DIGISOL™

DG-BR4000N/E

150Mbps Wireless Broadband Router

User Manual

V1.0

2012-08-22

As our products undergo continuous development the specifications are subject to change without prior notice

COPYRIGHT

Trademarks:

DIGISOL™ is a trademark of Smartlink Network Systems Ltd. All other trademarks are the property of the respective manufacturers.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

Index

1. Product Information

1-1 Introduction and Safety Information

Thank you for purchasing DG-BR4000N/E 802.11n 150Mbps Wireless Broadband Router. DG-BR4000N/E is the best choice for Small office / Home office users, all computers and network devices can share a single xDSL / cable modem internet connection at high speed. Easy install procedures allow any computer users to setup a network environment in very short time - within minutes, even inexperienced. When the number of your computers and network-enabled devices grow, you can also expand the number of network slots by connecting a hub or switch, to extend the scope of your network.

All computers and IEEE 802.11b/g/n wireless-enabled network devices (including PDA, cellular phone, game console, and more) can connect to this wireless router without additional cabling. With a compatible wireless card installed in your PC, you can transfer files up to 150Mbps (transfer data rate).

Other features of this Wireless USB adapter include:

- Supports IEEE802.11b, IEEE802.11g, IEEE802.11n, IEEE802.3, IEEE802.3u, IEEE802.11i and IEEE802.11e.
- Transmission data rate is up to 150 Mbps.
- Supports WEP and WPA for secured data transmission.
- Supports DHCP server.
- Supports manual configuration of static routing.
- Supports version upgrade through Web page.
- Supports restoring the factory default settings.
- Supports demilitarized zone (DMZ).
- Supports DNS proxy and forwarding.
- Supports QoS.
- Supports UPnP.

5

- Supports WPS.
- Supports port mapping.
- Supports port triggering.
- Supports wireless repeater.
- Supports guest network.
- Supports restricting IP bandwidth.
- Supports filtering by keyword and domain name.
- Supports wireless security authentication.
- Supports 3 types of WAN connection modes, including static IP, dynamic IP and PPPoE.
- Supports remote access control.
- Supports firewall.
- Supports system status display.
- Supports backup and restoration of configuration file.

1-2 Safety Information

Before operating the wireless router, read the following safety information carefully:

- Use the power adapter that is packed within the device package. **DO NOT** use any other power adapter or it will damage the product.

- Pay attention to the power load of the outlet or the prolonged lines. An overburdened power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.

- Proper space left for heat dissipation is necessary to avoid any damage caused by overheating the device. The long and thin holes on the router are designed for heat dissipation, to ensure that the device works normally. **DO NOT** cover these cooling holes.

- **DO NOT** put this device close to a place where a heat source exists or high temperature occurs. Avoid exposing the device to direct sunlight.

- **DO NOT** place this device close to a place which is over damp or watery.

- **DO NOT** spill any liquid on this device.

- **DO NOT** connect this device to any PC or electronic product, unless our customer, engineer or your broadband provider instructs you to do this, because any wrong connection may cause any power or fire risk.

- **DO NOT** place this device on an unstable surface or support.

- When the device is connected to a computer, hub, router or switch, the Ethernet cable should be less than 100 meters.

- **DO NOT** place this device on an unstable surface or support. **DO NOT** place this device on the ground.

- Keep the device clean. Avoid any metal in the device.

- Place the device in the center of the area, and try to optimize the wireless coverage.

1-3 System Requirements

- A desktop computer with a network adapter (wired / WLAN). The PC should be installed with the TCP/IP protocol and should be able to access internet.
- Windows 2000/XP/Vista or Windows 7.
- Web Browser (Microsoft Internet Explorer 6.0 or above, Mozilla Firefox, Opera web browser, or Safari web browser).
- AC Power socket (100-240V 50 / 60 Hz)

1-4 Package Contents

Before you start using this wireless broadband router, please check if there's anything missing in the package, and contact your dealer of purchase to claim for missing items:

- Wireless Broadband router
- Power adapter (12V DC, 500mA)
- Quick Installation Guide
- Installation Guide CD (includes User manual, QIG & Utility)
- Patch Cord (1No.)

1-5 Get familiar with your new wireless broadband router

Top Panel

There are 8 LED indicators on the front panel of the wireless router. By observing their status, you can check whether the device runs normally.

The following table describes the status of LED indicators on the front panel.

LED Name	Light Status	LED Color	Description
Power	On	Green	Power is on.
	Off	-	Power is off or the device is down.
WLAN	On	Green	Radio switch is turned on.
	Blink	Green	Data is being transmitted.
	Off	-	Radio switch is shut off.
WPS	On	Green	Connection succeeds under Wi-Fi Protected Setup.
	Blink	Green	Negotiation is in progress under Wi-Fi Protected Setup.
	Off	-	Wi-Fi Protected Setup is disabled.
WAN	On	Green	Connection succeeds.
	Blink		Data is being transmitted.
	Off		No WAN connection.
LAN1/LAN2/ LAN3/LAN4	On	Green	LAN connection succeeds.
	Blink		Data is being transmitted.
	Off		No LAN connection.

Rear Panel
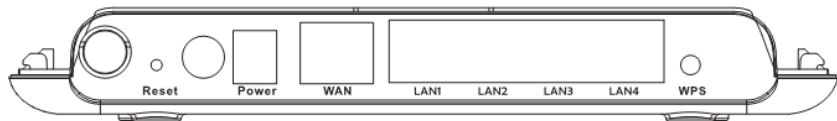
The following table describes interfaces and buttons on the rear panel.

Interface/Button	Description
Reset	Use a fine needle to press the Reset button gently until the unit reboots and then release the button. The unit reboots and restores to factory defaults.
Power	Power socket, for connecting the power adapter.
WAN	RJ45 WAN interface, for connecting WAN or the uplink network devices.
LAN1/LAN2/ LAN3/LAN4	RJ45 LAN interfaces, for connecting hub, switch or computer in a LAN.
WPS	This button is used for enabling WPS PBC mode. When WPS is enabled, press this button, and the AP starts accepting negotiation of PBC mode.

11

2. Connecting the Device

To connect the device, do as follows:

Step 1   Connect one end of the RJ45 cable to the LAN interface of the wireless router.

Step 2   Connect the other end of the RJ45 cable to your PC.

Step 3   Connect the power adapter to the power socket of the wireless router.

Power Adapter   PC
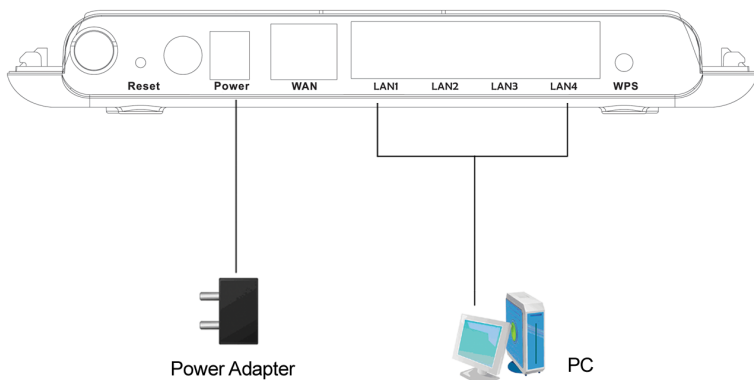
2-1 Operation Range

The operation range of the wireless router depends on the actual environment. The path and effect of signal transmission varies according to the deployment when in a house or an office. For example, the outdoor straight transmission distance for a certain device can be 300 meters and the indoor transmission distance can be 100 meters.

2-2 Roaming

Suppose several wireless routers run in the same network. Each wireless router serves as a BSS that has its coverage range. One wireless client (for example, a notebook PC or PDA) can roam from one AP to another AP accurately. In that case, the wireless client can communicate with the other devices within the coverage range of the wireless router.

For roaming in the coverage range of the wireless router by a wireless client, you need to set the APs properly as follows:

● Set the same SSID for different APs.

● The SSIDs of all the computers and PDAs should be consistent with that of APs.

● All the BSSs must use the same wireless channel.

● If the encryption function is enabled, all wireless routers must be configured with the same encryption mode and encryption key for establishing connection.

● Wireless routers must keep coverage of uninterrupted wireless signals in the whole operation environment. Hence, please place wireless routers at appropriate places.

2-3 TCP/IP Settings and Wireless Connection Introduction

By default, the LAN IP address of the wireless router is **192.168.2.1**, the subnet mask is **255.255.255.0** and the DHCP server is enabled.

It is recommended to set the network adapter to obtain an IP address automatically. Then, your PC obtains the TCP/IP settings, including the IP address, subnet mask, gateway and DNS address automatically through the wireless router. If you know the settings of the current LAN interface, you can manually set the TCP/IP properties of the network adapter, so that your PC can communicate with the wireless router.

To manually set the network adapter, do as follows:

Step 1   Right-click the icon of **My Network Places** and choose **Properties** from the menu. The **Network Connections** window appears.
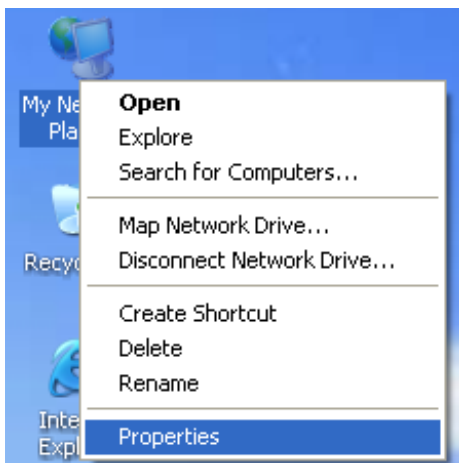
**Step 2**   Right-click the network adapter icon and choose **Properties** from the menu. The **Local Area Connections Properties** window appears.
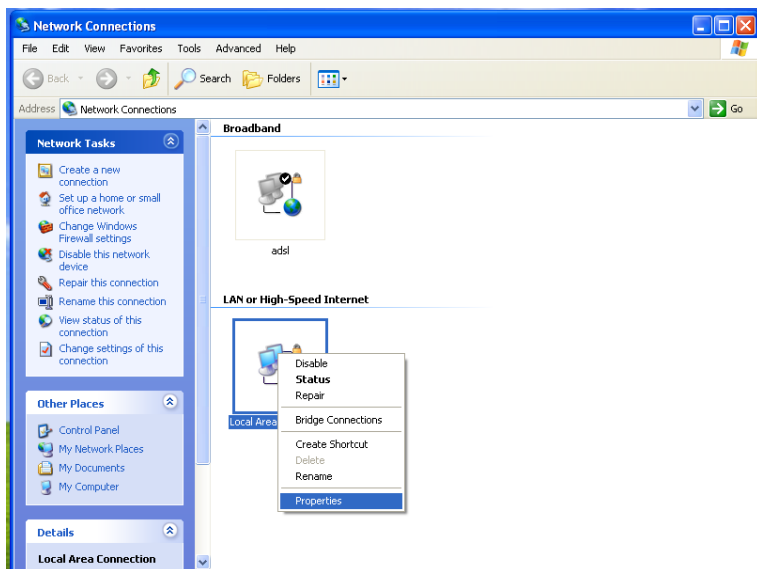
Note: If multiple network cards are installed on your PC, a window other than the Local Area Connection Properties window may appear.

Step 3   Double-click **Internet Protocol (TCP/IP)** and the **Internet Protocol (TCP/IP)**
             Properties window appears.
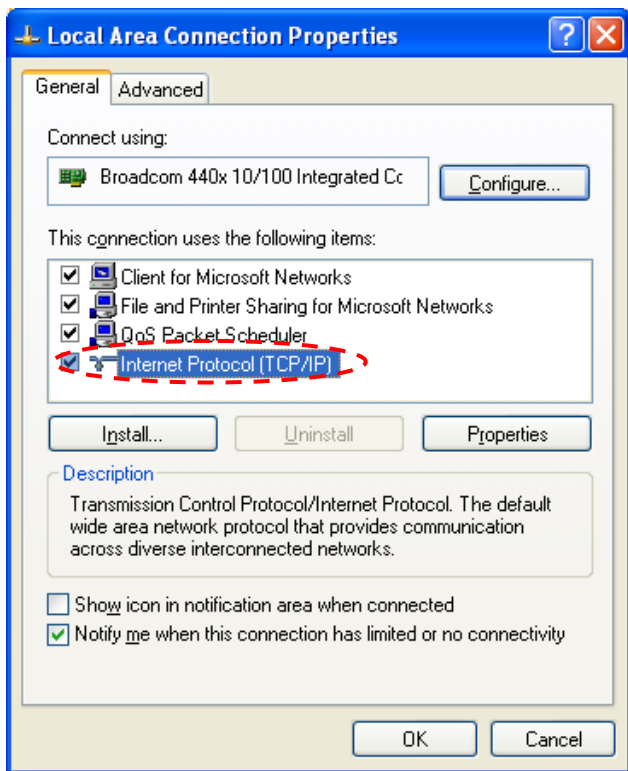
Step 4 Select Use the following IP address and enter the IP address of the network adapter. The IP address must be 192.168. 2. X (X is a number in the range of 2 to 254). If you want to access the Internet through a wireless router, you need to enter the default gateway and IP address of the DNS server correctly.
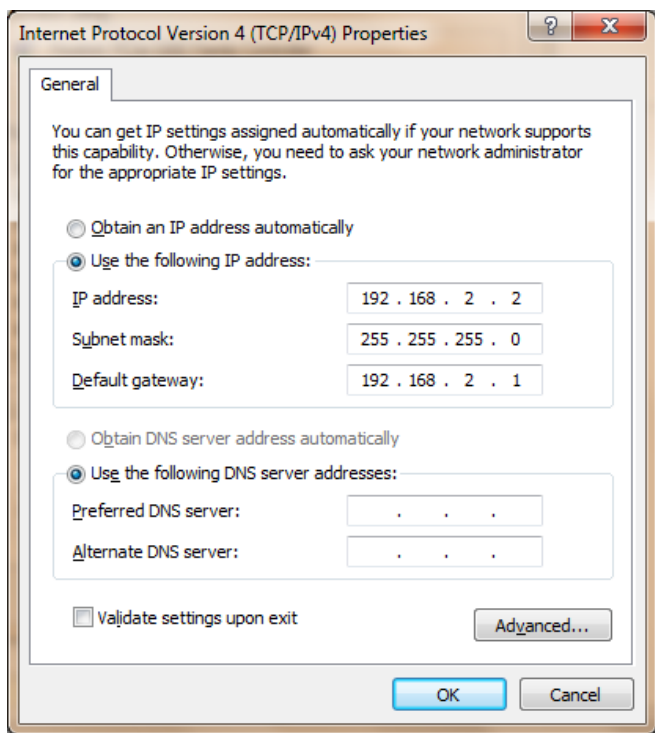
Step 5 Set the subnet mask and click **OK**.

17

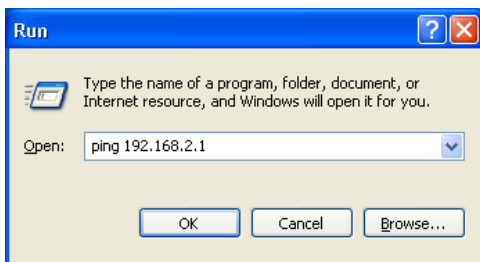**Step 6**   Next, you can ping the default IP address of the wireless router, to check whether the current connection between the PC and the wireless router is normal. Choose **Start > Run** from the desktop and enter ping 192.168.2.1.

Note: 192.168.2.1 in the ping command is the default IP address of the LAN interface. If the IP address changes, enter the current IP address instead.

Step 7   If the PC can ping through the default IP address of the wireless router, the following page appears, indicating that the connection between your PC and the wireless router is normal.

18
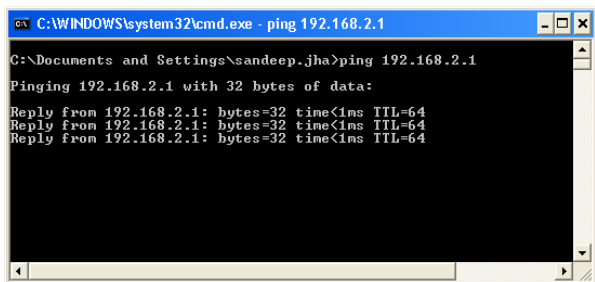
2-4 Wireless Connection

By default, the AP function of the wireless router is enabled. If you use a wireless network adapter, do as follows to establish the connection:

Step 1   Enable the wireless network adapter on your PC and ensure that the Wireless Zero Configuration tool is available. Right-click the **Wireless Network Connection** icon and choose **View Available Wireless Networks** from the menu.
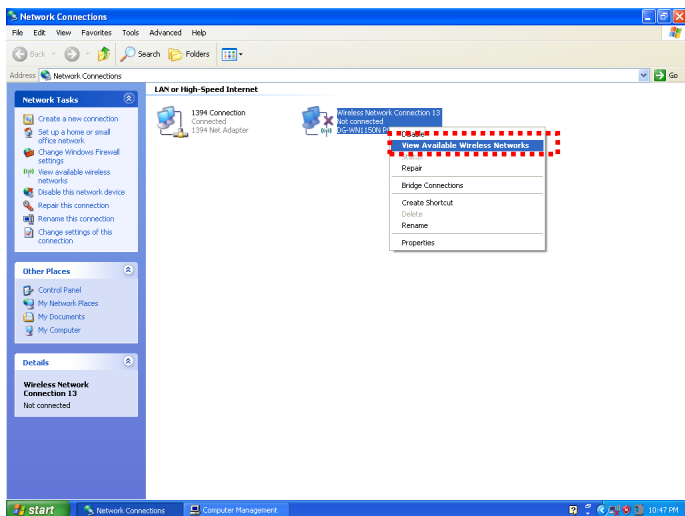
Step 2   In the Wireless Network Connection page, click Refresh network list and the network list is refreshed. The default SSID of the wireless router is DIGISOL. Select the wireless router that you want to connect and click **Connect**. The default wireless security mode is None, and you can connect the wireless router directly without the encryption key in this mode. If the wireless router is encrypted, you need to enter the correct key to connect to the wireless router.

20
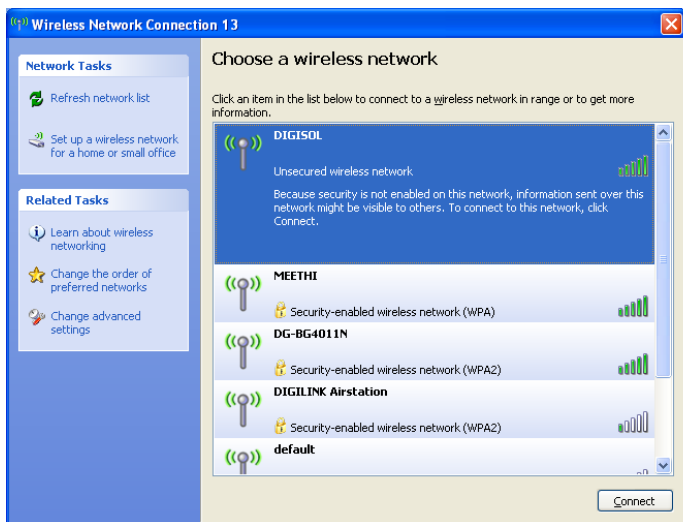
Step 3 If you are not sure of the available SSID, please log in to the Web page of the wireless router, and view the SSID in the **Wireless Basic Settings** page of the wireless settings. For more information about the wireless settings, please refer to **section 5-1 Wireless Basic Settings.**

Note: After your wireless network card connects to the wireless router successfully, you should set the network adapter to obtain an IP address automatically. The configuration of wireless connection is now complete.

21

3. Software Installation

➢ Insert the Setup CD into your CD-ROM drive of notebook/desktop computer.
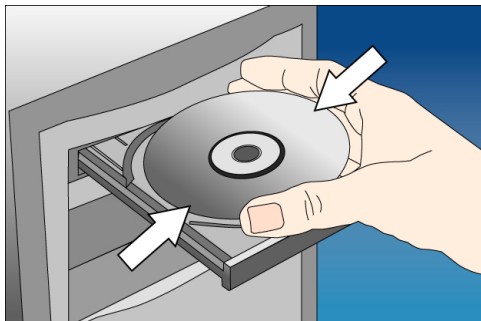
➢ Explore the CD and execute the "**Smart Wizard.exe**" file. Screen given below will be displayed. Click '**Next**' to continue.

➢ Connect one end of a network cable to the WAN port of the router and the other end to the DSL/Cable modem. Click '**Next**' to continue.
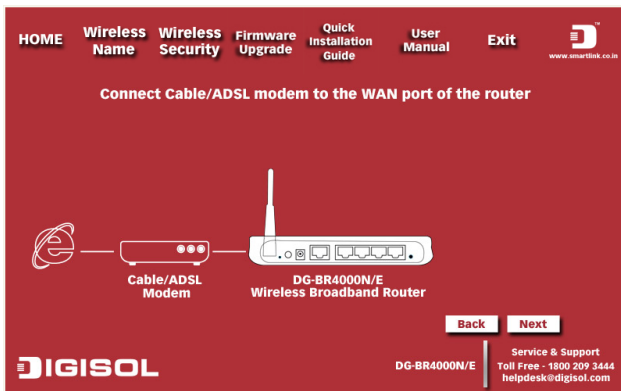
➢ Connect one end of the provided network cable to one of the LAN ports (1~4) of the router and the other end to your computer. Click '**Next**' to continue with the installation.
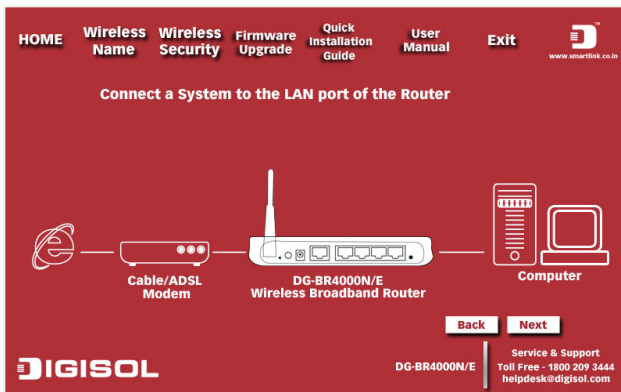
➢ Power on the Router. It will take approximately 30 seconds for the router to boot up completely. Ensure that all the LED's on the router are ON. If not, try the above steps again else click '**Next**' to continue.
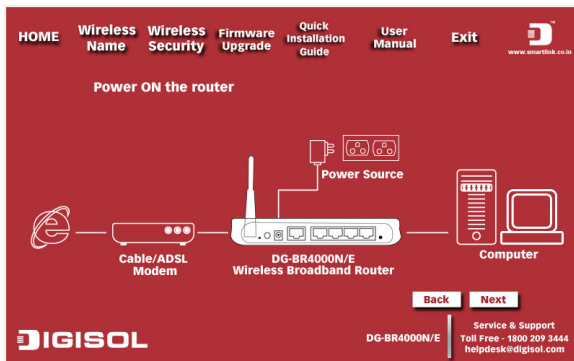
➢ Enter the Router's password to log in to the Router. The default password is "**1234**". Click **'Next'** to continue.
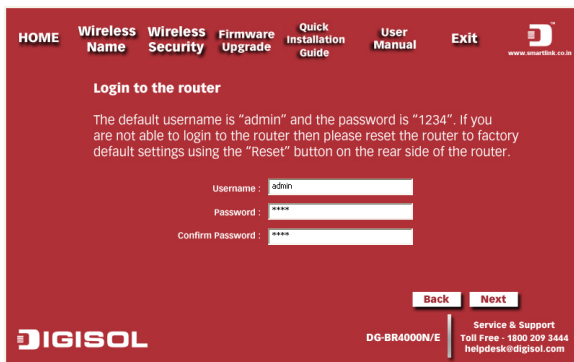
Note: The above mentioned steps are the common steps to be followed for all the types of internet connection. The procedure to be followed after these common steps for all the connection types have been explained below.

Dynamic IP (DHCP)

➢ Verify the Internet Connection Type the wizard has detected. If it is not correct, please configure it manually. Click '**Next**' to continue.
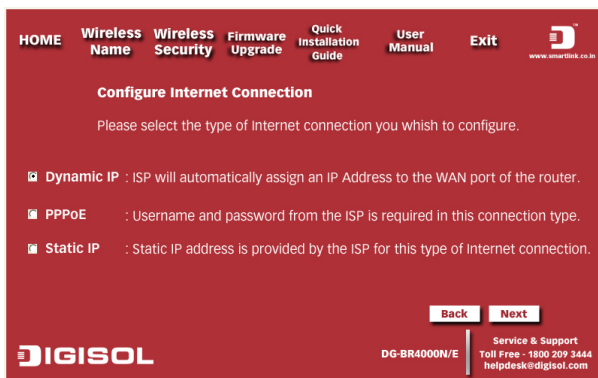
Note: If you are not sure which Internet Connection Type you use, please contact your Internet Service Provider for this information.

➢ Enter the host name and click on '**Next**'.

➢ Please wait while the Wizard tries to connect to the Internet. If you see the window "Internet Connection Successful", your router has been successfully connected to the Internet. Please click '**Next**' to configure the wireless settings.

26

➢ Configure a name for your wireless network. Click '**Next**' to continue.

➢ Click on '**Next**' and enter the preshared key in the screen shown below.

➢ Click on '**Next**' and the following summary will be displayed with the type of internet connection.

Static IP

➢ Select **'Static IP'** in the internet connection types and click on '**Next**'.

28

➢ Enter the static IP, the subnet mask, the default gateway and the DNS addresses as shown below. Then click on '**Next**'.

➢ Please wait while the Wizard tries to connect to the Internet. If you see the window "Internet Connection Successful", your router has been successfully connected to the Internet. Please click '**Next**' to configure the wireless settings.

29

➢ Configure a name for your wireless network. Click '**Next**' to continue.

➢ Click on '**Next**' and enter the preshared key in the screen shown below.

☎ 1800-209-3444 (Toll Free)
✉ helpdesk@digisol.com ✉ sales@digisol.com 🌐 www.digisol.com

➢ Click on '**Next**' and the following summary will be displayed with the type of internet connection.

PPPoE

➢ Select **'PPPoE'** in the internet connection types and click on '**Next**'.

➢ Enter the user name and password provided by your ISP then click **'Next'**.

➢ Please wait while the Wizard tries to connect to the Internet. If you see the window "Internet Connection Successful", your router has been successfully connected to the Internet. Please click 'Next' to configure the wireless settings.

➢ Configure a name for your wireless network. Click '**Next**' to continue.

➢ Click on '**Next**' and enter the preshared key in the screen shown below.

➢ Click on '**Next**' and the following summary will be displayed with the type of internet connection.

4. Logging In to the Web Page

Run the Internet Explorer (IE), enter **http://192.168.2.1/** (the default IP address of the wireless router) in the address bar, and press Enter.

In the window that is displayed as shown in the following figure, set the Language to English, enter the **user name** and **password**, and click Login.

Input username and password

UserName:

Password:

Login

Note: The default user name and password are admin and 1234 respectively.

35

After logging in to the Web page, you can view, configure and modify the router settings.

⚠ **Caution:**

If you are managing the wireless router through the Web page, do not cut off the power supply. Otherwise, the changed settings will not be saved

---

4-1 Web Configuration

Setup Wizard

You can set the basic network parameters for accessing Internet by following this wizard.

To configure the setup wizard, do as follows:

Step 1   After login, click Setup Wizard in the navigation bar on the left pane of the page. The Setup Wizard page shown below appears.

Setting up your internet

The smart setup wizard can detect the type of internet connection that you have.
Do you want the smart setup wizard to try and detect the connection type now?

⦿ Yes.
◯ No. I Want To Configure The Router Myself.
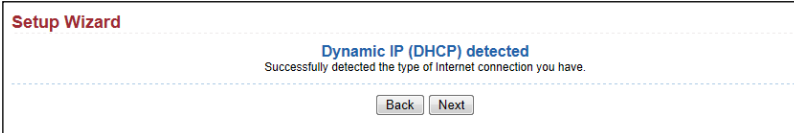
[Next]

If you are familiar with the router settings, you can select **No. I Want To Configure The Router Myself**. If you want to follow this wizard to configure the router, please select Yes and click **Next**. The router automatically detects the WAN connection mode.

Setup Wizard

||||||||||||||||||||||||||||||||||
Detecting Connection Type on Internet Port.
Please wait a moment ...

☎ 1800-209-3444 (Toll Free)
✉ helpdesk@digisol.com   ⧖ sales@digisol.com   🌐 www.digisol.com

Note: If you do not insert the network cable into the WAN interface of the wireless router, the previous page does not appear.

Step 2   The broadband type can be Dynamic IP (DHCP), Static IP (Fixed) or PPPoE.

1)   If the detected broadband type is Dynamic IP (DHCP), the following figure appears:

Setup Wizard

Dynamic IP (DHCP) detected
Successfully detected the type of Internet connection you have.

[Back] [Next]

Click **Next** and the following figure appears:

Dynamic IP Address

Account Name (If Required)   [   ]

[Finish] [Cancel]

Enter the host name provided by the Internet service provider (ISP) in the Account Name field. If the ISP does not provide it, you need not modify it.

In this mode, the WAN port of the wireless router obtains the network property information, including the IP address, subnet mask, gateway and IP address of the DNS server, from the connected DHCP server.

Next, click Apply and the settings take effect immediately. The setup wizard is now complete.

2) If the detected broadband type is Static IP (Fixed), the following figure appears:

Setup Wizard

Static IP (fixed) detected
Successfully detected the type of Internet connection you have.
If you believe you have received this message in error, please power cycle your modem (unplug the modem and plug it back in). Then close this screen, and reopen a new Web browser (e.g., Internet Explorer)

Back   Next

Click **Next** and the following figure appears:

Static IP (Fixed) Addresses

Your Internet service provides the static IP (Fixed) settings.

Be sure to enter the correct IP address for each static IP settings.For example, be sure to enter the Gateway IP Address in the Gateway Address fields and the IP Address in the IP Address fields without mixing them up.

Internet IP Address

IP Address	. . .
IP Subnet Mask	. . .
Gateway IP Address	. . .
Domain Name Server (DNS) Address	
Primary DNS	. . .
Secondary DNS	. . .

Finish   Cancel

The following table describes parameters in this page:

Item	Description
IP Address	Enter the IP address of the WAN interface.
IP Subnet Mask	Subnet mask of the WAN IP address. It is usually 255.255.255.0.
Gateway IP Address	Enter the IP address of the gateway if necessary.
Primary DNS	Enter the IP address of the primary DNS server if necessary.

Secondary DNS	If the ISP provides another DNS server, enter the IP address of that DNS server.

After the settings are done, click Apply and the settings will take effect immediately.

The setup wizard is now complete.

3) If the detected broadband type is PPPoE, the following figure appears:

Click **Next** and the following figure appears:

The following table describes parameters in this page:

Item	Description
Login	Enter the user name provided by the ISP.
Password	Enter the password provided by the ISP.
Service Name	Enter the service name provided by the ISP. If the ISP does

	not provide it, you need not enter any information.
Domain Name Server (DNS) Address	Select Use these DNS Servers and enter the IP address information of the DNS server provided by the ISP. If no DNS server information is available, select Get Automatically From ISP.
Primary DNS	Enter the IP address of the primary DNS server if necessary.
Secondary DNS	If the ISP provides another DNS server, enter the IP address of that DNS server.

Note: The user name and password are case-sensitive. If you have any querries about the user name and password, contact your ISP.

After the settings are done , click **Apply** and the settings take effect immediately. The setup wizard is now complete.

4-2 Running Status

Click **Running Status** and the extended navigation menu is shown as follows:
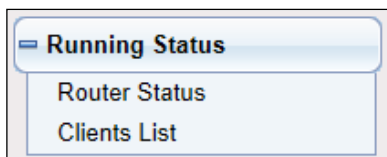
The submenu contains **Router Status** and **Clients List**.

4-3 Router Status

Choose **Running Status > Router Status** and the Router Status page appears.

Device Info

System Info	
Hardware Version	A
Firmware Version	V1.0.0
Product Name	DG-BR4000N/E 150 Mbps Wireless Broadband Router
Time and Date	2011-01-01 20:53:31
Internet Port	
MAC Address	00:17:7C:12:23:21
Internet Access Mode	Disconnected(DHCP)
IP address	0.0.0.0
IP Subnet mask	0.0.0.0
Default Gateway	0.0.0.0
Domain Name Server	0.0.0.0,0.0.0.0
LAN Port	
MAC Address	00:17:7C:12:23:20
IP Address	192.168.2.1
IP Subnet Mask	255.255.255.0
Wireless Port	
Wireless Network Name (SSID)	DIGISOL
Region	Asia
Wireless Channel	Auto
802.11 Mode	Mixed 802.11b/g/n
Wireless Radio	Enabled
Broadcast Name	ON
Wireless Isolation	OFF
Wi-Fi Protected Setup	ON
Wireless Security Mode	None

[Show Statistics] [Connection Status]

This page displays the information of the current running status of the device, including system information, connection status of the Internet port, LAN port, wireless port and traffic statistics of each port.

Click **Show Statistics** and the **Statistic Information page** as shown in the following figure appears:

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M/Full	1376	6115	0	98647	1461812	01:02:15
LAN 1	LinkDown						00:00:00
LAN 2	LinkDown	642	0	0	147632	0	00:00:00
LAN 3	LinkDown						00:00:00
LAN 4	LinkDown						00:00:00
WLAN	Auto	10591	76383	0	5833320	11332167	01:02:07

System Up Time   01:02:23

Poll Interval

5   (1~86400 secs) Set Interval   Stop

This page displays the performance statistics information of the router, including the number of sent and received packets at each port. The following table describes parameters in this page:

Item	Description
System Up Time	Displays the time period that the router is running.
Set Interval	Sets the interval for refreshing this page. Its value range is 1 to 86400 seconds. Enter a value in the field and click Set Interval. The settings take effect immediately. If you click Stop, this page displays the statistics information when the page is refreshed for the last time and it is not refreshed any more.

Click **Connection Status** in the Router Status page, and the Connection Status page appears.

This page displays the information of current connection on the router.

If the WAN connection is set to **PPPoE (Manually Connect)**, the Connection Status page is as shown in the following figure:
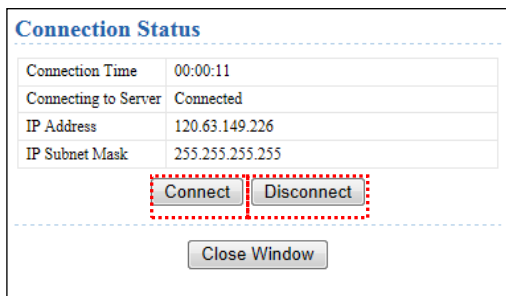
The following table describes buttons in this page:

Item	Description
Connect	Click the button to interrupt the WAN connection.
Disconnect	Click the button to start a new WAN connection.

If the WAN connection is set to **DHCP**, the Connection Status page is as shown in the following figure:

The following table describes buttons in this page:

Item	Description
Release	Click the button to release the IP address.
Renew	Click the button to obtain a new IP address.

If the WAN connection is set to any other mode, you can view the information, but not perform any settings, in the Connection Status page.

For detailed description of the WAN connection modes, refer to **section 4-7 WAN interface settings.**

4-4 Clients List

Choose **Running Status > Clients List** and the Clients List page appears.

Clients List

Wired Devices

#	IP Address	MAC Address	Device Name
1	192.168.2.3	14:FE:B5:C5:89:28	netadmin-PC

Wireless Devices(Wireless intruders also show up here)

#	IP Address	MAC Address	Device Name
1	192.168.2.5	00:17:7C:1B:E1:88	unknown

Refresh

This page displays the information of computers connected to the router, including the IP adress, device name and MAC address of each computer.
Click Refresh to refresh the information of the connected computers.

4-5 Network Settings

Click **Network Settings** and the extended navigation menu is shown as follows:

Network Settings
  LAN Interface Settings
  WAN Interface Settings
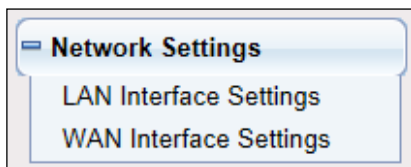
The submenu contains **LAN Interface Settings** and **WAN Interface Settings** as seen in the figure above.

4-6 LAN Interface Settings

Choose **Network Settings > LAN Interface Settings** and the LAN Interface Settings page appears.

In this page, you can configure the parameters of the LAN port. You can modify the IP address of the LAN port according to the actual network environment.

The following table describes parameters and buttons in this page:

Item	Description
IP Address	Set the IP address that a LAN user uses to access the router. The default IP is 192.168.2.1. You can change it if necessary.
IP Subnet Mask	Subnet mask of the LAN port. You can enter a different subnet mask according to the actual network status.
RIP Direction	The mode in which the router sends and receives RIP packets. If it is set to Both or Out Only, the router periodically broadcasts its routing table. If it is set to Both or In Only, the router integrates

	the received routing tables.
RIP Version	The format of the RIP packets and broadcast mode that the router sends them. RIP-1 is universally supported. Routing data sent by using RIP-2B or RIP-2M is in RIP-2 format. RIP-2B uses subnet broadcast and RIP-2M uses multicast.
Use Router as DHCP Server	If it is selected, the router serves as the DHCP server and automatically assigns IP addresses for all connected computers.
Starting IP Address	The first address in a consecutive IP address pool.
Ending IP Address	The last address in a consecutive IP address pool.
DHCP Lease Time (1 – 160 hours)	After the DHCP lease time elapsed, the router automatically assigns new IP addresses for all connected computers.
Address Reservation	If an IP address is reserved for the network card of a PC in a LAN, the network card obtains the same IP address every time the network card accesses the DHCP server.
Add	Click the button to add an entry in the Address Reservation page that is displayed.
Edit	Select an entry of reserved address and click the button to modify the IP address, MAC address or device name in the Address Reservation page that is displayed.
Delete	Select an entry of reserved address and click the button to delete it.

Click the **Add** button in the LAN Interface Settings page, and the **Address Reservation page** is as follows:

Address Reservation

	#	IP Address	Device Name	MAC Address
○	1	192.168.2.2	netadmin-PC	60:D8:19:21:9C:F1
○	2	192.168.2.4	smartlin-df86fc	00:17:7C:0B:C7:ED
○	3	192.168.2.3	netadmin-PC	14:FE:B5:C5:89:28
○	4	192.168.2.5	unknown	00:17:7C:1B:E1:88

IP Address

MAC Address

Device Name

Add Cancel Refresh

The following table describes parameters and buttons in this page:

Item	Description
Address Reservation Table	Displays entries of reserved addresses. You can select the information of the local computer, or enter the IP address, MAC address and device name of a computer, then click Add to add an entry to the Address Reservation Table.
IP Address	Enter the IP address to be reserved. It must be within the IP address pool.
MAC Address	Enter the MAC address of a computer whose IP address is to be reserved.
Device Name	Enter the device name of a computer whose IP address is to be reserved.
Add	Click the button to add the entry to the Address Reservation Table.
Cancel	Click the button to cancel the entry just set.
Refresh	Click the button to refresh the page.

48

After the settings are done, click **Add** to add an entry to the **Address Reservation Table**.

Note: 1) If your IP address is changed, you must use the new IP address to log in to the Web configuration page of the router and the default gateway of all hosts in the LAN must be set to the new IP address for Internet access.

2) The subnet mask of all hosts in the LAN must be consistent with the subnet mask specified in the LAN Interface Settings page.

4-7 WAN Interface Settings

Choose **Network Settings > WAN Interface Settings** and the WAN Interface Settings page appears.

49

The router supports 3 modes of WAN connection, including Dynamic IP (DHCP), Static IP (Fixed) or PPPoE. In this page, you can select the appropriate WAN connection and configure the relevant parameters according to the actual requirements.

● Dynamic IP (DHCP)

If you select static IP (DHCP), the router automatically obtains IP address, subnet mask and IP address of the gateway from the ISP. Select this connection mode if the ISP does not provide any IP network parameters. See the following figure:

WAN Interface Settings

Does your Internet Connection Require A Login?	○ Yes ● No
Account Name (If Required)	
Internet IP Address	
● Get Dynamically From ISP	
○ Use Static IP Address	
IP Address	
IP Subnet Mask	
Gateway IP Address	
Domain Name Server (DNS) Address	
● Get Automatically From ISP	
○ Use These DNS Servers	
Primary DNS	
Secondary DNS	
Router MAC Address	
● Use Default Address	
○ Use Computer MAC Address	
○ Use This MAC Address	00:17:7C:12:23:34

Apply   Cancel

The following table describes parameters in this page:

Item	Description
Does your Internet Connection Require A Login?	Select "No"
Account Name	Enter the host name provided by the ISP. If the ISP does not provide it, you need not modify it.
Internet IP Address	Select Get Dynamically From ISP.
Domain Name Service (DNS) Address	Enter the IP address of the DNS server provided by the ISP. If the ISP does not provide it, select Get Automatically From ISP.
Router MAC Address	Physical address of the router. Normally, you can select Use Default Address. If the ISP requires MAC address authentication, select Use Computer MAC Address or Use This MAC Address. If you select Use Computer MAC Address, the MAC address of the current computer serves as the MAC address of the router. If you select Use This MAC Address, you need to enter the MAC address of another computer. The format of a MAC address is XX:XX:XX:XX:XX:XX.

After the settings are done, click Apply to save the settings.

- Static IP (Fixed)

If the ISP provides information of IP address, subnet mask, gateway and DNS server, select Static IP (Fixed). For detailed settings, refer to your ISP.

WAN Interface Settings

Does your Internet Connection Require A Login?	○ Yes ● No
Account Name (If Required)	
Internet IP Address	
○ Get Dynamically From ISP	
● Use Static IP Address	
IP Address	
IP Subnet Mask	
Gateway IP Address	
Domain Name Server (DNS) Address	
○ Get Automatically From ISP	
● Use These DNS Servers	
Primary DNS	
Secondary DNS	
Router MAC Address	
● Use Default Address	
○ Use Computer MAC Address	
○ Use This MAC Address	00:17:7C:12:23:34

Apply   Cancel

The following table describes parameters in this page:

Item	Description
Does your Internet Connection Require A Login?	Select "No"
Account Name	Enter the host name provided by the ISP. If the ISP does not provide it, you need not modify it.
Internet IP Address	Select Use Static IP Address.
IP Address	Enter the WAN IP address provided by the ISP. It cannot be null.

52

IP Subnet Mask	Enter the WAN subnet mask provided by the ISP. It varies depending on the network type. It is usually 255.255.255.0 (Class C).
Gateway IP Address	Enter the IP address of the gateway provided by the ISP. It is the IP address used for connecting to the ISP.
Domain Name Service (DNS) Address	Select Use These DNS Servers.
Primary DNS	Enter the IP address of the primary DNS server if necessary.
Secondary DNS	If the ISP provides another DNS server, enter the IP address of that DNS server.
Router MAC Address	Physical address of the router. Normally, you can select Use Default Address. If the ISP requires MAC address authentication, select Use Computer MAC Address or Use This MAC Address. If you select Use Computer MAC Address, the MAC address of the current computer serves as the MAC address of the router. If you select Use This MAC Address, you need to enter the MAC address of another computer. The format of a MAC address is XX:XX:XX:XX:XX:XX.

After the settings are done, click Apply to save the settings.

● PPPoE

If the ISP provides the user name and password for PPPoE dialup, select PPPoE.

WAN Interface Settings

Does your Internet Connection Require A Login?	● Yes ○ No
Internet Service Provider	PPPoE ▼
Login	
Password	
Service Name (If Required)	
Connection Mode	Always On ▼
Idle Timeout (In minutes)	5
Domain Name Server (DNS) Address	
● Get Automatically From ISP	
○ Use These DNS Servers	
Primary DNS	
Secondary DNS	
Router MAC Address	
● Use Default Address	
○ Use Computer MAC Address	
○ Use This MAC Address	00:17:7C:12:23:34

Apply   Cancel

The following table describes parameters in this page:

Item	Description
Does your Internet Connection Require A Login?	Select "Yes"
Internet Service Provider	Select PPPoE.
Login	Enter the user name for PPPoE dialup provided by the ISP.
Password	Enter the password for PPPoE dialup provided by the ISP.

Service Name	If several PPPoE servers are available, specify one in this field.
Connection Mode	• Dial On Demand: If you select it, the system automatically establishes a connection when a network access request from the LAN is received. If no network access request is sent from the LAN within the set time of Idle Timeout, the system automatically interrupts the connection. If you pay for Internet access by time, you are recommended to use this connection mode, which effectively saves the expense of Internet access. • Always On: If you select it, the system automatically establishes a connection. If the network is disconnected because of external factors when you are using the Internet access service, the system tries connecting every time (for example, 10 seconds) until the connection is established. If you pay for Internet access in the monthly fee mode, you are recommended to use this connection mode. • Manually Connect: If you select it, you need to manually set dialup connection after startup.
Idle Timeout (In minutes)	If the system does not detect any Internet access behavior within the set time of idle timeout, the system interrupts the Internet connection.
Domain Name Server (DNS) Address	Enter the DNS address provided by the ISP. If the ISP does not provide it, select Get Automatically From ISP.
Primary DNS	Enter the IP address of the primary DNS server if necessary.
Secondary DNS	If the ISP provides another DNS server, enter the IP address of that DNS server.
Router MAC Address	Physical address of the router. Normally, you can select Use Default Address. If the ISP requires MAC address authentication, select Use Computer MAC Address or Use This MAC Address. If you select Use Computer MAC Address, the MAC address of the current computer serves as the MAC address of the router. If you

	select Use This MAC Address, you need to enter the MAC address of another computer. The format of a MAC address is XX:XX:XX:XX:XX:XX.

After the settings are done, click Apply to save the settings.

5. Wireless Settings

Click Wireless Settings and the extended navigation menu is shown as follows:

> ☐ **Wireless Settings**
> Wireless Basic Settings
> Guest Network
> WPS Setup
> Wireless Advanced Settings
> Wireless Repeater
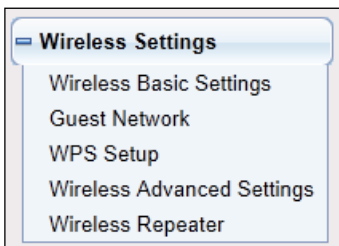
The submenu contains Wireless Basic Settings, Guest Network, WPS Setup, Wireless Advanced Settings and Wireless Repeater.

5-1 Wireless Basic Settings

Choose **Wireless Settings > Wireless Basic Settings** and the Wireless Basic Settings page appears. In this page, you can configure the basic wireless parameters.

Wireless Basic Settings	
Region Selection	
Region :	Asia
Wireless Network	
☑ Enable SSID Broadcast	
☐ Enable Wireless Isolation	
Name(SSID) :	DIGISOL
Mode :	Mixed 802.11b/g/n
Channel:	Auto
Band Width :	40M
Max Transmission Rate :	Auto Mbps
Security Options	
Security Options :	None

Apply   Cancel

The following table describes parameters in this page:

Item	Description
Region	Select the region where you are in from the drop-down list.
Enable SSID Broadcast	Enable or disable SSID broadcast. If it is enabled, the router broadcasts its SSID in the wireless network. In this way, wireless clients can find the SSID after scanning and hence join the corresponding wireless network.
Enable Wireless Isolation	Enable or disable wireless isolation. If it is selected, wireless clients that use this SSID can access the Internet, but cannot communicate with other wireless clients, Ethernet clients, or other devices.
Name (SSID)	Network name. The SSID can contain up to 32 characters and can be letters, numerals, hyphens and any combinations of them. The SSID is case-sensitive.
Mode	Select the appropriate wireless mode. The default is Mixed 802.11b/g/n. ● 802.11b only: The maximum rate is 11 Mbps. ● 802.11g only: The maximum rate is 54 Mbps. ● 802.11n only: For 20M bandwidth, the maximum rate is 72 Mbps (In short preamble); for 40M bandwidth, the maximum rate is 150 Mbps (In short preamble). You can select Long preamble or Short Preamble in the Wireless Advanced Settings page. For details, refer to section advanced wireless settings ● Mixed 802.11b/g: It is compatible with 802.11b and 802.11g. ● Mixed 802.11n/g: It is compatible with 802.11n and 802.11g. ● Mixed 802.11b/g/n: It is compatible with 802.11b, 802.11n and 802.11g.
Channel	Select the working channel of the wireless network. The default is Auto, which indicates that the wireless router automatically searches for the best channel in the available channels.

Band Width	Select the bandwidth.
Max Transmission Rate	Select one from the drop-down list that displays all rates that the system supports.
Security Options	Set the security encryption of the wireless network, to prevent unauthorized access and listening. You can select None, WEP, WPA-PSK(TKIP), WPA2-PSK(AES), or WPA-PSK(TKIP)+WPA2-PSK(AES). The following describes the security settings in detail.

Security Options

- None: Data encryption is not adopted and the network is not secure. Any station can access the network. This option is not recommended.

- WEP: Wired equivalent privacy. You can encrypt the data with WEP 64 bits or 128 bits.

The following table describes parameters related to the WEP mode:

Item	Description
Authentication Type	You can select Automatic or Shared Keys. The default is Automatic.
Encryption Strength	Select the encryption strength of WEP. You can select 64 bits or 128 bits.
Key 1/2/3/4	Select one from the four keys and enter the corresponding WEP key in the field. If the Encryption Strength is set to 64 bits, enter 10 hexadecimal digits. The key can be any combination of 0-9 and A-F. If the Encryption Strength is set to 128 bits, enter 26 hexadecimal digits. The key can be any combination of 0-9 and A-F.

- WPA-PSK (TKIP): Preshared key Wi-Fi protection access. It uses WPA-PSK standard encryption and Temporal Key Integrity Protocol (TKIP). TKIP has stronger encryption mechanism and integrates message integrity code (MIC) to protect against attacks of hackers.

The following table describes parameters related to the WPA-PSK (TKIP) mode:

Item	Description
PassPhrase	Enter 8-63 characters or 64 hexadecimal digits.

- WPA2-PSK(AES): Preshared key Wi-Fi protection access version 2. It uses WPA2-PSK standard encryption and Advanced Encryption Standard (AES). AES uses symmetric 128 bits block data to encrypt.

Security Options	
Security Options :	WPA2-PSK[AES]
Security Options(WPA2-PSK)	
PassPhrase :	(8-63 characters or 64 hex digits)

The following table describes parameters related to the WPA2-PSK(AES) mode:

Item	Description
PassPhrase	Enter 8-63 characters or 64 hexadecimal digits.

- WPA-PSK(TKIP)+ WPA2-PSK(AES): It allows the client to use WPA-PSK(TKIP) or WPA2-PSK (AES).

Security Options	
Security Options :	WPA-PSK[TKIP]+WPA2-PSK[AES]
Security Options(WPA-PSK+WPA2-PSK)	
PassPhrase :	(8-63 characters or 64 hex digits)
	Apply Cancel

The following table describes parameters related to the WPA-PSK(TKIP)+ WPA2-PSK(AES) mode:

Item	Description
PassPhrase	Enter 8-63 characters or 64 hexadecimal digits.

Note: After wireless settings are complete on the router, a host in the wireless network must have consistent wireless settings, including the SSID, with the router if the host wants to connect to the router. If the router has security settings, the host in the wireless network must have consistent security settings. For example, the passwords set on the host and the router must be the same. Otherwise, the host cannot connect to the router.

5-2 Guest Network

If you enable guest network, a visitor can use Internet connection in your home without knowing your wireless password.

Choose **Wireless Settings > Guest Network** and the Guest Network page appears.

Guest Network

Network Profiles

	Scheme	SSID	Security	Apply	SSID Broadcast
●	1	DIGISOL-Guest1	None	NO	YES
○	2	DIGISOL-Guest2	None	NO	YES

Wireless Settings--Profile 1

☐ Enable Guest Network
☑ Enable SSID Broadcast
☐ Allow Guest to access My Local Network
☐ Enable Wireless Isolation

Guest Wireless Network Name(SSID):   DIGISOL-Guest1

Security Options--Profile 1

Security Options :   None

[Apply] [Cancel]

The following table describes parameters in this page:

Item	Description
Network Profiles	Brief description of the created guest network. You can create up to four guest networks. A network profile contains the information of a guest network, including the number, SSID, encryption mode, whether the guest network is enabled and whether to broadcast SSID. You can select the radio button of a profile to view the detailed information or modify the settings.
Enable Guest Network	Enable or disable a guest network. After it is enabled, you and the visitor can connect to the network through the SSID of the guest network.
Enable SSID Broadcast	Enable or disable SSID broadcast. After it is enabled, the wireless AP broadcasts its SSID to all wireless stations.
Allow Guest to access My Local network	If it is enabled, users connected to the network of this SSID can access not only the Internet but also the LAN of the wireless router, like users connected to the network of the primary SSID. If this option is disabled, users connected to the network of this SSID cannot access the LAN of the wireless router.
Enable Wireless Isolation	Enable or disable wireless isolation. If it is enabled, wireless clients connected to the network of this SSID can access the Internet, but cannot communicate with other wireless clients or Ethernet clients.
Guest Wireless Network Name (SSID)	Name of the guest network. The SSID can contain up to 32 characters and can be any combination of letters, numerals and hyphen. It is case-sensitive.
Security Options	Refer to description and setting methods of Security Options in **section 10 Security options.**

After the settings are done, click Apply to save the settings.

5-3 WPS Setup

Choose **Wireless Settings > WPS Setup** and the WPS Setup page appears.

WPS Setup

New and easy way to connect to the Wireless Router via WiFi Protected setup (WPS)

A wireless client has to support WPS function in order to use this wizard to add the client to your WPS enabled Wireless Router.
Please check the user manual and gift box of your wireless client to see whether it supports the WPS function.
If your wireless client does not support the WPS function, you have to configure your wireless client manually so it has the same SSID and wireless security settings as on this router.

Next

WPS refers to Wi-Fi Protected Setup. You can use the WPS setup function to add a wireless client to a network, without setting specific parameters, such as SSID, security mode and password. To use this function, a wireless client must support WPS. If the wireless client does not support WPS, you must manually configure the wireless client to ensure that it has consistent SSID and wireless security settings with the router. There are two WPS modes: Push Button and PIN. Click Next to select the WPS mode.

● Push Button mode

Add WPS Client

Select a setup method:

◉ Push Button (recommended)

You can either press the Push Button physically on the router or press the Button below (soft Push Button). Start PBC

○ PIN (Personal Identification Number)

Select Push Button (recommended) and click Start PBC or press the WPS button on the router and the following page appears:

Connecting to New Wireless Client

Please click the software or hardware button on the client to start the WPS process...

Connecting[| | | | | | | | |]

Cancel

64

Press the button on the network card or click the button in the software page within two minutes to start WPS connection. After WPS connection is established, the following page appears. The client can now visit the LAN.

Success

The wireless client has been added to the network successfully.
Click OK to go back to the Wi-Fi Protected Setup page...

OK

- PIN mode

Add WPS Client

Select a setup method:

○ Push Button (recommended)

● PIN (Personal Identification Number)

If your Adapter supports WPS, please click on 'Generate a client Security Pin to input on the AP/Router/Gateway' and put the generated client PIN number here.

Enter Client's PIN: Start PIN
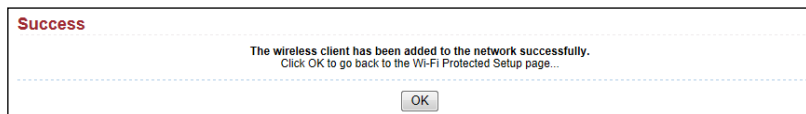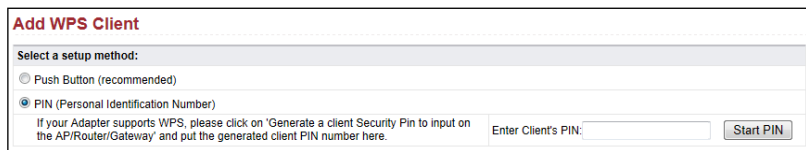
Select PIN (Personal Identification Number) and enter the PIN of the network (refer to the client of the network card), then click Start PIN to start WPS connection. The following page appears:

Connecting to New Wireless Client

The client's PIN is **47694965**.

Connecting[| | | |]

Cancel

Click the PIN button on the client of the network card within two minutes to start WPS connection. After WPS connection is established, the following page appears. The client can now visit the LAN.

Success

The wireless client has been added to the network successfully.
Click OK to go back to the Wi-Fi Protected Setup page...

OK
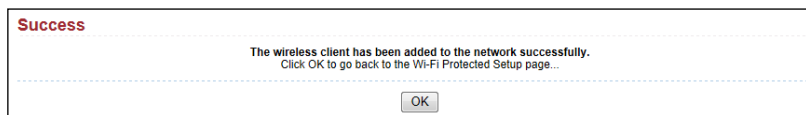
5-4 Wireless Advanced Settings

Choose **Wireless Settings > Wireless Advanced Settings** and the Wireless Advanced Settings page appears.

Wireless Advanced Settings

Wireless Advanced Setting	
☑ Enable Wireless Router Radio	
Fragmentation Length (256-2346)	2346
CTS/RTS Threshold (1-2347)	2346
Preamble Mode	Long preamble ▾
Transmit Power Control	100% ▾
WPS Settings	
Router's PIN:	12345670
☑ Enable WPS ☐ Disable Router's PIN ☑ Keep Existing Wireless Settings	
Wireless Access Control List	
Setup Access List	

Apply   Cancel

The following table describes parameters in this page:

Item	Description
Enable Wireless Router Radio	When this field is enabled you can connect to the router wirelessly.
Fragmentation Length (256-2346)	Set the threshold of fragmentation length. If the length of a packet is greater than the value, the packet is automatically fragmented into several packets. Because too many packets lead to low performance of the wireless network, the value of Fragmentation Length cannot be too small. The default value is 2346.
CTS/RTS Threshold (1-2347)	Set the CTS/RTS threshold. If the length of a packet is greater than the value, the router sends an RTS frame to the destination station to negotiate. After receiving the RTS frame, the wireless station responds with a Clear to Send (CTS) frame to the router,

	indicating that they can communicate with each other. The default value is 2346.
Preamble Mode	Set the preamble mode. The default is Long preamble. A preamble (especially the 802.11b High Rate/DSSS PHY field; 56 digits synchronized field for short preamble) defines the length of the CRC correction block for communication between wireless devices. Shorter settings should be applied in a network of intense traffics. Short preamble is mainly used to improve the efficiency of a wireless network for applications that have high requirement of real-time, such as streaming video and voice-over-IP telephony.
Transmit Power Control	Set the transmit power of the router. The default is 100%, which indicates to transmit full power.
Router's PIN	To configure wireless settings of the router through WPS, you need to enter PIN on the wireless client.
Enable WPS	Functions in the WPS Setup page are available only after this option is selected. If this option is not selected, the WPS Setup menu item is greyed out.
Disable Router's PIN	The PIN mode function in the WPS Setup page is available only after this option is selected. If this option is not selected, the PIN mode option is greyed out.
Keep Existing Wireless Settings	It determines whether WPS is configured on the router. If this option is not selected, newly added wireless clients change the wireless settings of the router into random SSID and security key that are automatically generated. You can select this option in the Wireless Basic Settings page.
Wireless Card Access Control List	You can set to allow only network cards of specific PCs to access your wireless network according to the MAC address of the network card of a PC. Click Setup Access List to add, edit, or delete entries in the Wireless Card Access List page.

Click Setup Access list button and the Wireless Card Access List page appears:

Wireless Access Control List

	Device Name	Mac Address
☐ Turn Access Control On		
	Add Edit Delete	

Apply Cancel

The following table describes parameters and buttons in this page:

Item	Description
Turn Access Control On	Enable or disable wireless access control. If it is selected, you can restrict wireless network cards according to their MAC addresses.
Add	Click the button to add an entry of wireless network card in the Wireless Card Access Setup page that is displayed.
Edit	Select an entry of wireless network card and click the button to modify the device name or MAC address in the Wireless Card Access Setup page that is displayed.
Delete	Select an entry of wireless network card and click the button to delete it.

Click the **Add** button and the **Wireless Card Access Setup** page appears:

Wireless Access Control Setup

Available Wireless Cards

	Device Name	Mac Address
○	netadmin-PC	60:D8:19:21:9C:F1
○	smartlin-df86fc	00:17:7C:0B:C7:ED
○	netadmin-PC	14:FE:B5:C5:89:28

Wireless Card Entry(Max of terms:16)

Device Name	
Mac Address	

Add Cancel Refresh

The following table describes parameters in this page:

Item	Description
Available Wireless Cards	It displays all the available wireless network cards of PCs and their MAC addresses. Click the radio button of a network card to select its MAC address. If the list does not contain your desired wireless network card, you can manually enter the MAC address of the wireless network card. You can enter up to 16 entries of MAC addresses.
Device Name	Name of the device. You can customize it.
Mac Address	Physical address of the network card. It is a string of 12 characters.

After the settings are done, click **Add** to add a wireless card entry. Then, click **Apply** to save the settings in the Wireless Advanced Settings page.

5-5 Wireless Repeater

Wireless distribution system (WDS) enables interconnection between APs in an IEEE 802.11 wireless network. It extends the wireless network through several APs, without connection of wired backbone network. This function is also called wireless repeating or bridging.

Choose **Wireless Settings > Wireless Repeating Function** and the Wireless Repeater page appears.

Wireless Repeater

☐ Enable Wireless Repeater

☐ Disable Wireless Clients Association

Wireless MAC of this router: 00:17:7C:12:23:20

◉ **Wireless Repeater**

Repeater IP Address: [192] [168] [2] [ ]

Basic Station MAC Address: [ ]

◯ **Wireless Basic Station**

Repeater MAC Address 1:   [ ]

Repeater MAC Address 2:   [ ]

Repeater MAC Address 3:   [ ]

Repeater MAC Address 4:   [ ]

[Apply] [Cancel]

The following table describes parameters in this page:

Item	Description
Enable Wireless Repeater	Enable or disable wireless repeating. If the channel is set to Auto, this function cannot be enabled. If you try enabling the function when the channel is set to Auto, the system gives an error and automatically switches to the Wireless Basic Settings page, where you can change the channel.

70

Disable Wireless Clients Association	If it is selected, clients cannot access the LAN.
Wireless Repeater	In this mode, the router serves as a repeater to communicate with the central base station.
Repeater IP Address	Enter the IP address of the repeater. It must be in the same network segment as the IP address of the central base station.
Basic Station MAC Address	Enter the physical address of the central base station.
Wireless Basic Station	In this mode, the router serves as the central base station to communicate with repeaters. You can add up to four repeaters. The central base station forwards the data of communication between repeaters to the destination repeaters. Repeaters should be configured accordingly.
Repeater MAC Address 1 2 3 4	Enter the physical address of the repeater.

After the settings are done, click Apply to save the settings.

6. Forwarding Rule

Click **Forwarding Rule** and the extended navigation menu is shown as follows:
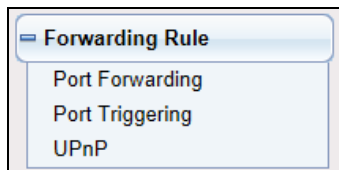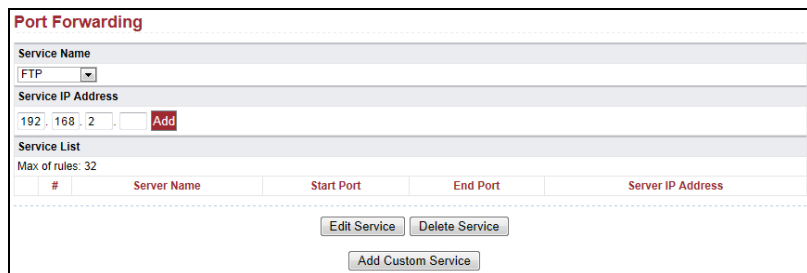
The submenu contains Port Forwarding, Port Triggering and UPnP.

6-1 Port Forwarding

By default, the firewall function of the router hides your LAN. As a result, other users on the Internet can detect only the router, but cannot access a certain PC in the LAN directly. If you want to access a PC in a LAN, you need to configure port forwarding on the router and map the desired port to the corresponding PC in the LAN. After receiving an access request from the Internet, the router forwards the packets to the PC according to the rule of port mapping. In this way, communication is successfully established between the Internet and the PC in the LAN.

Choose **Forwarding Rule > Port Forwarding** and the Port Forwarding page appears.

The following table describes parameters and buttons in this page:

Item	Description
Service Name	Select a service type from the drop-down list.
Service IP Address	Enter the IP address of the computer on which the service is to be provided.
Add	Click the button to add a service.
Service List	Displays the information of configured services, including the service name, start port, end port and server IP address.
Edit Service	Click the button to edit a service entry in the Ports - Custom Service page that is displayed.
Delete Service	Delete a service entry.
Add Custom Service	If the list does not contain your desired service, click the button to add a service in the Ports - Custom Service page that is displayed.

Click the Add Custom Service button and the Ports - Custom Service page appears:

Ports - Custom Service

Service Name:	
Protocol :	TCP
Starting Port	(1~65535)
Ending Port	(1~65535)
Server IP Address	192 . 168 . 2 .

Apply   Cancel

The following table describes parameters in this page:

Item	Description
Service Name	Add a custom name in this field.
Protocol	Indicate the protocol that is used at the mapping port. You can select TCP, UDP or TCP/UDP.
Starting Port	After the connection to the mapping port is established, the corresponding port is open and the application can initiate consequent connection requests to the open port.
Ending Port	Set the end port of the mapping port range.
Server IP Address	Enter the IP address of the computer on which the service is to be provided.

After the settings are done, click Apply to save the settings.

6-2 Port Triggering

Certain applications, such as WAN network games, video conferences and network calls, require multiple connections. Because of the firewall setting, these applications cannot work on a simple NAT router. However, certain special applications enable the applications to work on a NAT router. When an application sends a connection request to a trigger port, the corresponding ports are open, for later connection and service provision.

Choose **Forwarding Rule > Port Triggering** and the Port Triggering page appears.

Port Triggering

☐ Enable Port Triggering

Port Triggering Timeout(in minutes) 20 (1-9999)

Max of rules: 32

#	Server Name	Service Type	Required Inbound Connection	Service User

[Add Service] [Edit Service] [Delete Service]

[Apply] [Cancel]

74

The following table describes parameters in this page:

Item	Description
Enable Port Triggering	Enable or disable port triggering.
Port Triggering Timeout (in minutes)	Enter a value not greater than 9999. The timeout value controls the inactive timer at the specified ingress port. Upon timeout of the inactive timer, the ingress port is disabled.
Add Service	Click the button to add a rule in the Port Triggering – Services page that is displayed.
Edit Service	Click the button to edit a selected rule in the Port Triggering – Services page that is displayed.
Delete Service	Click the button to delete a selected rule.

Click the Add Service button and the Port Triggering – Services page appears:

The following table describes parameters in this page:

Item	Description
Service Name	Enter the service name.
Service User	You can select Any or Single address. • Any: Allow everybody in the user network to use the service. • Single address: Enter the IP address of the network card on the PC. Then, the service is applied only on the specific network card of the PC.
Service Type	Indicate the protocol used at the triggering port. You can select TCP, UDP or TCP/UDP.
Triggering Starting Port	The first port to which an application sends a connection request. All relevant ports can be open only after connection is established at this starting port. Otherwise, other relevant ports are not open.
Triggering Ending Port	Set the end port of the triggering port range.
Connection Type	You can select TCP, UDP or TCP/UDP.
Starting Port	When the connection to the triggering port is successful, the corresponding ports are open and the application can send consequent connection requests to the open ports.
Ending Port	Set the end port of the triggering port range.

After the settings are done, click Apply to add the rule of port triggering.

6-3 UPnP

By using the Universal Plug and Play (UPnP) protocol, a host at the LAN side can ask the router to realize specific port conversion, so that an external host can access resources on the internal host when necessary. For example, if MSN Messenger is installed on Windows ME and Windows XP operating systems, UPnP can be used for audio and video conversations. In this way, functions restricted by NAT can work properly.

Note: Only applications that support UPnP can use the function. The functionality of UPnP requires support by the application and operating systems such as Windows ME, Windows XP and Windows Vista.

Choose **Forwarding Rule > UPnP** and the UPnP page appears.

UPnP

☐ Turn UPnP On

Advertisement Period(in minutes)	30	
Advertisement Time To Live(in hops)	4	

UPnP Portable Table

Active	Protocol	Int. Port	Ext. Port	IP Address	Description

Apply   Cancel   Refresh

The following table describes parameters in this page:

Item	Description
Turn UPnP On	Enable or disable UPnP.
Advertisement Period (in minutes)	Set the broadcast interval. It indicates the interval for broadcasting the UPnP information by the router. The value should be in the range of 1 to 1440 minutes and the default is 30 minutes.
Advertisement Time To live (in hops)	The time for the broadcast to live. It is the number of hops after each UPnP packet is sent. The number of hops is the time taken for each packet to broadcast before it vanishes. The value should be in the range

77

	of 1 to 255 hops and the default is 4 hops.
UPnP Portable Table	This table shows the IP addresses of UPnP devices that are connected to the router and open (internal and external) ports on the devices. It also lists the types and status of the open ports.

7. Access Control

Click Access Control and the extended navigation menu is shown as follows:
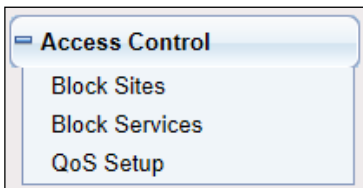
The submenu contains Block Sites, Block Services and QoS Setup.

7-1 Block Sites

Choose **Access Control > Block Sites** and the Block Sites page appears.

In this page, you can add or delete a filter rule of domain name or keyword, to block LAN users from accessing certain websites in the WAN. When a user tries accessing a restricted website, a message appears, indicating that the firewall restricts access to the website.

The following table describes parameters and buttons in this page:

Item	Description
Keyword Blocking	Select the mode of blocking. You can select Never, Per Schedule or Always. • Never: Website blocking is disabled. • Per Schedule: After you select it and set in System Tools > Schedules page, website blocking is enabled according to the settings in the Schedules page. • Always: Website blocking is always enabled.
Type Keyword or Domain Name Here	Enter the keyword or domain name that you want to block. Domain name: For example, www.facebook.com Keyword: Enter certain words, for example, blasphemy or erotic readings, included in a link.
Add Keyword	Click the button to add the keyword or domain name you entered to the list under the button.
Block Sites containing these Keywords or Domain Names	The list displays the blocked entries. It can contain up to 32 entries.
Delete Keyword	Select a keyword or domain name in the above list and click the button to delete it from the list.
Clear List	Click the button and all keywords and domain names are deleted from the list.
Allow Trusted IP Address To	After it is selected, the specified computer has the full authority of accessing the Internet.

Visit Blocked Sites	
Trusted IP Address	Specify the IP address of a computer. You need to enter only a numeral in the fourth field.

After the settings are done, click Apply to save the settings.

7-2 Block Services

Choose **Access Control > Block Services** and the Block Services page appears.

Block Services

Services Blocking
○ Never
○ Per Schedule
○ Always

Block Service Rules Table
Max of rules: 32

#	Service Name	Port	IP

Add   Edit   Delete

Apply   Cancel

In this page, you can set rules of service blocking, to block users from Internet access.

The following table describes parameters and buttons in this page:

Item	Description
Services Blocking	Select the mode of service blocking. You can select Never, Per Schedule or Always. • Never: Service blocking is disabled. • Per Schedule: After you select it and set in System Tools > Schedules page, service blocking is enabled according to the settings in the Schedules page. • Always: Service blocking is always enabled.
Block Service Rules Table	The table lists all services to be blocked. You can add, edit or delete a service entry according to your requirement.
Add	Click the button to add a rule of service blocking in the Block Services Setup page that is displayed.
Edit	Select a rule of service blocking in the Block Service Rules Table and click the button to edit the rule in the Block Services Setup page that is displayed.

Delete	Select a rule of service blocking in the Block Service Rules Table and click the button to delete it.

Click Add and the Block Services Setup page appears:

Block Services Setup

Service Type	User Defined
Protocol	TCP
Starting Port	(1~65535)
Ending Port	(1~65535)
Service Type/User Defined	
Filter Service For:	
○ Only This IP Address:	192 . 168 . 2 .
○ IP Address Range:	192 . 168 . 2 .
to	192 . 168 . 2 .
⦿ All IP Address:	

Add   Cancel

The following table describes parameters in this page:

Item	Description
Service Type	Select a service type from the drop-down list. If your desired type is not in the list, select User defined. Then, you need to select the protocol, enter the service name and specify the port range. For services that exist in the drop-down list, the corresponding information is already preset.
Protocol	Indicate the protocol that is used at the service ports. You can select TCP, UDP or TCP/UDP.
Starting Port	The first port to which an application sends a connection request. All relevant ports can be open only after connection is established at this starting port. Otherwise, other relevant ports are not open.
Ending Port	Set the end port of the service port range.

Service Type/User Defined	Enter the service name.
Filter Service For	It determines the computers to be blocked. Only This IP Address: Only one network card on a computer is blocked. You need to enter the IP address of a network card on a computer. IP Address Range: Network cards that correspond to a range of IP addresses are blocked. You need to enter the starting and ending addresses of the IP address range. All IP Address: Network cards of all computers are blocked.

After the settings are done, click **Add** to add a new rule. Then, click **Apply** to save the settings in the Block Services page.

7-3 QoS Setup

Choose **Access Control > QoS Setup** and the QoS Setup page appears.

The QoS function sets priority policies on applications, online games, Ethernet LAN ports and MAC addresses, sets an order for various network traffics, and thus optimizes your network performance.

The following table describes parameters in the QoS Setup page:

Item	Description
Enable WMM (Wi-Fi multi-media) Settings	Enable or disable WMM. Wireless Multimedia (WMM) is a subset of the 802.11e standard. It supports setting priorities of wireless traffics according to data types within a certain range. Time-related information such as audio and video has higher priority than normal data. To ensure proper performance of WMM, wireless clients must support WMM.
Turn Internet Qos Access On	Enable or disable QoS. After it is enabled, you can optimize the network access traffics according to the settings in the QoS Priority Table page.
Turn Bandwidth Control On	Set the maximum uplink bandwidth at the WAN port. If the value is in units of Kbps, the maximum value is 1000. If the value is in units of Mbps, the maximum value is 100.
Setup QoS rule	Click the button and the QoS Setup page is displayed
Enable Trusted IP Address	After it is enabled, you can reserve half egress bandwidth for a specified computer, to avoid impact to the computer because of Internet access behaviors by other users in the network.
Trusted IP Address	Specify the IP address of a computer. You need to enter only a numeral in the fourth field.

Click Setup QoS Rule and the QoS Setup page appears:

QoS Setup

#	QoS Policy	Priority	Description

Edit   Delete

Add Priority Rule

Apply

The following table describes the buttons in this page:

Item	Description
Edit	Click the button to change the priorities of the applications, LAN ports, online games and MAC addresses in the QoS Priority Table.
Delete	Click the button to delete a rule in the QoS Priority Table.
Add Priority Rule	Click the button to set priority policy for an online game, an application, an Ethernet LAN port, or the MAC address of a computer in the QoS – Priority Rules page that is displayed.

Click the Add Priority Rule button and the QoS – Priority Rules page for an application appears:

QoS - Priority Rules

Priority	
QoS Policy For	
Priority Category	Applications
Applications	Add A New Application
Priority	High

Specified Port Range	
Connection Type	TCP/UDP
Starting Port	(1 - 65535)
Ending Port	(1 - 65535)

Apply   Cancel

86

The following table describes parameters in this page:

Item	Description
QoS Policy For	Enter the name of the QoS policy.
Priority Category	Select Applications.
Applications	Select an application that you want to set. If your desired application is not in the drop-down list, select Add A New Application.
Priority	You can select Highest, High, Normal or Low.
Connection Type	Indicates the protocol that is used at the port. You can select TCP/UDP, TCP or UDP.
Starting Port	The first port to which an application sends a connection request. All relevant ports can be open only after connection is established at this starting port. Otherwise, other relevant ports are not open.
Ending Port	Set the end port of the port range.

The QoS - Priority Rules page for an online game is as follows:

87

The following table describes parameters in this page:

Item	Description
QoS Policy For	Enter the name of the QoS policy.
Priority Category	Select On-line Gaming.
On-line Gaming	Select an online game that you want to set. If your desired online game is not in the drop-down list, select Add a new Game.
Priority	You can select Highest, High, Normal or Low.
Connection Type	Indicates the protocol that is used at the port. You can select TCP/UDP, TCP or UDP.
Starting Port	The first port to which an application sends a connection request. All relevant ports can be open only after connection is established at this starting port. Otherwise, other relevant ports are not open.
Ending Port	Set the end port of the port range.

The QoS – Priority Rules page for a LAN port is as follows:

The following table describes parameters in this page:

Item	Description
QoS Policy For	Enter the name of the QoS policy.
Priority Category	Select Ethernet LAN Port.
Ethernet LAN Port	Select the LAN port that you want to set. You can select 1, 2, 3 or 4.
Priority	You can select Highest, High, Normal or Low.

The QoS - Priority Rules page for a MAC address is as follows:

QoS - Priority Rules

Priority

QoS Policy For				
Priority Category	MAC Address			

MAC Device Example List

	QoS Policy	Priority	Device Name	MAC Address
○	Pri_MAC_219CF1	Normal	netadmin-PC	60:D8:19:21:9C:F1
○	Pri_MAC_0BC7ED	Normal	smartlin-df86fc	00:17:7C:0B:C7:ED
○	Pri_MAC_C58928	Normal	netadmin-PC	14:FE:B5:C5:89:28

MAC Device Add List

QoS Policy	Priority	Device Name	MAC Address
MAC Address			
Device Name			
Priority	High		

Add Edit Delete Cancel

The following table describes parameters in this page:

Item	Description
QoS Policy For	Enter the name of the QoS policy.
Priority Category	Select MAC Address.
MAC Device List	Display the existing priority rules of computers that have higher

89

	priorities according to MAC addresses. Enter the MAC address and device name of a computer for which you want to set high priority, and then click Add to add the rule to the list.
MAC Address	Enter the MAC address of a computer for which you want to set high priority.
Device Name	Enter the device name of a computer for which you want to set high priority.
Priority	You can select Highest, High, Normal or Low.
Add	Click the button to add a priority rule to the MAC Device List.
Edit	Select a priority rule in the MAC Device List and click the button to modify the priority rule.
Delete	Select a priority rule in the MAC Device List and click the button to delete the priority rule from the list.
Cancel	On clicking cancel you will exit from the Priority rule and get back to the QOS set up

After the settings are done, click Apply to save the settings. Then, click Apply to save the settings in the QoS Setup page.

8. Dynamic DNS

Dynamic DNS (DDNS) is mainly used to map fixed domain names to dynamic IP addresses and vice versa. For a user using a dynamic IP address, after the user obtains a new IP address when accessing Internet, the dynamic domain name software installed in the host sends the IP address to the dynamic domain name resolution server provided by the DDNS service provider and updates the domain name resolution database. When another user on the Internet tries accessing the domain name, the dynamic domain name resolution server returns the correct IP address.

Click Dynamic DNS and the Dynamic DNS page appears. In this page, you can configure the DDNS parameteres.

Dynamic DNS

☐ Use a Dynamic DNS Service	
Service Provider	DynDNS.org ▾
Host Name	myhostname
User Name	User
Password	••••

Apply   Cancel

The following table describes parameters in this page:

Item	Description
User a Dynamic DNS Service	Enable this function if you already register to the DDNS service provider.
Service Provider	Select a server from the drop-down list. You can select DynDNS.org, 3322.org, freedns.afraid.org, DtDNS.com or www.oray.cn.
Host Name	Enter the host name or domain name provided by the DDNS service provider.

91

User Name	Enter the user name of the DDNS account.
Password	Enter the password of the DDNS account.

After the settings are done, click Apply to save the settings.

9. Static Routing

Static routing is a special type of routing that can be applied properly in a network to reduce the problem of routing selection and overload of data flow because of routing selection and to improve the forwarding speed of packets. You can set the destination IP address, subnet mask and gateway to specify a routing rule. The destination IP address and subnet mask are used to determine a destination network or host. Then, the router sends packets to the specified destination network or host through the gateway.

Click Static Routes and the Static Routes page appears. In this page, you can add, edit and delete a static routing rule, and view the current static routing table in the router.

Static Routes

Max of rules: 32

#	Active	Name	Destination	Gateway

Add   Edit   Delete

Click Add and the following figure appears:

Static Routes

Active	☐
Route Name	
Destination IP Address	
IP Subnet Mask	
Gateway IP Address	
Metric	

Apply Cancel

The following table describes parameters of adding a routing rule:

Item	Description
Active	Enable it to apply the routing rule.
Router Name	Enter the name of the static route.
Destination IP Address	Enter the destination IP address or network that you want to access.
IP Subnet Mask	Subnet mask of the destination IP address.
Gateway IP Address	IP address of the router or host to which packets are sent.
Metric	Indicates the number of hops in the user network. Its value range is 2 to 15. Usually, the value of 2 or 3 leads to the best performance. If the route is direct connection, set the Metric to 2.

After the settings are done, click Apply to save the settings.

10. Security Options
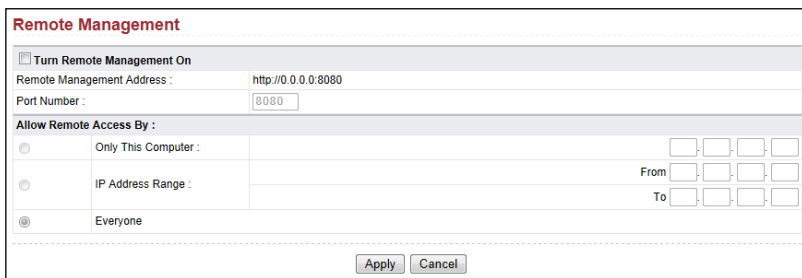
Click Security Options and the extended navigation menu is shown as follows:
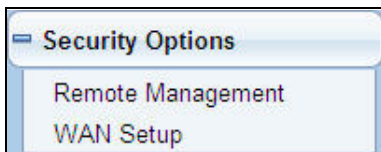
The submenu contains Remote Management and WAN Setup.

10-1 Remote Management

Choose **Security Options > Remote Management** and the Remote Management page appears.

The remote management function allows you to configure the router's WAN through the Web browser. In this way, you can manage the router from a remote host.

The following table describes parameters in this page:

Item	Description
Turn Remote Management On	Enable or disable remote Web management.
Remote Management Address	IP address that is used to access the router from the Internet. The default IP is **http://0.0.0.0:8080.** When accessing the router, you need to enter the WAN IP address of the router, along with **:** and the port number in the address bar (of IE) or the location bar (of Netscape).
Port Number	Specify the port of Web management for accessing the broadband router.
Allow Remote Access By	Set the IP address of the computer on which remote Web management is carried out to access the router. ● Only This Computer: Only the specified IP address can access the router. You need to enter an IP address. ● IP Address Range: A number of IP addresses on the Internet can access the router. You need to enter the starting and ending IP addresses to specify the range. ● Everyone: Everyone on the Internet can access the router.

After the settings are done, click Apply to save the settings.

10-2 WAN Setup

Choose **Security Options > WAN Setup** and the WAN Setup page appears.

WAN Setup

☑ Disable Port Scan and DOS Protection
☐ Respond to Ping on Internet Port
☑ Disable IGMP Proxying
☐ Default DMZ Server   192 168 2
MTU Size(616~1500 bytes)   1500

NAT Filtering

◉ Secured
○ Open
☐ Enable IPv6 Pass-Through

Apply   Cancel

In this page, you can set a default DMZ server and allow the router to respond to the ping command from the Internet. Do not use the two functions unless it is necessary because they lead to security risks. DMZ allows all ports of a PC in your LAN to be exposed to the WAN. Enter the IP address of a PC to set the PC to a DMZ host, which is not restricted by the firewall any more. In this way, the DMZ host can have mutually unrestricted communcation with a user or server on the WAN.

The following table describes parameters in this page:

Item	Description
Disable Port Scan and DOS Protection	This function protects your LAN against DoS attack. Do not disable this firewall function unless a special situation occurs.
Respond to Ping on Internet Port	If you want the router to respond to ping commands from the Internet, select the check box. The ping command can be used for diagnosis. Like a DMZ server, this function also leads to security risks. Hence, do not select the check box unless it is necessary.

Disable IGMP Proxying	IGMP proxy allows a PC in the LAN to receive certain multicast traffics from the Internet. If you do not want to use IGMP proxy, select the check box to disable IGMP proxy.
Default DMZ Server	Enter the IP address of a computer or server that serves as a DMZ server.
MTU Size (in bytes)	The maximum transmission unit. Normally, it is 1500 bytes for most Ethernet networks, 1492 bytes for PPPoE connection and 1436 bytes for PPTP connection. Certain ISPs may require smaller MTU, but this is a rare case. Do not modify the value of MTU size unless it is necessary for your ISP connection.
NAT Filtering	Determines the mode of the router to handle the input traffics. • Secured: It provides a secure firewall that protects personal computers in a LAN against attacks from the Internet. However, it causes malfunction of certain network games, point-to-point (P2P) applications and multimedia applications. • Open: It provides firewall settings of a lower security level. It allows running of almost all network applications.
Enable IPv6 Pass-Through	By default, IPv6 pass-through is disabled. If your configuration contains IPv6 devices and you want to replace IPv4 with IPv6, you can select the check box to enable IPv6 pass-through.

After the settings are done, click Apply to save the settings.

11. System Tools

Click System Tools and the extended navigation menu is shown as follows:

The submenu contains Schedules, SNTP, Backup Settings, Set Password and Router Upgrade

11-1 Schedules

Choose **System Tools > Schedules** and the Schedules page appears.

If you already set content filtering in the Block Sites page or set sevice filtering in the Block Services page, you can set a schedule to specify the time and mode of restricting Internet access.

The following table describes parameters in this page:

Item	Description
Days to Block	Select every day, one day, or several days.
Time of Day to Block (Use 24-hour clock)	If you want to fully restrict access every day, select All Day. If you want to restrict access in a specific time during certain days, select the days and enter the starting time and ending time. Note that the system uses 24-hour clock.

After settings are done, click Apply to save the settings.

11-2 SNTP

Choose **System Tools > SNTP** and the SNTP page appears.

In this page, you can set the time information of your router. It is strongly recommended to set the correct time on the router first. This ensures proper functioning of log, site blocking and schedule, because these functions are based on the time setting in this page.

The following table describes parameters in this page:

Item	Description
Time Setting	Automatically synchronize with Internet time servers: Enable or disable automatic synchronization with the network time server. • First NTP time server: Enter the URL of the primary network time server. • Second NTP time server: Enter the URL of the secondary time server.
Time Configuration	• Current Router Time: Displays the current system time of the router. • Time Zone: Select the time zone that the router is in from the drop-down list.
Enable Daylight Saving	Enable or disable daylight saving time (DST), which is a practice of temporarily advancing clocks during the summertime so that afternoons have more daylight and mornings have less. It helps saving the lighting power.
Daylight Saving Offset	Select a proper offset. If it is set to +1:00, 10:00 in the morning in standard time becomes 11:00 in the morning in DST.
Daylight Saving Dates	Set the starting time and ending time of DST.

After the settings are done, click Apply to save the settings.

11-3 Backup Settings

Choose **System Tools > Backup Settings** and the Backup Settings page appears.

Backup Settings

Save a Copy of Current Settings
[Backup]

Restore Saved Setting from a File
[Choose File] No file chosen
[Restore]

Revert to Factory Default Settings
[Erase]

Reboot Device
[Reboot]

In this page, you can export the configuration information of the router in a file to the computer for later use, import a previously saved or a new configuration file, restore the factory default settings of the router, and reboot the router.

- Backup

    Click Backup and select the path to save the configuration of the router as a local file.

- Restore

    Click Choose file to select the configuration file in your computer and click Restore to load the selected file to the router.

- Erase

    Click Erase to restore the factory default settings of the router. This action has the same effect of pressing the Reset button on the rear panel till the router reboots.

- Reboot

    Click Reboot to reboot the router.

⚠ **Caution:**

After a new configuration file is imported, the original configuration information of the router is lost. Hence, it is recommended to back up the configuration before importing a new configuration file. If the new configuration file is incorrect, you can import the previous backup file.
When the configuration file is loading, do not power off the router. Otherwise, the router may be damaged and fail to work.

11-4 Set Password

Choose **System Tools > Set Password** and the Set Password page appears.

Set Password

Set Password	
Old Password	
Set Password	
Repeat New Password	

Apply Cancel

Web Idle Time Out Settings		
Web Idle Time Out	5	(5 ~ 30 minutes)

Apply Cancel

In this page, you can change the password of the administrator and set the time of page timeout.

The following table describes parameters in this page:

Item	Description
Old Password	Enter the password for logging in to the router.
Set Password	Enter a new password.
Repeat New Password	Enter the new password again.
Web Idle Time Out Settings	Set the time of page timeout. Its value range is 5 to 30 minutes. If you do not operate on a page for a period longer than the set time after login, the system switches to the login page when you try performing the next operation on a page.

Note: For security measures, it is strongly recommended to change the default user name and password of the administrator. If you forget the password, you can restore the router to the default settings. The default user name and password are admin and 1234 respectively.

11-5 Router Upgrade

Choose **System Tools > Router Upgrade** and the Router Upgrade page appears.

Router Upgrade

Locate and select the upgrade file from your hard disk:

Choose File	No file chosen	☑ Clear Config

Upload   Cancel

In this page, you can upgrade the software of the router in the following steps:

Step 1   Click Choose File to navigate to the latest software.

Step 2   Select the correct upgrade file. If you select Clear Config, the router restores to the default settings after upgrade. If you do not select it, the current settings remain.

Step 3   Click Upload to start upgrading.

After the upgrade is complete, the router automatically reboots.

⚠ **Caution:**

To avoid losing previous configuration of the router, save the configuration before upgrade.

During upgrade, do not power off the router or press the Reset button.

12. Logout

The Logout control is in the lower right of the navigation bar. See the following figure:
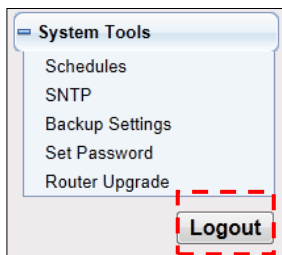
The logout function is used to log out the current login status. After logout, you need to log in again before accessing the configuration page of the router

To log out the router, do as follows:

Step 1   Click Logout under the System Tools menu and the following dialog box appear:

Step 2   Click OK to log out. See the following figure. To return to the configuration page, click Cancel.

**Thank you for using the Router Configuration Utility.
Goodbye!**

105

13. Appendix

13-1 Hardware Specifications

Flash: 4MB

RAM: 32MB

Antenna: One fixed dipole 3dBi antenna

Power supply: 12V DC, 500mA Switching power adapter

Network interface: 1 x 10/100 Mbps UTP WAN port

4 x 10/100 Mbps UTP LAN ports

Standards compliance: IEEE 802.3 10BASE-T Ethernet

IEEE 802.3u 100BASE-TX Fast Ethernet

IEEE 802.11b

IEEE 802.11g

IEEE 802.11n

Wireless frequency: 2.400~2.4835GHz

Wireless transmit power: 11b: 17+- 1.5dbm

11g: 15+- 1.5dbm

11n: 14+- 1.5dbm

Wireless security : WEP (64/128 bit), WPA-PSK (TKIP/AES), WPA2-PSK (TKIP/AES),WPS (PBC/PIN Mechanism), Disable SSID broadcast

Data rates: IEEE802.11b: 1/2/5.5/11Mbps

IEEE802.11g: 6/9/12/24/36/48/54Mbps

IEEE802.11n (20MHz): MCS0-7, up to 72Mbps

IEEE802.11n (40MHz): MCS0-7, up to 150Mbps

Operating temperature: 0°C ~ 45°C

Storage temperature: -20°C ~ 70°C

Operating humidity: 10 ~ 90% (Non-condensing)

Storage humidity: 5 ~ 90% (Non-condensing)

Net Dimension (L x W x H): 176.8 x 118.7 x 23.5 mm

Gross Dimension (L x W x H): 256 x 158 x 65 mm

Net Weight: 277 gms

Gross Weight: 677 gms

14. Troubleshooting

If you encounter any problem when you're using this wireless network adapter, don't panic. Before you call your dealer of purchase for help, please check this troubleshooting table, the solution to your problem could be very simple, and you can solve the problem yourself.

Scenario	Solution
Failure to configure the router through a web browser	1) Open the Web browser (for example, IE) and choose Tools > Internet Options from the main menu. 2) Click Delete Cookies and Delete Files.

Failure to establish wireless network connection	• Router is beyond the wireless coverage.
	   1) Place the router near the customer premises equipment (CPE).
	   2) Try modifying the channel setting.
	• Facing authentication problems.
	   1) Use a computer of wired connection to connect the router.
	   2) Check the network security settings.
	   3) Try a hard reset on the router.
	• The router cannot be detected.
	   1) Try hard reset on the router and test again.
	   2) Check the settings of the wireless network.
	   3) Check the settings of SSID and encryption.

Failure to connect to the Internet through the wireless router	1) Check whether the wireless network card connects to the correct AP (base station). 2) Check whether the wireless channel accords with the channel specified in your country or region. 3) Check the encryption settings.

	4) Check whether your ADSL cable is connected to the correct network interfaces. 5) Replace the network cable connected to the router
Failure to access the Internet	1) Check whether the status of indicators on the ADSL modem and the wireless router is normal. 2) Check whether the WAN indicator is on. If the WAN indicator is off, check whether the cable connected to the WAN interface is loose. 3) When the WAN indicator is on but does not blink, the router is connected to the Internet. 4) Reboot your PC. 5) Set the AP again. 6) Check whether the WAN indicator is on. 7) Check the encryption settings of the wireless network. 8) Check whether the PC that connects to the router can obtain the IP address through either the wireless network or the cable network. 9) Check the LAN settings of your Internet options, and do not use a proxy server for your LAN.

15. Glossary

Default Gateway (Router): Every non-router IP device needs to configure a default gateway IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it to the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.Broadbandrouter.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "Broadbandrouter.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

DMZ: DMZ is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an

110

external attacker only has access to equipment in the DMZ, rather than any other part of the network.

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

Idle Timeout: Idle Timeout is designed so that after there is no traffic on the Internet for a pre-configured amount of time, the connection will automatically get disconnected.

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, which identifies a single, unique Internet computer host in an IP network. Example: 192.168.2.1. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": aaa.aaa.aaa.aaa, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".": bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can be either 0 or 1.
A network mask is also a 32-bit binary pattern, and consists of consecutive leading

1's followed by consecutive trailing 0's, such as

11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as "x" number of leading 1's.

When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form,

11011001.10110000.10010000.00000111, and if its network mask is,

11111111.11111111.11110000.00000000

It means the device's network address is

11011001.10110000.10010000.00000000, and its host ID is,

00000000.00000000.00000000.00000111. This is a convenient and efficient method for routers to route IP packets to their destination.

ISP Gateway Address: (see ISP for definition). The ISP Gateway Address is an IP address for the Internet router located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as home or office). Your home network is considered a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that correspond to the

112

Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

NAT: Network Address Translation. This process allows all the computers on your home network to use one IP address. Using the broadband router's NAT capability, you can access Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port: Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UDP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723

PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

Port triggering: Port triggering is a configuration option on a NAT-enabled router that allows a host machine to dynamically and automatically forward a specific port back to itself. Port triggering opens an incoming port when your computer is using a specified outgoing port for specific traffic.

PPPoE: (Point-to-Point Protocol over Ethernet.) Point-to-Point Protocol is a secure data transmission method originally created for dial-up connections; PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers.

Protocol: A protocol is a set of rules for interaction agreed upon between multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

Router: A router is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is

114

used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocols. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

Web-based management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.

115