



Networks based on information,
Success, Friendship and more...



Package Contents

- **Wireless 802.11g VPN Router**
- **User Guide CD-ROM**
- **Ethernet Network Cable**
- **Power Supply**
- **Quick Installation**
- **User manual**



Networks based on information,
Success, Friendship and more...

Introduction

Welcome

The ALL0276 VPN Router from ALLNET is an advanced complete wireless networking solution for small business, education, enterprise or Hotspot requirements.

The ALLNET incorporates four networking functions in a single box.

- The **Wireless Access point** providing connectivity for 802.11 b/g devices
- Integrated **4 port full duplex 10/100 Switch** to connect wired Ethernet devices
- **Router** integrates all functions and lets the whole network share a high-speed cable or Internet Connection
- **VPN** function creates encrypted “tunnels” through the Internet enabling remote users to connect from off site or branch offices to a corporate network

The four Ethernet connections provide the ability to connect 4 PCs directly or provide connections to more hubs and switches to create a network as large as is needed.

Data and privacy are assured as the ALLNET can encrypt all wireless transmission with 128-bit WEP encryption, and also supports the additional security provided by 802.1x authentication and authorization.

The ALLNET can serve as a DHCP Server, has NAT technology with a powerful SPI firewall to protect against Internet intruders, supports VPN pass-through, and can be configured to filter internal users' access to the Internet. The system has MAC or IP address filtering so you can specify precisely who has access to your network.

The system is simple to configure with the intuitive web browser-based configuration utility. With a high-speed internet connection and application software it can easily be deployed as a hotspot in-a-box.

Understanding ALL0276 VPN Router

The Back Panel

The Router's ports, where a network cable is connected, are located on the back panel.



Figure 1: Back Panel

Internet The **Internet** port connects to your modem.

LAN (1-4) The **LAN** (Local Area Network) ports connect to your PC and other network devices.

Power The **Power** port is where you will connect the power adapter.

Reset Button There are two ways to **Reset** the Router's factory defaults. Either press the Reset Button, for approximately ten seconds, or restore the defaults from the Administration tab in the Router's Web based Utility.



Networks based on information,
Success, Friendship and more...

With these, your networking options are limitless.

Important: Resetting the Router will erase all of your settings (WEP Encryption, Wireless and LAN settings, etc.) and replace them with the factory defaults. Do not reset the Router if you want to retain these settings.

The Front Panel

The Router's LEDs, where information about network activity is displayed, are located on the front panel.



Figure 2: Front Panel

Power Green. The **Power** LED lights up when the Access Point is powered on.

WAN Orange. The **WAN** LED lights whenever there is a successful internet connection. If the LED is flickering, the Router is actively sending or receiving data to or from one of the devices on the network.

WLAN Green. The **WLAN** LED lights whenever there is a successful wireless connection.

LAN (1-4) Green. The **LAN** LED serves two purposes. If the LED is continuously lit, the Router is successfully connected to a device through the LAN port. If the LED is flickering, it is an indication of any network activity.

Connecting ALLNET Wireless 802.11g VPN Router

Overview

The Router's setup consists of more than simply plugging hardware together. You will have to configure your networked PCs to accept the IP addresses that the Router assigns them (if applicable), and you will also have to configure the Router with setting(s) provided by your Internet Service Provider (ISP).

The installation technician from your ISP should have left the setup information for your modem with you after installing your broadband connection. If not, you can call your ISP to request that data. Once you have the setup information you need for your specific type of Internet connection, you can begin installation and setup of the Router.

If you want to use a PC with an Ethernet adapter to configure the Router, continue to "Wired Connection to a PC." If you want to use a PC with a wireless adapter to configure the Router, continue to "Wireless Connection to a PC."

Wired Connection to a PC

1. Before you begin, make sure that all of your network's hardware is powered off, including the Router, PCs, and cable or DSL modem.
2. Connect one end of an Ethernet network cable to one of the LAN ports (labeled 1-4) on the back of the Router (see Figure Wired-1), and the other end to an Ethernet port on a PC.



Figure Wired-1

3. Repeat this step to connect more PCs, a switch, or other network devices to the Router.
4. Connect a different Ethernet network cable from your cable or DSL modem to the Internet port on the Router's rear panel (see Figure Wired-2). This is the only port that will work for your modem connection.



Figure Wired-2

5. Power on the cable or DSL modem.
6. Connect the power adapter to the Router's Power port (see Figure Wired-3), and then plug the power adapter into a power outlet.



Figure Wired-3



Networks based on information,
Success, Friendship and more...

The Power LED on the front panel will light up green as soon as the power adapter is connected properly.

The Power LED will flash for a few seconds, then it will light up steady when the self-test is complete. If the LED flashes for one minute or longer, see **“Troubleshooting.”**

7. Power on one of your PCs that is connected to the Router.

NOTE: You should always plug the Router's power adapter into a power strip with surge protection

NOTE: You should always change the SSID from its default, **wireless-g**, and enable WEP encryption.

Wireless Connection to a PC

If you want to use a wireless connection to access the Router, follow these instructions:

1. Before you begin, make sure that all of your network's hardware is powered off, including the Router, PCs, and cable or DSL modem.
2. Connect an Ethernet network cable from your cable or DSL modem to the Internet port on the Router's rear panel (see Figure Wired-2). This is the only port that will work for your modem connection.
3. Power on the cable or DSL modem.
6. Connect the power adapter to the Power port (see Figure Wired-3), and then plug the power adapter into a power outlet.

The Power LED on the front panel will light up green as soon as the power adapter is connected properly. The Power LED will flash for a few seconds, then light up steady when the self-test is complete. If the LED flashes for one minute or longer, see **“Troubleshooting.”**

5. Power on one of the PCs on your wireless network(s).
7. For initial access to the Router through a wireless connection, make sure the PC's wireless adapter has its SSID set to **wireless-g** (the Router's default setting), and its WEP encryption is disabled. After you have accessed the Router, you can change the Router and this PC's adapter settings to match the your usual network settings.

The Router's hardware installation is now complete. Go to **“Configuring the PCs.”**



Networks based on information,
Success, Friendship and more...

Configuring the PCs

Overview

The instructions in this chapter will help you configure each of your computers to be able to communicate with the Router.

To do this you need to configure your PC's network settings to obtain an IP (or TCP/IP) address automatically so, your PC can function as a DHCP client. Computers use IP addresses to communicate with the Router and each other across a network, such as the Internet.

First, find out which Windows operating system your computer is running. You can find out by clicking the **Start** button. Read the side panel of the **Start** menu to find out which operating system your PC is running.

You may need to do this for each computer you are connecting to the Router.

The next few pages tell you, step by step, how to configure your network settings based on the type of Windows operating system you are using. Make sure that an Ethernet or wireless adapter (also known as a network adapter) has been successfully installed in each PC you will configure. Once you've configured your computers, continue to **"Using the Router's Web-Based Utility."**

IMPORTANT: By default Windows 98, 2000, Me, and XP has TCP/IP installed and set to obtain an IP address automatic ally. If your PC does not have TCP/IP installed, click **Start** and then **Help**. Search for the keyword TCP/IP. Then follow the instructions to install TCP/IP

Configuring Windows 98 and Millennium PCs

1. Click the **Start** button. Select **Settings** and click the **Control Panel** icon. Double-click the **Network** icon.
2. On the Configuration tab, select the **TCP/IP** line for the applicable Ethernet adapter, as shown in Figure 5. Do not choose a TCP/IP entry whose name mentions DUN, PPPoE, VPN, or AOL. If the word TCP/IP appears by itself, select that line. Click the **Properties** button.

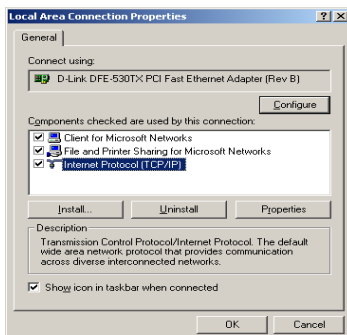


Figure 5

3. Click the **IP Address** tab. Select **Obtain an IP address automatically**. (See Figure 6.)

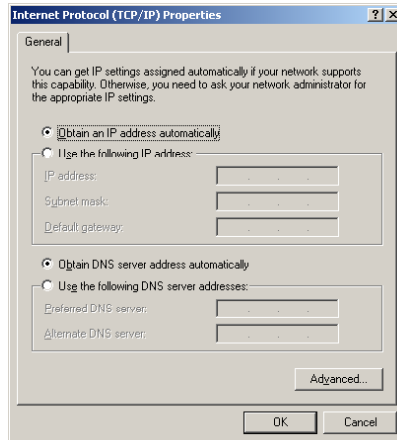


Figure 6

4. Now click the **Gateway** tab, and verify that the Installed Gateway field is blank. Click the **OK** button.
5. Click the **OK** button again. Windows may ask you for the original Windows installation disk or additional files. Check for the files at c:\windows\options\cabs, or insert your Windows CD-ROM into your CD-ROM drive and check the correct file location, e.g., D:\win98, D:\win9x, etc. (if "D" is the letter of your CD-ROM drive).
6. Windows may ask you to restart your PC. Click the **Yes** button. If Windows does not ask you to restart, restart your computer *anyway*. Go to "Using the Router's Web-Based Utility."

Configuring Windows 2000 PCs

1. Click the **Start** button. Select Settings and click the **Control Panel** icon. Double-click the **Network and Dialup Connections** icon.
2. Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the **Local Area Connection**. Click the **Properties** button. (See Figure 7.)

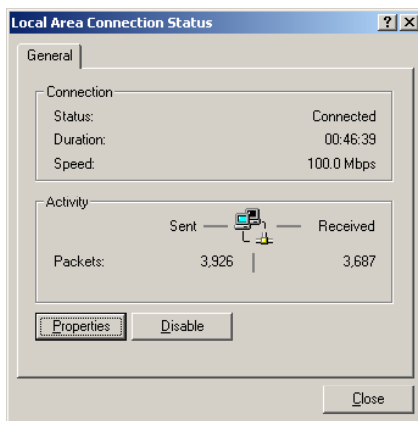


Figure 7

3. Make sure the box next to Internet Protocol (TCP/IP) is checked. Highlight Internet Protocol (TCP/IP), and click the **Properties** button. (See Figure 8.)

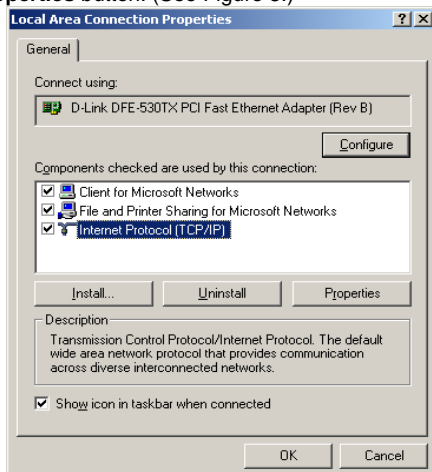


Figure-8



Networks based on information,
Success, Friendship and more...

4. Select **Obtain an IP address automatically**. Once the new window appears, click the **OK** button. Click the **OK** button again to complete the PC configuration. (See Figure 9.)

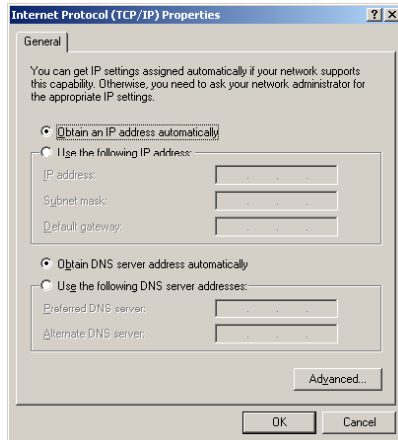


Figure 9

5. Restart your computer.
Go to “Using the Router’s Web-Based Utility.”

Configuring Windows XP PCs

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

1. Click the **Start** button and then the **Control Panel** icon. Click the **Network and Internet Connections** icon.
Then click the **Network Connections** icon.
2. Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the **Local Area Connection**. Click the **Properties** button. (See Figure 10.)



Figure 10

2. Make sure the box next to Internet Protocol (TCP/IP) is checked. Highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. (See Figure 11.)



Figure 11

3. Select **Obtain an IP address automatically**. (See Figure 12.) Once the new window appears, click the **OK** button. Click the **OK** button again to complete the PC configuration.



Figure 12

Go to “Using the Router’s Web-Based Utility.”

Configuring the Router

Use the Router's web-based utility to configure the Router. This chapter will describe each web page in the Utility and each page's key functions. The utility can be accessed via your web browser through use of a computer connected to the Router. For a basic network setup, most users only have to use the following screens of the Utility:

Basic Setup. On the Basic Setup screen, enter the settings provided by your ISP.

Management. Click the **Administration** tab and then the **Management** tab. The Router's default password is admin. To secure the Router, change the Password from its default.

There are seven main tabs: Setup, Wireless, Security, Access Restrictions, Applications, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

Note: The Router is designed to function properly after connecting the Router to your network. This chapter is provided solely for those who wish to perform more advanced configuration or monitoring.

Have You: Enabled TCP/IP on your PCs? PCs communicate over the network with this protocol. Refer to **Appendix D: Windows Help for more information on TCP/IP**.

Note: For added security, you should change the password through the Administration screen of the web-based utility.



Networks based on information,
Success, Friendship and more...

Setup

Basic Setup. Enter the Internet connection and network settings on this screen.

DDNS. To enable the Router's Dynamic Domain Name System (DDNS) feature, complete the fields on this screen.

MAC Address Clone. If you need to clone a MAC address onto the Router, use this screen.

Advanced Routing. On this screen, you can alter Network Address Translation (NAT), Dynamic Routing, and Static Routing configurations.

Hot Spot. Register with your Hot Spot service provider on this screen.

NAT (Network Address Translation). NAT Technology translates IP addresses of a local area network to a different IP address for the Internet.

Wireless

Basic Wireless Settings. You can choose your Wireless Network Mode and Wireless Security on this screen.

Wireless Security. You can choose your Wireless Security mode on this screen.

Wireless Network Access. This screen displays your network access list.

Advanced Wireless Settings. On this screen you can access the Advanced Wireless features of Authentication

Type, CTS Protection Modes, Basic Data Rates, Control Tx Rates, Beacon Interval, DTIM Interval, RTS Threshold, and Fragmentation Threshold.

Beacon Interval : The frequency interval of the beacon, which is a packet broadcast by a router to synchronize a wireless network.

DTIM (Delivery Traffic Indication Message):

A message included in data packets that can increase wireless efficiency.

RTS (Request To Send): A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

Fragmentation: Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

Security

Firewall. To block specific users from Internet access, you can set up IP address, port, and MAC address filtering on the Filter screen.

VPN. To enable or disable IPSec, PPPoE, and/or PPTP Pass-through, and set up VPN tunnels, use this screen.

802.1x. Use this screen to set up RADIUS authentication.

Access Restrictions

Access Restriction. This screen allows you to prevent or permit only certain users from attaching to your network.



Networks based on information,
Success, Friendship and more...

Applications

Port Range Forwarding. To set up public services or other specialized Internet applications on your network, click this tab.

Port Triggering. To set up triggered ranges and forwarded ranges for Internet applications, Click this tab. Upon Forwarding. Use this screen to alter Upon forwarding settings.

DMZ. To allow one local user to be exposed to the Internet for use of special-purpose services, use this screen.

Administration

Management. On this screen, alter router access privileges and UPnP settings.

Log. If you want to view or save activity logs, click this tab.

Diagnostics. If you want to perform ping test for diagnostic purpose, click this tab.

Factory Defaults. If you want to restore the Router's factory defaults, then use this screen.

Firmware Upgrade. Click this tab if you want to upgrade the Router's firmware.

Reboot. Click this tab to reboot the device.

Configure Management. Click this tab to download or upload Router's configuration file.

Status

Router. This screen provides status information about the Router.

Local Network. This provides status information about the local network.

Wireless. This provides status information about the wireless network

System Performance: This provides System Performance information on all network connections

How to Access the Web-based Utility

To access the web-based utility, launch Internet Explorer or Netscape Navigator, and enter the Router's default IP address, **192.168.1.1**, in the Address field. Then press Enter.

A password request page, shown in **(Figure Password screen)** will appear. (non-Windows XP users will see a similar screen.) Enter **admin** (the default user name) in the User Name field, and enter **admin** (the default password) in the Password field. Then click the **OK** button.

Figure-Password screen

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.



Networks based on information,
Success, Friendship and more...

The Setup Tab

The Basic Setup Tab

The first screen that appears is the Basic Setup tab. (See Figure Setup Tab DHCP/Internet connection Type.) This tab allows you to change the Router's general settings. Change these settings as described here and click the **Save Settings** button to save your changes or **Cancel Changes** to cancel your changes.

The screenshot displays the 'Setup' tab of an ALLNET 11g VPN Router. The 'Internet Setup' section is active, showing 'Automatic Configuration - DHCP' as the selected connection type. Below this, fields for IP Address (192.168.41.76), Host Name (ALLNET), and Domain Name (ALLNET) are visible. The MTU is set to 1472. The 'Network Setup' section shows the Gateway IP (192.168.1.1) and Subnet Mask (255.255.255.0). The 'Network Address Server Settings (DHCP)' section is also shown, with the Local DHCP Server enabled. The Start IP Address is 192.168.1.100, the Number of Address is 255, the IP Address Range is 192.168.1.100 - 254, and the DHCP IP Address is 192.168.1.1. The 'Time Setting' section shows the time set to 04:11:20 on 03/04/04.

Figure Setup Tab DHCP/Internet connection Type

Internet Setup

Internet Connection Type. The Router supports four connection types: Automatic Configuration - DHCP (the default connection type), Static IP, PPPoE and PPTP. Each Basic Setup screen and available features will differ depending on what kind of connection type you select.

Automatic Configuration - DHCP

By default, the Router's Configuration Type is set to Automatic Configuration - DHCP, and it should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address.

Static IP

(See Figure Static Internet connection Type)

If you are required to use a permanent IP address to connect to the Internet, then select Static IP.

- IP Address. This is the Router's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.
- Subnet Mask. This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.



Networks based on information,
Success, Friendship and more...

- Default Gateway. Your ISP will provide you with the Default Gateway Address, which is the ISP server's IP address.
- Primary DNS. (Required) and Secondary DNS (Optional). Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

Figure Static Internet connection Type

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

PPPoE

(See Figure PPPoE Connection Type.)

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE.

- **User Name and Password:** Enter the User Name and Password provided by your ISP.
- **Connect on Demand:** Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- **Keep Alive Option:** Redial Period. If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. In the Redial Period field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds.



Networks based on information,
Success, Friendship and more...

The screenshot shows the 'Setup' tab of the ALLNET 11g VPN Router configuration interface. The 'Internet Setup' section is active, showing the 'Internet Connection Type' as 'PPPoE'. The 'User Name' field is filled with 'ALLNET' and the 'Password' field is filled with '12345678'. The 'Connect on Demand' option is selected, with a 'Max Idle Time' of 5 minutes. The 'Keep Alive' option is also selected, with a 'Redial Period' of 30 seconds. The 'Host Name' field is filled with 'ALLNET' and the 'Domain Name' field is filled with 'ALLNET'. The 'MTU' is set to 'Manual' and the 'MTU Size' is 1492. A sidebar on the right contains a note about the Internet Connection Type and a warning to verify the connection type with the ISP.

Figure PPPoE connection Type

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

PPTP

(See Figure PPTP Connection Type.)

Point to Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only.

- **Internet IP Address.** This is the Router's IP address, when seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.
- **Subnet Mask.** This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.
- **Default Gateway.** Your ISP will provide you with the Default Gateway Address.
- **User Name and Password.** Enter the User Name and Password provided by your ISP.
- **Connect on Demand:** Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- **Keep Alive Option:** Redial Period. If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. To use this option, click the radio button next to **Keep Alive**. In the Redial Period field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds.



Networks based on information,
Success, Friendship and more...

Setup 11g VPN Router ALLNET/VPN

Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Setup DNS MAC Address Clone Advanced Routing

Internet Setup

Internet Connection Type

PPTP

IP Address: 0 0 0 0

Subnet Mask: 0 0 0 0

Default Gateway: 0 0 0 0

User Name:

Password:

☐ Connect on Demand Max Idle Time 5 Min.

☒ Keep Alive Reconnect Period 30 Sec.

Host Name: ALLNET

Domain Name: ALLNET

MTU: ☐ Manual ☒ Auto

MTU Size: 1472

Optional Settings (required by some ISPs)

Internet Connection Type: You may choose from Automatic Configuration - DHCP, Static IP, PPTP or PPPoE. Please check with your Internet Service Provider to verify which type of connection you will need to use.

Figure PPTP Connection Type

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Optional Settings (Required by some ISPs)

Host Name and Domain Name. These fields allow you to supply a host and domain name for the Router. Some ISPs require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

MTU. The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Select **Manual** and enter the value desired. It is recommended that you leave this value in the 1200 to 1500 range. For most DSL users, it is recommended to use the value 1492 (the default value). Alternatively, select **Auto** to automatically set MTU to 1500.

Network Setup

Gateway IP. The values for the Router's Local IP Address and Subnet Mask are shown here. In most cases, keeping the default values will work.

Local IP Address. The default value is 192.168.1.1.

Subnet Mask. The default value is 255.255.255.0.

Network Address Server Settings (DHCP). A Dynamic Host Configuration Protocol (DHCP) server automatically assigns an IP address to each PC on your network for you. Unless you already have one, it is highly recommended that you leave the Router enabled as a DHCP server.

Local DHCP Server. DHCP is already enabled by factory default. If you already have a DHCP server on your network, set the Router's DHCP option to Disable. If you disable DHCP, remember to assign a static IP address to the Router.



Networks based on information,
Success, Friendship and more...

Start IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. This value must be 192.168.1. 2 or greater, because the default IP address for the Router is 192.168.1.1.

Number of Address. Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. In order to determine the DHCP IP Address range, add the starting IP address (e.g., 100) to the number of DHCP users. The default value is 50. Using the default value and starting IP address of 100, add 50 to 100, and the IP address range is 192.168.1.100 to 192.168.1.149.

DHCP Address Range. The range of DHCP addresses is displayed here.

DNS IP Address. The DHCP Server has the ability to dynamically update the Domain Name System (DNS). Enter the IP Address for the Domain Name System in this field.

Time Setting. This is where you set the time for your Router. You can set the time and date manually or automatically, by setting the time zone.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

The DDNS Tab

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router. Before you can use this feature, you need to sign up for DDNS service at one of two DDNS service providers, DynDNS.org or TZO.com.

DDNS

DDNS Service. If your DDNS service is provided by DynDNS.org, then select DynDNS.org in the drop-down menu. **(See Figure DDNS.org.)** If your DDNS service is provided by TZO, then select TZO.com

. **(See Figure TZO.com.)** The features available on the DDNS screen will vary, depending on which DDNS service provider you use.

DynDNS.org

User Name, Password, and Host Name. Enter the **User Name, Password, and Host Name** of the account you set up with DynDNS.org.

Internet IP Address. The Router's current Internet IP Address is displayed here. Because it is dynamic, it will change.

Status. The status of the DDNS service connection is displayed here.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.



Setup | **11g VPN Router** | **ALLNETVPN**

Basic Setup | **DDNS** | MAC Address Clone | Advanced Routing

DDNS

DynDNS.org

User Name:

Password:

Host Name:

Internet IP Address: 192.168.41.76

Status: DDNS is disabled.

You may choose to disable DDNS function with the router. You must have an account with DynDNS.org or TZO.com in order to utilize this function.

[Save Settings](#) [Cancel Changes](#)

Figure DDNS.org

TZO.com Tab

Email Address, TZO Password Key, and Domain Name. Enter the **Email Address**, **TZO Password Key**, and **Domain Name** of the service you set up with TZO.

Internet IP Address. The Router's current Internet IP Address is displayed here. Because it is dynamic, this will change.

Status. The status of the DDNS service connection is displayed here.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Setup | **11g VPN Router** | **ALLNETVPN**

Basic Setup | **DDNS** | MAC Address Clone | Advanced Routing

DDNS

TZO.com

Email:

TZO Password Key:

Domain Name:

Internet IP Address: 192.168.41.76

Status: DDNS is disabled.

You may choose to disable DDNS function with the router. You must have an account with DynDNS.org or TZO.com in order to utilize this function.

[Save Settings](#) [Cancel Changes](#)

Figure TZO.com



MAC Address Clone Tab (See Figure MAC Address Clone.)



Figure MAC Address Clone

The Router's MAC address is a 12-digit code assigned to a unique piece of hardware for identification, like a social security number.

MAC Clone

- **MAC Clone Service.** To use MAC address cloning, select **Enable**.
- **MAC Address.** To manually clone a MAC address, enter the 12 digits of your adapter's MAC address in the onscreen fields (see Figure 6-25). Then click the **Save Settings** button.
- **Clone My MAC Address.** If you want to clone the MAC address of the PC you are currently using to configure the Router, then click the **Clone My MAC Address** button. The Router will automatically detect your PC's MAC address, so you do NOT have to call your ISP to change the registered MAC address to the Router's MAC address. It is recommended that the PC registered with the ISP is used to open the MAC Address Clone tab. When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.



Advanced Routing Tab

The Advanced Routing screen allows you to configure the dynamic routing and static routing settings. (See Figure Advanced Routing.)

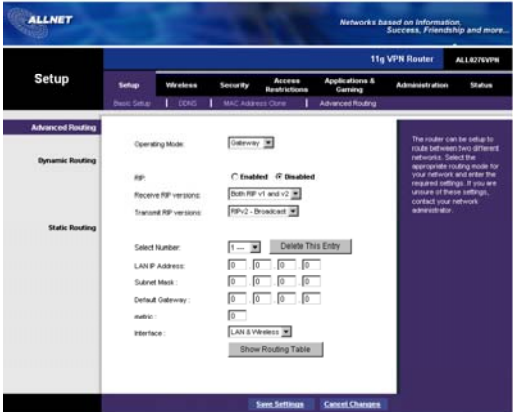


Figure-Advanced Routing

Advanced Routing

Operating Mode. Select Gateway or Router for the Operating Mode from the drop-down menu.

Dynamic Routing. With Dynamic Routing you can enable the Router to automatically adjust to physical changes in the network's layout. The Router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.

Receive RIP Version. To use dynamic routing for reception of network data, select the protocol you want: RIP1 only, RIP2 only or both RIP1 and RIP2. This can be disabled by selecting **Home**.

Transmit RIP Version. To use dynamic routing for transmission of network data, select the protocol you want: **RIP1**, **RIP2-Broadcast**, or **RIP2-Multicast**. This can be disabled by selecting **Home**.

Static Routing

If the Router is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network. To create a static route, change the following settings:

Select Number. Select the **number** of the static route from the drop- down menu. The Router supports up to 10 static route entries. **Delete This Entry.** If you need to delete a route, select its **number** from the drop-down menu, and click the **Delete Entry** button.

LAN IP Address. The LAN IP Address is the address of the remote network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route. If you are building a route to an entire network, be sure that the network portion of the IP address is set to 0.



For example, the Router's standard IP address is 192.168.1.1. Based on this address, the address of the routed network is 192.168.1, with the last digit determining the Router's place on the network. Therefore you would enter the IP address 192.168.1.0 if you wanted to route to the Router 's entire network, rather than just to the Router.

Subnet Mask. The Subnet Mask (also known as the Network Mask) determines which portion of an IP address is the network portion, and which portion is the host portion. Take, for example, a network in which the Subnet Mask is 255.255.255.0. This determines (by using the values 255) that the first three numbers of a network IP address identify this particular network, while the last digit (from 1 to 254) identifies the specific host.

Default Gateway. This IP address should be the IP address of the gateway device that allows for contact between the Router and the remote network or host.

Metric. This determines the maximum number of steps between network nodes that data packets will travel. A node is any device on the network, such as PCs, print servers, routers, etc

Interface. Select **LAN & Wireless or Internet**, depending on the location of the static route's final destination.

Show Routing Table. Click the **Show Routing Table** button to open a screen displaying how data is routed through your LAN. For each route, the Destination LAN IP address, Subnet Mask, Default Gateway, and Interface are displayed. Click the **Refresh** button to update the information. [See Figure Routing Table.](#)

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes

The Wireless Tab

Basic Wireless Settings

This screen allows you to choose your wireless network mode and wireless security. (See Figure Basic Wireless Setting)



Figure Basic Wireless Setting



Networks based on information,
Success, Friendship and more...

Wireless Network

Wireless Network Mode. If you have 802.11g and 802.11b devices in your network, then keep the default setting,

Mixed. If you have only 802.11g devices, select **G-Only**. If you have only 802.11b devices, select **B-only**. If you want to disable wireless networking, select **Disable**.

Wireless Network Name. Enter the Wireless Network Name (SSID) into the field. The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. For added security, ALLNET recommends that you change the default SSID (wireless-g) to a unique name of your choice.

Wireless Channel. Select the appropriate channel from the list provided to correspond with your network settings, between 1 and 11 (in North America). All devices in your wireless network must use the same channel in order to function correctly.

Wireless SSID Broadcast. When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting, **Enabled**. If you do not want to broadcast the Router's SSID, then select **Disabled**.

Wireless Security

The Wireless Security settings configure the security of your wireless network. There are four wireless security mode options supported by the Router: WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP.

WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption.

WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service. These four are briefly discussed here. To disable wireless security, keep the default setting,

Disabled.

An acronym for Wired Equivalent Privacy, WEP is an encryption method used to protect your wireless data communications. WEP uses 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission. To decode data transmissions, all devices 802.11b and g in a network must use an identical WEP key.

WPA Pre-Shared Key

To enter Security Mode field, select WPA Pre-Shared Key (no authentication server required). **WPA Algorithms.** For WPA algorithm, select **TKIP**. This is the approved and certified algorithm. Though it supports AES (Advanced Encryption System), interoperability among various vendors' products have not been certified. You can try AES on your router and client; if it works, AES provides even greater security.

WPA Shared Key. Enter a WPA Shared Key of 8-63 characters. Create a key that would not be easily compromised. You will need the same key for the client network card.

Key Renewal Timeout. Enter a Key Renewal period. This instructs the Router how often it should change the encryption keys (See Figure WPA-Pre-Shared Key).



Networks based on information,
Success, Friendship and more...

ALLNET
Networks based on information, Success, Friendship and more...

11g VPN Router ALLNET11gVPN

Wireless

Setup Wireless Settings | Wireless Security | Access Restrictions | Applications & Gaming | Administration | Status

Wireless Security

Security Mode: WPA Pre-Shared Key

WPA Algorithm: TKIP

WPA Shared Key:

Key Renewal Timeout: 120 seconds

Save Settings Cancel Changes

The router supports four different types of security settings for your wireless: WPA Protected Access (WPA), WPA Pre-Shared Key (WPA-PSK), Protected Access (WPA), WPA Pre-Shared Key (WPA-PSK), WPA Protected Access (WPA), WPA Pre-Shared Key (WPA-PSK), and WPA Protected Access (WPA).

WPA Pre-Shared Key: These are the most common security settings for your wireless. WPA-PSK uses a shared key to protect your wireless network. WPA-PSK is the most secure and is recommended for use in most environments. WPA-PSK is the most secure and is recommended for use in most environments.

WPA Protected Access: These are the most common security settings for your wireless. WPA-PSK uses a shared key to protect your wireless network. WPA-PSK is the most secure and is recommended for use in most environments. WPA-PSK is the most secure and is recommended for use in most environments.

More...

Figure- WPA Pre-Shared Key

WPA RADIUS

This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) Select the type of WPA algorithm you want to use. Then enter the RADIUS server's IP Address and Port Number, along with a key shared between the Router and the server. Last, enter a Key Renewal Timeout, which instructs the Router how often it should change the encryption keys (See Figure WPA RADIUS)

ALLNET
Networks based on information, Success, Friendship and more...

11g VPN Router ALLNET11gVPN

Wireless

Setup Wireless Settings | Wireless Security | Access Restrictions | Applications & Gaming | Administration | Status

Wireless Security

Security Mode: WPA RADIUS

RADIUS Server IP Address: 192.168.1.1

WPA Algorithm: TKIP

RADIUS Server Port: 1812

Shared Secret:

Key Renewal Timeout: 120 seconds

Save Settings Cancel Changes

The router supports four different types of security settings for your wireless: WPA Protected Access (WPA), WPA Pre-Shared Key (WPA-PSK), Protected Access (WPA), WPA Pre-Shared Key (WPA-PSK), WPA Protected Access (WPA), WPA Pre-Shared Key (WPA-PSK), and WPA Protected Access (WPA).

WPA RADIUS: WPA RADIUS uses a RADIUS server to authenticate users. WPA RADIUS is the most secure and is recommended for use in most environments. WPA RADIUS is the most secure and is recommended for use in most environments.

More...

Figure-WPA RADIUS

RADIUS

This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router).

First, enter the RADIUS server's IP Address into the RADIUS Server IP Address field, and port number into the RADIUS Server Port field, along with a key shared between the Router and the server in the Shared Key field.



Next, select the level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**, and Default Transmit Key (choose which Key to use). Last, either generate a WEP key using the Passphrase or enter the WEP key manually (See Figure-RADIUS).



Figure-RADIUS

WEP

(See Figure -WEP)



Figure- WEP

WEP is a basic encryption method, which is not as secure as WPA. The WEP screen allows you to configure your WEP settings. **Default Transmit Key**. Select which WEP key (1-4) will be used when the Router sends data. Make sure the receiving device is using the same key.

WEP Encryption. Select the level of WEP encryption you wish to use, 64-bit 10 hex digits or 128-bit 26 hex digits. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

Keys 1-4. WEP keys enable you to create an encryption scheme for wireless LAN transmissions.



If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes. These are not valid key values.) If you are using 64-bit WEP encryption, then the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, then the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are "0"- "9" and "A"- "F". When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Wireless Network Access

(See Figure-Wireless Network Access.)

Wireless Network Access. If this function is not disabled, only the computers on the list will be allowed access to the wireless network. Click **Disabled** to disable the function. To add a computer to the network, click the **Permit to access** button, and enter the MAC address in the fields. Click the **Select MAC Address From Networked Computers** button, and the screen in Figure 6-17 will appear. Select the **MAC Address** from the list and click the **Select** button.

To prevent access, click the **Prevent from accessing** button, then click **Select MAC Address from Networked Computers**. From the screen in (Figure-Networked Computers), select the **MAC Address** from the list, and click the **Select** button. Click the **Refresh** button if you want to refresh the screen. Click the **close** button to return to the previous screen.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.



Figure-Wireless Network Access

Networked Computers



Figure- Networked Computers



Networks based on information,
Success, Friendship and more...

Advanced Wireless Settings

(See Figure-Advanced Wireless Settings.)

On this screen you can access the Advanced Wireless features, including Authentication Type, CTS Protection Mode, Basic Data Rates, Control Tx Rates, Beacon Interval, DTIM Interval, RTS Threshold, and Fragmentation Threshold.

Authentication Type. The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. For Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. For Shared Key authentication, the sender and recipient use a WEP key for authentication. If you want to use only Shared Key authentication, then select **Shared Key**.

CTS Protection Mode. Ensures that your wireless router does not interfere with neighboring network. 802.11g network can cause collisions on 802.11b network so the Protection Mode forces the 802.11g network to negotiate around the 802.11b network. To enable CTS Protection Mode, select **Auto**. Select **Disable** to disable this feature.

Basic Data Rates. Select **1-2 Mbps**, **All**, or **Default**, from the drop-down menu.

Control Tx Rates. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or select **Auto**, to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client

Beacon Interval. The default value is 100. Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network.

DTIM Interval The default value is 1. This value, between 1 and 255 milliseconds, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.

RTS Threshold This value should remain at its default setting of 2346. The range is 0- 2346 bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

Fragmentation Threshold This value should remain at its default setting of 2347. The range is 800 - 2347 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended



Wireless

Setup | **Wireless** | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Wireless Settings | Wireless Security | Wireless Network Access | **Advanced Wireless Settings**

Advanced Wireless

Authentication Type:

CTS Protection Mode:

Wireless Isolation:

Basic Data Rates:

Control Tx Rates:

Beacon Interval: ms (range 1 - 65535, default 100)

DTIM Interval: ms (range 1 - 255, default 1)

RTS Threshold: (range 0 - 2348, default 2348)

Fragmentation Threshold: (range 000 - 2347, default 2347)

Authentication Type: You may choose between Open and Shared. Please note that all computers on your network must have the same configuration in order to communicate.

Basic Data Rate: This defines the basic data rates your router will advertise.

Control Tx Rates: This determines the speed with which your router will communicate with wireless clients. Unless you are experiencing difficulties communicating with wireless clients, it is best to leave this setting at Auto.

[More...](#)

Figure-Advanced Wireless Settings

The Security Tab

Firewall

When you click the Security tab, you will see the Firewall screen (see Figure -Firewall). This screen contains Filters and Block WAN Requests. Filters block specific internal users from accessing the Internet and block anonymous Internet requests and/or multicasting. **Firewall.** To add Firewall Protection, click **Enabled**. If you do not want Firewall Protection, click **Disabled**.

Filter Proxy. Use of WAN proxy servers may compromise the Router's security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click **Enabled**.

Filter Cookies. A cookie is data stored on your PC and used by Internet sites when you interact with them. To enable cookie filtering, click **Enabled**.



Networks based on information,
Success, Friendship and more...

Filter Java Applets. Java is a programming language for websites. If you deny Java Applets, you run the risk of not having access to Internet sites created using this programming language. To enable Java Applet filtering, click **Enabled**.

Filter ActiveX. ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. To enable ActiveX filtering, click **Enabled**.

Filter Multicast. Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. Select **Enabled** to filter multicasting, or **Disabled** to disable this feature.

Block Anonymous Internet Requests. This keeps your network from being "pinged" or detected and reinforces your network security by hiding your network ports, so it is more difficult for intruders to work their way into your network. Select **Enabled** to block anonymous Internet requests, or **Disabled** to allow anonymous Internet requests. When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

The screenshot shows the ALLNET 11g VPN Router configuration interface. The top navigation bar includes 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. The 'Security' section is expanded, showing 'Firewall', 'VPN Passthrough', and 'VPN Tunnel'. The 'Firewall' tab is active, displaying the following settings:

Section	Setting	Enabled	Disabled
Additional Filters	Firewall Protection:	<input checked="" type="radio"/>	<input type="radio"/>
	Filter Proxy:	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
	Filter Cookies:	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
	Filter Java Applets:	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
	Filter ActiveX:	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
Filter Multicast:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	
Block WAN Requests	Block Anonymous Internet Requests:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled

At the bottom of the page are two buttons: 'Save Settings' and 'Cancel Changes'.

Firewall Protection: You may choose to enable or disable the router's Stateful Packet Inspection (SPI) firewall. Your network will become less secure if you choose to disable this setting.

Filter Proxy: Use of WAN proxy services may compromise the Router's security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click **Enabled**.

Filter Cookies: A cookie is data stored on your PC and used by Internet sites when you interact with them. To enable cookie filtering, click **Enabled**.

Misc...

Figure-Firewall



Networks based on information,
Success, Friendship and more...

VPN PassThrough

(See Figure-VPN PassTrough)

- **IPSec Passthrough.** Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec Passthrough, click the **Enabled** button. To disable IPSec Passthrough, click the **Disabled** button.
- **PPTP Pass Through.** Point-to-Point Tunneling Protocol Passthrough is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP Passthrough, click the **Enabled** button. To disable PPTP Passthrough, click the **Disabled** button.
- **L2TP Pass Through.** Layering 2 Tunneling Protocol Passthrough is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by to enable the operation of a virtual private network (VPN) over the Internet. To allow L2TP Passthrough, click the **Enabled** button. To disable L2TP Passthrough, click the **Disabled** button.

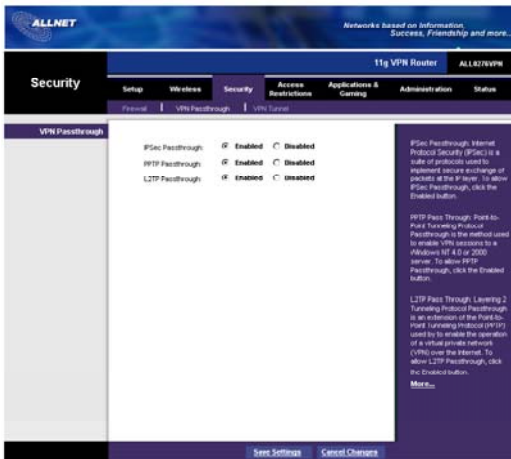


Figure-VPN PassThrough

VPN Tunnel

The VPN Router creates a tunnel or channel between two endpoints, so that the data or information between these endpoints is secure.

To **establish** this tunnel, select the tunnel you wish to create in the Select Tunnel Entry drop-down box. It is possible to create up to 50 simultaneous tunnels. Then click **Enabled** to enable the tunnel. Once the tunnel is enabled, enter the name of the tunnel in the **Tunnel Name** field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel. If you want to route all the traffic through the tunnel, and not just the ones destined for remote secure group, click **Enabled** for the VPN Gateway.



Networks based on information,
Success, Friendship and more...

Local Secure Group and Remote Secure Group. The Local Secure Group is the computer(s) on your LAN that can access the tunnel. Enter the **IP Address** and **Subnet Mask** of the local VPN Router in the fields. Local Secure Group defines the endpoint on local site. It can be one IP Address, IP Range, Subnet, or None (Host). From the drop-down menu, select **Subnet** to include the entire network for the tunnel; **IP Address** if you want a specific computer; **IP Range** if you want to include a range of IP addresses; or **Host** which is used with Port Forwarding to direct the traffic to the correct computer. The screen will change depending on the selected option. The options are described below. Subnet. Enter the **IP Addr.** and **Mask** of the local VPN Router in the fields. To allow access to the entire IP subnet, enter 0 for the last set of IP Addresses. (e.g. 192.168.1.0). IP Address. Enter the **IP Address** of the local VPN Router in the field. The **Mask** value will be displayed.

IP Range. Enter the starting and ending numbers for the **IP Address** range in the fields. Host. The VPN Tunnel will terminate at the router with this setting. Use Port Range Forwarding to direct traffic to the correct computer. Refer to the Port Range Forwarding tab of the Applications tab. The **Remote Secure Group** is the computer (s) on the remote end of the tunnel that can access the tunnel, Remote Secure Group defines the endpoint on remote site. It also supports ANY remote local style. From the drop-down menu, select **Subnet** to include the entire network for the tunnel; **IP Address** if you want a specific computer; **IP Range** if you want to include a range of IP addresses; **Host** if the VPN terminates at the Router instead of the PC; or **Any** to allow any computer to access the tunnel. The screen will change depending on the selected option. The options are described below. Subnet. Enter the **IP Addr.** and **Mask** of the remote VPN Router in the fields. To allow access to the entire IP subnet, enter 0 for the last set of IP Addresses. (e.g. 192.168.1.0).

IP Address. Enter the **IP Address** of the remote VPN Router in the field. The **Mask** value will be displayed.

IP Range. Enter the starting and ending numbers for the **IP Address** range in the fields. Host. The VPN Tunnel will terminate at the remote router with this setting. Use Port Range Forwarding to direct traffic to the correct computer.

The **Remote Secure Gateway** specifies the remote gateway location. It can be **IP Addr.**, **FQDN**, or **Any**. It is a VPN device, such as a second VPN Router, on the remote end of the VPN tunnel. Enter the **IP Address** of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Router, a VPN Server, or a computer with VPN client software that supports IPSec. The IP Address may either be static (permanent) or dynamic (changing), depending on the settings of the remote VPN device.

Make sure that you have entered the IP Address correctly, or the connection cannot be made. Remember, this is NOT the IP Address of the local VPN Router, but the IP Address of the remote VPN Router or device with which you wish to communicate.

Encryption. Using Encryption also helps make your connection more secure. There are two different types of encryption: DES or 3DES (3DES is recommended because it is more secure). You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting Disable. In Figure 6-18, DES (which is the default) has been selected.



Authentication. Authentication acts as another level of security. There are two types of authentication: MD5 and SHA (SHA is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to Disable authentication. In Figure 6-18, MD5 (the default) has been selected.

Key Management. Select Auto (IKE) and enter a series of numbers or letters in the **Pre-shared Key** field. Check the box next to **PFS (Perfect Forward Secrecy)** to ensure that the initial key exchange and IKE proposals are secure. Based on this word, which **MUST** be entered at both ends of the tunnel if this method is used, a key is generated to scramble (encrypt) the data being transmitted over the tunnel, where it is unscrambled (decrypted). You may use any combination of up to 24 numbers or letters in the **Pre-Shared Key** and **RSA Signature** fields No special characters or spaces are allowed. In the **Key Lifetime** field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be useful, or leave it blank for the key to last indefinitely. **Status.** Click the **Advanced VPN Tunnel Setup** key and the Advanced VPN Tunnel Setup screen will appear. See Figure –Advanced VPN Setup .

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Advanced VPN Tunnel Setup

(See Figure -Advanced VPN Setup)

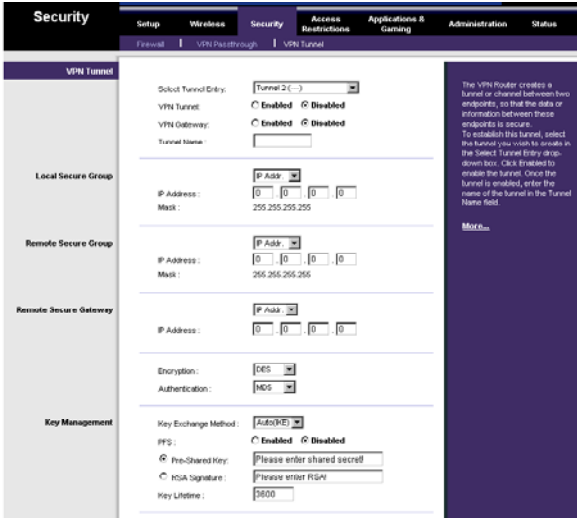


Figure -Advanced VPN Setup



Networks based on information,
Success, Friendship and more...

From the Advanced VPN Tunnel Setup screen, shown in **Figure -Advanced VPN Setup**, you can adjust the settings for specific VPN tunnels.

Phase 1

Phase 1 is used to create a security association (SA), often called the IKE SA. After Phase 1 is completed, Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions. **Operation Mode.** There are two modes: **Main** and **Aggressive**, and they exchange the same IKE payloads in different sequences. Main mode is more common; however, some people prefer Aggressive mode because it is faster. Main mode is for normal usage and includes more authentication requirements than Aggressive mode. Main mode is recommended because it is more secure. No matter which mode is selected, the VPN Router will accept both Main and Aggressive requests from the remote VPN device.

Encryption. Select the length of the key used to encrypt/decrypt ESP packets. There are two choices: DES and 3DES. 3DES is recommended because it is more secure.

Authentication. Select the method used to authenticate ESP packets. There are two choices: MD5 and SHA. SHA is recommended because it is more secure.

Group. There are three Diffie-Hellman Groups to choose from: 768-bit and 1024-bit and 1536-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

Key Life Time. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Phase 2

Encryption. The encryption method selected in Phase 1 will be displayed.

Authentication. The authentication method selected in Phase 1 will be displayed.

Group. There are three Diffie-Hellman Groups to choose from: 768-bit and 1024-bit and 1536-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

Key Life Time. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Other Options, giving you the flexibility to enable or disable the following features:

NetBIOS broadcast

Anti-replay

Keep Alive

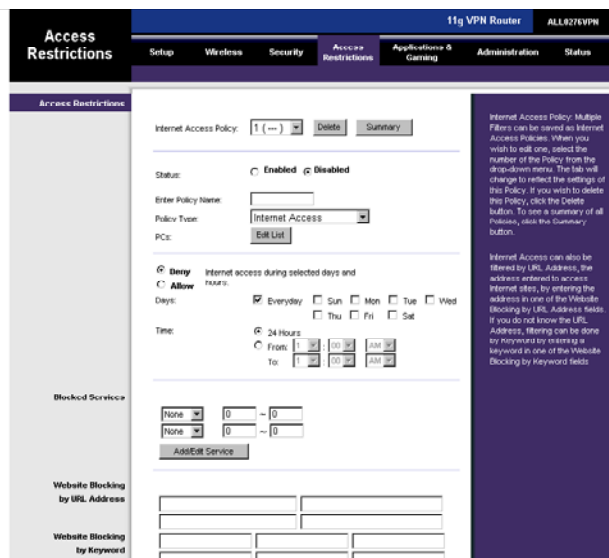
If IKE failed more than <number> times, block this unauthorized IP for <number> seconds

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. For further help on this tab, click the **help** button.

The Access Restrictions Tab

Access Restriction

The Access Restrictions tab, shown in Figure **Access Restriction**, allows you to block or allow specific kinds of Internet usage. You can set up Internet access policies for specific PCs and set up filters by using network port numbers.



Access Restrictions

11g VPN Router ALLNET/VPN

Setup Wireless Security **Access Restrictions** Application & Gaming Administration Status

Access Restrictions

Internet Access Policy: 1 (—) Delete Summary

Status: ☒ Enabled ☐ Disabled

Enter Policy Name:

Policy Type: Internet Access

PCs:

☒ Deny Internet access during selected days and times

Days: ☒ Everyday ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Time: ☒ 24 Hours

From: 1:00 AM To: 12:00 AM

Blocked Services

None ~ None

Add/Edit Service

Website Blocking by URL Address

Website Blocking by Keyword

Internet Access Policy: Multiple Filters can be saved as Internet Access Policies. When you wish to edit one, select the number of the Policy from the drop-down menu. The tab will change to reflect the settings of this Policy. If you wish to delete this Policy, click the Delete button. To see a summary of all Policies, click the Summary button.

Internet Access can also be filtered by URL Address, the address entered to access Internet sites, by entering the address in one of the Website Blocking by URL Address fields. If you do not know the URL Address, filtering can be done by keywords by entering a keyword in one of the Website Blocking by Keyword fields.

Figure- Access Restriction

Internet Access Policy. Multiple Filters can be saved as **Internet Access Policies**. When you wish to edit one, select the number of the Policy from the drop-down menu. The tab will change to reflect the settings of this Policy. If you wish to delete this Policy, click the **Delete** button. To see a summary of all Policies, click the **Summary** button.

The summaries are listed on this screen, shown in Figure Internet Access Policy, with their name and settings. To return to the Filters tab, click the **Close** button.



Networks based on information,
Success, Friendship and more...

Enter Policy Name. Policies are created from the fields presented here.

To create an Internet Access policy:

1. Enter a Policy Name in the field provided. Select **Internet Access** as the Policy Type.

Internet Access Policy: 1 (---) [Details] [Summary]

Status: ☐ Enabled ☒ Disabled

Enter Policy Name: []

Policy Type: [Inbound Traffic]

From Internal IP Address	Protocol	Port Number	To Internal IP Address
0 . 0 . 0 . 0	Any	0 to 0	192.168.1 . 0
0 . 0 . 0 . 0	Any	0 to 0	192.168.1 . 0
0 . 0 . 0 . 0	Any	0 to 0	192.168.1 . 0
0 . 0 . 0 . 0	Any	0 to 0	192.168.1 . 0

☒ Deny Internet access during selected days and hours.

☐ Allow

Days: ☒ Everyday ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Time: ☒ 24 Hours

☐ From: [] To: []

[Save Settings] [Cancel Changes]

Internet Access Policy: Multiple filters can be saved as Internet Access Policies. When you wish to edit one, select the number of the Policy from the drop-down menu. This list will change to reflect the settings of this Policy. If you wish to delete this Policy, click the Delete button. To see a summary of all Policies, click the Summary button.

Internet Access can also be filtered by URL Address, the address entered to access Internet sites, by entering the address in one of the Web site Blocking by URL Address fields. If you do not know the URL Address, filtering can be done by Keyword by entering a keyword in one of the Web site Blocking by Keyword fields.

Figure-Internet Access Policy

List of PCs

Enter MAC Address of the PCs in this format: (xxxxxxxxxxxx)

MAC 01: [00:00:00:00:00:00] MAC 05: [00:00:00:00:00:00]

MAC 02: [00:00:00:00:00:00] MAC 06: [00:00:00:00:00:00]

MAC 03: [00:00:00:00:00:00] MAC 07: [00:00:00:00:00:00]

MAC 04: [00:00:00:00:00:00] MAC 08: [00:00:00:00:00:00]

Enter the IP Address of the PCs

IP 01: 192.168.1 . [0] IP 04: 192.168.1 . [0]

IP 02: 192.168.1 . [0] IP 05: 192.168.1 . [0]

IP 03: 192.168.1 . [0] IP 06: 192.168.1 . [0]

Enter the IP Range of the PCs

IP Range 01: 192.168.1 . [0] ~ [0] IP Range 02: 192.168.1 . [0] ~ [0]

[Apply] [Cancel] [Close]

Figure-List of PCs



Networks based on information,
Success, Friendship and more...

2. Click the **Edit List** button. This will open the List of PCs screen, shown in Figure-List of PCs. From this screen, you can enter the IP address or MAC address of any PC to which this policy will apply. You can even enter ranges of PCs by IP address. Click the **Apply** button to save your settings, the **Cancel** button to undo any changes, and the **Close** button to return to the Access Restrictions tab.
3. If you wish to Deny or Allow Internet access for those PCs you listed on the List of PCs screen, click the option.
4. You can filter access to various services accessed over the Internet, such as FTP or Telnet, by selecting a service from the drop-down menus next to Blocked Services. If a service isn't listed, you can click the **Add Service** button to open the Service screen, shown in **Figure-Blocked services**, and add a service to the list. You will need to enter a Service name, as well as the Protocol and Port Range used by the service.

Figure-Blocked services

5. By selecting the appropriate setting next to Days and Time, choose when Internet access will be filtered.
6. Lastly, click the **Save Settings** button to activate the policy.

To create an Inbound Traffic Policy

1. Enter a Policy Name in the field provided. Select **Inbound Traffic** as the Policy Type.
2. Enter the **IP Address** from which you want to block. Select the Protocol: **TCP**, **UDP**, or **Both**. Enter the **port** number or select **Any**. Enter the IP Address to which you want to block.
3. Select **Deny** or **Allow** as appropriate.
4. By selecting the appropriate setting next to Days and Time, choose when the Inbound Traffic will be filtered. Lastly, click the **Save Settings** button to activate the policy.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Internet Access can also be filtered by URL Address, the address entered to access Internet sites, by entering the address in one of the **Website Blocking by URL Address** fields. If you do not know the URL Address, filtering can be done by Keyword by entering a keyword in one of the **Website Blocking by Keyword** fields.



Networks based on information,
Success, Friendship and more...

The Applications Tab

Port Range Forwarding

The Port Forwarding screen sets up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.) (See Figure-Port Range Forwarding.)

Application	Start	End	Protocol	IP Address	Enabled
<input type="text"/>	<input type="text"/> 0	to <input type="text"/> 0	<input type="text"/> Both	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> 0	to <input type="text"/> 0	<input type="text"/> Both	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> 0	to <input type="text"/> 0	<input type="text"/> Both	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> 0	to <input type="text"/> 0	<input type="text"/> Both	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> 0	to <input type="text"/> 0	<input type="text"/> Both	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> 0	to <input type="text"/> 0	<input type="text"/> Both	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> 0	to <input type="text"/> 0	<input type="text"/> Both	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> 0	to <input type="text"/> 0	<input type="text"/> Both	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> 0	to <input type="text"/> 0	<input type="text"/> Both	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/> 0	to <input type="text"/> 0	<input type="text"/> Both	192.168.1.0	<input type="checkbox"/>

The Port Forwarding screen sets up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.) When users send this type of request to your network via the Internet, the Router will forward those requests to the appropriate PC. Any PC whose port is being forwarded must have its DHCP client function disabled and must have a new static IP address assigned to it because its IP address may change when using the DHCP function.

[More...](#)

[Save Settings](#) [Cancel Changes](#)

Figure-Port Range Forwarding

When users send this type of request to your network via the Internet, the Router will forward those requests to the appropriate PC. Any PC whose port is being forwarded must have its DHCP client function disabled and must have a new static IP address assigned to it because its IP address may change when using the DHCP function.

Application. Enter the name you wish to give each application.

Start and End. Enter the starting and ending numbers of the port you wish to forward.

Protocol. Select the type of protocol you wish to use for each application: TCP, UDP, or Both **IP**

Address. Enter the IP Address and Click Enabled.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.



Networks based on information,
Success, Friendship and more...

Port Triggering

Port Triggering is used for special Internet applications whose outgoing ports differ from the incoming ports. For this feature, the Router will watch outgoing data for specific port numbers. (See Figure –Port Triggering.) The Router will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

Application	Triggered Range		Forwarded Range		Protocol	Enabled
	Start Port	End Port	Start Port	End Port		
	0	to 0	0	to 0	Both	<input type="checkbox"/>
	0	to 0	0	to 0	Both	<input type="checkbox"/>
	0	to 0	0	to 0	Both	<input type="checkbox"/>
	0	to 0	0	to 0	Both	<input type="checkbox"/>
	0	to 0	0	to 0	Both	<input type="checkbox"/>
	0	to 0	0	to 0	Both	<input type="checkbox"/>
	0	to 0	0	to 0	Both	<input type="checkbox"/>
	0	to 0	0	to 0	Both	<input type="checkbox"/>
	0	to 0	0	to 0	Both	<input type="checkbox"/>
	0	to 0	0	to 0	Both	<input type="checkbox"/>

Port Triggering is used for special Internet applications whose outgoing ports differ from the incoming ports. For this feature, the router will watch outgoing data for specific port numbers. The Router will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

Application: Enter the name you wish to give each application.

Start Port and End Port: Enter the starting and ending Triggered range numbers and the Forwarded Range numbers of the port you wish to forward.

Protocol: Select the type of protocol you wish to use for each application: TCP, UDP, or Both.

Save Settings Cancel Changes

Figure –Port Triggering

Application. Enter the name you wish to give each application.

Start Port and End Port. Enter the starting and ending Triggered range numbers and the Forwarded Range numbers of the port you wish to forward.

Protocol. Select the type of protocol you wish to use for each application: **TCP** , **UDP** , or **Both**.

Click **Enabled** .

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.



Networks based on Information,
Success, Friendship and more...

UPnP Forwarding

The UPnP screen provides options for customisation of port services for applications (See Figure UPnP Forwarding.) Application. You can specify up to ten applications in the available fields.

Application	Ext. Port	Int. Port	Protocol	IP Address	Enabled
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	192.168.1.0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	192.168.1.0	<input type="checkbox"/>

UPnP Forwarding can be used to set up public services on your network. When users from the Internet make certain requests on your network, the Router will forward those requests to computers equipped to handle the requests. If, for example, you set the port number **80** (HTTP) to be forwarded to IP Address 192.168.1.2, then all HTTP requests from outside users will be forwarded to 192.168.1.2. You must disable the Router's **DMZ** function to utilize port forwarding.

[More...](#)

Figure-UPnP Forwarding

The preset applications are among the most widely used Internet applications. They include the following: **FTP** (File Transfer Protocol). A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc). For example, after developing the HTML pages for a website on a local machine, they are typically uploaded to the web server using FTP.

Telnet. A terminal emulation protocol commonly used on Internet and TCP/IP based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

SMTP (Simple Mail Transfer Protocol). The standard e-mail protocol on the Internet. It is a TCP/IP Protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.

DNS (Domain Name System). The way that Internet domain names are located and translated into IP addresses. A domain name is a meaningful and easy to remember "handle" for an Internet address.

TFTP (Trivial File Transfer Protocol). A version of the TCP/IP FTP protocol that has no directory or password capability **Finger**. A UNIX command widely used on the Internet to find out information about a particular user such as a telephone number, whether the user is currently logged on and the last time the user was logged on. The person being "fingered" must have placed his or her profile on the system in order for the information to be available. Fingering requires entering the full user domain address.



Networks based on information,
Success, Friendship and more...

HTTP (Hyper Text Transfer Protocol). The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client web browser.

POP3 (Post Office Protocol 3). A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system with little selectivity. All pending messages and attachments are downloaded at the same time. POP3 uses the SMTP messaging protocol.

NNTP (Network News Transfer Protocol). The protocol used to connect to Usenet groups on the Internet. Usenet newsreaders support the NNTP protocol.

SNMP (Simple Network Management Protocol). A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, ridge, etc) to the workstation console used to oversee the network. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc)

Ext. Port and Int. Port. Enter the numbers of the port used by the server
Protocol. Select the type of protocol you wish to use for each application: **TCP, UDP or BOTH.**

IP Address. Enter the IP Address and click **Enabled.**

Enter the Application in the field. Then enter the External and Internal Port Numbers in the fields. Select the type of protocol you wish to use for each application: TCP, UDP or Both. Enter the IP address in the field.

Click Enabled to enable UPnP forwarding for the chosen application

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

DMZ

The DMZ screen (see **Figure-DMS**) allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing, through Software DMZ, or a user can use LAN Port 4 as a DMZ Port, through Hardware DMZ. Whereas Port Range Forwarding can only forward a maximum of 10 ranges of ports, DMZ hosting forwards all the ports for one PC at the same time.

Software DMZ. This feature allows one local user to be exposed to the Internet for use of a special purpose service such as Internet gaming and videoconferencing. To use this feature, select **Enabled**. To disable DMZ, select **Disabled**.

DMZ Host IP Address. To expose one PC, enter the computer's IP address. To get the IP address of a computer, refer to "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter." Deactivate DMZ by entering a 0 in the field.

Hardware DMZ. This feature allows a user to use LAN Port 4 as a DMZ Port. To use this feature, select **Enabled**. To disable DMZ, select **Disabled**.

Private DMZ Host IP. If Private IP is selected, enter the Private DMZ Host IP in this field.

Public DMZ Host IP. If Public IP is selected, enter the Public DMZ Host IP in this field (which is provided by your ISP.)



Networks based on information,
Success, Friendship and more...

Hardware DMZ IP Address. Enter the IP Address in the fields.

Hardware DMZ Netmask. Enter the Netmask in the fields.

Destination IP Address. Enter the IP Address of the destination in the fields.

Subnet Mask. Enter the Subnet Mask in the fields.

Default Gateway. Enter the Default Gateway in the fields **metric.** Enter the metric.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

The screenshot shows the ALLNET 11g VPN Router web interface. The top navigation bar includes 'Applications & Gaming', 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. The 'DMZ' tab is selected. The main content area is divided into two sections: 'Software DMZ' and 'Hardware DMZ'. Both sections have a radio button for 'Enabled' and 'Disabled'. The 'Software DMZ' section has a 'DMZ Host IP Address' field with the value '192.168.1.0'. The 'Hardware DMZ' section has a 'Private DMZ Host IP' field with the value '192.168.1.0' and a 'Public DMZ Host IP' field with the value '0.0.0.0'. A 'More...' link is visible on the right side of the Hardware DMZ section. At the bottom, there are 'Save Settings' and 'Cancel Changes' buttons.

Figure DMZ



Networks based on information,
Success, Friendship and more...

The Administration Tab

Management

The Management screen, shown in **Figure Management**, allows you to change the Router's access settings as well as configure the SNMP and UPnP (Universal Plug and Play) features.

Figure-Management

Router Password

Local Router Access. To ensure the Router's security, you will be asked for your password when you access the Router's Web-based Utility. The default password is admin.

User Name. Enter the default admin.

Router Password. It is recommended that you change the default password to one of your choice.

Re-enter to confirm. Re-enter the Router's new Password to confirm it.

Remote Router Access. This feature allows you to access the Router from a remote location, via the Internet.

Remote Management. This feature allows you to manage the Router from a remote location, via the Internet. To enable Remote Management, click **Enabled**.

Management Port. Select the port number you will use to remotely access the Router from the drop-down menu



Networks based on information,
Success, Friendship and more...

SNMP

Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol. To enable SNMP, click **Enabled**. To disable SNMP, click **Disabled**. **Identification**. In the Contact field, enter contact information for the Router. In the Device Name field, enter the name of the Router. In the Location field, specify the area or location where the Router resides.

Get Community. Enter the password that allows read only access to the Router's SNMP information
Set Community. Enter the password that allows read/ write access to the Router's SNMP information

SNMP Trusted Host. You can restrict the router's SNMP information by IP Address. Enter the IP address in the SNMP Trusted Host field. If this field is left blank, then access from any IP address is permitted.

SNMP Trap-Community. Enter the password required by the remote host computer that will receive trap messages or notices sent by the router

SNMP Trap- Destination. Enter the IP address of the remote host computer that will receive the trap messages

UPnP

UPnP allows Windows XP to automatically configure the Router for various Internet applications, such as gaming and videoconferencing. To enable UPnP, click **Enabled**.

Allow User to make Configuration Changes. When enabled, this feature allows you to make manual changes while still using the UPnP feature.

Allow users to disable Internet access. When enabled, this feature allows you to prohibit any and all Internet connections.

Log

The Log tab, shown in **Figure-Log** provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection.

Log

Email Alert

E-Mail Alert: ☐ Enabled ☐ Disabled

E-Mail Address for General Logs:

E-Mail Address for Alert Logs:

Return E-Mail address:

E-Mail Server IP Address:

Syslog Notification

☐ Enabled ☐ Disabled

Device Name:

Syslog Server IP Address:

Syslog Priority:

Application Queue Length

Log Queue Length: entries

Log Time Threshold: seconds

Alert Log

☐ Syn Flooding ☐ Ping Of Death

☐ P Spoofting ☒ Unauthorized Login Attempt

☐ Win Nuke

General Log

☒ System Error Messages ☒ Authorized Login

☐ Deny Policies ☒ Configuration Changes

More...

Figure-Log



Networks based on information,
Success, Friendship and more...

Email Alert

To enable E-Mail Alert, click **Enabled**.

E-Mail Address for General Logs. Enter the **E-Mail Address for General Logs** in the field.

E-Mail Address for Alert Logs. Enter the **E-Mail Address for Alert Logs** in the field.

Return E-Mail address. Enter the **address for the return E-Mail**.

E-Mail Server IP Address. Enter the **IP Address of the E-Mail Server** in the fields.

Syslog Notification

To enable Syslog, click **Enabled**.

Device Name. Enter the **Device Name** in the field.

Syslog Server IP Address. Enter the **IP Address of the Syslog Server**.

Syslog Priority. Select the **priority** from the drop-down list

Notification Queue Length

Log queue Length. Enter the **number** of entries in the log queue in the field.

Log Time Threshold. Enter the **time** for the threshold in the field.

Alert Log

Select the type of attacks that you want to be alerted to. Select Syn Flooding, IP Spoofing, Win Nuke, Ping of Death, or Unauthorized Login attempt.

General Log.

Select the type of activity you would like to log. Select System Error Messages, Deny Policies, Allow Policies, Content Filtering, Data Inspection, authorized Login, or Configuration Changes. When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Diagnostics

Ping Test (See Figure-Ping Test.)

The screenshot shows the 'Administration' tab of the ALLNET 11g VPN Router. The 'Diagnostics' sub-tab is selected, and the 'Ping Test' page is displayed. The page has a title bar 'Ping Test' and a subtitle 'Ping Test Parameters'. The configuration fields are as follows:

- Ping Target IP: 0 . 0 . 0 . 0
- No. of Pings: 4
- Ping Size: 64 bytes
- Ping Interval: 1000 Milliseconds
- Ping Timeout: 5000 Milliseconds

Below these fields is a large text area for results, and at the bottom are three buttons: 'Start Test', 'Abort Test', and 'Clear Result'. On the right side of the page, there is a help text area with the following instructions:

- Ping Target IP: Enter the IP Address that you want to ping in the field.
- No. of Pings: Enter the number of times that you want to ping.
- Ping Size: Enter the size of the ICMP Packet.
- Ping Interval: Enter the ping interval in Milliseconds.
- Ping Timeout: Enter the time in Milliseconds.

Figure- Ping Test



Ping Test

Ping Test Parameters

Ping Target IP. Enter the IP Address that you want to ping in the field.

No. of Pings. Enter the number of times that you want to ping.

Ping Size. Enter the size of the ping packets.

Ping Interval. Enter the ping interval in Milliseconds.

Ping Timeout. Enter the time in Milliseconds.

Click the **Start Test** button to start the Ping Test. Click the **Abort Test** button to stop the test.

Click the **Refresh**

Result button to clear the results. The results of the test will display in the window..

Factory Default

(See Figure Factory Default.)



Figure Factory Default

If you have exhausted all other options and wish to restore the Router to its factory default settings and lose all your settings, click **Yes**.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.



Firmware Upgrade

(See Figure Firmware Upgrade)

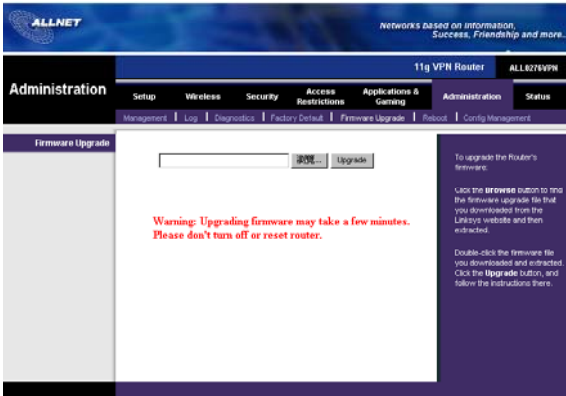


Figure Firmware Upgrade

To upgrade the Router's firmware:

1. Click the **Browse** button to find the firmware upgrade file that you downloaded from the ALLNET website and then extracted.
2. Double-click the firmware file you downloaded and extracted. Click the **Upgrade** button, and follow the instructions there.

Reboot

(See Figure-Reboot.)

Warm reboot this device. If you wish to reboot the device, click on **Yes**. Then click the **Save Settings** button to apply the changes.

Else, click the **Cancel Changes** button to undo your changes



Figure-Reboot



Config Management

(See Figure Config Management)

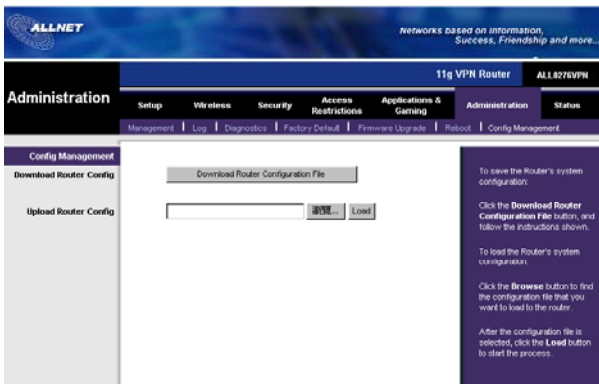


Figure Config Management

To save the Router's configuration file, click the **Download Router Configuration File** button, and follow the instructions shown.

To load the Router's system configuration, click the **Browse** button to find the configuration file that you want to load to the router. After the configuration file has been selected, click the Load button to start the loading process.



Networks based on information,
Success, Friendship and more...

Status

Router

This screen displays information about your Router and its WAN (Internet) Connections. (See Figure Router)

Information

The information displayed is the Hardware Version, Software Version, MAC Address, Local MAC Address, and System Up Time.

WAN Connections

The WAN Connections displayed are the Network Access, WAN IP Address, Subnet Mask, Default Gateway, and DNS.

To release the DHCP IP Address for the WAN connection, click on **DHCP Release**.

To renew the DHCP IP Address for the WAN connection, click on the **DHCP Renew**.

Click the **Refresh** button if you want to Refresh your screen.

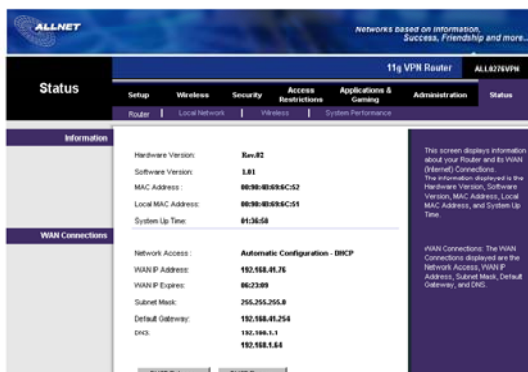


Figure: Router



Local Network

See Figure Local Network.

The Local Network information that is displayed is the IP Address, Subnet Mask, DHCP Server, and DHCP Client

Lease Info. To view the DHCP Clients Table, click the **DHCP Clients** button.

The DHCP Active IP Table, Figure 6-39, displays the computer name, IP Address, MAC Address and the expiration time. Click the **Close** button to return to the Local Network screen.

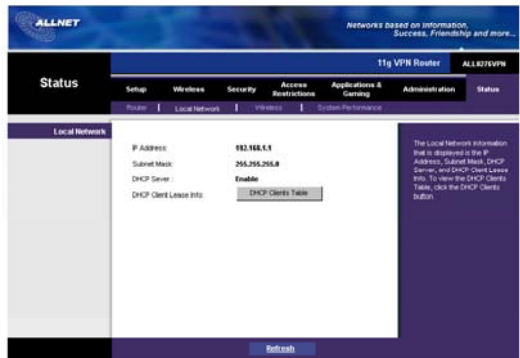


Figure Local Network

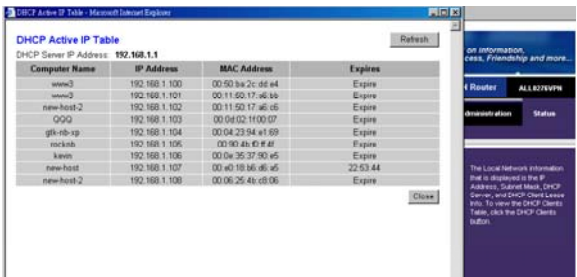


Figure-DHCP Active IP Table

Wireless

The Wireless Network information that is displayed is the MAC Address, Mode, SSID, Channel, and Encryption Function. (See Figure Wireless.)

Click the **Refresh** button if you want to Refresh your screen.



Figure Wireless

System Performance

The System Performance information that is displayed is the Wireless, Internet, and/or LAN information for the IP Address, MAC Address, Connection Status, Packets Received, Packets Sent, Bytes Received, Bytes Sent, Error Packets Received, and Dropped Packets Received. (See Figure System Performance.)

Click the **Refresh** button if you want to Refresh your screen

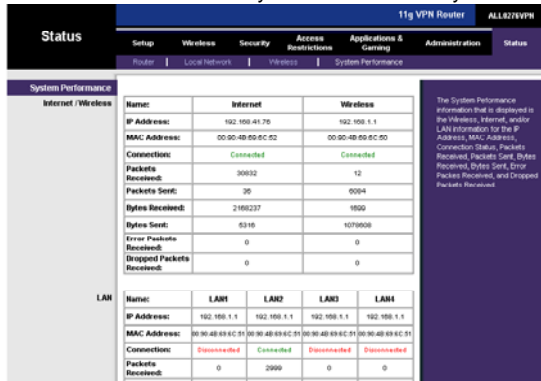


Figure System Performance



Troubleshooting

This appendix consists of two parts: "Common Problems and Solutions" and "Frequently Asked Questions." Provided are possible solutions to problems that may occur during the installation and operation of the Router. Read the descriptions below to help you solve your problems. If you can't find an answer here, check the ALLNET website at www.allnet.de

Common Problems and Solutions

1. I need to set a static IP address on a PC.

You can assign a static IP address to a PC by performing the following steps:

For Windows 98 and Me:

1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network** .
2. In The following network components are installed box, select the TCP/IP-> associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the Properties button.
3. In the TCP/IP properties window, select the IP address tab, and select Specify an IP address. Enter a unique IP address that is not used by any other computer on the network connected to the Router. Make sure that each IP address is unique for each PC or network device.
4. Click the **Gateway** tab, and in the New Gateway prompt, enter 192.168.1.1, which is the default IP address of the Router. Click the Add button to accept the entry.
5. Click the **DNS** tab, and make sure the DNS Enabled option is selected. Enter the Host and Domain names (e.g., John for Host and home for Domain). Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
6. Click the **OK** button in the TCP/IP properties window, and click Close or the OK button for the Network window.
7. Restart the computer when asked. For Windows 2000:
 1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connection**
 2. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the Properties option.
 3. In the Components checked are used by this connection box, highlight Internet Protocol (TCP/IP), and click the **Properties** button. Select **Use the following IP address** option
 4. Enter a unique IP address that is not used by any other computer on the network connected to the Router.
 5. Enter the Subnet Mask, 255.255.255.0.
 6. Enter the Default Gateway, 192.168.1.1 (Router's default IP address).
 7. Toward the bottom of the window, select Use the following DNS server addresses, and enter the 8. Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.



Networks based on information,
Success, Friendship and more...

8. Click the OK button in the Internet Protocol (TCP /IP) Properties window, and click the OK button in the Local Area Connection Properties window.
9. Restart the computer if asked. For Windows XP: The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.
 1. Click **Start** and **Control Panel**
 2. Click the **Network and Internet Connections** icon and then the **Network Connections** icon
 3. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the Properties option
 4. In the **This connection uses the following items** box, highlight **Internet Protocol (TCP/IP)** . Click the **Properties** button
 5. Enter a unique IP address that is not used by any other computer on the network connected to the Router
 6. Enter the Subnet Mask, 255.255.255.0.
 7. Enter the Default Gateway, 192.168.1.1 (Router's default IP address).
 8. Toward the bottom of the window, select Use the following DNS server addresses, and enter the
 9. Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
10. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window. Click the **OK** button in the Local Area Connection Properties window.



Networks based on information,
Success, Friendship and more...

2. I want to test my Internet connection.

A. Check your TCP/IP settings.

For Windows 98, Me, 2000, and XP:

Refer to "Chapter 4: Configure the PCs" for details. Make sure Obtain IP address automatically is selected in the settings.

For Windows NT 4.0:

Click **Start**, **Settings**, and **Control Panel**. Double-click the **Network** icon.

Click the Protocol tab, and double-click on TCP/IP Protocol.

When the window appears, make sure you have selected the correct Adapter for your Ethernet adapter and set it for **Obtain an IP address** from a DHCP server.

Click the OK button in the TCP/IP Protocol Properties window, and click the **Close** button in the Network window.

Restart the computer if asked.

B Open a command prompt.

For Windows 98 and Me:

Click **Start** and **Run**. In the Open field, type in command. Press the **Enter** key or click the **OK** button.

For Windows NT, 2000, and XP:

Click **Start** and **Run**. In the Open field, type cmd. Press the **Enter** key or click the **OK** button.

In the command prompt, type ping 192.168.1.1 and press the Enter key.

If you get a reply, the computer is communicating with the Router.

If you do NOT get a reply, please check the cable, and make sure Obtain an IP address automatically is selected in the TCP/IP settings for your Ethernet adapter.

C In the command prompt, type ping followed by your Internet or WAN IP address and press the **Enter** key.

The Internet or WAN IP Address can be found on the Status screen of the Router's web-based utility.

For example, if your Internet or WAN IP address is 1.2.3.4, you would enter ping 1.2.3.4 and press the Enter key.

If you get a reply, the computer is connected to the Router.

If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

D In the command prompt, type ping www.yahoo.com and press the **Enter** key.

If you get a reply, the computer is connected to the Internet.

If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.



3. I am not getting an IP address on the Internet with my Internet connection.

Refer to “Problem #2, I want to test my Internet connection” to verify that you have connectivity.

1. If you need to register the MAC address of your Ethernet adapter with your ISP, please see **“Appendix D: Finding the MAC address and IP Address for Your Ethernet Adapter.”** If you need to clone the MAC address of your Ethernet adapter onto the Router, see the System section of “Chapter 6: The Router’s Web-based Utility” for details.
2. Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of “Chapter 6: The Router’s Web-based Utility” for details on Internet connection settings.
3. Make sure you have the right cable. Check to see if the Internet column has a solidly lit Link/Act LED.
4. Make sure the cable connecting from your cable or DSL modem is connected to the Router’s Internet port. Verify that the Status page of the Router’s web-based utility shows a valid IP address from your ISP.
5. Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the Status tab of the Router’s web-based utility to see if you get an IP address

4. I am not able to access the Setup page of the Router’s web-based utility.

Refer to “Problem #2, I want to test my Internet connection” to verify that your computer is properly connected to the Router.

1. Refer to “Appendix D: Finding the MAC Address and IP address for Your Ethernet Adapter” to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
2. Set a static IP address on your system; refer to “Problem #1: I need to set a static IP address.”
3. Refer to “Problem #10: I need to remove the proxy settings or the dial-up pop-up window (for PPPoE users).”

5. I can’t get my Virtual Private Network (VPN) working through the Router.

Access the Router’s web interface by going to <http://192.168.1.1> or the IP address of the Router, and go to the Security tab. Make sure you have IPsec pass-through and/or PPTP passthrough enabled.

VPNs that use IPsec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPsec session will work through the Router; however, simultaneous IPsec sessions may be possible, depending on the specifics of your VPNs. VPNs that use IPsec and AH (Authentication Header known as protocol 51) are incompatible with the Router. AH has limitations due to occasional incompatibility with the NAT standard. Change the IP address for the Router to another subnet to avoid a conflict between the VPN



Networks based on information,
Success, Friendship and more...

IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Router will have difficulties routing information to the right location. If you change the Router's IP address to 192.168.2.1, that should solve the problem. Change the Router's IP address through the Setup tab of the web interface. If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.

Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPSec server. Refer to "Problem #7, I need to set up online game hosting or use other Internet applications" for details.

Check the ALLNET website for more information at www.allnet.de

6. I need to set up a server behind my Router and make it available to the public.

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed.

Follow these steps to set up port forwarding through the Router's web-based utility. We will be setting up web, ftp, and mail servers.

1. Access the Router's web-based utility by going to <http://192.168.1.1> or the IP address of the Router.

Go to the Applications and Gaming => Port Forwarding tab

2. Enter any name you want to use for the Customized Application.
3. Enter the External Port range of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
4. Check the protocol you will be using, TCP and/or UDP.
5. Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
6. Check the Enable option for the port services you want to use. Consider the example below:

Customized External Port TCP UDP IP Address Enable Application

Web server 80 to 80 X X 192.168.1.100 X

FTP server 21 to 21 X 192.168.1.101 X

SMTP (outgoing) 25 to 25 X 192.168.1.102 X

POP3 (incoming) 110 to 110 X X 192.168.1.102 X

When you have completed the configuration, click the **Save Settings** button.



7. I need to set up online game hosting or use other Internet applications.

If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the Router to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

1. Access the Router's web interface by going to <http://192.168.1.1> or the IP address of the Router. Go to the Applications and Gaming => Port Forwarding tab.
2. Enter any name you want to use for the Customized Application.
3. Enter the External Port range of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.
4. Check the protocol you will be using, TCP and/or UDP.
5. Enter the IP address of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.

6. Check the **Enable** option for the port services you want to use. Consider the example below:

Customized External Port TCPUDP IP Address Enable
Application

UT 7777 to 27900 X X 192.168.1.100 X

HalfLife 27015 to 27015 X X 192.168.1.105 X

PC Anywhere 5631 to 5631 X 192.168.1.102 X

VPN IPSEC 500 to 500 X 192.168.1.100 X

When you have completed the configuration, click the **Save Settings** button.

8. I can't get the Internet game, server, or application to work.

If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one PC to the Internet using DeMilitarized Zone (DMZ) hosting. This option is available when an application requires too many ports or when you are not sure which port services to use. Make sure you disable all the forwarding entries if you want to successfully

use DMZ hosting, since forwarding has priority over DMZ hosting. (In other words, data that enters the Router will be checked first by the forwarding settings. If the port number that the data enters from does not have port forwarding, then the Router will send the data to whichever PC or network device you set for DMZ hosting.)

Follow these steps to set DMZ hosting:

1. Access the Router's web-based utility by going to <http://192.168.1.1> or the IP address of the Router.

Go to the Applications and Gaming => DMZ tab.

2. Disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.

Once completed with the configuration, click the **Save Settings** button.



Networks based on information,
Success, Friendship and more...

9. I forgot my password, or the password prompt always appears when I am saving settings to the router.

Reset the Router to factory default by pressing the Reset button for 10 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:

1. Access the Router's web-based utility by going to <http://192.168.1.1> or the IP address of the Router. Enter the default password admin, and click the **Administrations => Management** tab.
2. Enter a different password in the Router Password field, and enter the same password in the second field to confirm the password.
3. Click the **Save Settings** button.

10. I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window.

If you have proxy settings, you need to disable these on your computer. Because the Router is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

For Microsoft Internet Explorer 5.0 or higher:

1. Click **Start, Settings, and Control Panel**. Double-click Internet Options.
2. Click the **Connections** tab.
3. Click the **LAN settings** button and remove anything that is checked.
4. Click the **OK** button to go back to the previous screen.
5. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.

For Netscape 4.7 or higher:

1. Start **Netscape Navigator**, and click **Edit, Preferences, Advanced, and Proxies**.
2. Make sure you have Direct connection to the Internet selected on this screen.
3. Close all the windows to finish.

11. To start over, I need to set the Router to factory default.

Hold the **Reset** button for 10 seconds and then release it. This will return the password, forwarding, and other settings on the Router to the factory default settings. In other words, the Router will revert to its original factory configuration.

12. I need to upgrade the firmware.

In order to upgrade the firmware with the latest features, you need to go to the ALLNET website and download the latest firmware at www.allnet.de

Follow these steps:

1. Go to the ALLNET website at <http://www.allnet.de> and download the latest firmware.
2. To upgrade the firmware, follow the steps in the System section found in "Chapter 6: The Router's Web-based Utility."



Networks based on information,
Success, Friendship and more...

13. The firmware upgrade failed, and/or the Power LED is flashing.

The upgrade could have failed for a number of reasons. Follow these steps to upgrade the firmware and/or make the Power LED stop flashing:

If the firmware upgrade failed, use the TFTP program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.

Set a static IP address on the PC; refer to "Problem #1, I need to set a static IP address." Use the following IP address settings for the computer you are using:

IP Address: 192.168.1.50

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

Perform the upgrade using the TFTP program or the Router's web-based utility through its Administration tab.

14. My DSL service's PPPoE is always disconnecting.

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet. There is a setup option to "keep alive" the connection. This may not always work, so you may need to reestablish connection periodically.

1. To connect to the Router, go to the web browser, and enter <http://192.168.1.1> or the IP address of the Router.
2. Enter the password, if asked. (The default password is admin.)
3. On the Setup screen, select the option **Keep Alive**, and set the Redial Period option at 20 (seconds).
4. Click the **Save Settings** button.
5. Click the **Status** tab, and click the **Connect** button.
6. You may see the login status display as Connecting. Press the F5 key to refresh the screen, until you see the login status display as Connected.
Click the **Save Settings** button to continue.
If the connection is lost again, follow steps 1- 6 to re-establish connection.



15. I can't access my e-mail, web, or VPN, or I am getting corrupted data from the Internet.

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492.

If you are having some difficulties, perform the following steps:

1. To connect to the Router, go to the web browser, and enter `http://192.168.1.1` or the IP address of the Router.
2. Enter the password, if asked. (The default password is admin.)
3. Look for the MTU option, and select **Manual**. In the Size field, enter 1492.
4. Click the **Save Settings** button to continue.

If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved:

1462
1400
1362
1300

16. The Power LED flashes continuously.

The Power LED lights up when the device is first powered up. Meantime, the system will boot up itself and check for proper operation. After finishing the checking procedure, the LED remains steady to show that the system is working fine. If the LED continues to flash after this time, the device is not working properly. Try to flash the firmware by assigning a static IP address to the computer, and then upgrade the firmware. Try using the following settings, IP Address: 192.168.1.50 and Subnet Mask: 255.255.255.0

17. When I enter a URL or IP address, I get a time-out error or am prompted to retry.

Check if other PCs work. If they do, ensure that your workstation's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.

If the PCs are configured correctly, but still not working, check the Router. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)

If the Router is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Router to verify a direct connection. Manually configure the TCP/IP settings with a DNS address provided by your ISP.

Make sure that your browser is set to connect directly and that any dial-up is disabled.

For Internet Explorer, click **Tools, Internet Options**, and then the **Connection** tab.

Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit, Preferences, Advanced**, and **Proxy**.

Make sure that Netscape Navigator is set to **Direct connection to the Internet**.



Networks based on information,
Success, Friendship and more...

Frequently Asked Questions

- What is the maximum number of IP addresses that the Router will support?
The Router will support up to 253 IP addresses.
- Is IPSec Pass-Through supported by the Router?
Yes, it is a built-in feature that the Router automatically enables.
- Where is the Router installed on the network?
In a typical environment, the Router is installed between the cable/DSL modem and the LAN. Plug the Router into the cable/DSL modem's Ethernet port.
- Does the Router support IPX or AppleTalk?
No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications. IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used for LAN to LAN connections, but those protocols cannot connect from the Internet to a LAN.
- Does the Internet connection of the Router support 100Mbps Ethernet?
The Router's current hardware design supports up to 100Mbps Ethernet on its Internet port; however, the Internet connection speed will vary depending on the speed of your broadband connection. The Router also supports 100Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Router.
- What is Network Address Translation and what is it used for?
Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Router to be used with low cost Internet accounts, such as DSL or cable modems, when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.
- Does the Router support any operating system other than Windows 95, Windows 98SE, Windows Millennium, Windows 2000, or Windows XP?
Yes, but ALLNET does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.
- Does the Router support ICQ send file?
Yes, with the following fix: click ICQ menu -> preference -> connections tab->, and check I am behind a firewall or proxy. Then set the firewall time-out to 80 seconds in the firewall setting. The Internet user can then send a file to a user behind the Router.



Networks based on information,
Success, Friendship and more...

- I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do?
If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 ~ 27900. If you want to use the UT Server Admin, forward another port. (Port 8080 usually works well but is used for remote admin. You may have to disable this.) Then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and Server-Name to the IP assigned to the Router from your ISP.
- Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?
It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.
- How do I get Half-Life: Team Fortress to work with the Router?
The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up.
This lets multiple computers connect to the same server. One problem: Version 1.0.1.6 won't let multiple computers with the same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.
- How can I block corrupted FTP downloads?
If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.
The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on The screen.
- What do I need to do?
Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control P panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at www.allnet.de for more information.
- If all else fails in the installation, what can I do?
Reset the Router by holding down the reset button until the Power LED fully turns on and off. Reset your cable or DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the ALLNET website, www.allnet.de



Networks based on information,
Success, Friendship and more...

- How will I be notified of new Router firmware upgrades?
All ALLNET firmware upgrades are posted on the ALLNET website at www.allnet.de where they can be downloaded for free. To upgrade the Router's firmware, use the System tab of the Router's web-based utility. If the Router's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use. Downloading a more current version of Router firmware will not enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.
- Will the Router function in a Macintosh environment?
Yes, but the Router's setup pages are accessible only through Internet Explorer 4.0 or Netscape Navigator 4.0 or higher for Macintosh.
- I am not able to get the web configuration screen for the Router. What can I do?
You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.
- What is DMZ Hosting?
Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ Hosting. To get the LAN IP address, see "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter." If DMZ
- Hosting is used, does the exposed user share the public IP with the Router?
- If DMZ Hosting is used, does the exposed user share the public IP with the Router?
No.
- Does the Router pass PPTP packets or actively route PPTP sessions?
The Router allows PPTP packets to pass through.
- Is the Router cross-platform compatible?
Any platform that supports Ethernet and TCP/IP is compatible with the Router.



Networks based on information,
Success, Friendship and more...

- How many ports can be simultaneously forwarded?
Theoretically, the Router can establish 520 sessions at the same time, but you can only forward 10 ranges of ports.
- What are the advanced features of the Router?
The Router's advanced features include Advanced Wireless settings, Filters, Port Forwarding, Routing, and DDNS.
- What is the maximum number of VPN sessions allowed by the Router?
The maximum number depends on many factors. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.
- How can I check whether I have static or DHCP IP Addresses?
Consult your ISP to obtain this information.
How do I get mIRC to work with the Router?
Under the Port Forwarding tab, set port forwarding to 113 for the PC on which you are using mIRC.
- Can the Router act as my DHCP server?
Yes. The Router has DHCP server software built-in.
- Can I run an application from a remote computer over the wireless network?
This will depend on whether or not the application is designed to be used over a network. Consult the application's documentation to determine if it supports operation over a network.
- What is the IEEE 802.11g standard?
It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard. The 802.11g standard states a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.
- What IEEE 802.11b features are supported?
The product supports the following IEEE 802.11b functions:
CSMA/CA plus Acknowledge protocol
Multi-Channel Roaming
802.11g VPN Broadband Router
Automatic Rate Selection
RTS/CTS feature
Fragmentation
Power Management



Networks based on information,
Success, Friendship and more...

- **What is ad-hoc mode?**
When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other. The ad-hoc wireless network will not communicate with any wired network.
- **What is infrastructure mode?**
When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.
- **What is roaming?**
Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the workstation must make sure that it is the same channel number with the access point of dedicated coverage area.
To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone. As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.
- **What is ISM band?**
The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

- **What is Spread Spectrum?**
Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).
- **What is DSSS? What is FHSS? And what are their differences?**
Frequency-Hopping Spread-Spectrum (FHSS) uses a narrow band carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.
- **Will the information be intercepted while it is being transmitted through the air?**
WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control.
- **What is WEP?**
WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.



Networks based on information,
Success, Friendship and more...

- What is a MAC Address?

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

- How do I reset the Router?

Press the Reset button on the back panel for about ten seconds . This will reset the Router to its default settings.

- How do I resolve issues with signal loss?

There is no way to know the exact range of your wireless network without testing. Every obstacle placed between the Router and a wireless PC will create signal loss. Lead glass, metal, concrete floors, water and walls will inhibit the signal and reduce range. Start with the Router and your wireless PC in the same room and move it away in small increments to determine the maximum range in your environment. You may also try using different channels, as this may eliminate interference affecting only one channel.

I have excellent signal strength, but I cannot see my network.

WEP is probably enabled on the Router, but not on your wireless adapter (or vice versa). Verify that the same WEP keys and levels (64 or 128) are being used on all nodes of your wireless network.

- How many channels/frequencies are available with the Router?

There are fourteen available channels, ranging from 1 to 14.



Networks based on information,
Success, Friendship and more...

Specifications

Standards 11g VPN Router/ ALL0276VPN

Ports One Internet, Ethernet (1-4), Power

Buttons One Reset Button, One Power Switch

Cabling Type UTP CAT 5 or better

Data Rate Up to 54Mbps (802.11g)

Transmit Power 18dBm

LEDs Power, Internet, Ethernet (1, 2, 3, 4),

WEP Key Bits 64, 128

Dimensions 7.32" x 6.89" x 1.89"

(W x H x D) 200mm (L) x 155mm(W) x 30mm (H)

Unit Weight 538 +/- 5g

Power External, 5V DC, 2.5A

Certifications FCC, CE

Operating Temp. 0°C to 40°C (32°F to 104°F)

Storage Temp. -20°C to 70°C (-4°F to 158°F)

Operating Humidity 10% to 85% Non-Condensing

Storage Humidity 5% to 90% Non-Condensing