the device are LAN ports, including the port labeled WAN. There is no WAN port.
- The DHCP server on your device is disabled. In AP mode there must be a device with a DHCP server on your network such as a router or gateway which can allocate IP addresses.

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

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

**Table 70** Maintenance > Sys OP Mode > General

LABEL	DESCRIPTION
System Operation Mode	
Router	Select <b>Router</b> if your device routes traffic between a local network and another network such as the Internet. This mode offers services such as a firewall or content filter.
Access Point	Select <b>Access Point</b> if your device bridges traffic between clients on the same network.
Apply	Click <b>Apply</b> to save your settings.
Reset	Click <b>Reset</b> to return your settings to the default ( <b>Router</b> )

Note: If you select the incorrect System Operation Mode you cannot connect to the Internet.



Company Confidential

## Language

### 25.1 Language Screen

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

Click the language you prefer. The Web Configurator language changes after a while without restarting the NBG4604.

**Figure 120** Language



Company Confidential

# Troubleshooting

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](#)
- [NBG4604 Access and Login](#)
- [Internet Access](#)
- [Resetting the NBG4604 to Its Factory Defaults](#)
- [Wireless Router/AP Troubleshooting](#)

## 26.1 Power, Hardware Connections, and LEDs

---

The NBG4604 does not turn on. None of the LEDs turn on.

---

- 1 Make sure you are using the power adaptor or cord included with the NBG4604.
- 2 Make sure the power adaptor or cord is connected to the NBG4604 and plugged in to an appropriate power source. Make sure the power source is turned on.
- 3 Disconnect and re-connect the power adaptor or cord to the NBG4604.
- 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 1.5 on page 22](#).
- 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 NBG4604.
- 5 If the problem continues, contact the vendor.

## 26.2 NBG4604 Access and Login

---

I don't know the IP address of my NBG4604.

---

- 1 The default IP address is **192.168.1.1**.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the NBG4604 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 NBG4604 (it depends on the network), so enter this IP address in your Internet browser. Set your device to **Router Mode**, login (see the Quick Start Guide for instructions) and go to the **Device Information** table in the **Status** screen. Your NBG4604's IP address is available in the **Device Information** table.
  - If the **DHCP** setting under **LAN information** is **None**, your device has a fixed IP address.
  - If the **DHCP** setting under **LAN information** is **Client**, then your device receives an IP address from a DHCP server on the network.
- 3 If your NBG4604 is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.
- 4 Reset your NBG4604 to change all settings back to their default. This means your current settings are lost. See [Section 26.4 on page 203](#) in the **Troubleshooting** for information on resetting your NBG4604.

---

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 26.4 on page 203](#).

---

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 is [192.168.1.1](#).
  - If you changed the IP address ([Section 7.3 on page 102](#)), 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 NBG4604](#).
- 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 JavaScripts and Java enabled. See [Appendix B on page 221](#).
- 4 Make sure your computer is in the same subnet as the NBG4604. (If you know that there are routers between your computer and the NBG4604, skip this step.)
  - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Section 7.3 on page 102](#).
  - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG4604. See [Section 7.3 on page 102](#).
- 5 Reset the device to its factory defaults, and try to access the NBG4604 with the default IP address. See [Section 7.3 on page 102](#).
- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

#### Advanced Suggestions

- If your computer is connected to the WAN port or is connected wirelessly, use a computer that is connected to a LAN/ETHERNET port.

---

I can see the **Login** screen, but I cannot log in to the NBG4604.

---

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

- 2 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.
- 3 Disconnect and re-connect the power adaptor or cord to the NBG4604.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 26.4 on page 203](#).

## 26.3 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 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 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.
  - Go to Network > Wireless LAN > General > WDS and check if the NBG4604 is set to bridge mode. Select **Disable** and try to connect to the Internet again.
- 4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 5 Go to Maintenance > Sys OP Mode > General. Check your System Operation Mode setting.
  - Select **Router** if your device routes traffic between a local network and another network such as the Internet.
  - Select **Access Point** if your device bridges traffic between clients on the same network.
- 6 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NBG4604), 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 1.5 on page 22](#).
- 2 Reboot the NBG4604.
- 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 1.5 on page 22](#). If the NBG4604 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 NBG4604 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 NBG4604.
- 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.

## 26.4 Resetting the NBG4604 to Its Factory Defaults

If you reset the NBG4604, you lose all of the changes you have made. The NBG4604 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 NBG4604,

- 1 Make sure the power LED is on.



- 2 Press the **RESET** button for longer than 1 second to restart/reboot the NBG4604.
- 3 Press the **RESET** button for longer than five seconds to set the NBG4604 back to its factory-default configurations.

If the NBG4604 restarts automatically, wait for the NBG4604 to finish restarting, and log in to the Web Configurator. The password is "1234".

If the NBG4604 does not restart automatically, disconnect and reconnect the NBG4604's power. Then, follow the directions above again.

## 26.5 Wireless Router/AP Troubleshooting

---

I cannot access the NBG4604 or ping any computer from the WLAN (wireless AP or router).

---

- 1 Make sure the wireless LAN is enabled on the NBG4604
  - 2 Make sure the wireless adapter on the wireless station 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 NBG4604.
  - 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG4604.
  - 5 Check that both the NBG4604 and your wireless station are using the same wireless and wireless security settings.
  - 6 Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the NBG4604.
  - 7 Make sure you allow the NBG4604 to be remotely accessed through the WLAN interface. Check your remote management settings.
    - See the chapter on Wireless LAN in the User's Guide for more information.
- to select Router Mode.

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

---

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

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

---

I can access the Internet, but I cannot open my network folders.

---

In the **Network > LAN > Advanced** screen, make sure **Allow between LAN and WAN** is checked. This is not checked by default to keep the LAN secure.

If you still cannot access a network folder, make sure your account has access rights to the folder you are trying to open.

---

I can access the Web Configurator after I switched to AP mode.

---

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

Refer to [Appendix C on page 229](#) for instructions on how to change your computer's IP address.

Company Confidential

## Product Specifications

The following tables summarize the NBG4604's hardware and firmware features.

**Table 71** Hardware Features

Dimensions (W x D x H)	140 mm x 110 mm x 30 mm
Weight	190 g
Power Specification	Input: 100~240 AC, 50~60 Hz Output: 12 V DC 1A
Ethernet ports	Auto-negotiating: 10/100/1000 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables.
4-5 Port Switch	A combination of switch and router makes your NBG4604 a cost-effective and viable network solution. You can add up to four computers to the NBG4604 without the cost of a hub when connecting to the Internet through the WAN port. You can add up to five computers to the NBG4604 when you connect to the Internet in AP mode. Add more than four computers to your LAN by using a hub.
LEDs	PWR, LAN1-4, WAN, WLAN, WPS
Reset Button	The reset button is built into the rear panel. Use this button to restore the NBG4604 to its factory default settings. Press for 1 second to restart the device. Press for 5 seconds to restore to factory default settings.
WPS button	Press the WPS on two WPS enabled devices within 120 seconds for a security-enabled wireless connection.
Antenna	The NBG4604 is equipped with a 2dBi (2.4GHz) detachable antenna to provide clear radio transmission and reception on the wireless network.
Operation Environment	Temperature: 0° C ~ 40° C / 32°F ~ 104°F Humidity: 20% ~ 90%
Storage Environment	Temperature: -30° C ~ 70° C / -22°F ~ 158°F Humidity: 20% ~ 95%

**Table 72** Firmware Features

FEATURE	DESCRIPTION
Default LAN IP Address	192.168.1.1 (router) 192.168.1.2. (AP)
Default LAN Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.33 to 192.168.1.64
Wireless Interface	Wireless LAN
Default Wireless SSID	ZyXEL
Device Management	Use the Web Configurator to easily configure the rich range of features on the NBG4604.
Wireless Functionality	Allows IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the NBG4604 wirelessly. Enable wireless security ( WPA(2)-PSK) and/or MAC filtering to protect your wireless network.  Note: The NBG4604 may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the Web Configurator to put it on the NBG4604.  Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the NBG4604's configuration and put it back on the NBG4604 later if you decide you want to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert a single public IP address to multiple private IP addresses for the computers on your network.
Firewall	You can configure firewall on the NBG4604 for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.
Content Filter	The NBG4604 blocks or allows access to web sites that you specify and blocks access to web sites with URLs that contain keywords that you specify. You can define time periods and days during which content filtering is enabled. You can also include or exclude particular computers on your network from content filtering.  You can also subscribe to category-based content filtering that allows your NBG4604 to check web sites against an external database.

**Table 72** Firmware Features

FEATURE	DESCRIPTION
Bandwidth Management	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the NBG4604.
Wireless LAN Scheduler	You can schedule the times the Wireless LAN is enabled/disabled.
Time and Date	Get the current time and date from an external server when you turn on your NBG4604. You can also set the time manually. These dates and times are then used in logs.
Port Forwarding	If you have a server (mail or web server for example) on your network, then use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the NBG4604 assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, <a href="http://www.zyxel.com">www.zyxel.com</a> for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP Multicast is used to send traffic to a specific group of computers. The NBG4604 supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Logging	Use logs for troubleshooting. You can view logs in the Web Configurator.
PPPoE	PPPoE mimics a dial-up Internet access connection.
PPTP Encapsulation	Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The NBG4604 supports one PPTP connection at a time.
Universal Plug and Play (UPnP)	The NBG4604 can communicate with other UPnP enabled devices in a network.

## 27.1 Wall-mounting Instructions

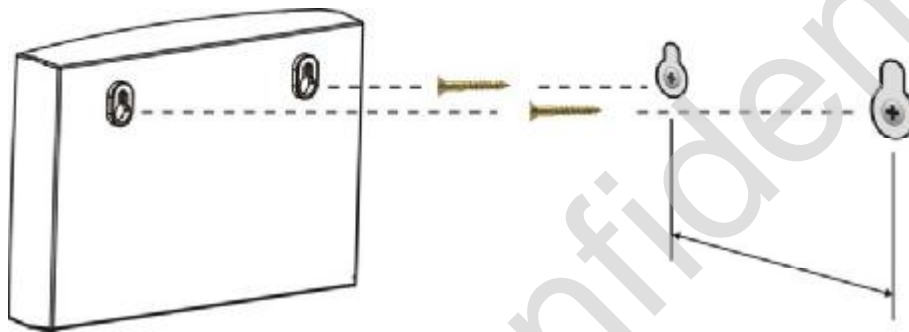
Complete the following steps to hang your NBG4604 on a wall.

- 1 Select a position free of obstructions on a sturdy wall.
- 2 Drill two holes for the screws.

**Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.**

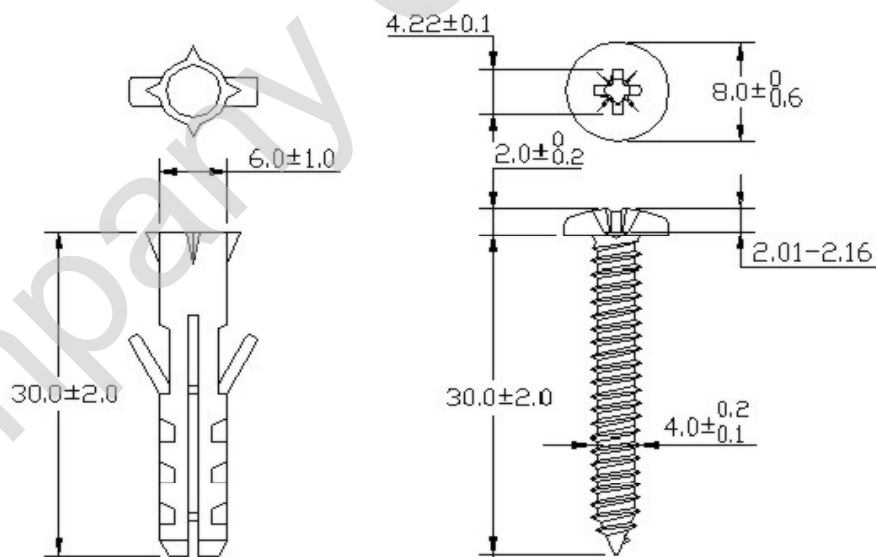
- 3 Do not insert the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.
- 4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the NBG4604 with the connection cables.
- 5 Align the holes on the back of the NBG4604 with the screws on the wall. Hang the NBG4604 on the screws.

**Figure 121** Wall-mounting Example



The following are dimensions of an M4 tap screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

**Figure 122** Masonry Plug and M4 Tap Screw



# A

## IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

### Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

### Structure

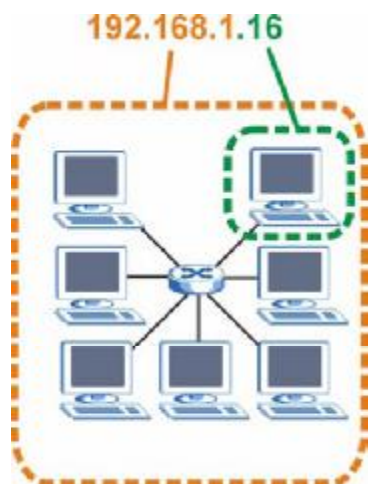
An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.



The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

**Figure 123** Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

**Table 73** Subnet Mask - Identifying Network Number

	<b>1ST OCTET: (192)</b>	<b>2ND OCTET: (168)</b>	<b>3RD OCTET: (1)</b>	<b>4TH OCTET (2)</b>
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	11111111	11111111	11111111	00000000

**Table 73** Subnet Mask - Identifying Network Number

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
Network Number	11000000	10101000	00000001	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

**Table 74** Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

## Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

**Table 75** Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

## Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

**Table 76** Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

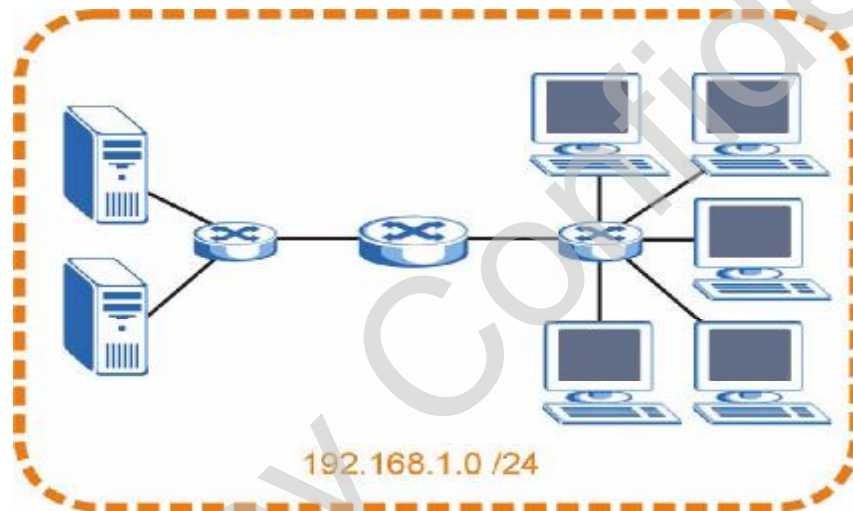
## Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of  $2^8 - 2$  or 254 possible hosts.

The following figure shows the company network before subnetting.

**Figure 124** Subnetting Example: Before Subnetting

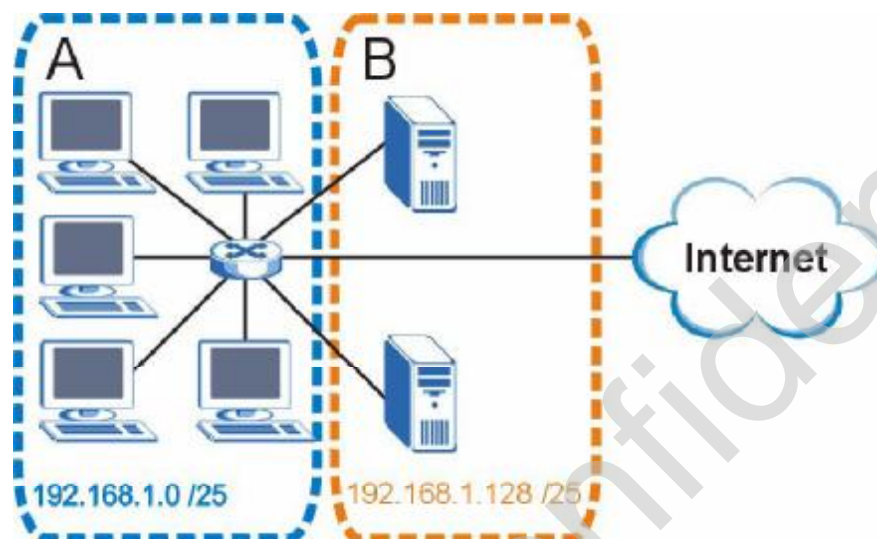


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The "borrowed" host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, A and B.

**Figure 125** Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of  $2^7 - 2$  or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet A itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet A is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet B is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving  $2^6 - 2$  or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

**Table 77** Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

**Table 78** Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

**Table 79** Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

**Table 80** Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000

**Table 80** Subnet 4 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

## Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

**Table 81** Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

## Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

**Table 82** 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

**Table 83** 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

## Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the NBG4604.

Once you have decided on the network number, pick an IP address for your NBG4604 that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your NBG4604 will compute the subnet mask automatically based on the IP address



that you entered. You don't need to change the subnet mask computed by the NBG4604 unless you are instructed to do otherwise.

### Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space*.

# 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: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

## Internet Explorer Pop-up Blockers

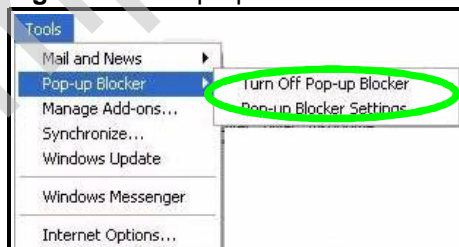
You may have to disable pop-up blocking to log into your device.

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**.

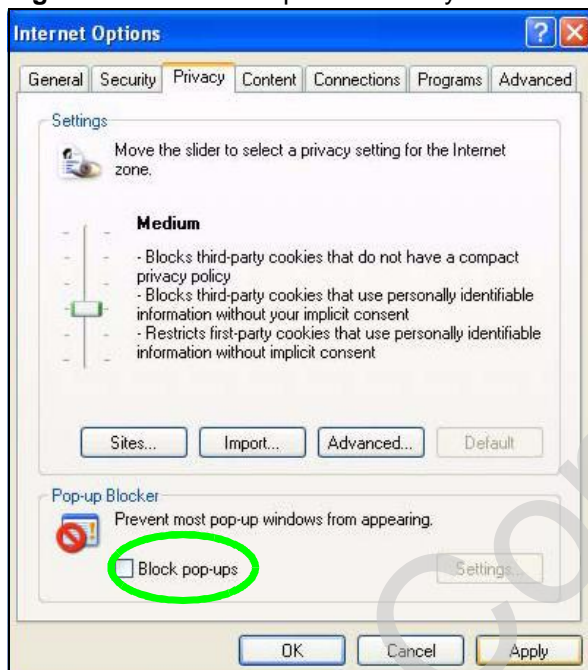
Figure 126 Pop-up Blocker



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 127** Internet Options: Privacy



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

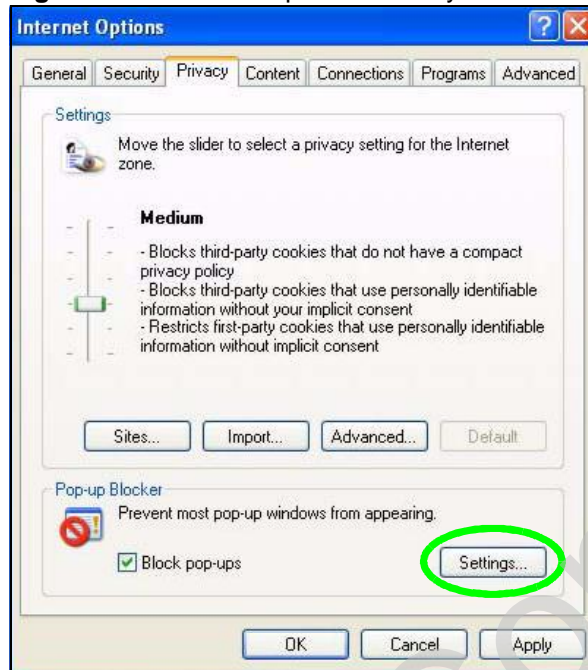
### Enable pop-up Blockers with Exceptions

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.

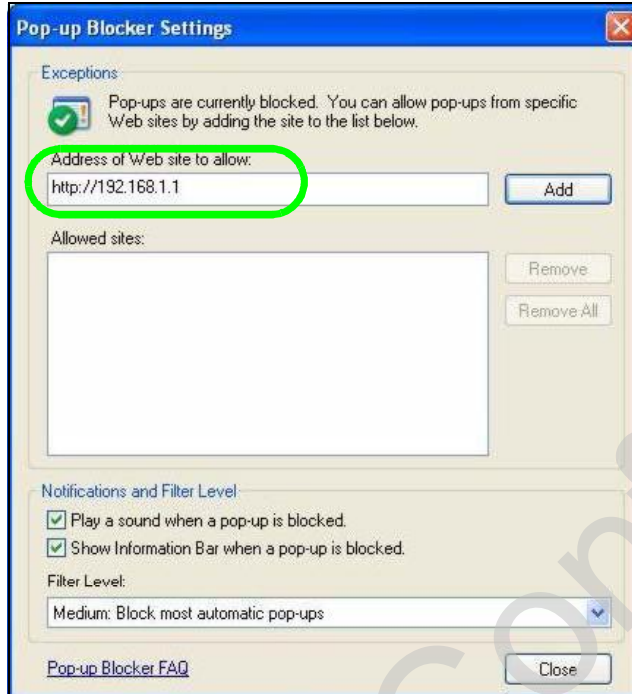
**Figure 128** Internet Options: Privacy



- 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 129** Pop-up Blocker Settings



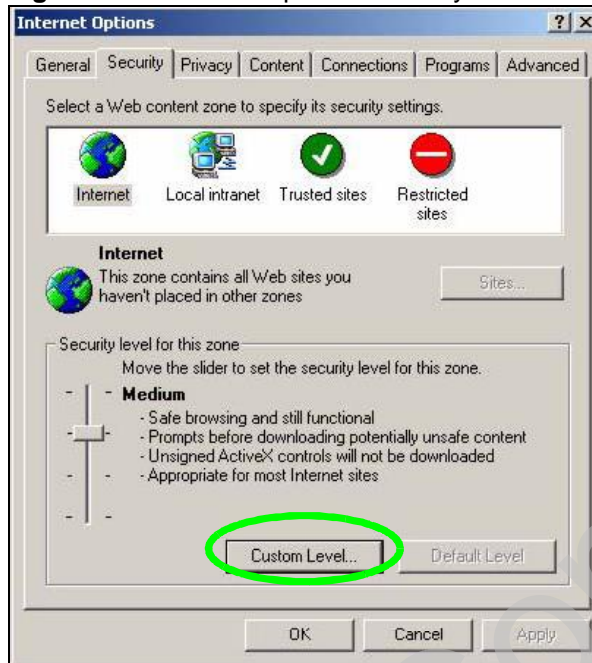
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

## JavaScripts

If pages of the Web Configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

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

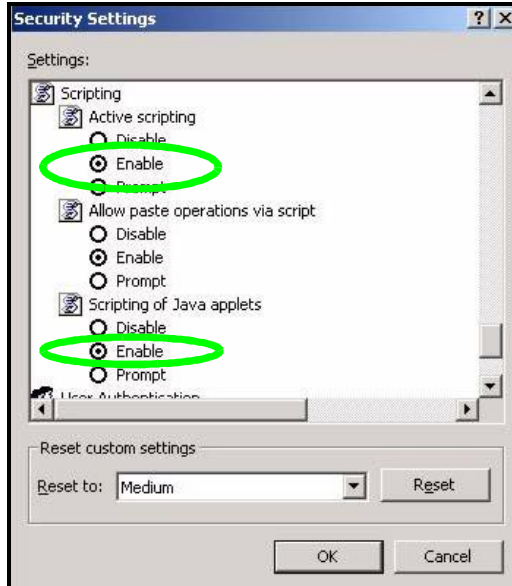
**Figure 130** Internet Options: Security



- 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 131** Security Settings - Java Scripting

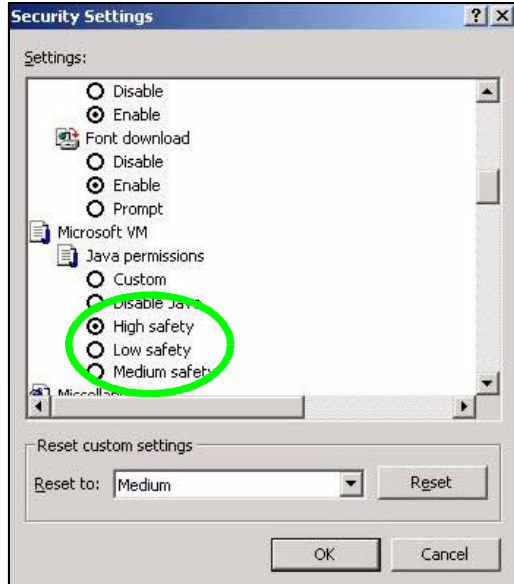


## Java Permissions

- 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 132** Security Settings - Java



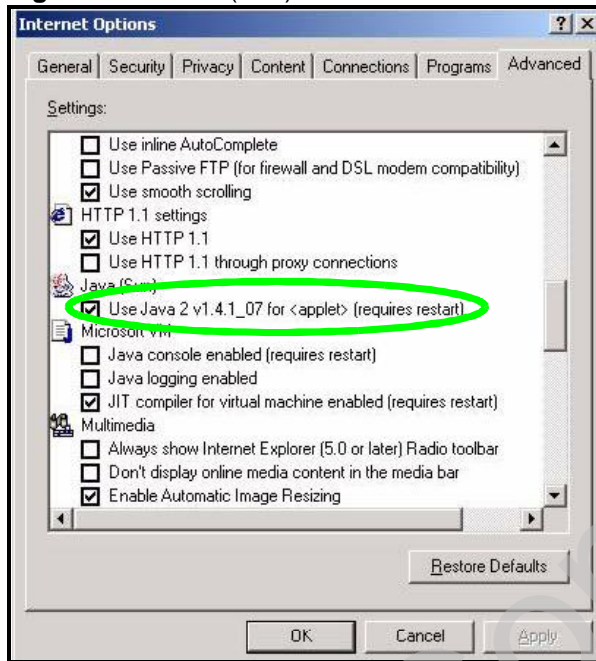
### JAVA (Sun)

- 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 133** Java (Sun)



C

## Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

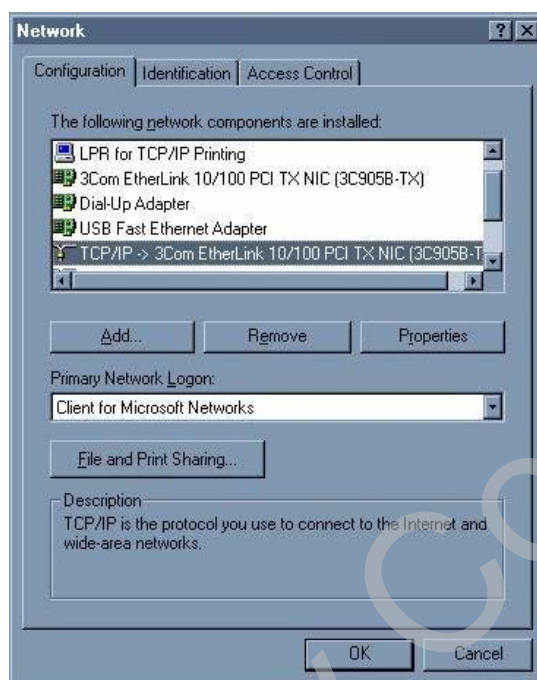
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

## Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

**Figure 134** Windows 95/98/Me: Network: Configuration



### Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.

- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

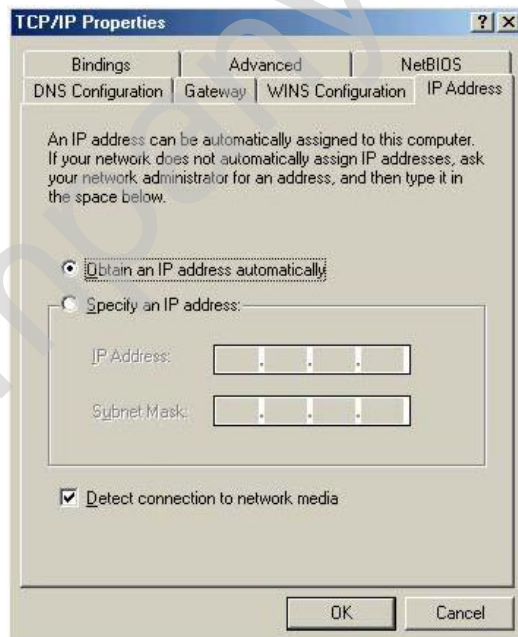
If you need Client for Microsoft Networks:

- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.
- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

## Configuring

- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
  - If your IP address is dynamic, select **Obtain an IP address automatically**.
  - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

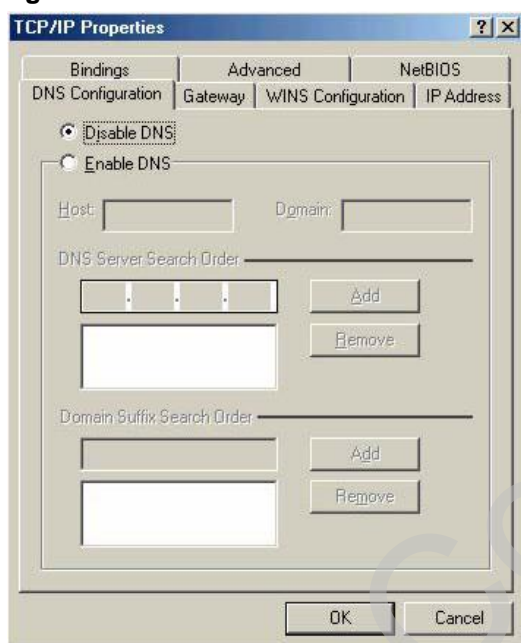
**Figure 135** Windows 95/98/Me: TCP/IP Properties: IP Address



3 Click the **DNS Configuration** tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 136** Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway** field and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your Prestige and restart your computer when prompted.

### Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

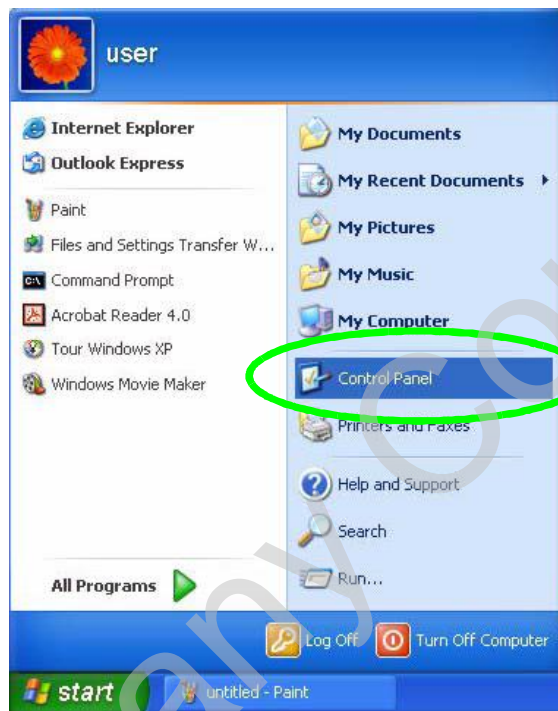
- 3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

- 1 Click start (Start in Windows 2000/NT), Settings, Control Panel.

**Figure 137** Windows XP: Start Menu



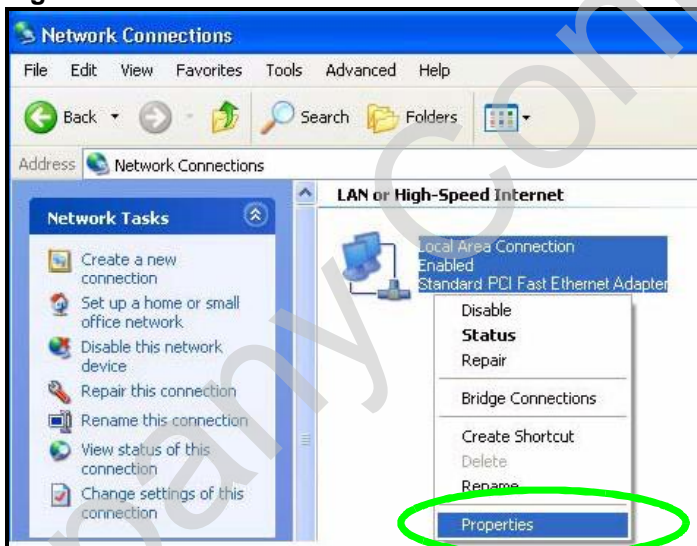
- 2 In the Control Panel, double-click Network Connections (Network and Dial-up Connections in Windows 2000/NT).

Figure 138 Windows XP: Control Panel



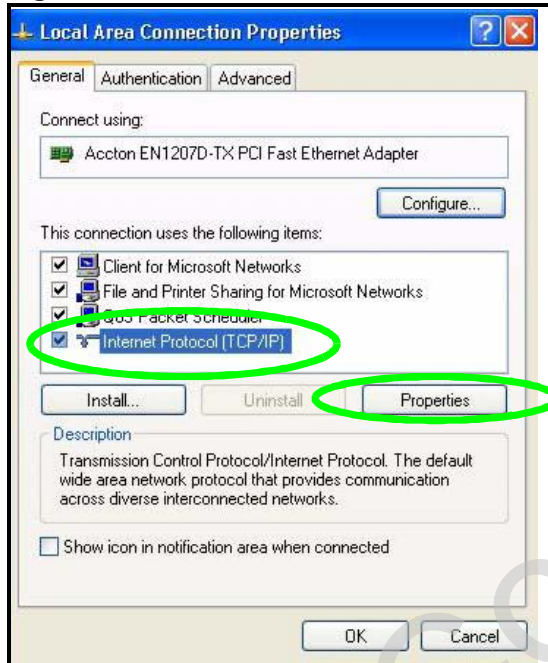
- 3 Right-click Local Area Connection and then click Properties.

Figure 139 Windows XP: Control Panel: Network Connections: Properties



- 4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

**Figure 140** Windows XP: Local Area Connection Properties

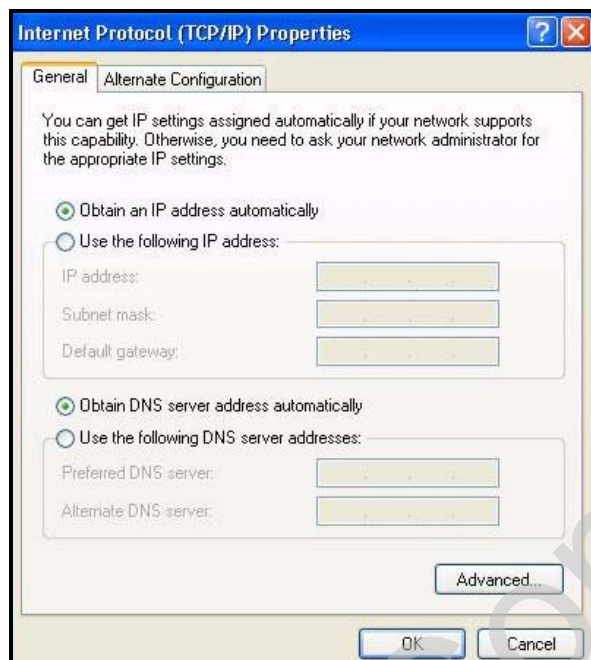


- 5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).
  - If you have a dynamic IP address click **Obtain an IP address automatically**.
  - If you have a static IP address click **Use the following IP Address** and fill in the IP address, Subnet mask, and Default gateway fields.



- Click **Advanced**.

**Figure 141** Windows XP: Internet Protocol (TCP/IP) Properties



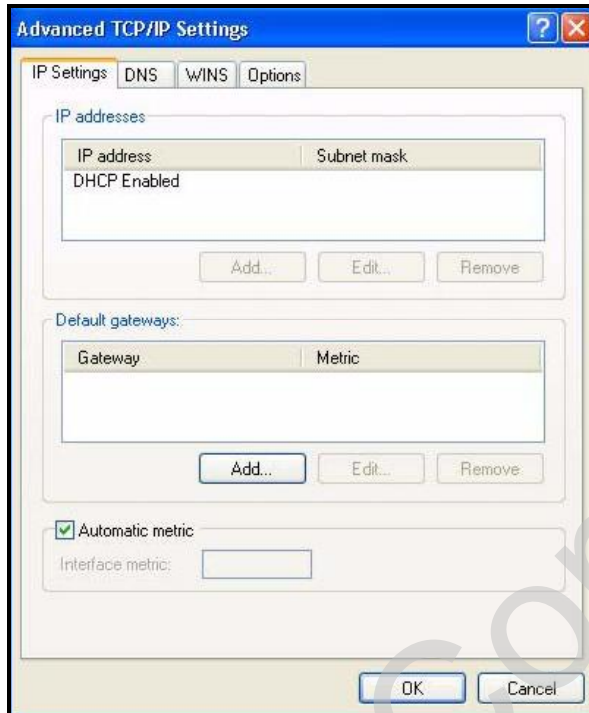
- 6 If you do not know your gateway's IP address, remove any previously installed gateways in the IP Settings tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in **IP addresses**, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

**Figure 142** Windows XP: Advanced TCP/IP Properties

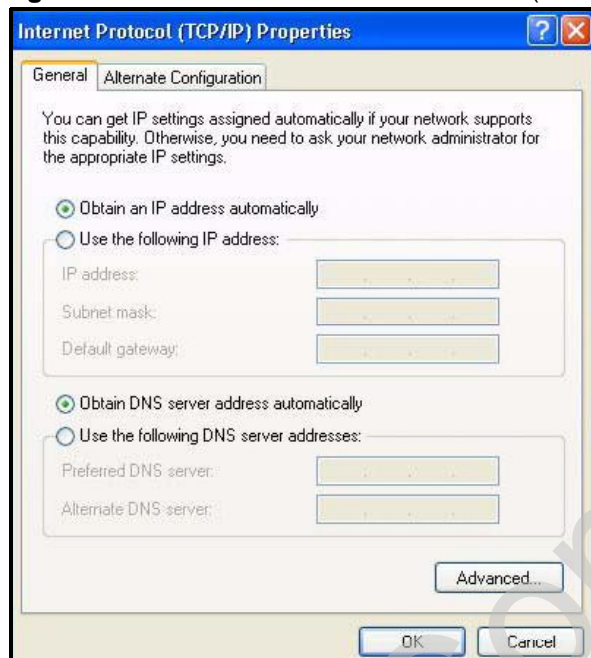


**7** In the Internet Protocol TCP/IP Properties window (the General tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the Preferred DNS server and Alternate DNS server fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 143** Windows XP: Internet Protocol (TCP/IP) Properties



- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 Click **Close (OK in Windows 2000/NT)** to close the **Local Area Connection Properties** window.
- 10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).
- 11 Turn on your Prestige and restart your computer (if prompted).

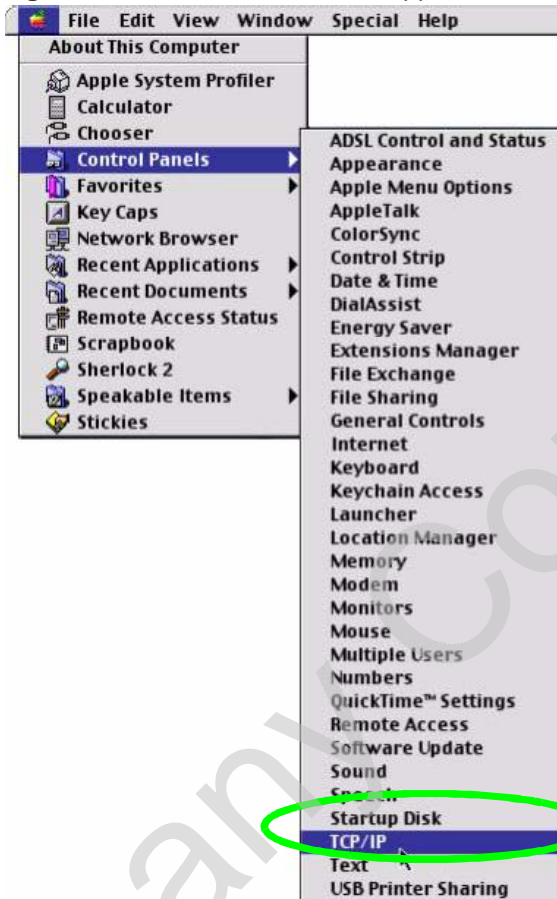
### Verifying Settings

- 1 Click **Start, All Programs, Accessories** and then **Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS 8/9

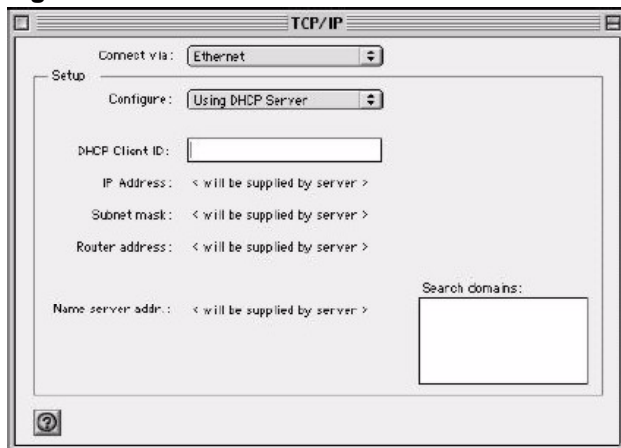
- 1 Click the **Apple menu**, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

**Figure 144** Macintosh OS 8/9: Apple Menu



- 2 Select **Ethernet built-in** from the **Connect via** list.

**Figure 145** Macintosh OS 8/9: TCP/IP



- 3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your Prestige in the **Router address** box.
- 5 Close the **TCP/IP Control Panel**.
- 6 Click **Save** if prompted, to save changes to your configuration.
- 7 Turn on your Prestige and restart your computer (if prompted).

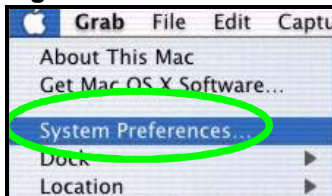
### Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

## Macintosh OS X

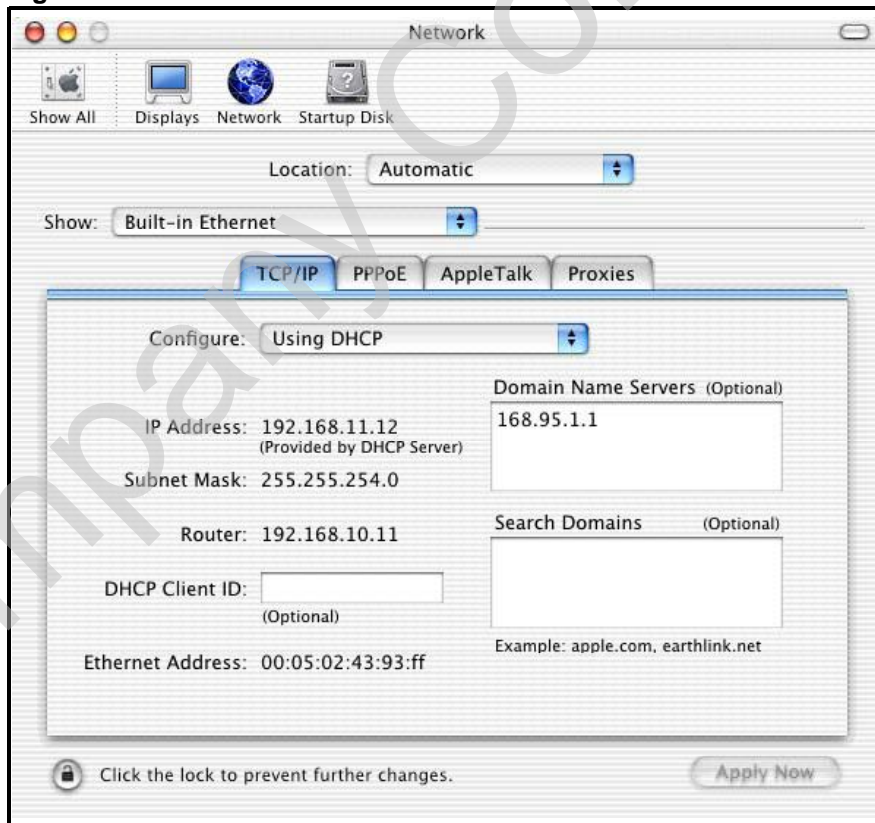
- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 146** Macintosh OS X: Apple Menu



- 2 Click **Network** in the icon bar.
  - Select **Automatic** from the **Location** list.
  - Select **Built-in Ethernet** from the **Show** list.
  - Click the **TCP/IP** tab.
- 3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 147** Macintosh OS X: Network



- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your Prestige in the **Router address** box.
- 5 Click **Apply Now** and close the window.
- 6 Turn on your Prestige and restart your computer (if prompted).

### Verifying Settings

Check your TCP/IP properties in the **Network** window.

## Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

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

### Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

- 1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

**Figure 148** Red Hat 9.0: KDE: Network Configuration: Devices



- 2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

**Figure 149** Red Hat 9.0: KDE: Ethernet Device: General



- If you have a dynamic IP address click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
  - If you have a static IP address click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.
- 3 Click **OK** to save the changes and close the **Ethernet Device General** screen.
  - 4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

**Figure 150** Red Hat 9.0: KDE: Network Configuration: DNS





- 5 Click the **Devices** tab.
- 6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes** to save the changes in all screens.

**Figure 151** Red Hat 9.0: KDE: Network Configuration: Activate



- 7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

### Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

- 1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.
  - If you have a dynamic IP address, enter `dhcp` in the `BOOTPROTO=` field. The following figure shows an example.

**Figure 152** Red Hat 9.0: Dynamic IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter `static` in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

**Figure 153** Red Hat 9.0: Static IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- 2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

**Figure 154** Red Hat 9.0: DNS Settings in `resolv.conf`

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

- 3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

**Figure 155** Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:           [OK]
Shutting down loopback interface:      [OK]
Setting network parameters:            [OK]
Bringing up loopback interface:        [OK]
Bringing up interface eth0:            [OK]
```

## 27.1.1 Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

**Figure 156** Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717  errors:0  dropped:0  overruns:0  frame:0
          TX packets:13  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

# Wireless LANs

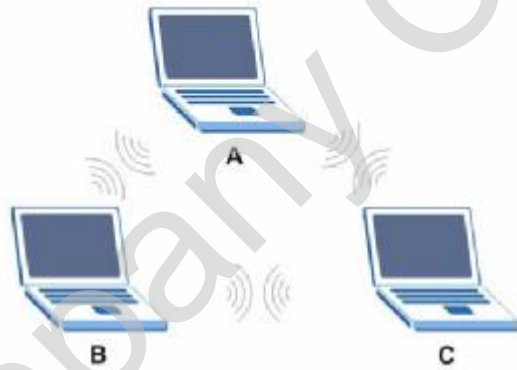
## Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

### Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

**Figure 157** Peer-to-Peer Communication in an Ad-hoc Network



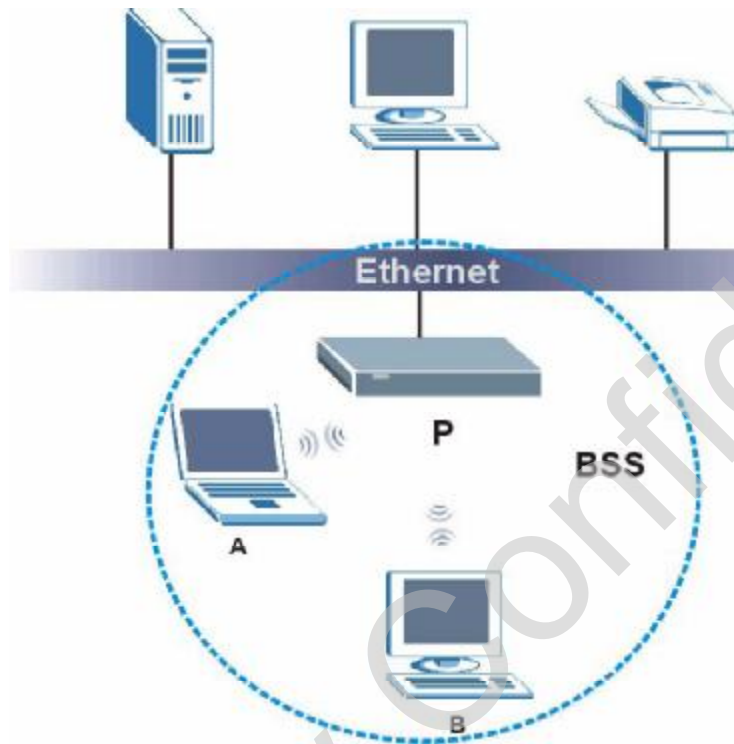
### BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate

with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

**Figure 158** Basic Service Set



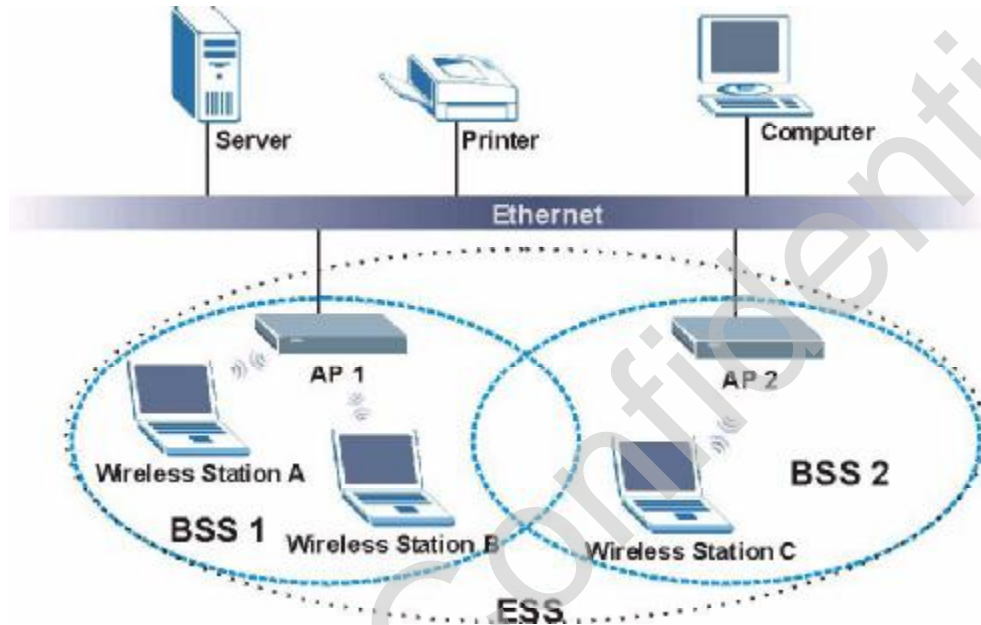
## ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS Identification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

**Figure 159** Infrastructure WLAN



## Channel

A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

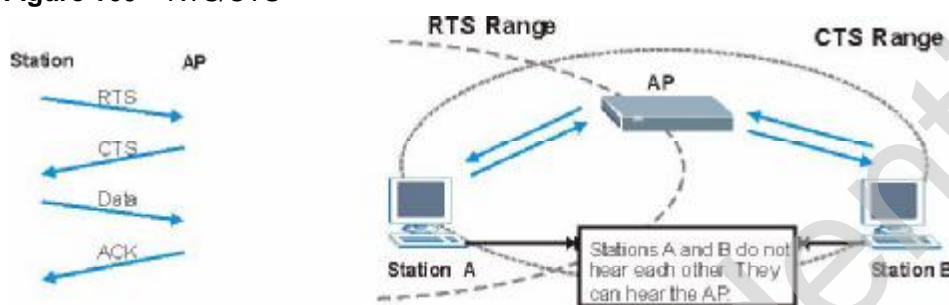
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

## RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or

wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

**Figure 160** RTS/CTS



When station A sends data to the AP, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An RTS/CTS defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the RTS/CTS value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified RTS/CTS directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure RTS/CTS if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the RTS/CTS value is greater than the Fragmentation Threshold value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach RTS/CTS size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

## Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the **RTS** (Request To Send)/**CTS** (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

## Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

Note: The AP and the wireless stations **MUST** use the same preamble mode in order to communicate.

## IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has



several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

**Table 84** IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/ 48/54	OFDM (Orthogonal Frequency Division Multiplexing)

## IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

## RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication  
Determines the identity of the users.
- Authorization  
Determines the network services available to authenticated users once they are connected to the network.
- Accounting  
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless station and the network RADIUS server.

## Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- **Access-Request**  
Sent by an access point requesting authentication.
- **Access-Reject**  
Sent by a RADIUS server rejecting access.
- **Access-Accept**  
Sent by a RADIUS server allowing access.
- **Access-Challenge**  
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- **Accounting-Request**  
Sent by the access point requesting accounting.
- **Accounting-Response**  
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

## Types of Authentication

This appendix discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

### EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

### **EAP-TLS (Transport Layer Security)**

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

### **EAP-TTLS (Tunneled Transport Layer Service)**

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

### **PEAP (Protected EAP)**

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

### **LEAP**

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

### **Dynamic WEP Key Exchange**

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with dynamic WEP key exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

**Table 85** Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

## WPA(2)

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.

### Encryption

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

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

WPA2 AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

### **User Authentication**

WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2 -PSK (WPA2 -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

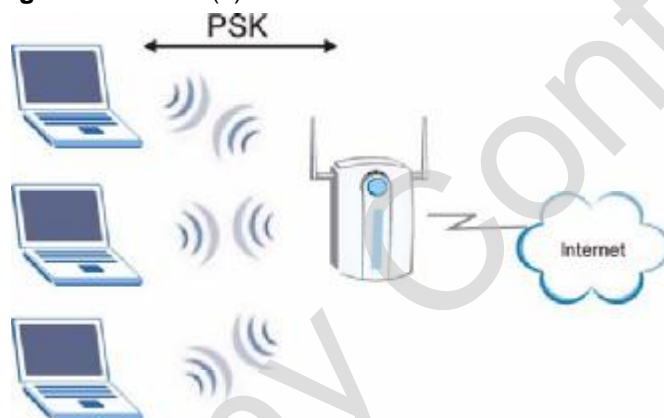
Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

## 27.1.2 WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
- 3 The AP derives and distributes keys to the wireless clients.
- 4 The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

**Figure 161** WPA(2)-PSK Authentication



## 27.1.3 WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

## Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

**Table 86** Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP	No	Enable
WPA-PSK	TKIP	Yes	Enable
WPA2	AES	No	Enable
WPA2-PSK	AES	Yes	Enable

# E

## Services

The following table lists some commonly-used services and their associated protocols and port numbers.

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

**Table 87** Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP	7648	A popular videoconferencing solution from White Pines Software.
	TCP/UDP	24032	
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (e.g. <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.



**Table 87** Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
FTP	TCP	20	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
	TCP	21	
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP	137	The Network Basic Input/Output System is used for communication between computers in a LAN.
	TCP/UDP	138	
	TCP/UDP	139	
	TCP/UDP	445	
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.

**Table 87** Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC: 1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.

**Table 87** Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP UDP	7000 user- defined	A videoconferencing solution. The UDP port number is specified in the application.

# Open Software Announcements

## End-User License Agreement for “NBG4604”

**WARNING:** ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED.

### 1. Grant of License for Personal Use

ZyXEL Communications Corp. (“ZyXEL”) grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the “Software”), including any documentation files accompanying the Software (“Documentation”), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

### 2. Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

### 3. Copyright

The Software and Documentation contain material that is protected by International Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

### 4. Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL listed in the below Table (collectively the “Open-Sourced Components”) You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components, which have been provided on the License Notice as below for the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the forego-

ing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the Software, and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

### 5. Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

### 6. No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERRUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

### 7. Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

### 8. Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

### 9. Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

### 10. Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying

or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11. General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

**NOTE:** Some components of this product incorporate source code covered under the open source code licenses. To obtain the source code covered under those Licenses, please check ZyXEL Technical Support ([support@zyxel.com.tw](mailto:support@zyxel.com.tw)) to get it.

### Open-Sourced Components

3rd party software	Version	Web Address Of The Software License Term
Linux Kernel-2.6.21	2.6.21	<a href="http://www.kernel.org/">http://www.kernel.org/</a>
busybox-1.7.5	1.7.5	<a href="http://www.busybox.net/">http://www.busybox.net/</a>
libesmtplib-1.0.4	1.0.4	<a href="http://www.stafford.uklinux.net/libesmtplib">http://www.stafford.uklinux.net/libesmtplib</a>
libupnp-1.6.0	1.6.0	<a href="http://pupnp.sourceforge.net/">http://pupnp.sourceforge.net/</a>
pcrc-6.7	6.7	<a href="http://www.pcre.org/">http://www.pcre.org/</a>
igmpproxy-0.1-beta2	0.1-beta2	<a href="http://sourceforge.net/projects/igmpproxy">http://sourceforge.net/projects/igmpproxy</a>
dnsmasq-2.39	2.39	<a href="http://thekelleys.org.uk/dnsmasq/doc.html">http://thekelleys.org.uk/dnsmasq/doc.html</a>
iproute2-2.6.16	2-2.6.16	<a href="http://www.linuxfoundation.org/en/Net:Iproute2">http://www.linuxfoundation.org/en/Net:Iproute2</a>
rp-pppoe-3.8	3.8	<a href="http://www.roaringpenguin.com/products/pppoe">http://www.roaringpenguin.com/products/pppoe</a>
iptables-1.3.8	1.3.8	<a href="http://www.netfilter.org/projects/iptables/index.html">http://www.netfilter.org/projects/iptables/index.html</a>
updatedd-2.6	2.6	<a href="http://freshmeat.net/projects/updatedd/">http://freshmeat.net/projects/updatedd/</a>
linuxigd-1	1	<a href="http://linux-igd.sourceforge.net/index.php">http://linux-igd.sourceforge.net/index.php</a>
wireless_tools-2.8	2.8	<a href="http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html">http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html</a>
bridge-utils-1.2	1.2	<a href="http://www.linuxfoundation.org/en/Net:Main_Page">http://www.linuxfoundation.org/en/Net:Main_Page</a>
pptp-client-1.7.1	1.7.1	<a href="http://pptpclient.sourceforge.net/">http://pptpclient.sourceforge.net/</a>
ppp-2.4.3	2.4.3	<a href="http://ppp.samba.org/">http://ppp.samba.org/</a>
udhcp-0.9.9-pre	0.9.9-pre	<a href="http://sources.busybox.net/index.py/trunk/udhcp-web/index.html?revision=9967">http://sources.busybox.net/index.py/trunk/udhcp-web/index.html?revision=9967</a>
ez-ipupdate-3.0.11b8	3.0.11b8	<a href="http://ez-ipupdate.com/">http://ez-ipupdate.com/</a>
uboot-1.1.3	1.1.3	<a href="http://www.denx.de/wiki/U-Boot">http://www.denx.de/wiki/U-Boot</a>
uclibc-0.9.29	0.9.29	<a href="http://www.uclibc.org/">http://www.uclibc.org/</a>
mtid-utils-1.2	1.2	<a href="http://git.infradead.org">http://git.infradead.org</a>
zlib-1.2.3	1.2.3	<a href="http://www.zlib.net/">http://www.zlib.net/</a>
usb_modeswitch-0.9.7	0.9.7	<a href="http://www.draisberghof.de/usb_modeswitch/">http://www.draisberghof.de/usb_modeswitch/</a>

#### Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes Linux Kernel-2.6.21, busybox-1.7.5, libesmtplib-1.0.4, igmpproxy-0.1-beta2, dnsmasq-2.39, iproute2-2.6.16, rp-pppoe-3.8, iptables-1.3.8, updatedd-2.6, linuxigd-1, wireless\_tools-2.8, bridge-utils-1.2, pptp-client-1.7.1, ppp-2.4.3, udhcp-0.9.9-pre, ez-ipupdate-3.0.11b8, uboot-1.1.3, mtd-utils-1.2, usb\_modeswitch-0.9.7 software under GPL 2.0 license.

#### GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

#### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

#### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)



These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system

in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes uclibc-0.9.29 software under LGPL license.

#### GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.  
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

#### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Pub-

lic Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get

it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it. For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODI-

## FICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").

Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote

it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable

source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not

compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities.

This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE

COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS.

This Product includes gcc-3.4.6 software under GPL 3.0 license

#### GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

##### Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program—to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

##### TERMS AND CONDITIONS

###### 0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well. To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently vis-

ible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

### 1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work’s System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

### 2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

### 3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work’s users, your or third parties’ legal rights to forbid circumvention of technological measures.

### 4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

### 5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

- a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
- b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.
- c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
- d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the



compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

**6. Conveying Non-Source Forms.**

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

- a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
- b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
- c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
- d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
- e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

**7. Additional Terms.**

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such

- material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

#### 8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

#### 9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

#### 10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party’s predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

#### 11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor’s “contributor version”.

A contributor’s “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor’s essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient’s use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate,

modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

#### **12. No Surrender of Others' Freedom.**

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

#### **13. Use with the GNU Affero General Public License.**

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

#### **14. Revised Versions of this License.**

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation. If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program. Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

#### **15. Disclaimer of Warranty.**

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

#### **16. Limitation of Liability.**

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### **17. Interpretation of Sections 15 and 16.**

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

#### **How to Apply These Terms to Your New Programs**

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

```
<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>
```

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>. Also add information on how to contact you by electronic and paper mail. If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

```
<program> Copyright (C) <year> <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box". You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/why-not-lgpl.html>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/licenses/why-not-lgpl.html>.

This Product includes libupnp-1.6.0, pcre-6.7, ppp-2.4.3 under BSD license

#### BSD

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes zlib-1.2.3 software under below license



License

/\* zlib.h -- interface of the 'zlib' general purpose compression library  
version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly [jloup@gzip.org](mailto:jloup@gzip.org)

Mark Adler [madler@alumni.caltech.edu](mailto:madler@alumni.caltech.edu)

\*/



# Legal Information

## Copyright

Copyright © 2010 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

## Disclaimer

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

## 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 Radiation Exposure Statement**

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- 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.

### IMPORTANT NOTE:

#### IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

### 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。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。減少電磁波影響，請妥適使用。

### Notices

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

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

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

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.



## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. 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](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](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.

## End-User License Agreement for "NBG-417N"

**WARNING:** ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

## 1 Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

## 2 Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

## 3 Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

## 4 Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL on its Open Source web site (<ftp://opensource.zyxel.com>) (collectively the "Open-Sourced Components") You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise

permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the online electronic documentation for the Software (<ftp://opensource.zyxel.com>), and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

#### 5 Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

#### 6 No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERRUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

#### 7 Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

#### 8 Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

#### 9 Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

#### 10 Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

## 11 General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

Note: NOTE: Some components of the Vantage CNM 2.3 incorporate source code covered under the Apache License, GPL License, LGPL License, Sun License, and Castor License. To obtain the source code covered under those Licenses, please check <ftp://opensource.zyxel.com> to get it.

# Index

## A

Address Assignment [102](#)  
Alert [183](#)  
alternative subnet mask notation [214](#)  
AP [21](#)  
AP (Access Point) [249](#)  
AP Mode  
  menu [58](#)  
  overview [55](#)  
  status screen [56](#)  
AP+Bridge [21](#)  
Auto-bridge [112](#)

## B

Backup configuration [190](#)  
Bandwidth management  
  overview [147](#)  
  priority [152](#)  
  services [153](#)  
BitTorrent [154](#)  
Bridge/Repeater [21](#)  
BSS [247](#)

## C

CA [254](#)  
Certificate Authority [254](#)  
certifications [281](#)  
  notices [283](#)  
  viewing [283](#)  
Channel [31](#), [57](#), [249](#)  
  Interference [249](#)  
channel [78](#)  
Configuration  
  backup [190](#)  
  reset the factory defaults [192](#)

  restore [191](#)  
content filtering [139](#)  
  by keyword (in URL) [140](#)  
  by web feature [139](#)  
copyright [281](#)  
CPU usage [31](#), [57](#)  
CTS (Clear to Send) [250](#)

## D

Daylight saving [180](#)  
DDNS [131](#)  
  see also Dynamic DNS  
  service providers [132](#)  
DHCP [34](#), [117](#)  
  DHCP server  
  see also Dynamic Host Configuration Protocol  
DHCP client information [120](#)  
DHCP client list [120](#)  
DHCP server [114](#), [117](#)  
DHCP table [34](#), [120](#)  
  DHCP client information  
  DHCP status  
Dimensions [207](#)  
disclaimer [281](#)  
DNS [50](#), [119](#)  
  DNS server  
  see also Domain name system  
DNS Server [102](#)  
DNS server [119](#)  
Domain name [41](#)  
  vs host name. see also system name  
Domain Name System [119](#)  
Domain Name System. See DNS.  
duplex setting [32](#), [58](#)  
Dynamic DNS [131](#)  
Dynamic Host Configuration Protocol [117](#)  
Dynamic WEP Key Exchange [254](#)  
DynDNS [132](#)

DynDNS see also DDNS [132](#)  
DynDNS Wildcard [131](#)

## E

EAP Authentication [253](#)  
e-mail [92](#)  
Encryption [255](#)  
encryption [80](#)  
    and local (user) database [80](#)  
    key [81](#)  
    WPA compatible [80](#)  
ESS [248](#)  
ESSID [204](#)  
Extended Service Set [248](#)  
Extended wireless security [44](#)

## F

Factory LAN defaults [114](#), [117](#)  
FCC interference statement [281](#)  
File Transfer Program [153](#)  
Firewall  
    ICMP packets [137](#)  
    ZyXEL device firewall [136](#)  
firewall  
    stateful inspection [135](#)  
Firmware upload [187](#)  
    file extension  
    using HTTP  
firmware version [31](#), [57](#)  
Fragmentation Threshold [251](#)  
FTP. see also File Transfer Program [153](#)

## G

gateway [144](#)  
General wireless LAN screen [81](#)

## H

Hidden Node [249](#)  
HTTP [153](#)  
Hyper Text Transfer Protocol [153](#)

## I

IANA [220](#)  
IBSS [247](#)  
IEEE 802.11g [251](#)  
IGMP [103](#)  
    see also Internet Group Multicast Protocol  
    version  
IGMP version [103](#)  
Independent Basic Service Set [247](#)  
Internet Assigned Numbers Authority  
    See IANA  
Internet connection  
    Ethernet  
    PPPoE. see also PPP over Ethernet  
    PPTP  
    WAN connection  
Internet connection wizard [44](#)  
Internet Group Multicast Protocol [103](#)  
IP Address [115](#), [125](#)  
IP address [50](#)  
    dynamic  
IP Pool [118](#)

## L

LAN [113](#)  
    IP pool setup [114](#)  
LAN overview [113](#)  
LAN setup [113](#)  
LAN TCP/IP [114](#)  
Language [197](#)  
Link type [32](#), [57](#)  
local (user) database [79](#)  
    and encryption [80](#)  
Local Area Network [113](#)

Log [184](#)

## M

MAC [87](#)

MAC address [79](#), [103](#)

cloning [52](#), [103](#)

MAC address filter [79](#)

MAC address filtering [87](#)

MAC filter [87](#)

Management Information Base (MIB) [168](#)

managing the device

good habits [22](#)

using the Web Configurator. See Web Configurator.

using the WPS. See WPS.

MBSSID [21](#)

Media access control [87](#)

Memory usage [31](#), [57](#)

Metric [145](#)

mode [21](#)

Multicast [103](#)

IGMP [103](#)

## N

NAT [123](#), [124](#), [172](#), [219](#)

how it works [123](#)

overview [123](#)

routers [172](#)

see also Network Address Translation

NAT traversal [159](#)

Navigation Panel [32](#), [58](#)

navigation panel [32](#), [58](#)

NetBIOS [104](#)

see also Network Basic Input/Output System [104](#)

Network Address Translation [123](#), [124](#)

## O

Operating Channel [31](#), [57](#)

operating mode [21](#)

## P

P2P [154](#)

peer-to-peer [154](#)

Point-to-Point Protocol over Ethernet [46](#), [106](#)

Point-to-Point Tunneling Protocol [47](#), [108](#)

Pool Size [118](#)

Port forwarding [125](#)

default server [125](#)

local server [125](#)

port speed [32](#), [58](#)

Power Specification [207](#)

PPPoE [46](#), [106](#)

benefits [46](#)

dial-up connection

see also Point-to-Point Protocol over Ethernet [46](#)

PPTP [47](#), [108](#)

see also Point-to-Point Tunneling Protocol [47](#)

Preamble Mode [251](#)

product registration [284](#)

## Q

Quality of Service (QoS) [90](#)

## R

RADIUS [252](#)

Shared Secret Key [253](#)

RADIUS Message Types [253](#)

RADIUS Messages [253](#)

RADIUS server [79](#)

registration

product [284](#)

related documentation [3](#)

Remote management [155](#)

and NAT [156](#)

and the firewall [155](#)

limitations [156](#)



- remote management session [155](#)
- system timeout [156](#)
- Reset button [29](#), [192](#)
- Reset the device [29](#)
- Restore configuration [191](#)
- RF (Radio Frequency) [208](#)
- RFC 3489 [172](#)
- Roaming [89](#)
- RTS (Request To Send) [250](#)
- RTS Threshold [249](#), [250](#)
- RTS/CTS Threshold [78](#), [89](#)

## S

- safety warnings [8](#)
- Scheduling [95](#)
- Security Parameters [258](#)
- Service and port numbers [154](#)
- Service Set [82](#)
- Service Set IDentification [82](#)
- Service Set IDentity. See SSID.
- services
  - and port numbers [259](#)
  - and protocols [259](#)
- Session Initiated Protocol [153](#)
- Simple Network Management Protocol, see SNMP
- SIP [153](#)
- SNMP [167](#), [168](#)
  - agents [168](#)
  - Get [168](#)
  - GetNext [168](#)
  - Manager [168](#)
  - managers [168](#)
  - MIB [168](#)
  - network components [167](#)
  - Set [168](#)
  - Trap [168](#)
  - versions [167](#)
- SSID [31](#), [78](#), [82](#)
- stateful inspection firewall [135](#)
- Static DHCP [118](#)
- Static Route [144](#)
- Status [30](#)

- subnet [211](#)
- Subnet Mask [115](#)
- subnet mask [50](#), [212](#)
- subnetting [215](#)
- Summary
  - DHCP table [34](#)
  - Packet statistics [35](#)
  - Wireless station status [36](#)
- syntax conventions [6](#)
- Sys Op Mode [193](#)
- System General Setup [177](#)
- System Name [178](#)
- System name [40](#)
  - vs computer name
- System restart [192](#)

## T

- TCP/IP configuration [117](#)
- Temperature [207](#)
- Time setting [179](#)
- trigger port [128](#)
- Trigger port forwarding [128](#)
  - example [129](#)
  - process [129](#)

## U

- Universal Plug and Play [159](#)
  - application [160](#)
- UPnP [159](#)
  - security issues [160](#)
- URL Keyword Blocking [141](#)
- Use Authentication [256](#)
- user authentication [79](#)
  - local (user) database [79](#)
  - RADIUS server [79](#)
- User Name [133](#)

**V**VoIP [153](#)VPN [108](#)**W**

## WAN

IP address assignment [49](#)WAN (Wide Area Network) [101](#)WAN advanced [111](#)WAN IP address [49](#)WAN IP address assignment [51](#)WAN MAC address [103](#)warranty [284](#)note [284](#)Web Configurator [22](#)how to access [27](#)Overview [27](#)

Web configurator

navigating [29](#)WEP Encryption [85](#)WEP encryption [84](#)WEP key [84](#)Wildcard [131](#)Wireless association list [36](#)wireless channel [204](#)wireless LAN [204](#)wireless LAN scheduling [95](#)Wireless LAN wizard [42](#)

## Wireless network

basic guidelines [78](#)channel [78](#)encryption [80](#)example [77](#)MAC address filter [79](#)overview [77](#)security [78](#)SSID [78](#)Wireless security [78](#)overview [78](#)type [78](#)wireless security [204](#)Wireless tutorial [55, 63](#)WPS [63](#)Wizard setup [39](#)complete [53](#)Internet connection [44](#)system information [40](#)wireless LAN [42](#)

## WLAN

Interference [249](#)Security Parameters [258](#)World Wide Web [153](#)WPA compatible [80](#)WPA, WPA2 [255](#)WPS [22](#)WWW [92, 153](#)**X**Xbox Live [154](#)

Company Confidential