D-Link DIR-605 無線寬頻路由器

Wireless N Router

中文快速安裝/設定指南

RECYCLABLE

Preface

D-Link reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes.

Manual Revisions

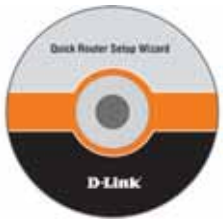
Revision	Date	Description
1.0	July 31, 2008	• Updated for revision

Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Table of Contents

Package Contents

D-Link DIR-605 Wireless N Router	
Power Adapter	
Ethernet Cable	
CD-ROM	

Note: Using a power supply with a different voltage rating than the one included with the DIR-605 will cause damage and void the warranty for this product.

System Requirements

Network Requirements	• An Ethernet-based Cable or DSL modem • IEEE 802.11n-draft/g wireless clients • 10/100 Ethernet
Web-based Configuration Utility Requirements	Computer with the following: • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter Browser Requirements: • Internet Explorer 6.0 or higher • Mozilla 1.7.12 or higher • Firefox 1.5 or higher • Safari 1.0 or higher (with Java 1.3.1 or higher) • Flock 0.7.14 or higher • Opera 6.0 or higher Windows® Users: Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.
CD Installation Wizard Requirements	Computer with the following: • Windows® XP with Service Pack 2 or Vista® • An installed Ethernet adapter • CD-ROM drive

Features

- Faster Wireless Networking - The DIR-605 provides up to 300Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.

- Compatible with 802.11g Devices - The DIR-605 is still fully compatible with the IEEE 802.11g standard, so it can connect with existing 802.11g PCI, USB and Cardbus adapters.

- Advanced Firewall Features - The Web-based user interface displays a number of advanced network management features including:

    - Content Filtering - Easily applied content filtering based on MAC Address, URL, and/or Domain Name.

    - Filter Scheduling - These filters can be scheduled to be active on certain days or for a duration of hours or minutes.

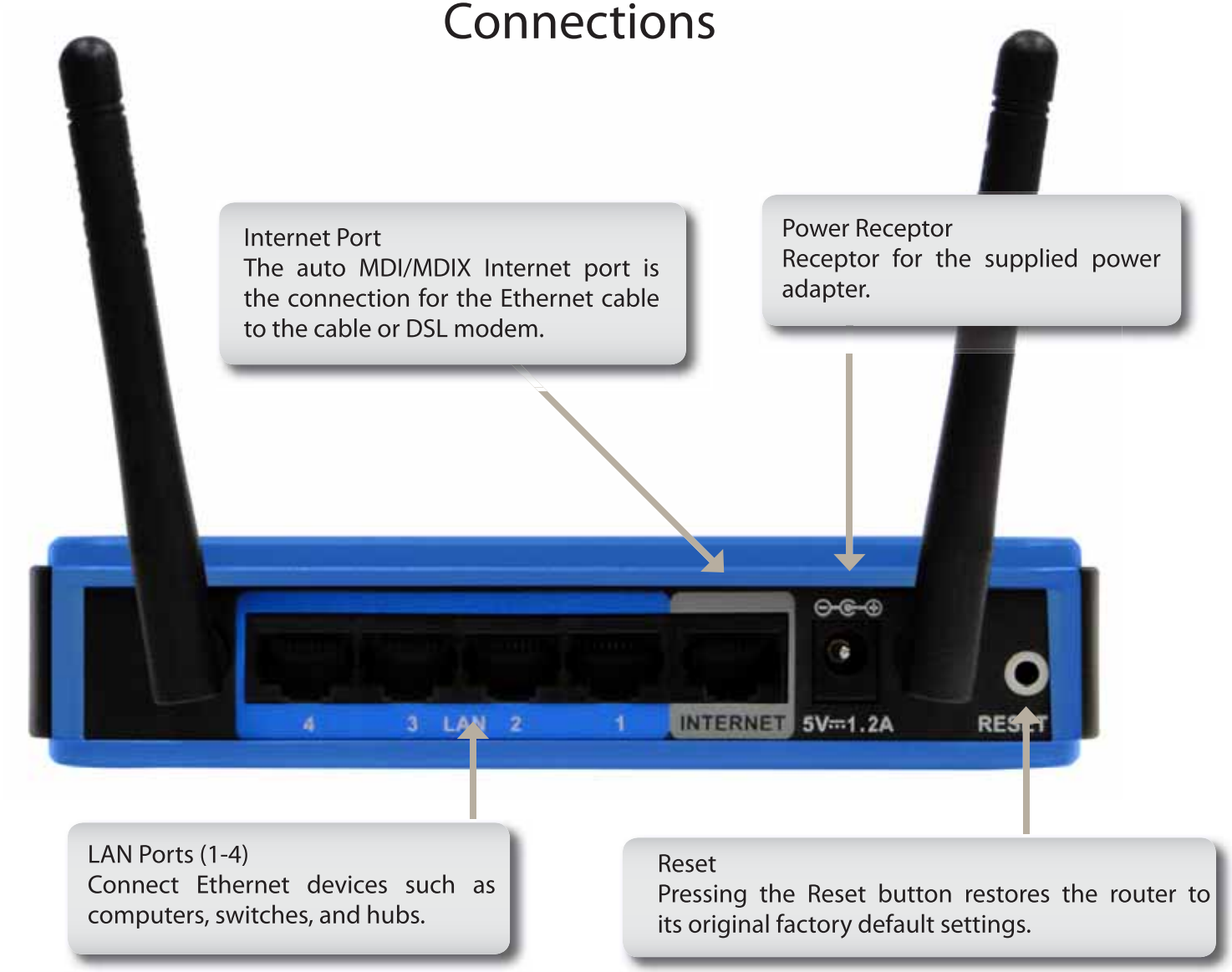
    - Secure Multiple/Concurrent Sessions - The DIR-605 can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-605 can securely access corporate networks.

- User-friendly Setup Wizard - Through its easy-to-use Web-based user interface, the DIR-605 lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company's server. Configure your router to your specific settings within minutes.

* Maximum wireless signal rate derived from IEEE Standard 802.11g and Draft 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

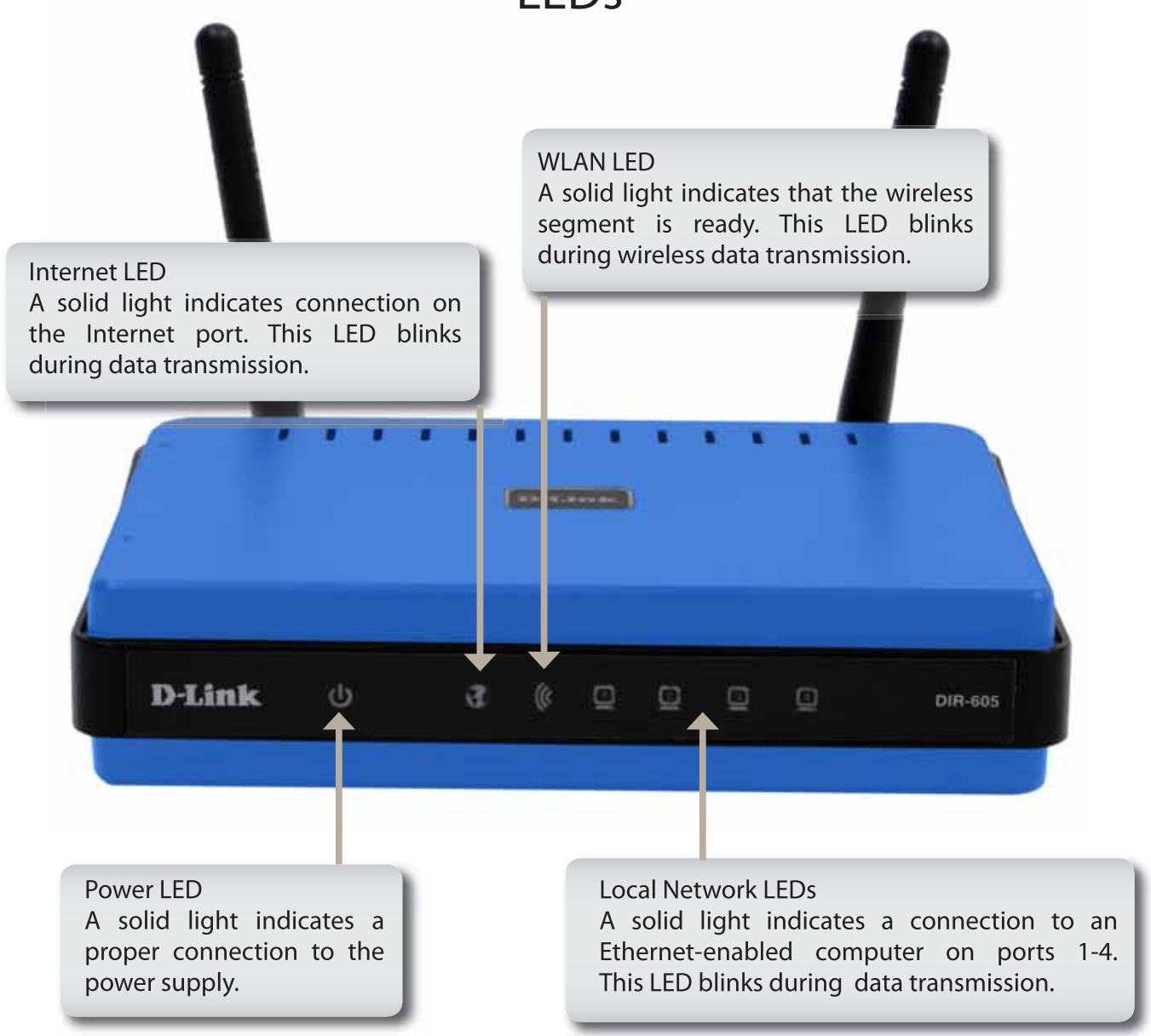
Hardware Overview

Connections



Hardware Overview

LEDs



Installation

This section will walk you through the installation process. Placement of the router is very important. Do not place the router in an enclosed area such as a closet, cabinet, or in the attic or garage.

Before you Begin

- Please configure the router with the computer that was last connected directly to your modem.
- You can only use the Ethernet port on your modem. If you were using the USB connection before using the router, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the Internet port on the router, and then turn the modem back on. In some cases, you may need to call your ISP to change connection types (USB to Ethernet).
- If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoet, Broadjump, or Enternet 300 from your computer or you will not be able to connect to the Internet.
- When running the Setup Wizard from the D-Link CD, make sure the computer you are running the CD from is connected to the Internet and online or the wizard will not work. If you have disconnected any hardware, re-connect your computer back to the modem and make sure you are online.

Wireless Installation Considerations

The D-Link wireless router lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.

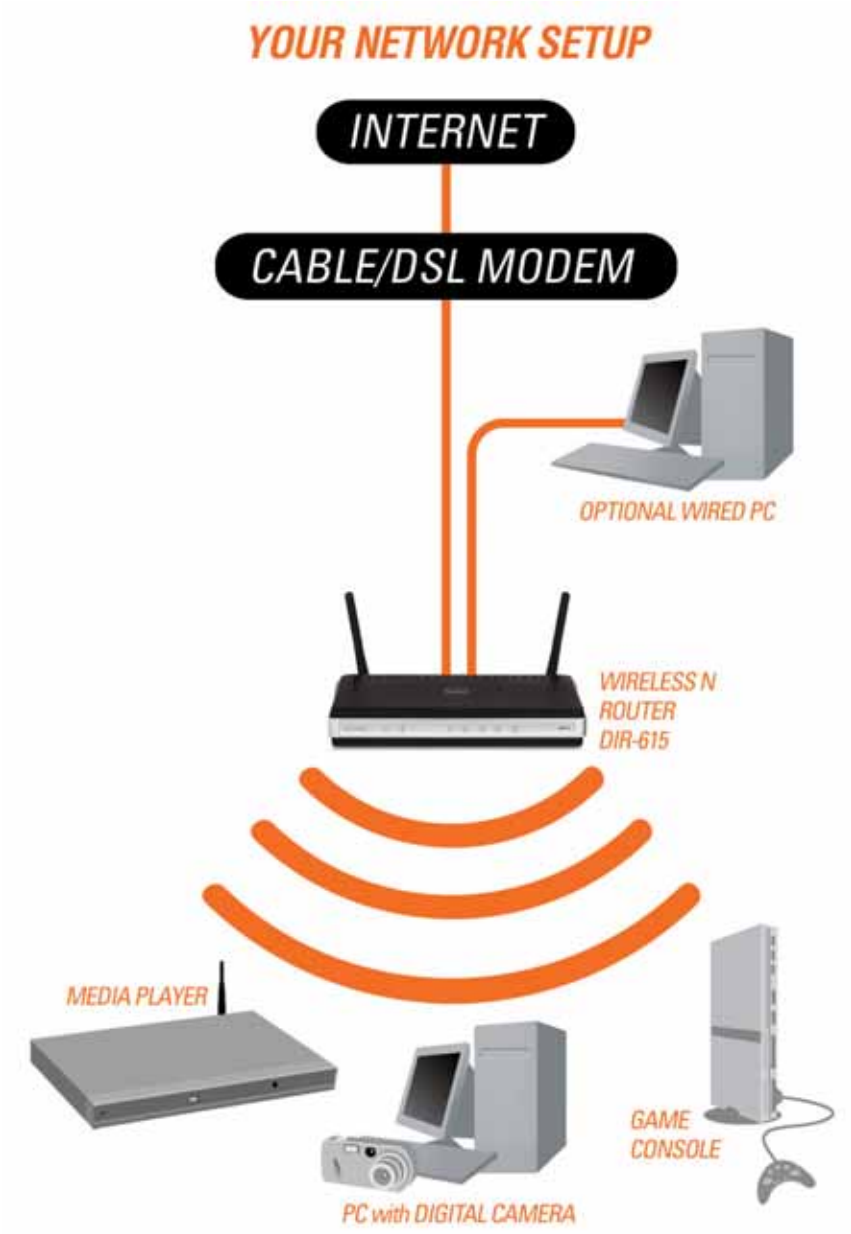
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

3. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.

4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

5. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in not in use.

Network Diagram



Connect to Cable/DSL/Satellite Modem

If you are connecting the router to a cable/DSL/satellite modem, please follow the steps below:

1. Place the router in an open and central location. Do not plug the power adapter into the router.

2. Turn the power off on your modem. If there is no on/off switch, then unplug the modem's power adapter. Shut down your computer.

3. Unplug the Ethernet cable (that connects your computer to your modem) from your computer and place it into the Internet port on the router.

4. Plug an Ethernet cable into one of the four LAN ports on the router. Plug the other end into the Ethernet port on your computer.

5. Turn on or plug in your modem. Wait for the modem to boot (about 30 seconds).

6. Plug the power adapter to the router and connect to an outlet or power strip. Wait about 30 seconds for the router to boot.

7. Turn on your computer.

8. Verify the link lights on the router. The power light, Internet light, and the LAN light (the port that your computer is plugged into) should be lit. If not, make sure your computer, modem, and router are powered on and verify the cable connections are correct.

9. Skip to page 13 to configure your router.

Connect to Another Router

If you are connecting the D-Link router to another router to use as a wireless access point and/or switch, you will have to do the following before connecting the router to your network:

- Disable UPnP™
- Disable DHCP
- Change the LAN IP address to an available address on your network. The LAN ports on the router cannot accept a DHCP address from your other router.

To connect to another router, please follow the steps below:

1. Plug the power into the router. Connect one of your computers to the router (LAN port) using an Ethernet cable. Make sure your IP address on the computer is 192.168.0.xxx (where xxx is between 2 and 254). Please see the Networking Basics section for more information. If you need to change the settings, write down your existing settings before making any changes. In most cases, your computer should be set to receive an IP address automatically in which case you will not have to do anything to your computer.

2. Open a web browser and enter http://192.168.0.1 and press Enter. When the login window appears, set the user name to Admin and leave the password box empty. Click Log In to continue.

3. Click on Advanced and then click Advanced Network. Uncheck the Enable UPnP checkbox. Click Save Settings to continue.

4. Click Setup and then click Network Settings. Uncheck the Enable DHCP Server server checkbox. Click Save Settings to continue.

5. Under Router Settings, enter an available IP address and the subnet mask of your network. Click Save Settings to save your settings. Use this new IP address to access the configuration utility of the router in the future. Close the browser and change your computer's IP settings back to the original values as in Step 1.

6. Disconnect the Ethernet cable from the router and reconnect your computer to your network.

7. Connect an Ethernet cable in one of the LAN ports of the router and connect it to your other router. Do not plug anything into the Internet port of the D-Link router.

8. You may now use the other 3 LAN ports to connect other Ethernet devices and computers. To configure your wireless network, open a web browser and enter the IP address you assigned to the router. Refer to the Configuration and Wireless Security sections for more information on setting up your wireless network.

Getting Started

The DIR-605 includes a Quick Router Setup Wizard CD. Follow the simple steps below to run the Setup Wizard to guide you quickly through the installation process. You may manually configure your router without the wizard. Refer to the next page to manually setup your router.

Insert the Quick Router Setup Wizard CD in the CD-ROM drive. The step-by-step instructions that follow are shown in Windows® XP or Vista®. The steps and screens are similar for the other Windows® operating systems.

If the CD autorun function does not automatically start on your computer, go to Start > Run. In the run box type "D:\DIR605.exe" (where D: represents the drive letter of your CD-ROM drive).

When the autorun screen appears, click Install Router and follow the on-screen instructions.

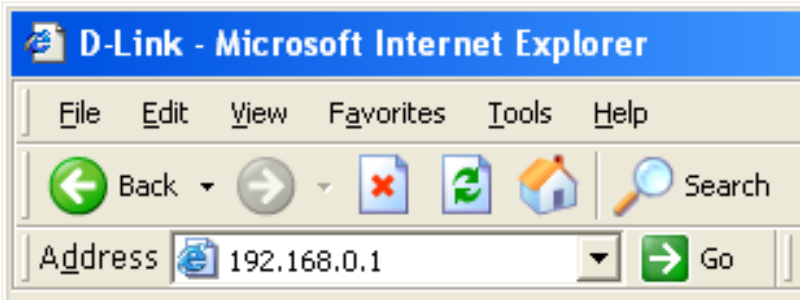
Note: It is recommended to write down the login password on the provided CD holder.

Configuration

This section will show you how to configure your new D-Link wireless router using the web-based configuration utility.

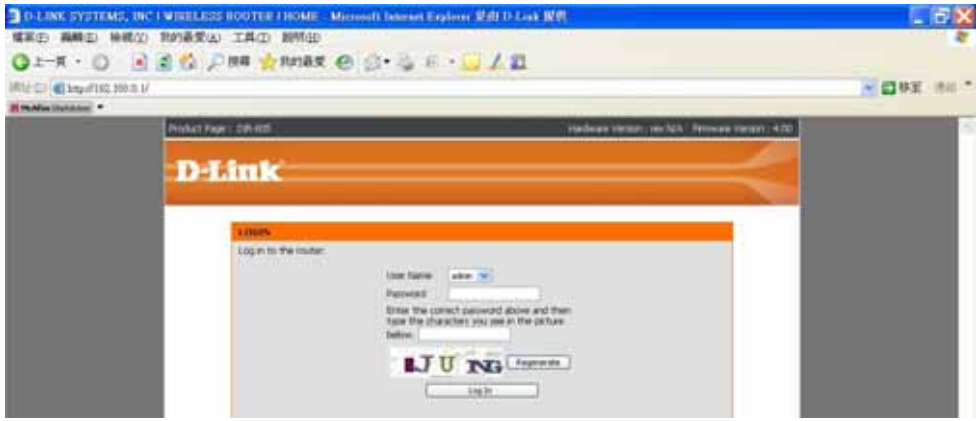
Web-based Configuration Utility

To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the router (192.168.0.1).



Select Admin from the drop-down menu and then enter your password. Leave the password blank by default.

If you get a Page Cannot be Displayed error, please refer to the Troubleshooting section for assistance.

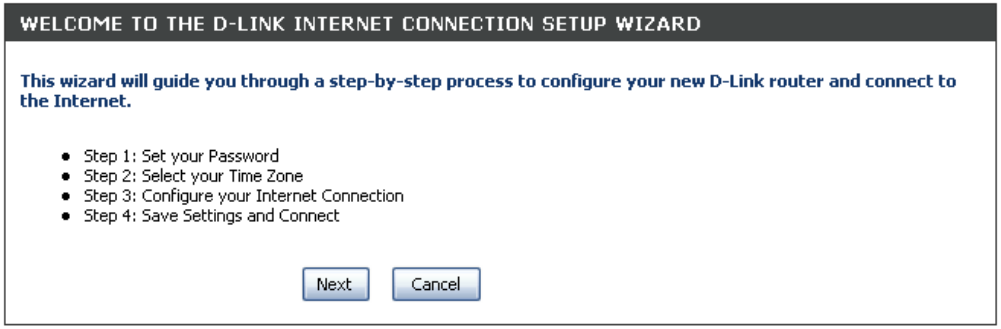


Internet Connection Setup Wizard

Once logged into the web interface of the router, the Setup > Internet page will appear. Click the Internet Connection Setup Wizard button to quickly configure your router using the setup wizard.

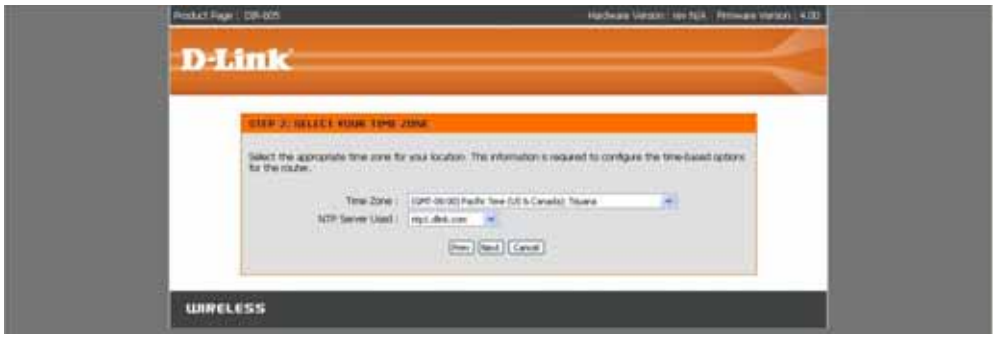
If you want to enter your settings without running the wizard, click Manual Internet Configuration Wizard and skip to page 19.

Click Next to continue.



Create a new password and then click Next to continue.

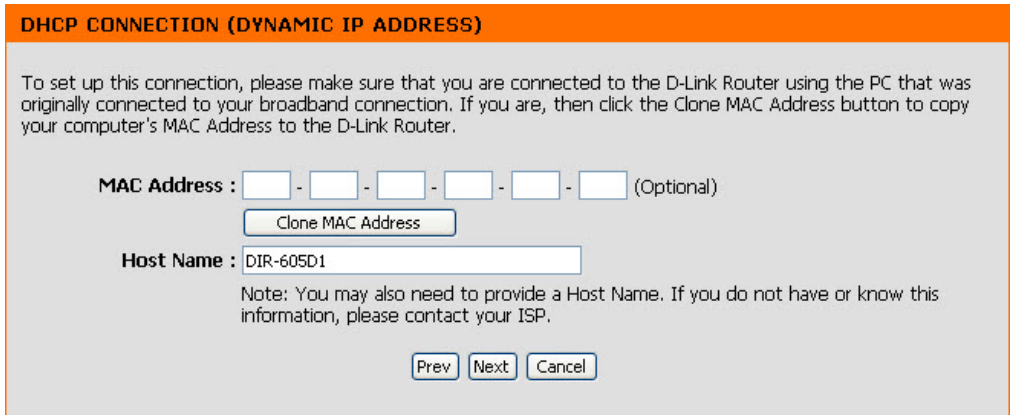
Select your time zone from the drop-down menu and then click Next to continue.



Select the type of Internet connection you use and then click Next to continue.

If you selected Dynamic, you may need to enter the MAC address of the computer that was last connected directly to your modem. If you are currently using that computer, click Clone Your PC's MAC Address and then click Next to continue.

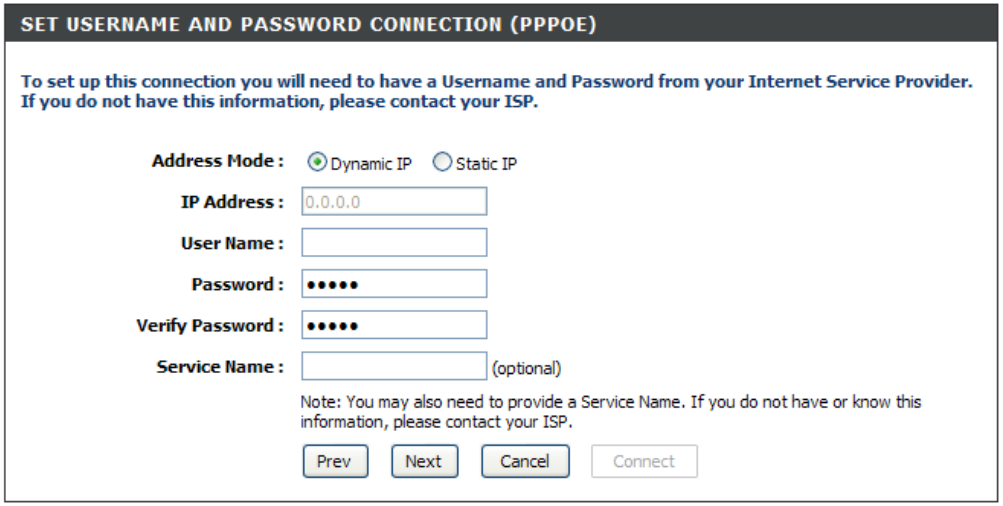
The Host Name is optional but may be required by some ISPs. The default host name is the device name of the Router and may be changed.



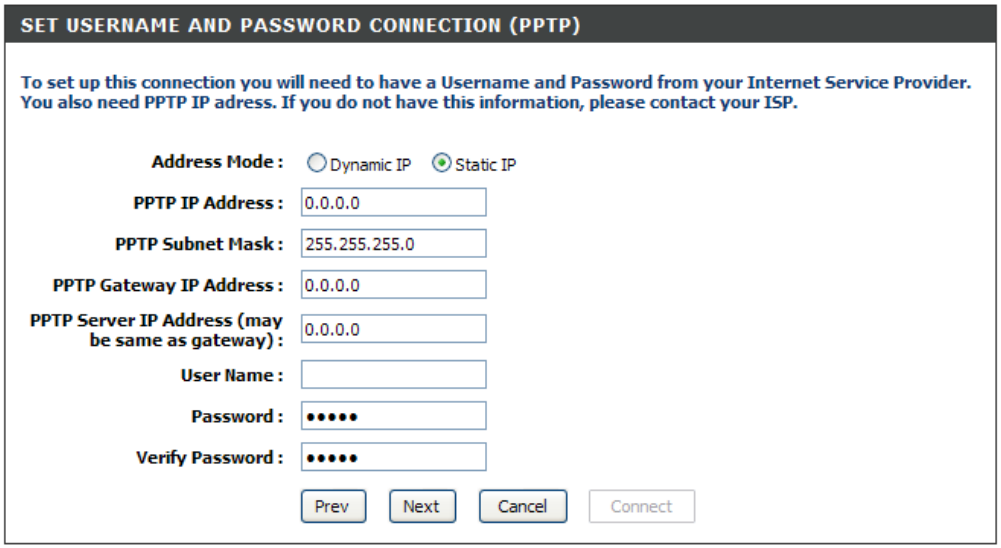
If you selected PPPoE, enter your PPPoE username and password. Click Next to continue.

Select Static if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses.

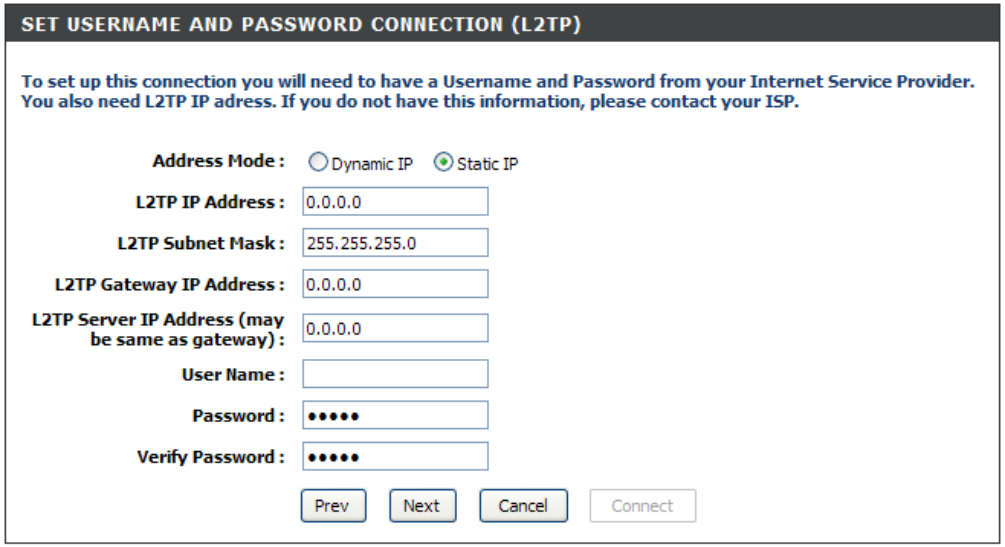
Note: Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.



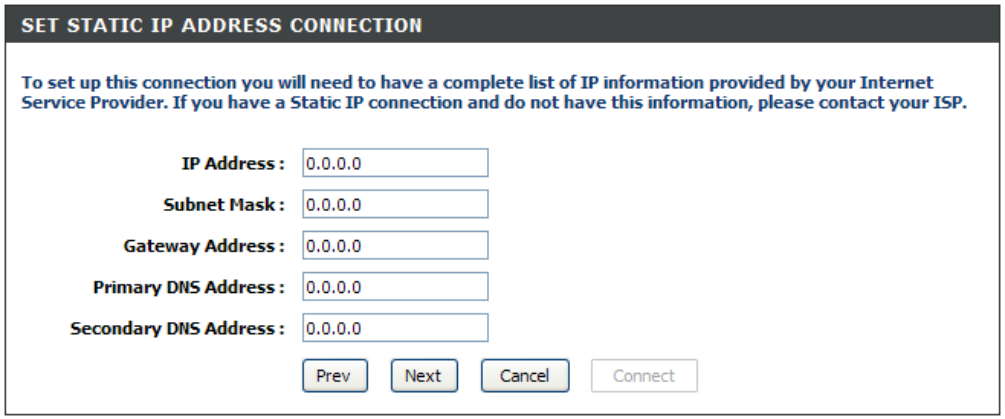
If you selected PPTP, enter your PPTP username and password. Click Next to continue.



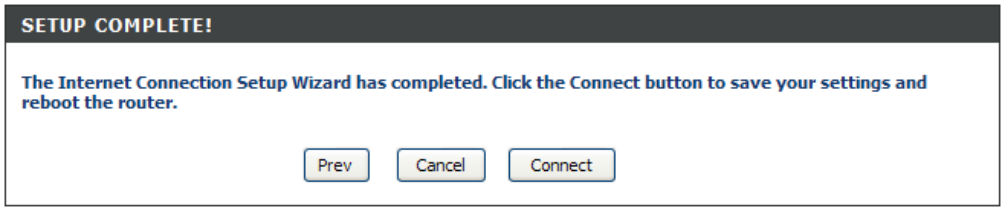
If you selected L2TP, enter your L2TP username and password. Click Next to continue.



If you selected Static, enter your network settings supplied by your Internet provider. Click Next to continue.



Click Connect to save your settings. Once the router is finished rebooting, click Continue. Please allow 1-2 minutes to connect.



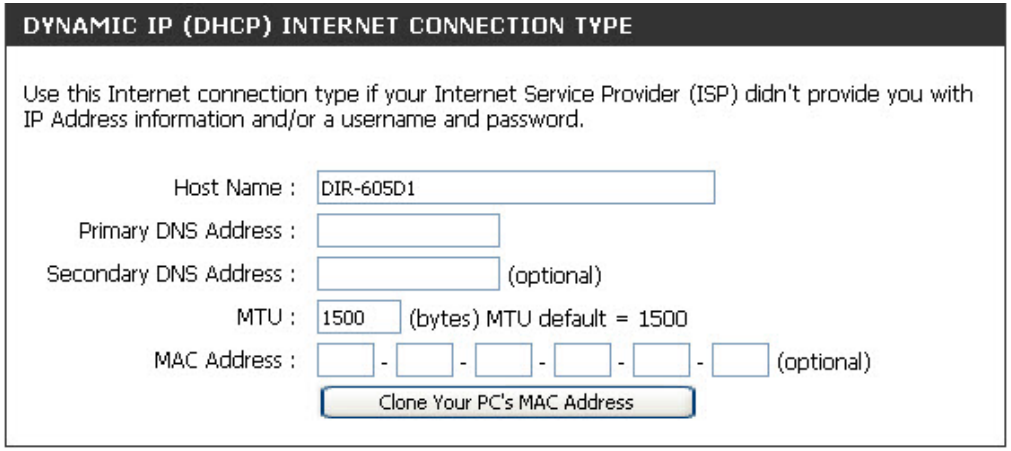
Manual Configuration
Dynamic (Cable)

If you opt to set up your Internet connection manually, you will be redirected to a WAN page that allows you to select your Internet type and enter the correct configuration parameters.

Select your Internet connection type using the "My Internet Connection is" drop-down menu.

Click the Save Settings button when you have configured the connection.

Dynamic IP Address (DHCP)



My Internet Connection: Select Dynamic IP (DHCP) to obtain IP Address information automatically from your ISP. Select this option if your ISP does not give you any IP numbers to use. This option is commonly used for Cable modem services.

Host Name: The Host Name is optional but may be required by some ISPs.

Use Unicasting: Check the box if you are having problems obtaining an IP address from your ISP.

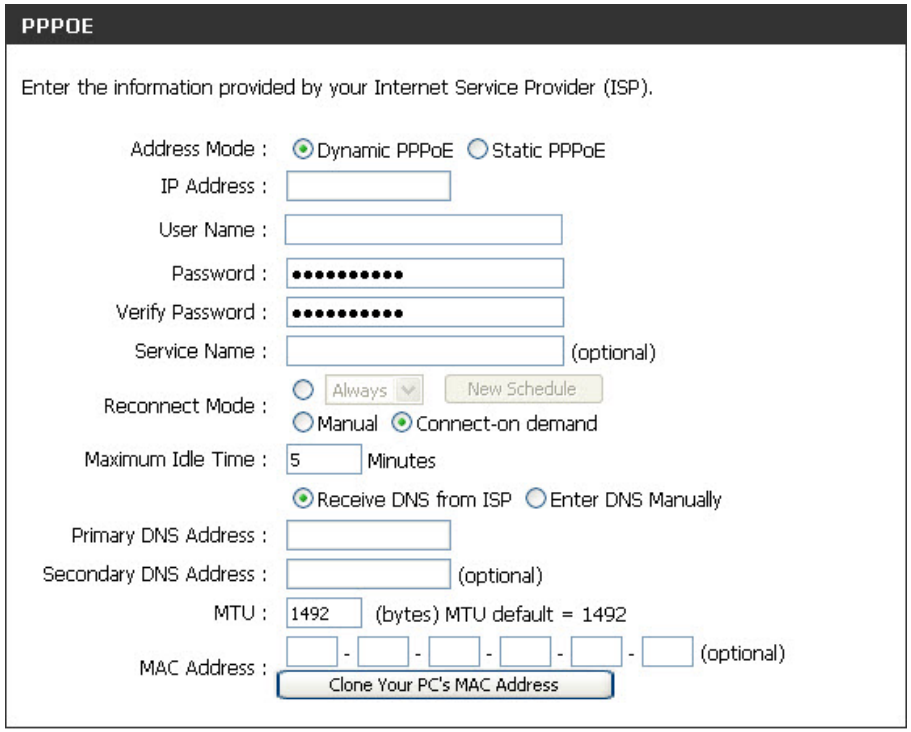
DNS Addresses: Enter the Primary DNS server IP address assigned by your ISP.

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the Clone Your PC's MAC Address button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

PPPoE (DSL)

Choose PPPoE (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.



My Internet Connection: Select PPPoE (Username/Password) from the drop-down menu.

Address Mode: Select Static if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select Dynamic.

IP Address: Enter the IP address (Static PPPoE only).

User Name: Enter your PPPoE user name.

Password: Enter your PPPoE password and then retype the password in the next box.

Service Name: Enter the ISP Service Name (optional).

Reconnection Mode: Select either Always-on, On-Demand, or Manual.

Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

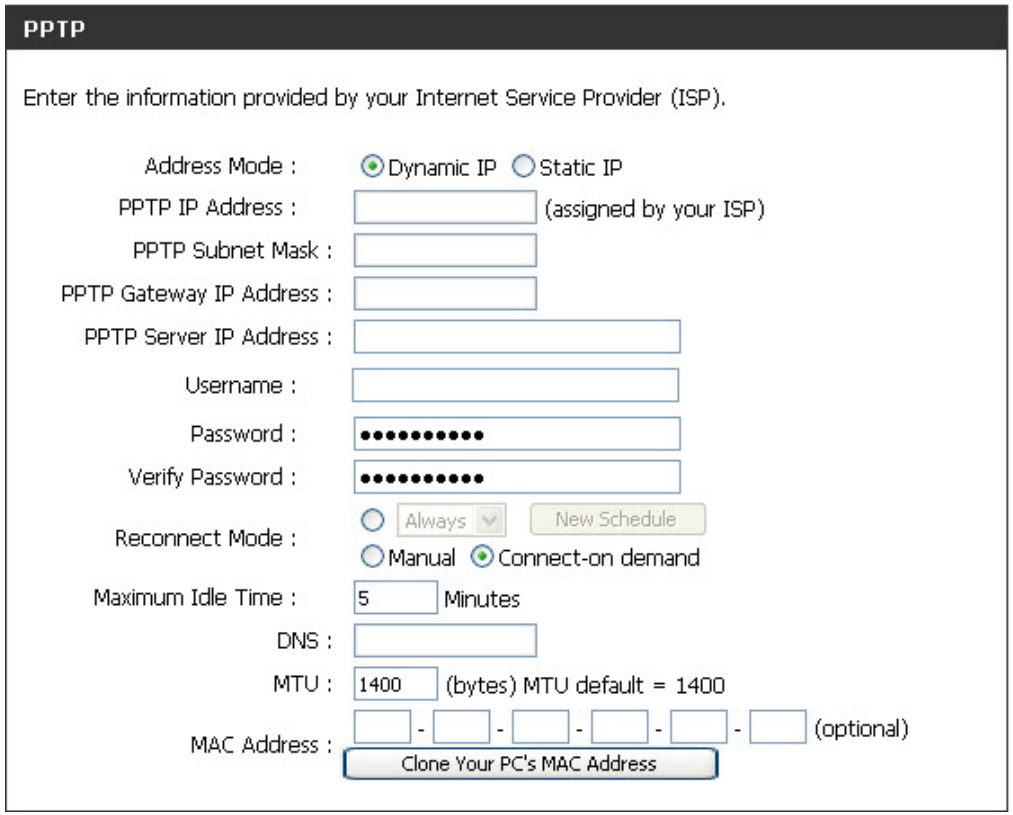
DNS Addresses: Enter the Primary and Secondary DNS Server Addresses (Static PPPoE only).

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU.

MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the Clone Your PC's MAC Address button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

PPTP

Choose PPTP (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.



Address Mode: Select Static if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select Dynamic.

PPTP IP Address: Enter the IP address (Static PPTP only).

PPTP Subnet Mask: Enter the Primary and Secondary DNS Server Addresses (Static PPTP only).

PPTP Gateway: Enter the Gateway IP Address provided by your ISP.

PPTP Server IP: Enter the Server IP provided by your ISP (optional).

Username: Enter your PPTP username.

Password: Enter your PPTP password and then retype the password in the next box.

Reconnect Mode: Select either Always-on, On-Demand, or Manual.

Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

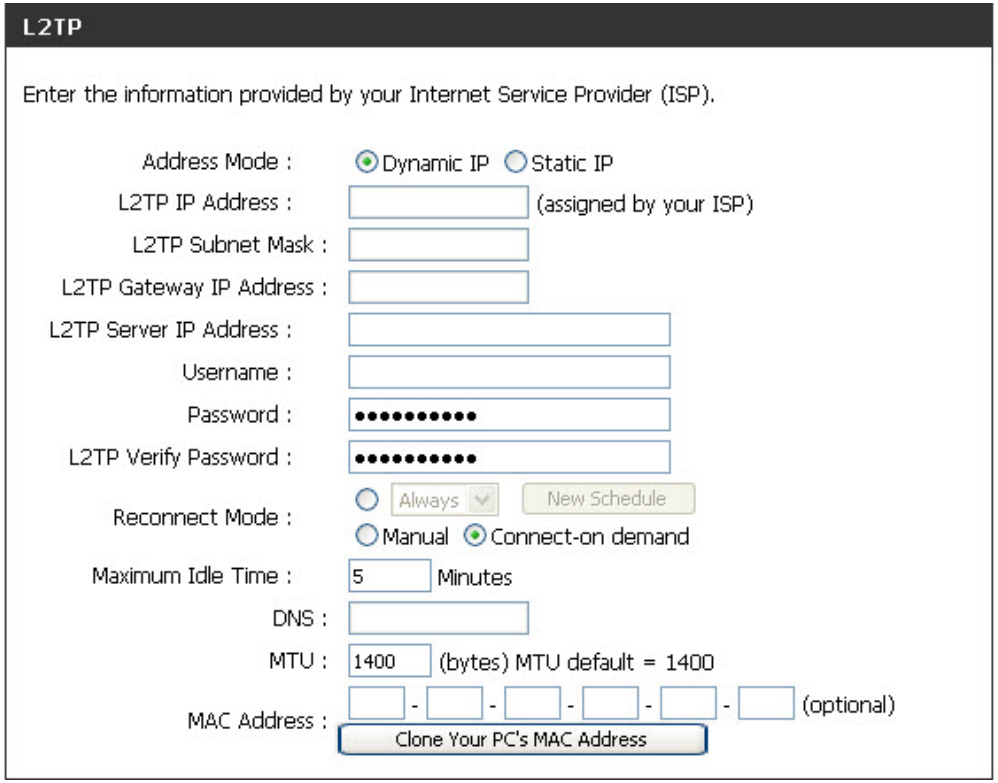
DNS Servers: The DNS server information will be supplied by your ISP (Internet Service Provider.)

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.

MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the Clone Your PC's MAC Address button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

L2TP

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.



Address Mode: Select Static if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select Dynamic.

L2TP IP Address: Enter the L2TP IP address supplied by your ISP (Static only).

L2TP Subnet Mask: Enter the Subnet Mask supplied by your ISP (Static only).

L2TP Gateway: Enter the Gateway IP Address provided by your ISP.

L2TP Server IP: Enter the Server IP provided by your ISP (optional).

Username: Enter your L2TP username.

Password: Enter your L2TP password and then retype the password in the next box.

Reconnect Mode: Select either Always-on, On-Demand, or Manual.

Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

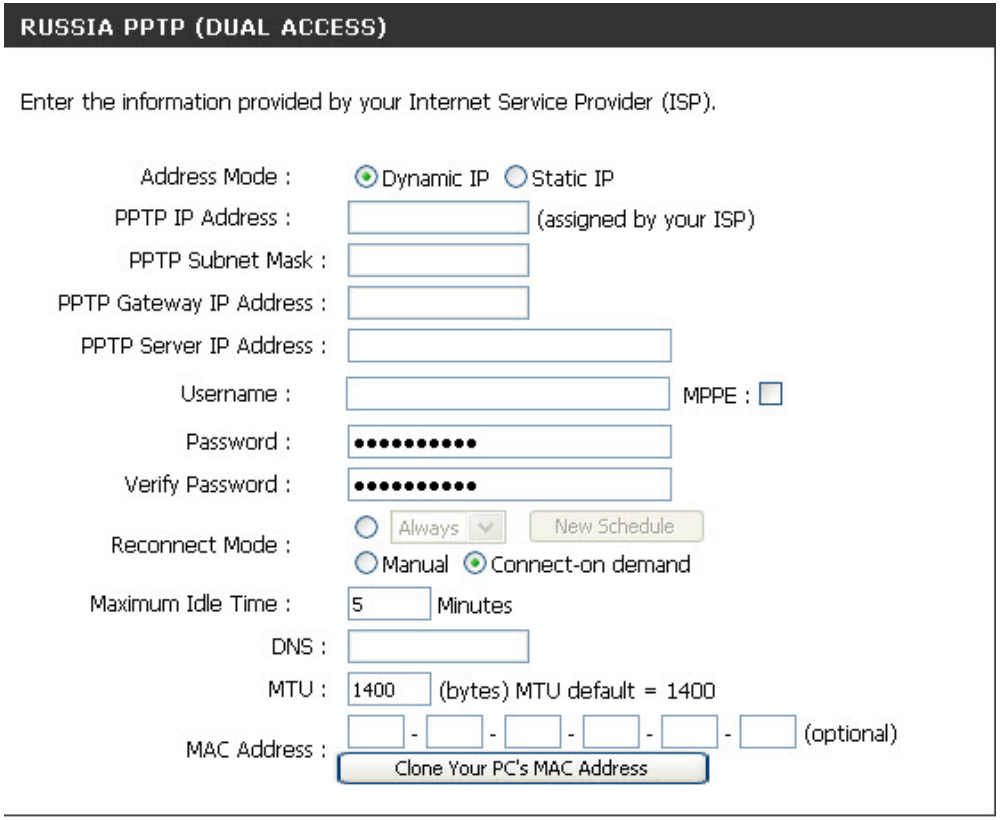
DNS Servers: Enter the Primary and Secondary DNS Server Addresses (Static L2TP only).

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.

Clone MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the Clone Your PC's MAC Address button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Russia PPTP

Choose Russia PPTP (Dual Access) if your ISP uses a PPTP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.



Address Mode: Select Static if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select Dynamic.

PPTP IP Address: Enter the IP address (Static PPTP only).

PPTP Subnet Mask: Enter the Primary and Secondary DNS server Addresses (Static PPTP only).

PPTP Gateway: Enter the Gateway IP Address provided by your ISP.

PPTP Server IP: Enter the Server IP provided by your ISP (optional).

Username: Enter your PPTP username.

Password: Enter your PPTP password and then retype the password in the next box.

Reconnect Mode: Select either Always-on, On-Demand, or Manual.

Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

DNS Servers: Enter the Primary and Secondary DNS Server Addresses (Static L2TP only).

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.

Clone MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the Clone Your PC's MAC Address button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Russia PPPoE

Choose Russia PPPoE (Dual Access) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.

Internet Connection: Save your settings after configuring your Internet Connection method.

Access Point Mode: Enable to turn your router into an access point.

Internet Connection Type: Choose your Internet Connection type.

Address Mode: Select Static if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select Dynamic.

PPPoE IP Address: Enter the IP address (Static PPPoE only).

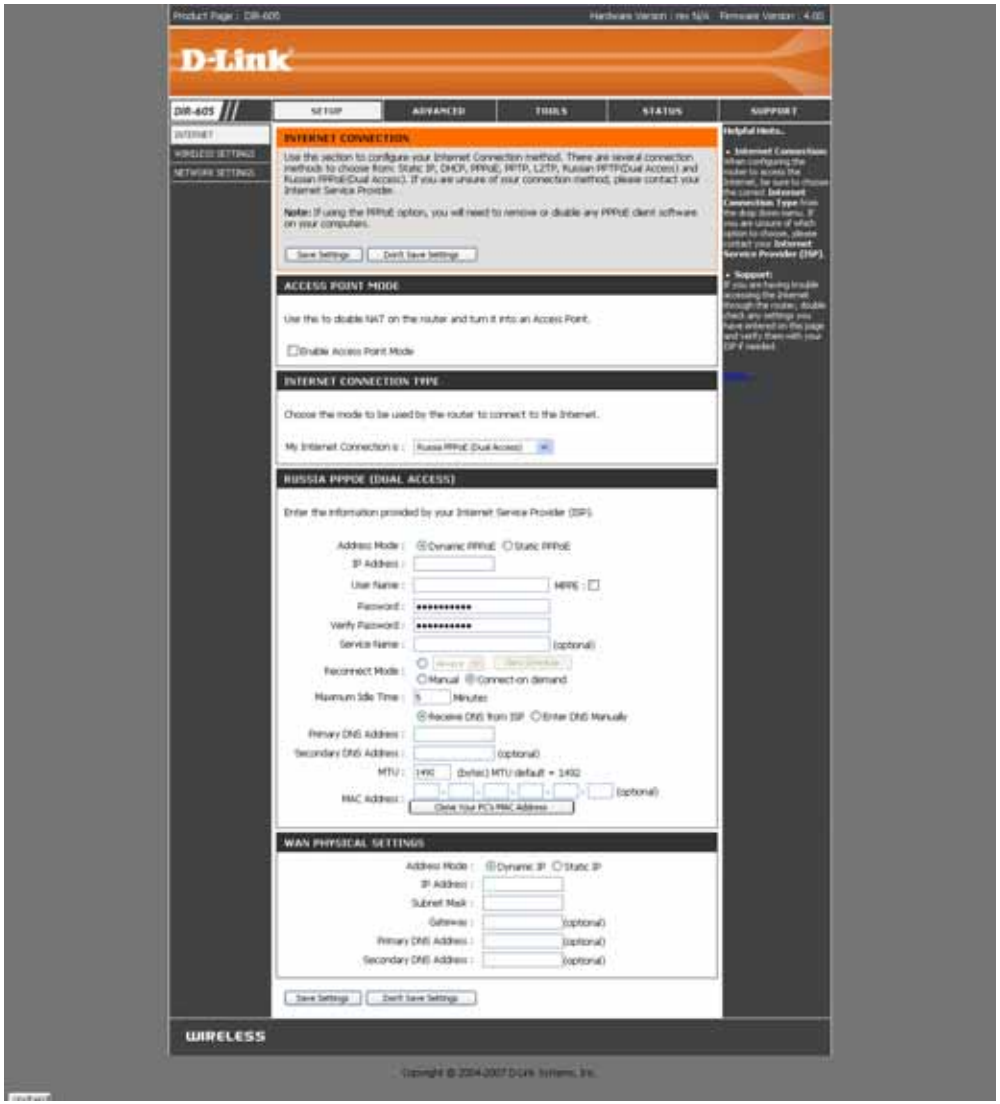
PPPoE Subnet Mask: Enter the Primary and Secondary DNS server Addresses (Static PPPoE only).

PPPoE Gateway: Enter the Gateway IP Address provided by your ISP.

PPPoE Server IP: Enter your PPPoE password and then retype the password in the next box.

Username: Select either Always-on, On-Demand, or Manual.

Password: Enter your PPPoE password and then retype the password in the next box.



Reconnect Mode:	Select either Always-on, On-Demand, or Manual.
Maximum Idle Time:	Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.
DNS Servers:	Enter the Primary and Secondary DNS Server Addresses (Static L2TP only).
MTU:	Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.
Clone MAC Address:	The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the Clone Your PC's MAC Address button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Static IP Address

Select Static IP Address if all the Internet port's IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

IP Address: Enter the IP address assigned by your ISP.

Subnet Mask: Enter the Subnet Mask assigned by your ISP.

Default Gateway: Enter the Gateway assigned by your ISP.

DNS Servers: The DNS server information will be supplied by your ISP (Internet Service Provider.)

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

MAC Address The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the Clone Your PC's MAC Address button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Wireless Settings

If you want to configure the wireless settings on your router using the wizard, click Wireless Connection Setup Wizard and refer to page 80.

Click Add Wireless Device with WPS if you want to add a wireless device using Wi-Fi Protected Setup (WPS) and refer to page 83.

If you want to manually configure the wireless settings on your router click Manual Wireless Network Setup and refer to the next page.

Manual Wireless Network Setup

Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions. Click Add New to create your own time schedule to enable the wireless function.

Wireless Network Name: Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.

802.11 Mode: Select one of the following:

802.11g Only - Select if all of your wireless clients are 802.11g.

Mixed 802.11g and 802.11b - Select if you are using both 802.11b and 802.11g wireless clients.

802.11b Only - Select if all of your wireless clients are 802.11b.

802.11n Only - Select only if all of your wireless clients are 802.11n.

Mixed 802.11n, 802.11b, and 802.11g - Select if you are using a mix of 802.11n, 11g, and 11b wireless clients.

Mixed 802.11n and 802.11g - Select if you are using a mix of 802.11n and 802.11g wireless clients.

Enable Auto Channel Scan: The Auto Channel Scan setting can be selected to allow the DIR-605 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DIR-605. By default the channel is set to 6. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable Auto Channel Scan, this option will be greyed out.

Transmission Rate: Select the transmit rate. It is strongly suggested to select Best (Auto) for best performance.

Select the Channel Width:

Channel Width: Auto 20/40 - Select if you are using both 802.11n and non-802.11n wireless devices.
20MHz - Select if you are not using any 802.11n wireless clients. This is the default setting.

Enable Hidden Wireless: Select to enable hidden wireless.

Wireless Security: Refer to page 79 for more information regarding wireless security.

Network Settings

This section will allow you to change the local network settings of the router and to configure the DHCP settings.

IP Address: Enter the IP address of the router. The default IP address is 192.168.0.1.

If you change the IP address, once you click Apply, you will need to enter the new IP address in your browser to get back into the configuration utility.

Subnet Mask: Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

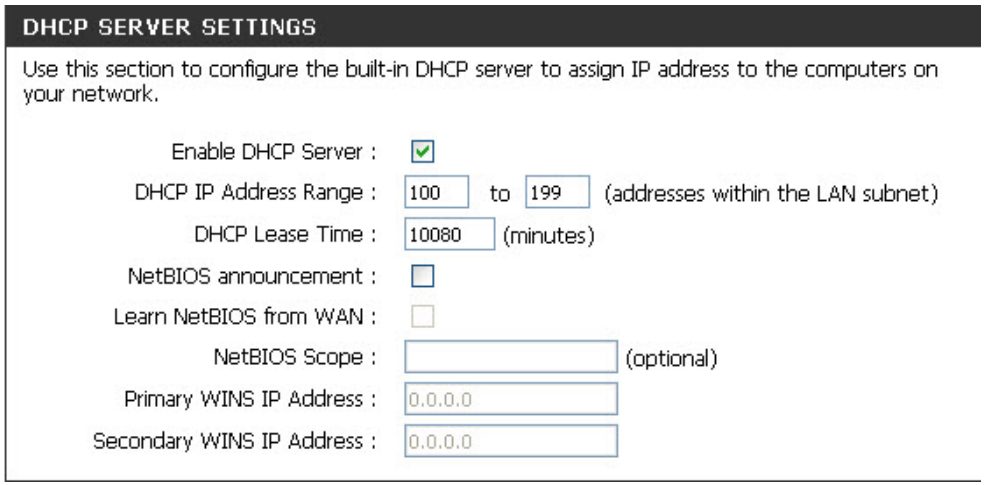
Local Domain: Enter the Domain name (Optional).

Device Name: Enter the Device name (set to "dlinkrouter" by default).

Enable DNS Relay: Uncheck the box to transfer the DNS server information from your ISP to your computers. If checked, your computers will use the router for a DNS server.

DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DIR-605 has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DIR-605. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.



Enable DHCP Server: Check this box to enable the DHCP server on your router. Uncheck to disable this function.

DHCP IP Address Range: Enter the starting and ending IP addresses for the DHCP server's IP assignment.

Note: If you statically (manually) assign IP addresses to your computers or devices, make sure the IP addresses are outside of this range or you may have an IP conflict.

Lease Time: The length of time for the IP address lease. Enter the Lease time in minutes.

NetBIOS Announcement: The NetBIOS API allows applications on seperate computers to communicate over LAN. The user can check this option to enable this function.

Learn NetBIOS from WAN: Each computers in the network have both NetBIOS name and IP address corresponding to the Host name. The user may simply use the NetBIOS name to log in router web interface. (The default is "dlinkrouter")

NetBIOS Scope (optional): The users may add some characters behind the NetBIOS name to differentiate it from other D-Link routers. It follows the naming rule for DNS names.

Primary/ Secondary WINS IP Address: Use this function to allow the seperate computers in a seperate subnet to search the computers in the same workgroup.

DHCP Reservation

If you want a computer or device to always have the same IP address assigned, you can create a DHCP reservation. The router will assign the IP address only to that computer or device.

Note: This IP address must be within the DHCP IP Address Range.

Computer Name: Enter the computer name or select from the drop-down menu and click <<.

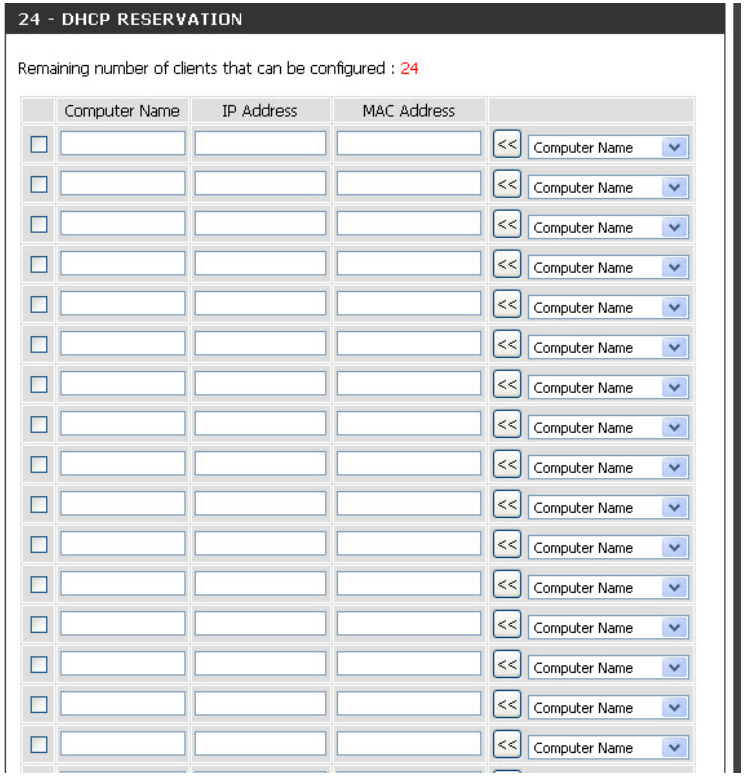
IP Address: Enter the IP address you want to assign to the computer or device. This IP Address must be within the DHCP IP Address Range.

MAC Address: Enter the MAC address of the computer or device.

Save: Click Save to save your entry. You must click Save Settings at the top to activate your reservations.

Number of Dynamic DHCP Clients: In this section, you can see what LAN devices are currentl leasing IP addresses.

Reserve: The Reserve option converts this dynamic IP allocation into a DHCP Reservation and adds the corresponding entry to the DHCP Reservations List.



Virtual Server

The DIR-605 can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network).

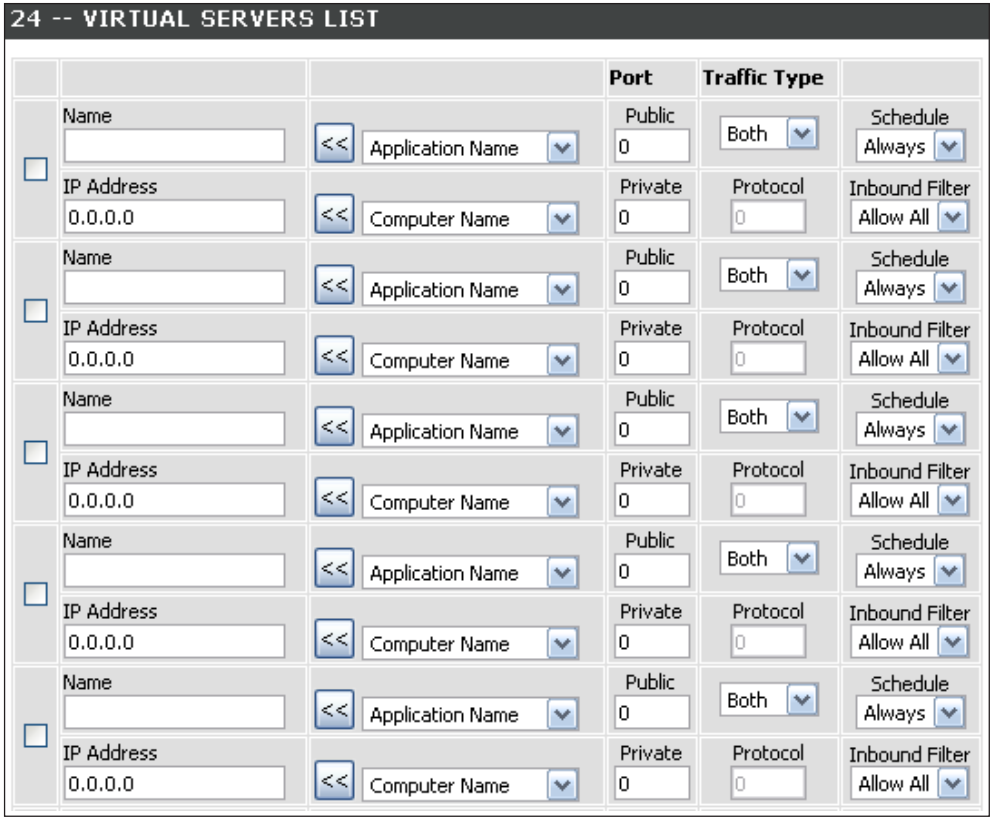
The DIR-605 firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DIR-605 are invisible to the outside world. If you wish, you can make some of the LAN computers accessible from the Internet by enabling Virtual Server. Depending on the requested service, the DIR-605 redirects the external service request to the appropriate server within the LAN network.

The DIR-605 is also capable of port-redirection meaning incoming traffic to a particular port may be redirected to a different port on the server computer.

Each virtual service that is created will be listed at the bottom of the screen in the Virtual Servers List. There are pre-defined virtual services already in the table. You may use them by enabling them and assigning the server IP to use that particular virtual service.

For a list of ports for common applications, please visit http://support.dlink.com/faq/view.asp?prod_id=1191.

This will allow you to open a single port. If you would like to open a range of ports, refer to the next page.



Name: Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the "Computer Name" drop-down menu. Select your computer and click <<.

Private Port/ Public Port: Enter the port that you want to open next to Private Port and Public Port. The private and public ports are usually the same. The public port is the port seen from the Internet side, and the private port is the port being used by the application on the computer within your local network.

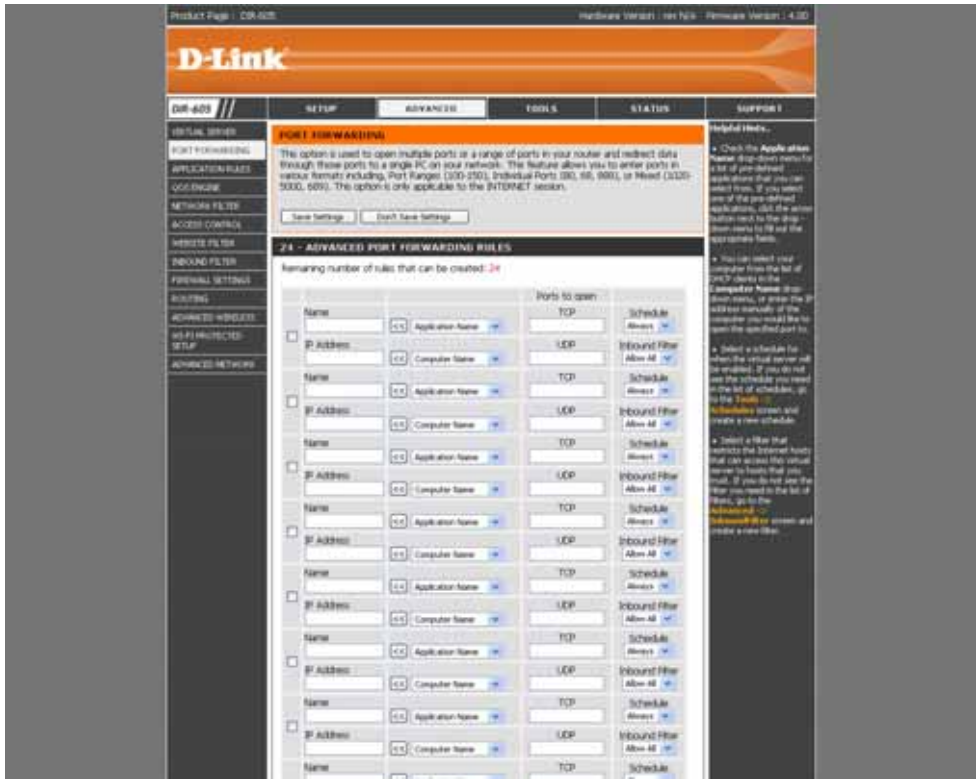
Protocol Type: Select TCP, UDP, or Both from the drop-down menu.

Inbound Filter: Select Allow All (most common) or a created Inbound filter. You may create your own inbound filters in the Advanced > Inbound Filter page.

Schedule: The schedule of time when the Virtual Server Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the Tools > Schedules section.

Port Forwarding

This will allow you to open a single port or a range of ports.



Name: Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the "Computer Name" drop-down menu. Select your computer and click <<.

TCP/UDP: Enter the TCP and/or UDP port or ports that you want to open. You can enter a single port or a range of ports. Separate ports with a common.

Example: 24,1009,3000-4000

Inbound Filter: Select Allow All (most common) or a created Inbound filter. You may create your own inbound filters in the Advanced > Inbound Filter page.

Schedule: The schedule of time when the Virtual Server Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the Tools > Schedules section.

Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Special Applications makes some of these applications work with the DIR-605. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the firewall (public) ports associated with the trigger port to open them for inbound traffic.

The DIR-605 provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

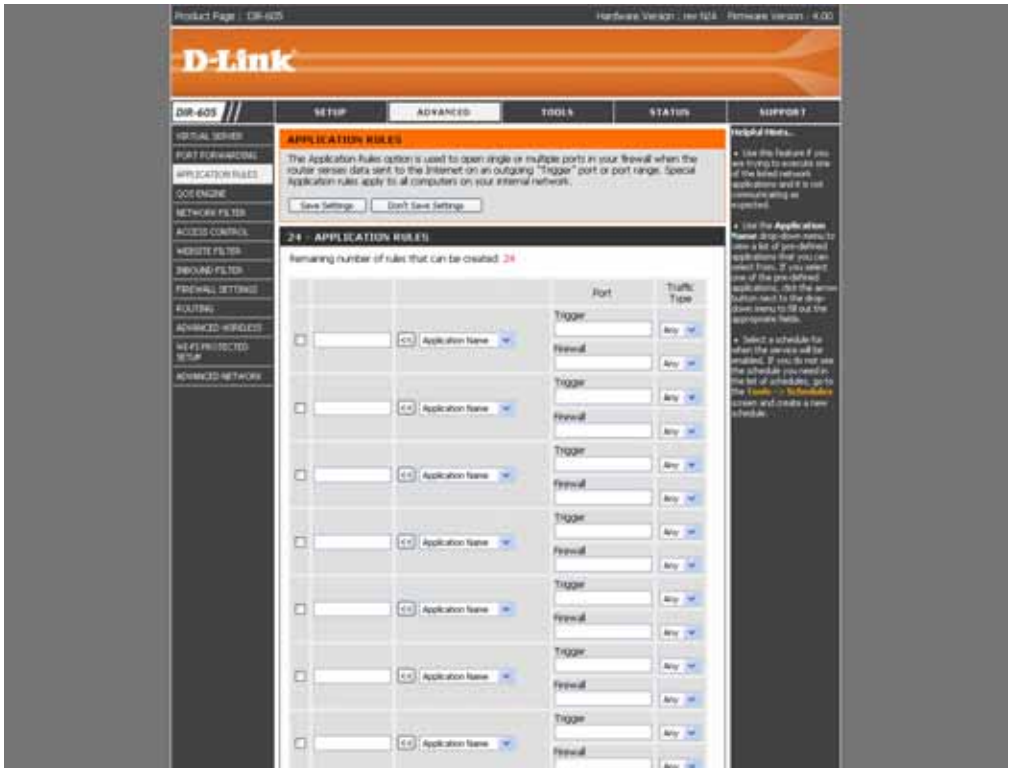
Name: Enter a name for the rule. You may select a pre-defined application from the drop-down menu and click <<.

Trigger: This is the port used to trigger the application. It can be either a single port or a range of ports.

Traffic Type: Select the protocol of the trigger port (TCP, UDP, or Both).

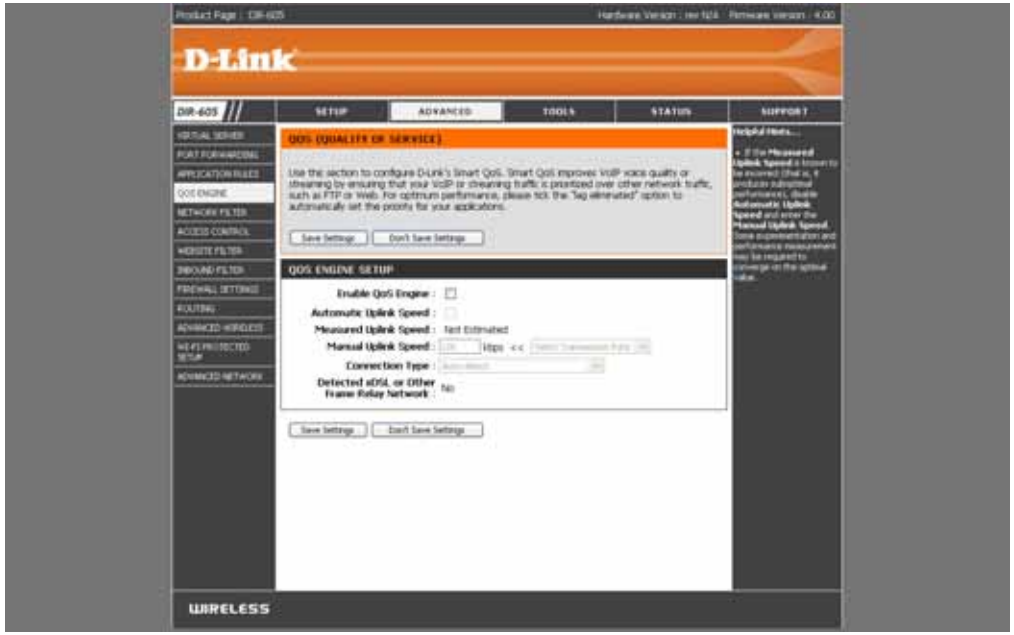
Firewall: This is the port number on the Internet side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.

Traffic Type: Select the protocol of the firewall port (TCP, UDP, or Both).



QoS Engine

The QoS Engine option helps improve your network gaming performance by prioritizing applications. By default the QoS Engine settings are disabled and application priority is not classified automatically.



Enable QoS Engine: This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

Automatic Uplink Speed: This option is enabled by default when the QoS Engine option is enabled. This option will allow your router to automatically determine the uplink speed of your Internet connection.

Measured Uplink Speed: This displays the detected uplink speed.

Manual Uplink Speed: The speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISP's offer speed as a download/upload pair. For example, 1.5Mbits/284Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as www.dslreports.com.

Connection Type: This option allows you to select your connection type.

Detected xDSL or Other Frame Relay Network: This displays if xDSL or other frame relay network has been detected.

Network Filters

Use MAC (Media Access Control) Filters to allow or deny LAN (Local Area Network) computers by their MAC addresses from accessing the Network. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the Broadband Router.

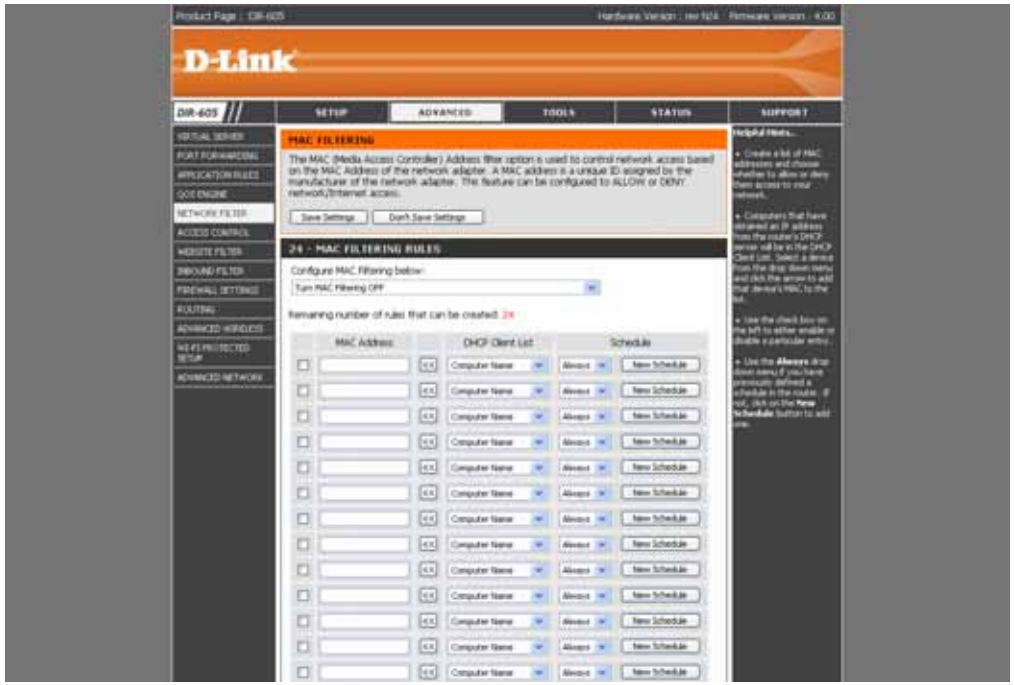
Configure MAC Filtering: Select Turn MAC Filtering Off, allow MAC addresses listed below, or deny MAC addresses listed below from the drop-down menu.

MAC Address: Enter the MAC address you would like to filter.

To find the MAC address on a computer, please refer to the Networking Basics section in this manual.

DHCP Client: Select a DHCP client from the drop-down menu and click << to copy that MAC Address.

New Schedule: Select to set the new schedule.



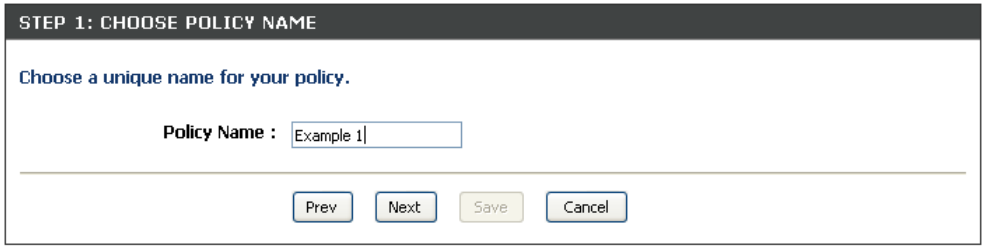
Access Control

The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

Add Policy: Check the Enable Access Control check box and click the Add Policy button to start the Access Control Wizard.

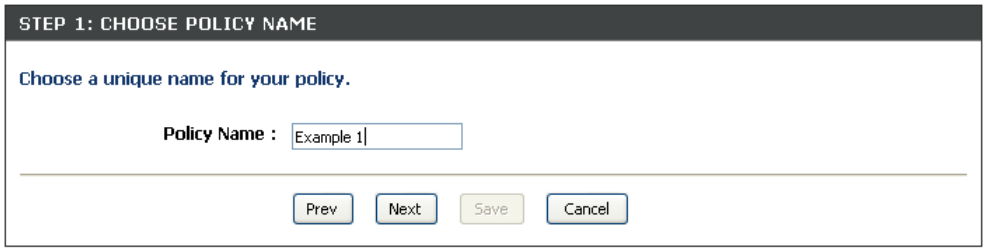
Access Control Wizard

Click Next to continue with the wizard.

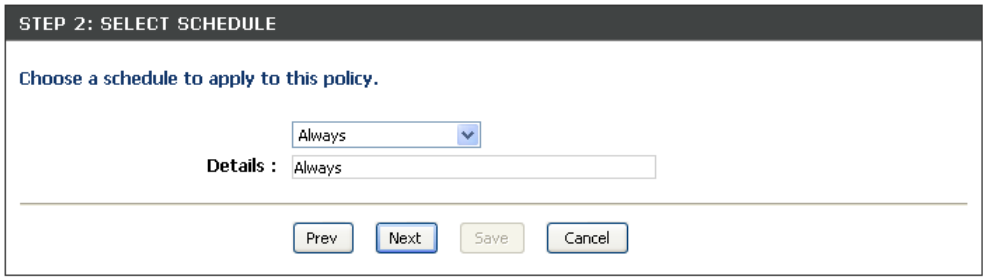


Access Control Wizard (continued)

Enter a name for the policy and then click Next to continue.

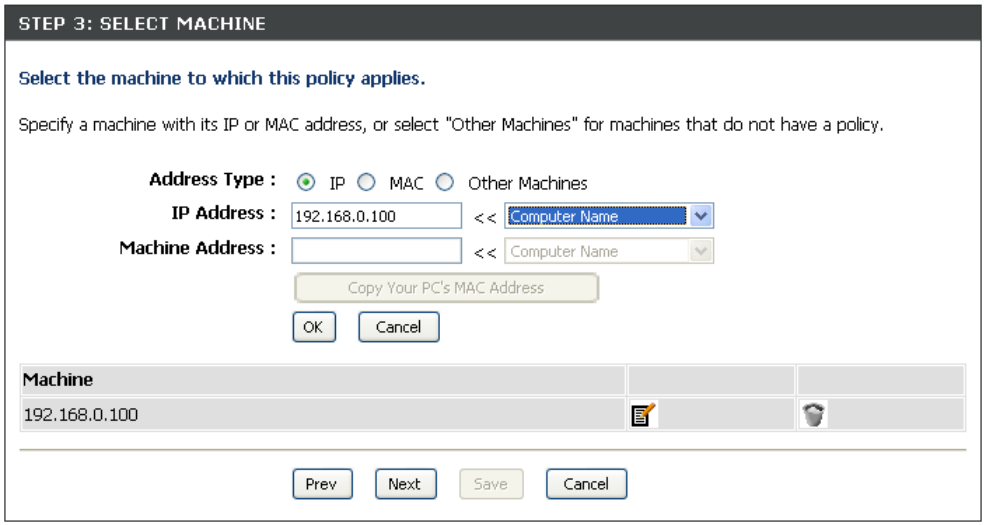


Select a schedule (I.E. Always) from the drop-down menu and then click Next to continue.



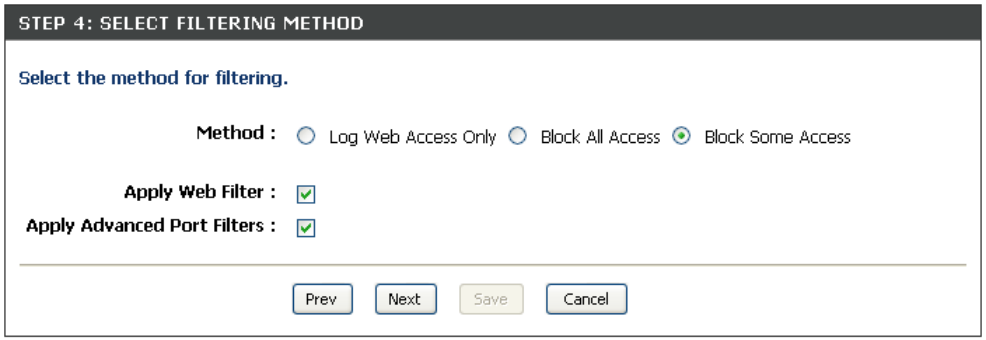
Enter the following information and then click Next to continue.

- Address Type - Select IP address, MAC address, or Other Machines.
- IP Address - Enter the IP address of the computer you want to apply the rule to.



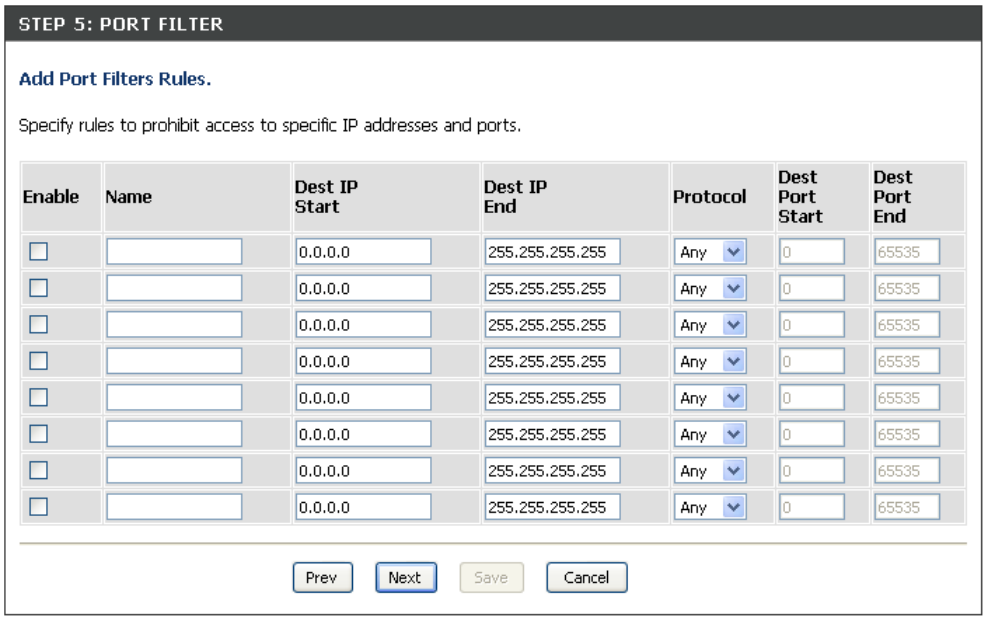
Access Control Wizard (continued)

Select the filtering method and then click Next to continue.



Enter the rule:

Enable - Check to enable the rule.
Name - Enter a name for your rule.
Dest IP Start - Enter the starting IP address.
Dest IP End - Enter the ending IP address.
Protocol - Select the protocol.
Dest Port Start - Enter the starting port number.
Dest Port End - Enter the ending port number.



To enable web logging, click Enable.

Click Save to save the access control rule.

Website Filters

Website Filters are used to allow you to set up a list of allowed Web sites that can be used by multiple users through the network. To use this feature select to Allow or Deny, enter the domain or website and click Add, and then click Save Settings. You must also select Apply Web Filter under the Access Control section (page 40).

Configure Website Filter Below: Select Deny or Allow computers access to only these sites.

Clear the list below: Click to delete all entries in the list.

Website URL/ Domain: Enter the keywords or URLs that you want to allow or deny.

New Schedule: Select to set the new scheulde.

Inbound Filters

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range. Inbound Filters can be used with Virtual Server, Port Forwarding, or Remote Administration features.

Name: Enter a name for the inbound filter rule.

Action: Select Allow or Deny.

Enable: Check to enable rule.

Source IP Start: Enter the starting IP address. Enter 0.0.0.0 if you do not want to specify an IP range.

Source IP End: Enter the ending IP address. Enter 255.255.255.255 if you do not want to specify and IP range.

Save: Click the Save button to apply your settings. You must click Save Settings at the top to save the settings.

Inbound Filter Rules List: This section will list any rules that are created. You may click the Edit icon to change the settings or enable/disable the rule, or click the Delete icon to remove the rule.

Firewall Settings

A firewall protects your network from the outside world. The D-Link DIR-605 offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

Enable SPI: SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol.

NAT Endpoint Filtering: Select one of the following for TCP and UDP ports:
Endpoint Independent - Any incoming traffic sent to an open port will be forwarded to the application that opened the port. The port will close if idle for 5 minutes.

Address Restricted - Incoming traffic must match the IP address of the outgoing connection.

Address + Port Restriction - Incoming traffic must match the IP address and port of the outgoing connection.

Enable Anti-Spoof Checking: Enable this option to provide protection from certain kinds of "spoofing" attacks.

Enable DMZ Host: If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer.

Note: Placing a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

IP Address: Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains its IP address automatically using DHCP, be sure to make a static reservation on the System > Network Settings page so that the IP address of the DMZ machine does not change.

Advanced Network Settings (Routing)

UPnP Settings: To use the Universal Plug and Play (UPnP™) feature, click on Enabled. UPNP provides compatibility with networking equipment, software and peripherals.

WAN Ping: Unchecking the box will not allow the device to respond to pings. Blocking the ping may provide some extra security from hackers. Check the box to allow the Internet port to be "pinged".

WAN Port Speed: You may set the speed of the Internet port to 10Mbps, 100Mbps, or auto. Older cable/DSL modems may require you to set your port speed to 10Mps.

Multicast Streams: Check the box to allow multicast traffic to pass through the router from the Internet.

Advanced Wireless Settings

Transmit Power: Set the transmit power of the antennas.

Beacon Period: Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting and is recommended.

RTS Threshold: This value should remain at its default setting of 2432. If inconsistent data flow is a problem, only a minor modification should be made.

Fragmentation Threshold: The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.

DTIM Interval: (Delivery Traffic Indication Message) 3 is the default setting. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

WLAN Partition: This enables 802.11d operation. 802.11d is a wireless specification developed to allow implementation of wireless networks in countries that cannot use the 802.11 standard. This feature should only be enabled if you are in a country that requires it.

WMM Enable: WMM is QoS for your wireless network. This will improve the quality of video and voice applications for your wireless clients.

Short GI: Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

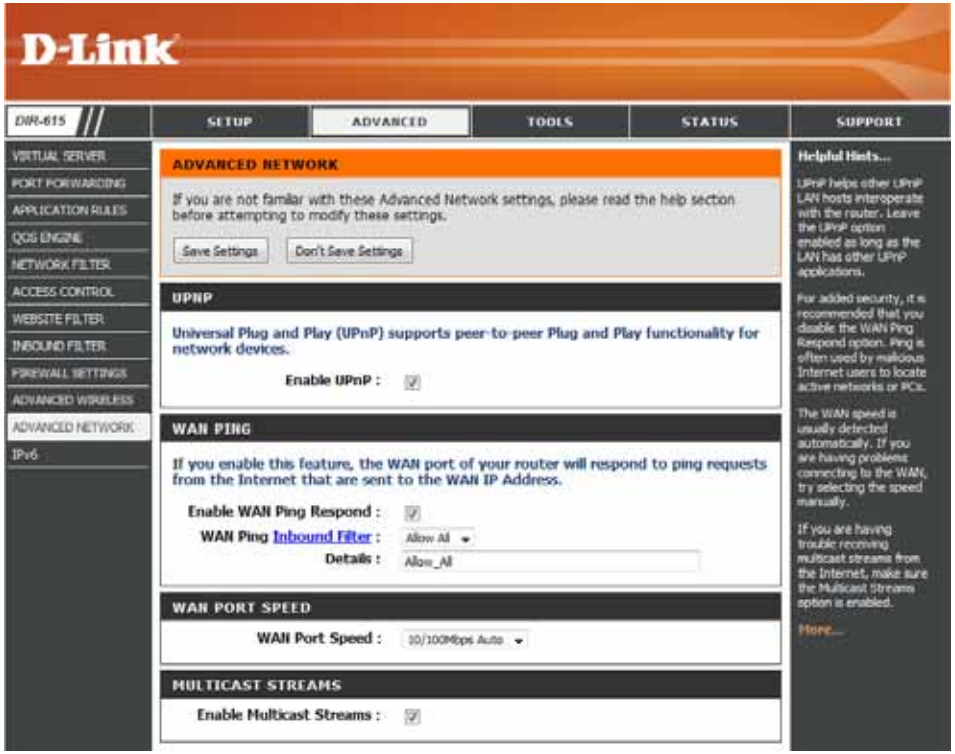
Advanced Network Settings

UPnP Settings: To use the Universal Plug and Play (UPnP™) feature click on Enabled. UPNP provides compatibility with networking equipment, software and peripherals.

WAN Ping: Unchecking the box will not allow the DIR-605 to respond to pings. Blocking the Ping may provide some extra security from hackers. Check the box to allow the Internet port to be "pinged".

WAN Port Speed: You may set the port speed of the Internet port to 10Mbps, 100Mbps, or auto. Some older cable or DSL modems may require you to set the port speed to 10Mbps.

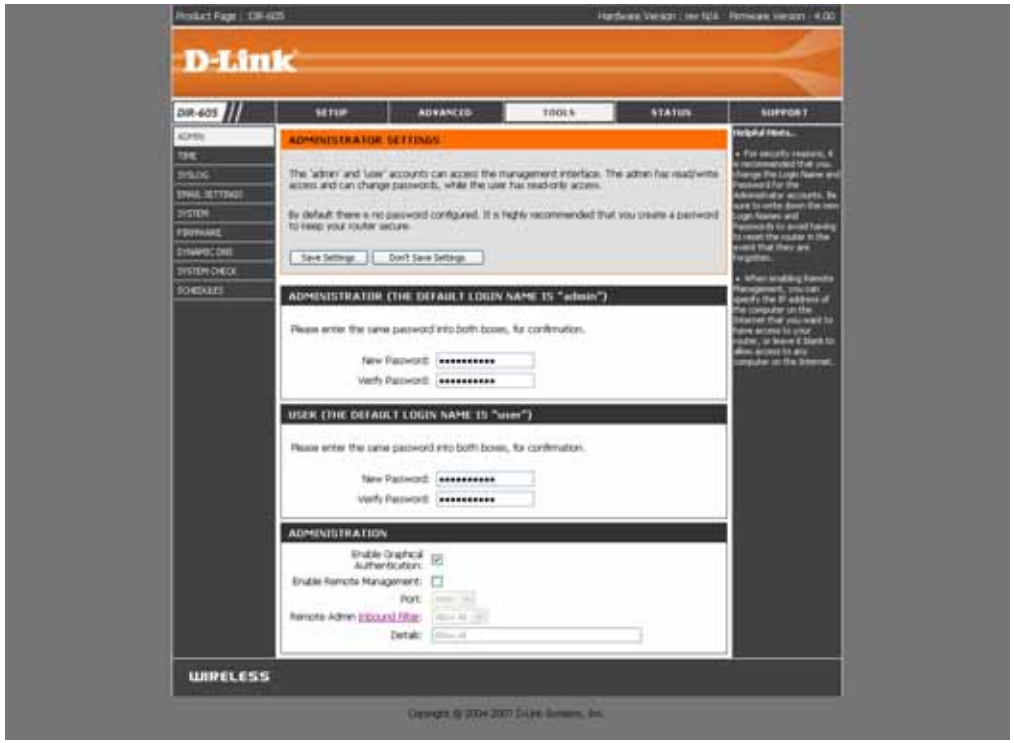
Multicast Streams: Check the box to allow multicast traffic to pass through the router from the Internet.



My IPv6 Connection:	Select PPPoE from the drop-down menu.
PPPoE:	Enter the PPPoE account settings supplied by your Internet provider (ISP).
Address Mode:	Select Static if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select Dynamic.
	Enter the IP address (Static PPPoE only).
IP Address:	Enter your PPPoE user name.
User Name:	Enter your PPPoE password and then retype the password in the next box.
Password:	Enter the ISP Service Name (optional).
	Select either Always-on, On-Demand, or Manual.
Service Name:	
	Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature,
Reconnection Mode:	enable Auto-reconnect.
Maximum Idle Time:	Select either Obtain DNS server address automatically or Use the following DNS Address.
	Enter the primary and secondary DNS server addresses.

Administrator Settings

This page will allow you to change the Administrator and User passwords. You can also enable Remote Management. There are two accounts that can access the management interface through the web browser. The accounts are admin and user. Admin has read/write access while user has read-only access. User can only view the settings but cannot make any changes. Only the admin account has the ability to change both admin and user account passwords.



Admin Password: Enter a new password for the Administrator Login Name. The administrator can make changes to the settings.

User Password: Enter the new password for the User login. If you login as the User, you can only see the settings, but cannot change them.

Remote Management: Remote management allows the DIR-605 to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.

Remote Admin Port: The port number used to access the DIR-605. Example: http://x.x.x.x:8080 whereas x.x.x.x is the Internet IP address of the DIR-605 and 8080 is the port used for the Web Management interface.

Inbound Filter: This section will list any rules that are created. You may click the Edit icon to change the settings or enable/disable the rule, or click the ADVANCED-Inbound filter web page to configure.

Enable Graphical Authentication: The device supports this function to prevent phishing.

Time Settings

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the Time Server. Daylight Saving can also be configured to automatically adjust the time when needed.

Time Zone: Select the Time Zone from the drop-down menu.

Daylight Saving: To select Daylight Saving time manually, select enabled or disabled, and enter a start date and an end date for daylight saving time.

Sync your Computer's Time Settings: Press this button to set the device's time the same to local PC.

Enable NTP Server: NTP is short for Network Time Protocol. NTP synchronizes computer clock times in a network of computers. Check this box to use a NTP server. This will only connect to a server on the Internet, not a local server.

NTP Server Used: Enter the NTP server or select one from the drop-down menu, then the DIR-605 will sync the same time to D-Link Internet time server.

Manual: To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second and then click Set Time.

SysLog

The Broadband Router keeps a running log of events and activities occurring on the Router. You may send these logs to a SysLog server on your network.

Save Log Files to Local Hard Drive: Click on the Save button to save log file to local hard drive which can later send to the network administrator for troubleshooting.

Enable Logging to SysLog Server: Check this box to send the router logs to a SysLog Server.

SysLog Server IP Address: The address of the SysLog server that will be used to send the logs. You may also select your computer from the drop-down menu (only if receiving an IP address from the router via DHCP).

E-mail Settings

The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your e-mail address.

Enable Email Notification: When this option is enabled, router activity logs are e-mailed to a designated e-mail address.

From Email Address: This e-mail address will appear as the sender when you receive a log file or firmware upgrade notification via e-mail.

To Email Address: Enter the e-mail address where you want the e-mail sent.

SMTP Server Address: Enter the SMTP server address for sending e-mail. If your SMTP server requires authentication, select this option.

Enable Authentication: Check this box if your SMTP server requires authentication.

Account Name: Enter your account for sending e-mail.

Password: Enter the password associated with the account. Re-type the password associated with the account.

On Log Full: When this option is selected, logs will be sent via e-mail when the log is full.

On Schedule: Selecting this option will send the logs via e-mail according to schedule.

Schedule: This option is enabled when On Schedule is selected. You can select a schedule from the list of defined schedules. To create a schedule, go to Tools > Schedules.

System Settings

Save Settings to Local Hard Drive: Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the Save button. You will then see a file dialog, where you can select a location and file name for the settings.

Load Settings from Local Hard Drive: Use this option to load previously saved router configuration settings. First, use the Browse control to find a previously save file of configuration settings. Then, click the Load button to transfer those settings to the router.

Restore to Factory Default Settings: This option will restore all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current router configuration settings, use the Save button above.

Reboot Device: Click to reboot the router.

Clear Language Pack: This is to restore the device back to English version only. Remove other languages installed for the system web pages.

Update Firmware

You can upgrade the firmware of the Router here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on Browse to locate the firmware file to be used for the update. Please check the D-Link support site for firmware updates at http://support.dlink.com. You can download firmware upgrades to your hard drive from the D-Link support site.

Firmware Information: Displays the current firmware version and date.

You can also check the availability of a new firmware version online. If so, download the new firmware to your hard drive.

Firmware Upgrade: After you have downloaded the new firmware, click Browse to locate the firmware update on your hard drive. Click Upload to complete the firmware upgrade.

Language Pack Upgrade: This function allows the user to transfer the language of GUI from English to theirs by upgrading the language pack.

DDNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc…) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter in your domain name to connect to your server no matter what your IP address is.

DDNS: Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP Address. Check the box to enable DDNS.

Server Address: Choose your DDNS provider from the drop down menu.

Host Name: Enter the Host Name that you registered with your DDNS service provider.

Username or Key: Enter the Username for your DDNS account.

Password or Key: Enter the Password for your DDNS account.

DDNS Account Testing: This is to test if the DDNS account is valid for use.

System Check

The System Check feature allows you to verify the physical connectivity on both LAN and Internet interface.

Ping Test: The Ping Test is used to send Ping packets to test if a computer is on the Internet. Enter the IP Address that you wish to Ping, and click Ping.

Ping Results: The results of your ping attempts will be displayed here.

System Check: The System Check tool can be used to verify the physical connectivity on both the LAN and Internet interfaces.

Schedules

Name: Enter a name for your new schedule.

Days: Select a day, a range of days, or All Week to include every day.

Time: Check All Day - 24hrs or enter a start and end time for your schedule.

Save: Click Save to save your schedule. You must click Save Settings at the top for your schedules to go into effect.

Schedule Rules List: The list of schedules will be listed here. Click the Edit icon to make changes or click the Delete icon to remove the schedule.

Device Information

This page displays the current information for the DIR-605. It will display the LAN, WAN (Internet), and Wireless information.

If your Internet connection is set up for a Dynamic IP address then a Release button and a Renew button will be displayed. Use Release to disconnect from your ISP and use Renew to connect to your ISP.

If your Internet connection is set up for PPPoE, a Connect button and a Disconnect button will be displayed. Use Disconnect to drop the PPPoE connection and use Connect to establish the PPPoE connection.

See the following page for more information.

General: Displays the router's time and firmware version.

Internet: Displays the MAC address and the public IP settings for the router.

LAN: Displays the MAC address and the private (local) IP settings for the router.

Wireless LAN: Displays the wireless MAC address and your wireless settings such as SSID and Channel.

LAN Computers: Displays computers and devices that are connected to the router via Ethernet and that are receiving an IP address assigned by the router (DHCP).

IGMP Multicast Memberships: Displays the Multicast Group IP Address.

Log

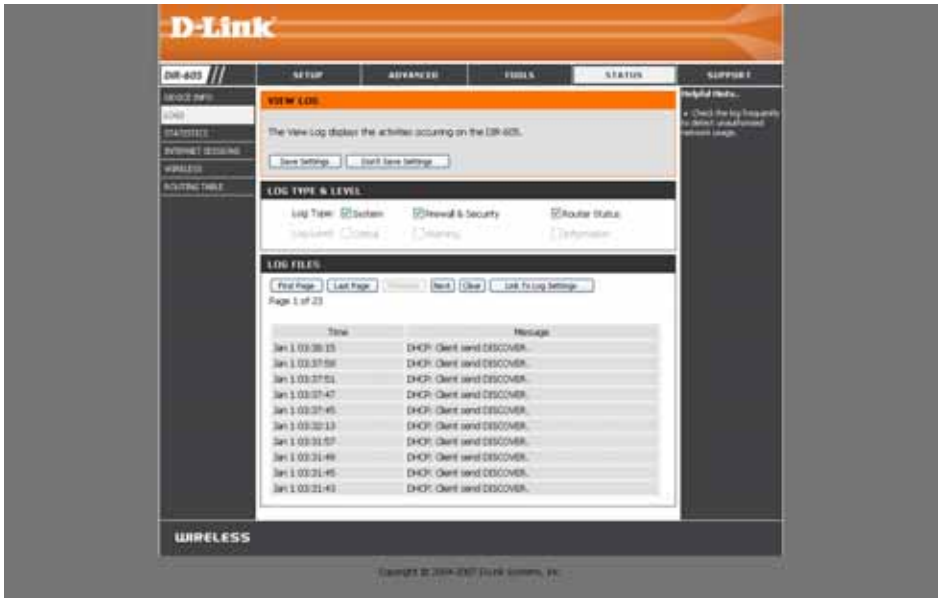
The router automatically logs (records) events of possible interest in it's internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

What to View: You can select the types of messages that you want to display from the log. Firewall & Security, System, and Router Status messages can be selected.

View Levels: There are three levels of message importance: Informational, Warning, and Critical. Select the levels that you want displayed in the log.

Clear: Clears all of the log contents.

Link to Log Settings: The user can click the button to " link to log settings" and save the logs to local hard drive or to syslog server.



Stats

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DIR-605 on both the Internet and the LAN ports. The traffic counter will reset if the device is rebooted.

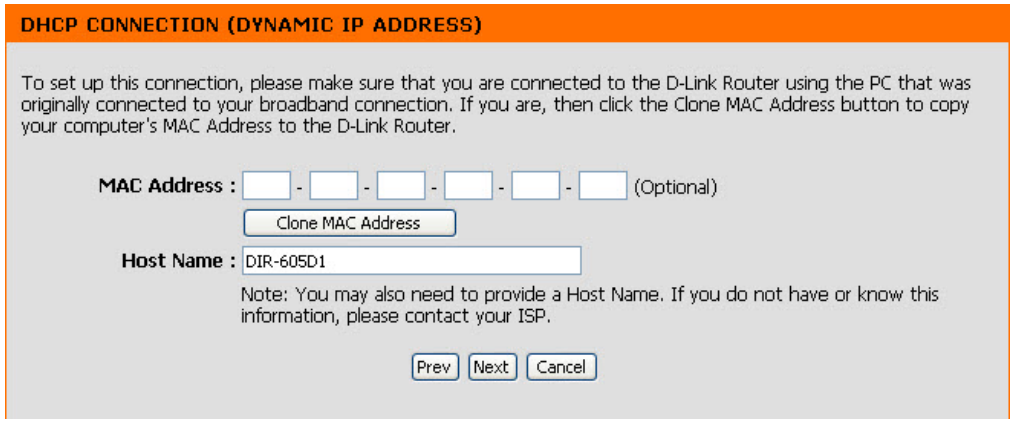
Internet Sessions

The Internet Sessions page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.

IP Address: The IP address and, where appropriate, port number of the local application.

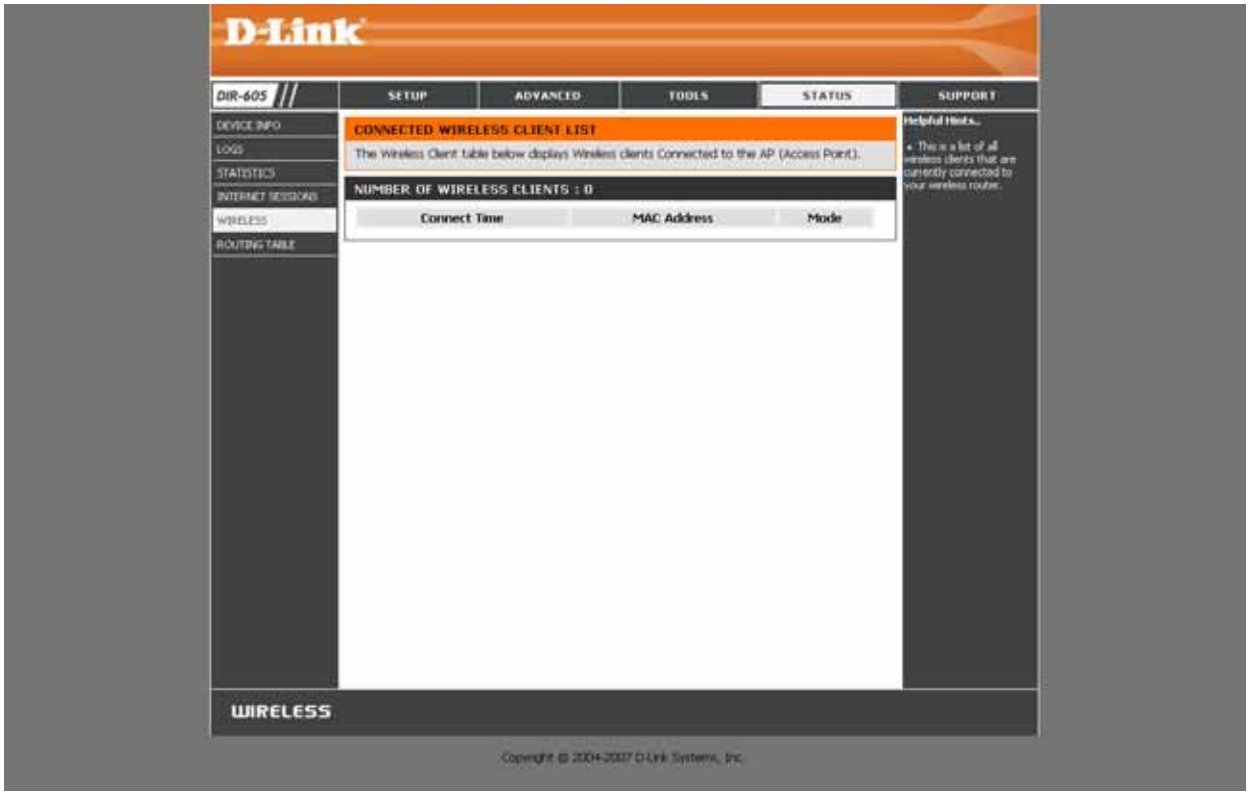
TCP Session: This shows the number of TCP packets being sent from the source IP address.

UDP Session: This shows the number of UDP packets being sent from the source IP address.



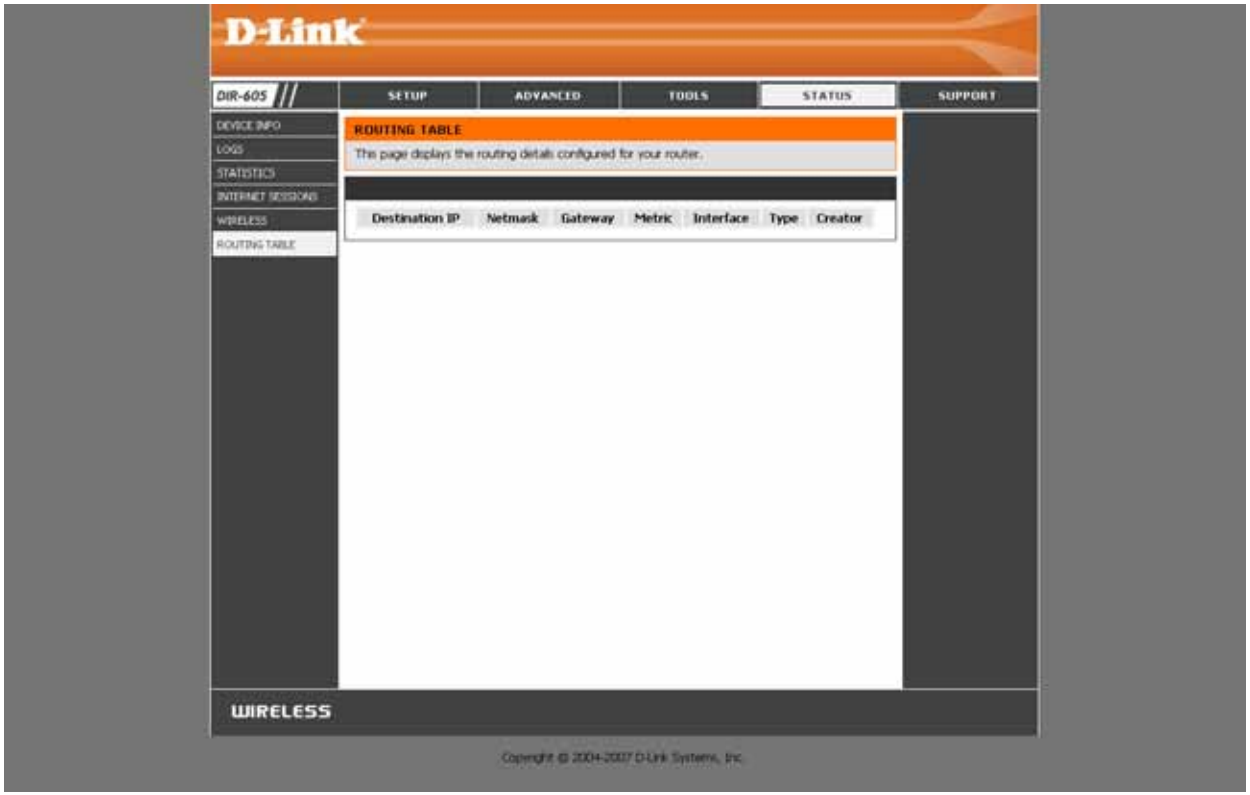
Wireless

The wireless client table displays a list of current connected wireless clients. This table also displays the connection time and MAC address of the connected wireless clients.



Routing Table

The routing table displays all routing related information configured for your router.



Support


D-Link
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT
SUPPORT MENU
Setup
Advanced
Tools
Status
WIRELESS

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-605 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WPA2-PSK(Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

What is WPA?

WPA, or Wi-Fi Protected Access, is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.

- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

Wireless Connection Setup Wizard

To run the security wizard, browse to the Setup page and then click the Wireless Connection Setup Wizard button.

Click Next to continue.

Enter the SSID (Service Set Identifier). The SSID is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.

Select the level of security for your wireless network:

- Best - WPA2 Authentication
- Better - WPA Authentication
- None - No security

Click Next to continue.

If you selected Best or Better, enter a password between 8-63 characters.

If you selected Good, enter 13 characters or 26 Hex digits.

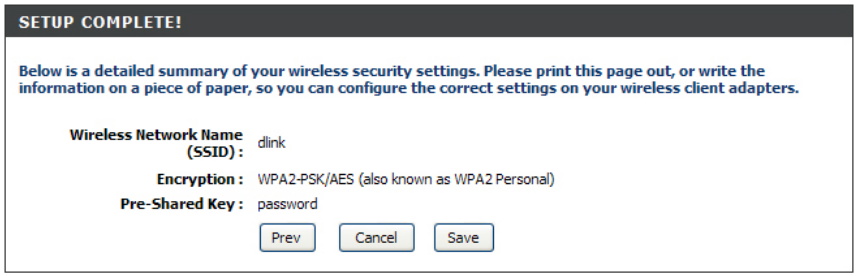
Click Next to continue.

If you selected Better, the following screen will show you your Pre-Shared Key to enter on your wireless clients.

Click Save to finish the Security Wizard.

If you selected Best, the following screen will show you your Pre-Shared Key to enter on your wireless clients.

Click Save to finish the Security Wizard.



If you selected WPA-Enterprise, the RADIUS information will be displayed. Click Save to finish the Security Wizard.

Add Wireless Device with WPS Wizard

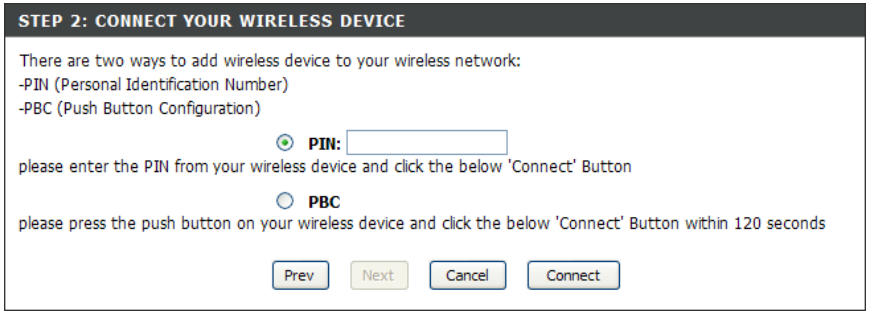
From the Setup > Wireless Settings screen, click Add Wireless Device with WPS.

Select Auto to add a wireless client using WPS (Wi-Fi Protected Setup). Once you select Auto and click Connect, you will have a 120 second time limit to apply the settings to your wireless client(s) and successfully establish a connection.

If you select Manual, a settings summary screen will appear. Write down the security key and enter this on your wireless clients.

PIN: Select this option to use PIN method. In order to use this method you must know the wireless client's 8 digit PIN and click Connect.

PBC: Select this option to use PBC (Push Button) method to add a wireless client. Click Connect.



Configure WPA-Personal (PSK)

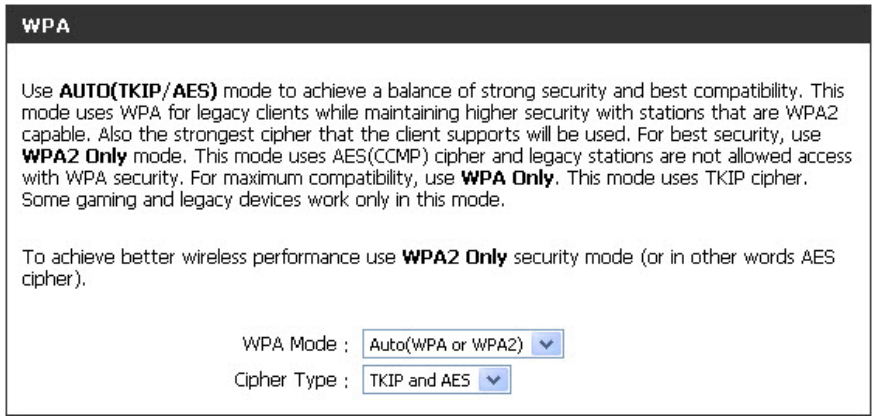
It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on Setup and then click Wireless Settings on the left side.

2. Next to Security Mode, select WPA-Personal.

3. Next to WPA Mode, select Auto, WPA2 Only, or WPA Only. Use Auto if you have wireless clients using both WPA and WPA2.

4. Next to Cypher Type, select TKIP and AES, TKIP, or AES. If you have wireless clients that use both types, use TKIP and AES.



5. Next to Group Key Update Interval, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).

6. Next to Pre-Shared Key, enter a key (passphrase). The key is entered as a pass-phrase in ASCII format at both ends of the wireless connection. The pass-phrase must be between 8-63 characters.

7. Click Save Settings to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the router.

Configure WPA-Enterprise (RADIUS)

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on Setup and then click Wireless Settings on the left side.

2. Next to Security Mode, select WPA-Enterprise.

3. Next to WPA Mode, select Auto, WPA2 Only, or WPA Only. Use Auto if you have wireless clients using both WPA and WPA2.

4. Next to Cypher Type, select TKIP and AES, TKIP, or AES. If you have wireless clients that use both types, use TKIP and AES.

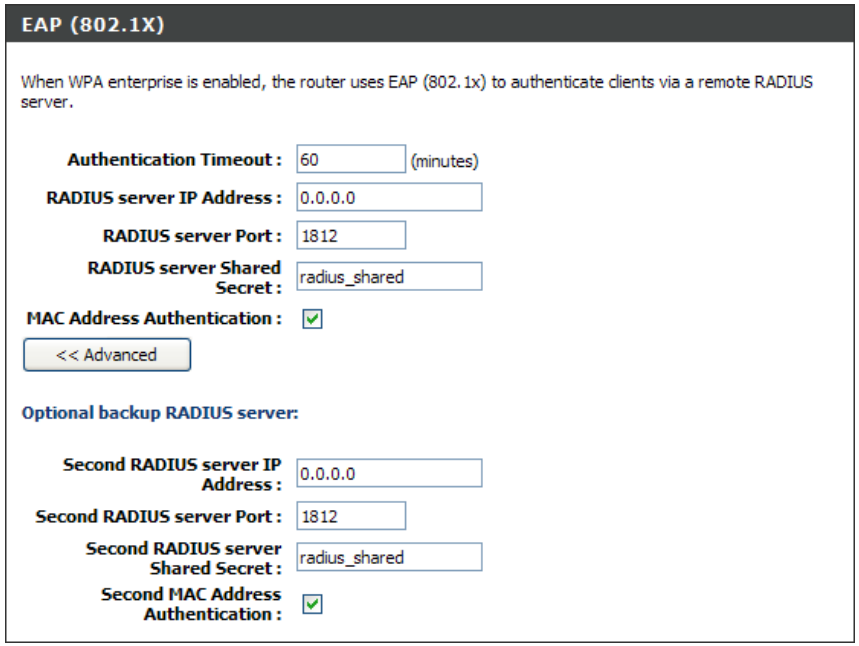
5. Next to Group Key Update Interval, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).

6. Next to Authentication Timeout, enter the amount of time before a client is required to re-authenticate (60 minutes is default).

7. Next to RADIUS Server IP Address enter the IP Address of your RADIUS server.

8. Next to RADIUS Server Port, enter the port you are using with your RADIUS server. 1812 is the default port.

9. Next to RADIUS Server Shared Secret, enter the security key.


EAP (802.1X)
When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.
Authentication Timeout :
60
(minutes)
RADIUS server IP Address :
0.0.0.0
RADIUS server Port :
1812
RADIUS server Shared Secret :
radius_shared
MAC Address Authentication :
<< Advanced
Optional backup RADIUS server:
Second RADIUS server IP Address :
0.0.0.0
Second RADIUS server Port :
1812
Second RADIUS server Shared Secret :
radius_shared
Second MAC Address Authentication :

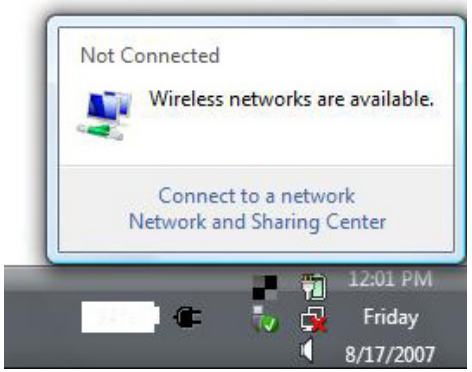
Connect to a Wireless Network
Using Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows Vista® utility as seen below.

If you receive the Wireless Networks Detected bubble, click on the center of the bubble to access the utility.

or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select Connect to a network.



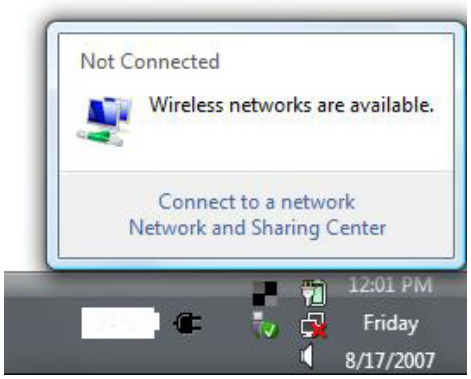
The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the Connect button.

If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.

Configure WPA/WPA2

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select Connect to a network.



2. Highlight the wireless network (SSID) you would like to connect to and click Connect.

3. Enter the same security key or passphrase that is on your router and click Connect.

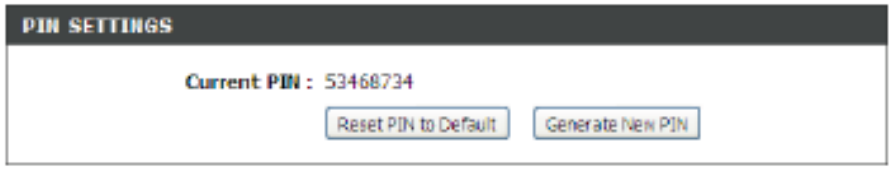
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

Connect Using WCN 2.0

The router supports Wi-Fi protection, referred to as WCN 2.0 in Windows Vista®. The following instructions for setting this up depends on whether you are using Windows Vista® to configure the router or third party software.

When you first set up the router, Wi-Fi protection is disabled and unconfigured. To enjoy the benefits of Wi-Fi protection, the router must be both enabled and configured. There are three basic methods to accomplish this: use Windows Vista's built-in support for WCN 2.0, use software provided by a third party, or manually configure.

If you are running Windows Vista®, log into the router and click the Enable checkbox in the Basic > Wireless section. Use the Current PIN that is displayed on the Advanced > Wi-Fi Protected Setup section or choose to click the Generate New PIN button or Reset PIN to Default button.

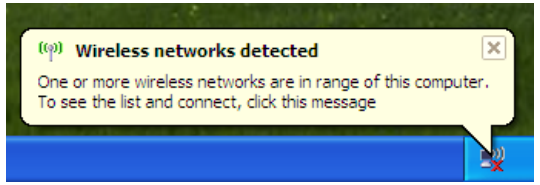


If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.

Using Windows® XP

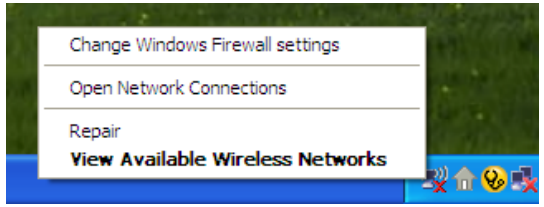
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

If you receive the Wireless Networks Detected bubble, click on the center of the bubble to access the utility.



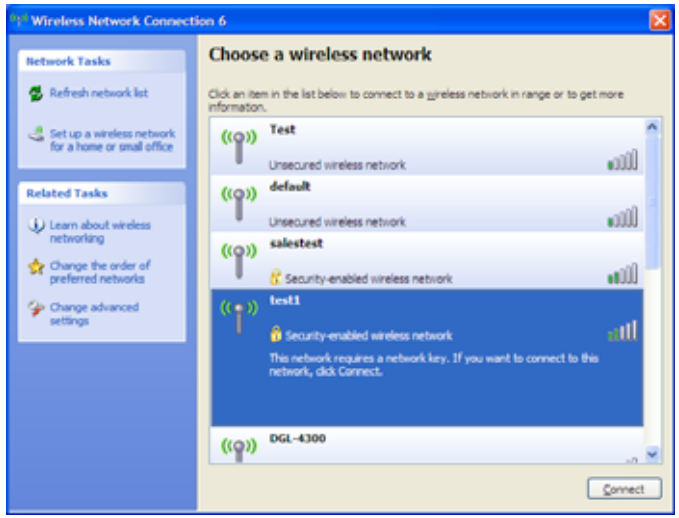
or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select View Available Wireless Networks.



The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the Connect button.

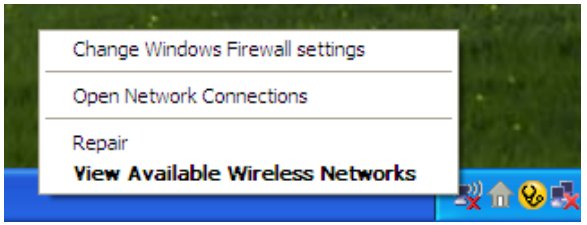
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.



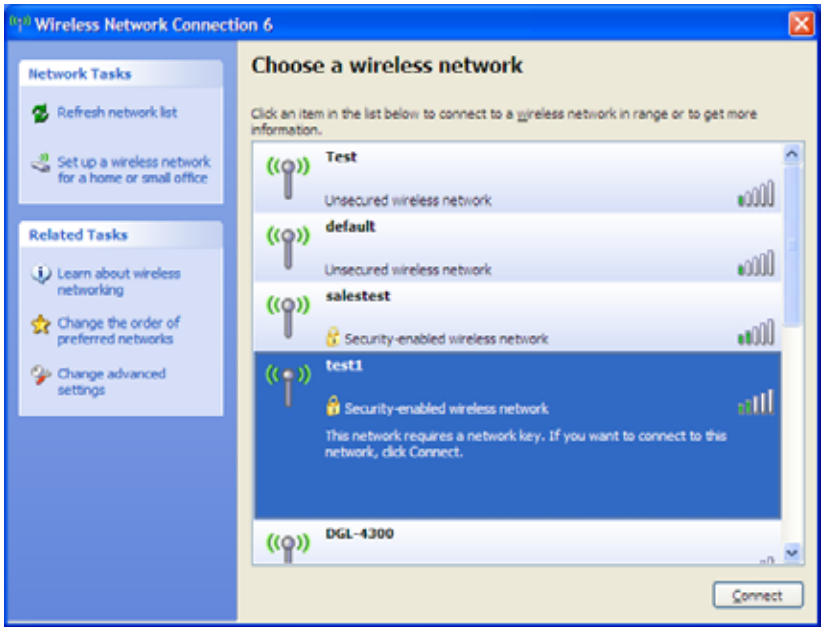
Configure WPA-PSK

It is recommended to enable WEP on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WEP key being used.

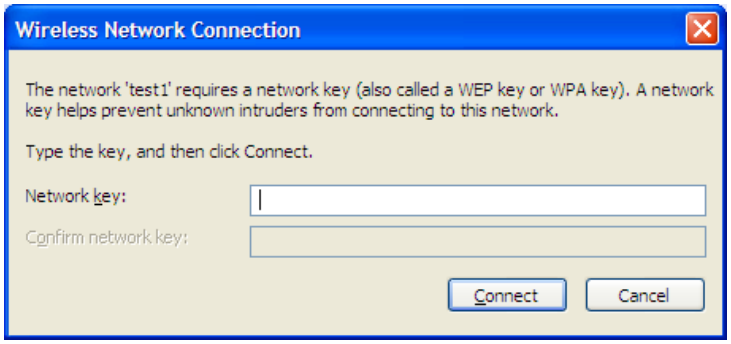
1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select View Available Wireless Networks.



2. Highlight the wireless network (SSID) you would like to connect to and click Connect.



3. The Wireless Network Connection box will appear. Enter the WPA-PSK passphrase and click Connect.



It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA-PSK settings are correct. The WPA-PSK passphrase must be exactly the same as on the wireless router.

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-605. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screen shots on your computer will look similar to the following examples.)

1. Why can't I access the web-based configuration utility?

When entering the IP address of the D-Link router (192.168.0.1 for example), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

• Make sure you have an updated Java-enabled web browser. We recommend the following:

- Internet Explorer 6.0 or higher
- Netscape 8 or higher
- Mozilla 1.7.12 (5.0) or higher
- Opera 8.5 or higher
- Safari 1.2 or higher (with Java 1.3.1 or higher)
- Camino 0.8.4 or higher
- Firefox 1.5 or higher

• Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.

• Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

• Configure your Internet settings:

  • Go to Start > Settings > Control Panel. Double-click the Internet Options Icon. From the Security tab, click the button to restore the settings to their defaults.

  • Click the Connection tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click OK.

  • Go to the Advanced tab and click the button to restore these settings to their defaults. Click OK three times.

  • Close your web browser (if open) and open it.

• Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your the web management.

• If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

2. What can I do if I forgot my password?

If you forgot your password, you must reset your router. Unfortunately this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.0.1. When logging in, the username is admin and leave the password box empty.

3. Why can't I connect to certain sites or send and receive e-mails when connecting through my router?

If you are having a problem sending or receiving e-mail, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

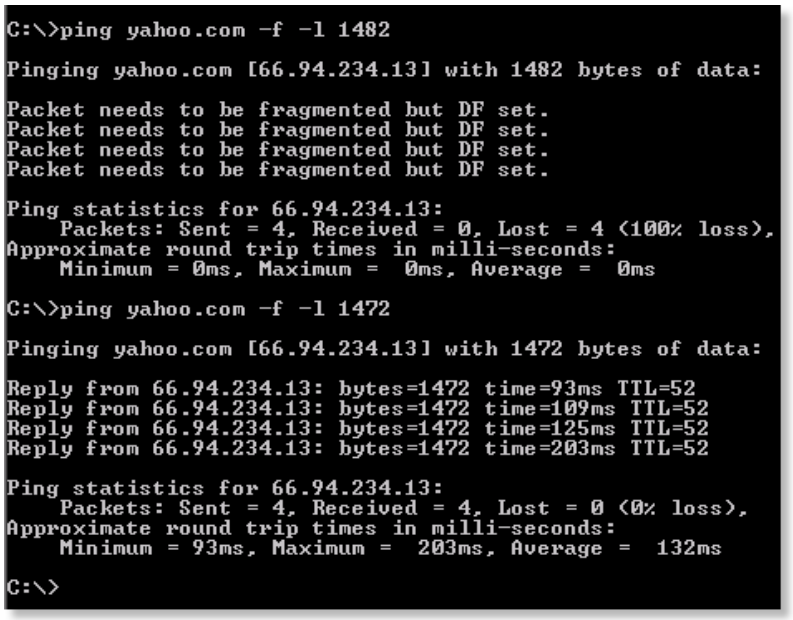
Note: AOL DSL+ users must use MTU of 1400.

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.

- Click on Start and then click Run.
- Windows® 95, 98, and Me users type in command (Windows® NT, 2000, and XP users type in cmd) and press Enter (or click OK).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

  ping [url] [-f] [-l] [MTU value]

Example: ping yahoo.com -f -l 1472



You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, lets say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with (1452+28=1480).

Once you find your MTU, you can now configure your router with the proper MTU size.

To change the MTU rate on your router follow the steps below:

- Open your browser, enter the IP address of your router (192.168.0.1) and click OK.
- Enter your username (admin) and password (blank by default). Click OK to enter the web configuration page for the device.
- Click on Setup and then click Manual Configure.
- To change the MTU enter the number in the MTU field and click Save Settings to save your settings.
- Test your e-mail. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Wireless Basics

D-Link wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, the D-Link wireless family of products will allow you to securely access the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A Wireless Router is a device used to provide this link.

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

Why D-Link Wireless?

D-Link is the worldwide leader and award winning designer, developer, and manufacturer of networking products. D-Link delivers the performance you need at a price you can afford. D-Link has all the products you need to build your network.

How does wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away.

Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology as become so popular in recent years that almost everyone is using it, whether it's for home, office, business, D-Link has a wireless solution for it.

Home

- Gives everyone at home broadband access
- Surf the web, check e-mail, instant message, and etc
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

- Stay on top of everything at home as you would at office
- Remotely access your office network from home
- Share Internet connection and printer with multiple computers
- No need to dedicate office space

Where is wireless used?

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots".

Using a D-Link Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

Wireless network is easy to setup, but if you're installing it for the first time it could be quite a task not knowing where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

Tips

Here are a few things to keep in mind, when you install a wireless network.

Centralize your router or Access Point

Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal to extend the range.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This would significantly reduce any interference that the appliances might cause since they operate on same frequency.

Security

Don't let you next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to product manual for detail information on how to set it up.

Wireless Modes

There are basically two modes of networking:

- Infrastructure – All wireless clients will connect to an access point or wireless router.

- Ad-Hoc – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DIR-605 wireless network Cardbus adapters.

An Infrastructure network contains an Access Point or wireless router. All the wireless devices, or clients, will connect to the wireless router or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

Networking Basics

Check your IP address

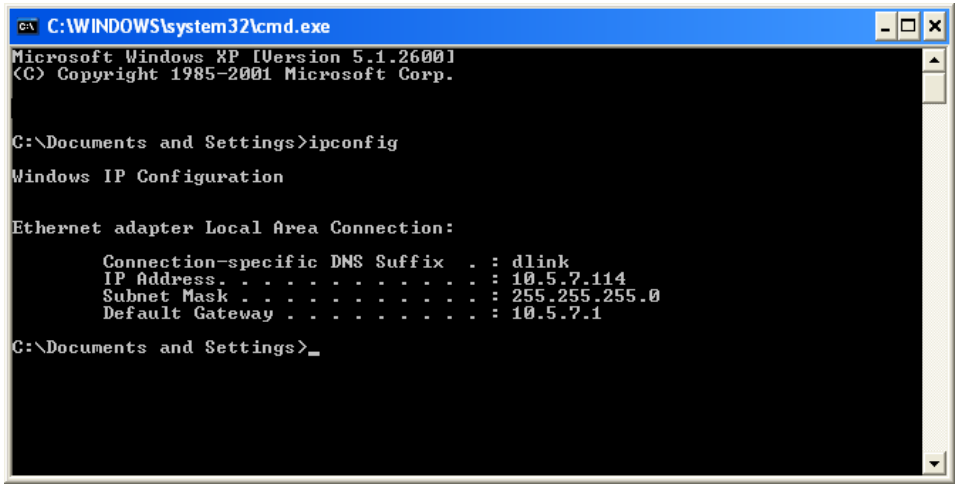
After you install your adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on Start > Run. In the run box type cmd and click OK. (Windows Vista® users type cmd in the Start Search box.)

At the prompt, type ipconfig and press Enter.

This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.



Statically Assign an IP address

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Step 1

Windows Vista® - Click on Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections.

Windows® XP - Click on Start > Control Panel > Network Connections.

Windows® 2000 - From the desktop, right-click My Network Places > Properties.

Step 2

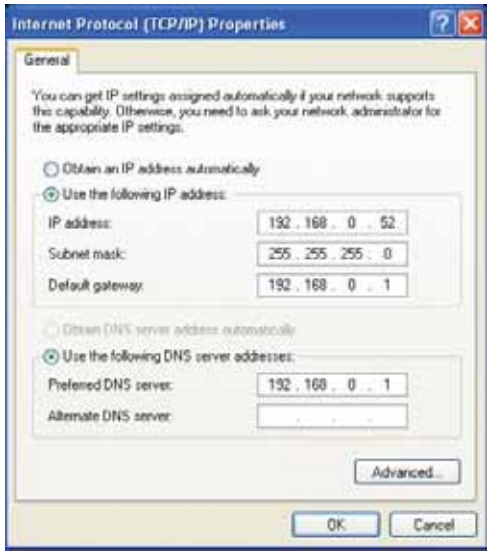
Right-click on the Local Area Connection which represents your network adapter and select Properties.

Step 3

Highlight Internet Protocol (TCP/IP) and click Properties.

Step 4

Click Use the following IP address and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.



Example: If the router´s LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5

Click OK twice to save your settings.

CE Mark Warning:

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

FCC Caution:

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

注意 !

依據　低功率電波輻射性電機管理辦法

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

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

IC EMI(ICES-003)

"This Class B digital apparatus complies with Canadian ICES-003."
"Cet appareil numérique de la classe Class B est conforme à la norme NMB-003 du Canada."

Operation is subject to the following two conditions:
1) this device may not cause interference, and
2) this device must accept any interference, including interference that may cause undesired operation of the device.
IMPORTANT NOTE:
IC Radiation Exposure Statement:
This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.