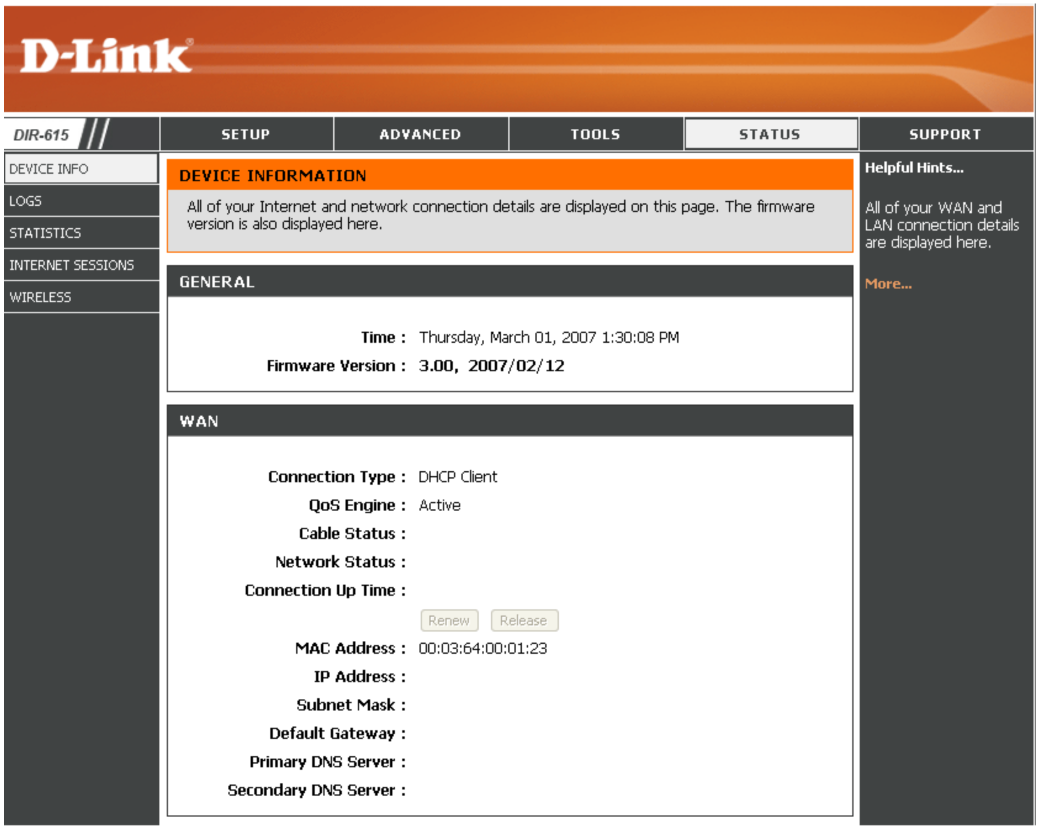
Device Information

This page displays the current information for the DIR-615. 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.



DEVICE INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

All of your WAN and LAN connection details are displayed here.

GENERAL

Time : Thursday, March 01, 2007 1:30:08 PM
Firmware Version : 3.00, 2007/02/12

WAN

Connection Type : DHCP Client
QoS Engine : Active
Cable Status :
Network Status :
Connection Up Time :
MAC Address : 00:03:64:00:01:23
IP Address :
Subnet Mask :
Default Gateway :
Primary DNS Server :
Secondary DNS Server :

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

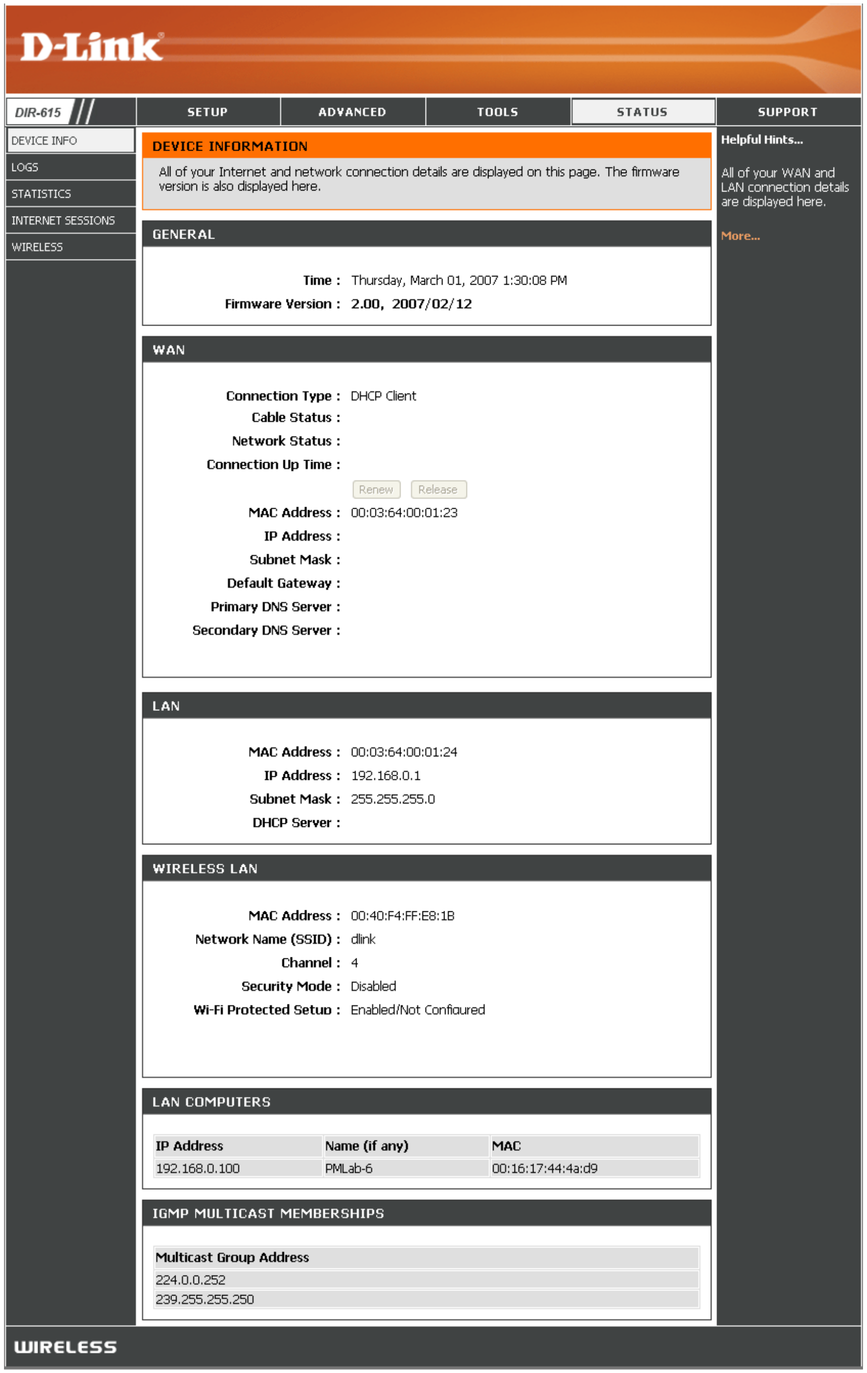
WAN: Displays the MAC address and the public IP settings for the router.

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.



DEVICE INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

GENERAL

Time : Thursday, March 01, 2007 1:30:08 PM
Firmware Version : 2.00, 2007/02/12

WAN

Connection Type : DHCP Client
Cable Status :
Network Status :
Connection Up Time :
MAC Address : 00:03:64:00:01:23
IP Address :
Subnet Mask :
Default Gateway :
Primary DNS Server :
Secondary DNS Server :

LAN

MAC Address : 00:03:64:00:01:24
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server :

WIRELESS LAN

MAC Address : 00:40:F4:FF:E8:1B
Network Name (SSID) : dlink
Channel : 4
Security Mode : Disabled
Wi-Fi Protected Setup : Enabled/Not Configured

LAN COMPUTERS

IP Address	Name (if any)	MAC
192.168.0.100	PMLab-6	00:16:17:44:4a:d9

IGMP MULTICAST MEMBERSHIPS

Multicast Group Address
224.0.0.252
239.255.255.250

Helpful Hints...

All of your WAN and LAN connection details are displayed here.

More...

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.

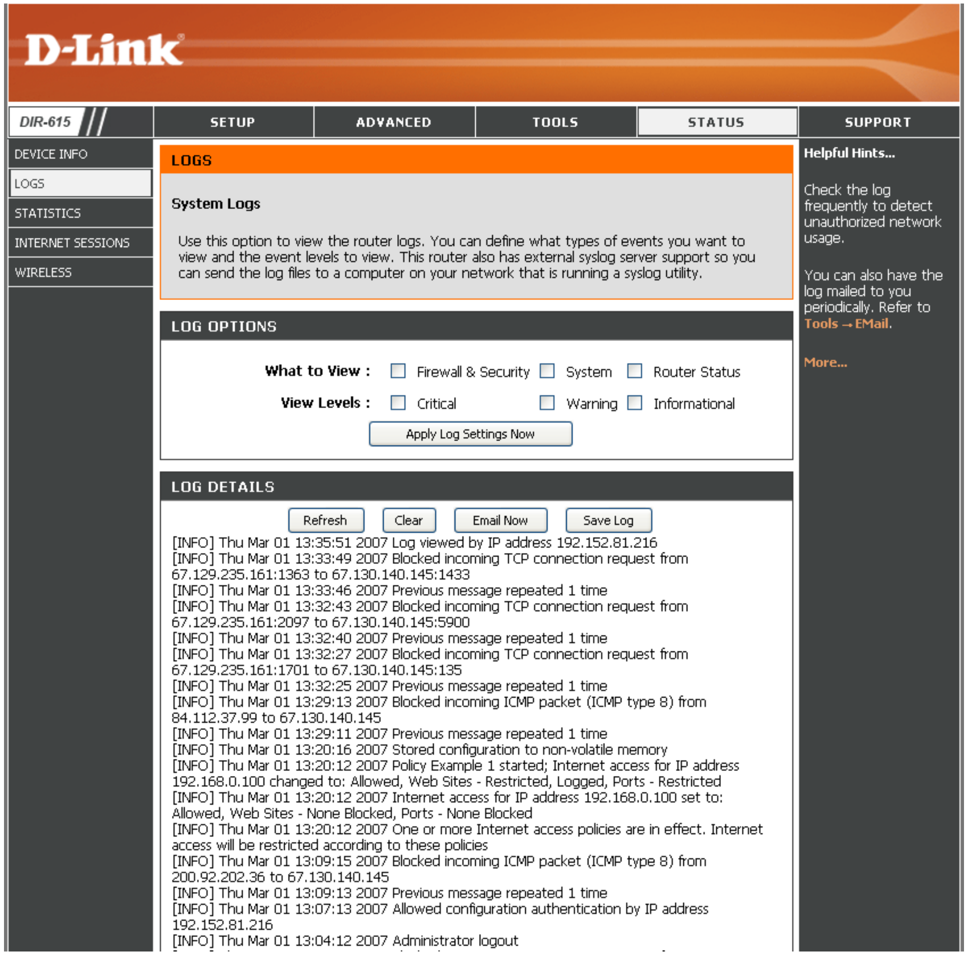
Apply Log Settings: Will filter the log results so that only the selected options appear.

Refresh: Updates the log details on the screen so it displays any recent activity.

Clear: Clears all of the log contents.

Email Now: This option will send a copy of the router log to the e-mail address configured in the **Tools > Email Settings** screen.

Save Log: This option will save the router to a log file on your computer.



LOGS

System Logs

Use this option to view the router logs. You can define what types of events you want to view and the event levels 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.

LOG OPTIONS

What to View : □ Firewall & Security □ System □ Router Status

View Levels : □ Critical □ Warning □ Informational

LOG DETAILS

```
[INFO] Thu Mar 01 13:35:51 2007 Log viewed by IP address 192.152.81.216
[INFO] Thu Mar 01 13:33:49 2007 Blocked incoming TCP connection request from
67.129.235.161:1363 to 67.130.140.145:1433
[INFO] Thu Mar 01 13:33:46 2007 Previous message repeated 1 time
[INFO] Thu Mar 01 13:32:43 2007 Blocked incoming TCP connection request from
67.129.235.161:2097 to 67.130.140.145:5900
[INFO] Thu Mar 01 13:32:40 2007 Previous message repeated 1 time
[INFO] Thu Mar 01 13:32:27 2007 Blocked incoming TCP connection request from
67.129.235.161:1701 to 67.130.140.145:135
[INFO] Thu Mar 01 13:32:25 2007 Previous message repeated 1 time
[INFO] Thu Mar 01 13:29:13 2007 Blocked incoming ICMP packet (ICMP type 8) from
84.112.37.99 to 67.130.140.145
[INFO] Thu Mar 01 13:29:11 2007 Previous message repeated 1 time
[INFO] Thu Mar 01 13:20:16 2007 Stored configuration to non-volatile memory
[INFO] Thu Mar 01 13:20:12 2007 Policy Example 1 started; Internet access for IP address
192.168.0.100 changed to: Allowed, Web Sites - Restricted, Logged, Ports - Restricted
[INFO] Thu Mar 01 13:20:12 2007 Internet access for IP address 192.168.0.100 set to:
Allowed, Web Sites - None Blocked, Ports - None Blocked
[INFO] Thu Mar 01 13:20:12 2007 One or more Internet access policies are in effect. Internet
access will be restricted according to these policies
[INFO] Thu Mar 01 13:09:15 2007 Blocked incoming ICMP packet (ICMP type 8) from
200.92.202.36 to 67.130.140.145
[INFO] Thu Mar 01 13:09:13 2007 Previous message repeated 1 time
[INFO] Thu Mar 01 13:07:13 2007 Allowed configuration authentication by IP address
192.152.81.216
[INFO] Thu Mar 01 13:04:12 2007 Administrator logout
```

Helpful Hints...

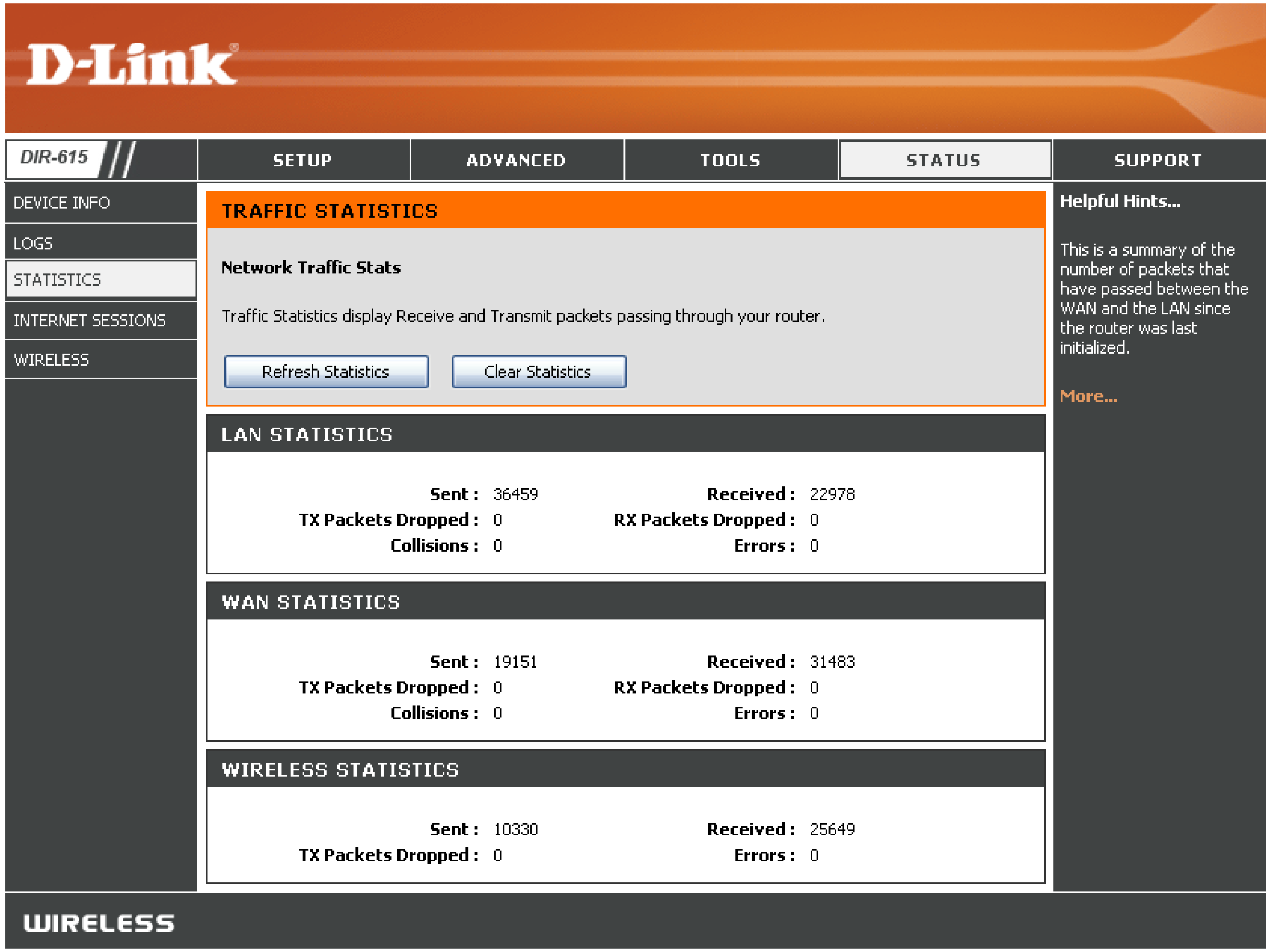
Check the log frequently to detect unauthorized network usage.

You can also have the log mailed to you periodically. Refer to Tools → EMail.

More...

Stats

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DIR-615 on both the Internet and the LAN ports. The traffic counter will reset if the device is rebooted.



TRAFFIC STATISTICS

Network Traffic Stats

Traffic Statistics display Receive and Transmit packets passing through your router.

LAN STATISTICS

Sent :	36459	**Received :**	22978
TX Packets Dropped :	0	**RX Packets Dropped :**	0
Collisions :	0	**Errors :**	0

WAN STATISTICS

Sent :	19151	**Received :**	31483
TX Packets Dropped :	0	**RX Packets Dropped :**	0
Collisions :	0	**Errors :**	0

WIRELESS STATISTICS

Sent :	10330	**Received :**	25649
TX Packets Dropped :	0	**Errors :**	0

Helpful Hints...

This is a summary of the number of packets that have passed between the WAN and the LAN since the router was last initialized.

Internet Sessions

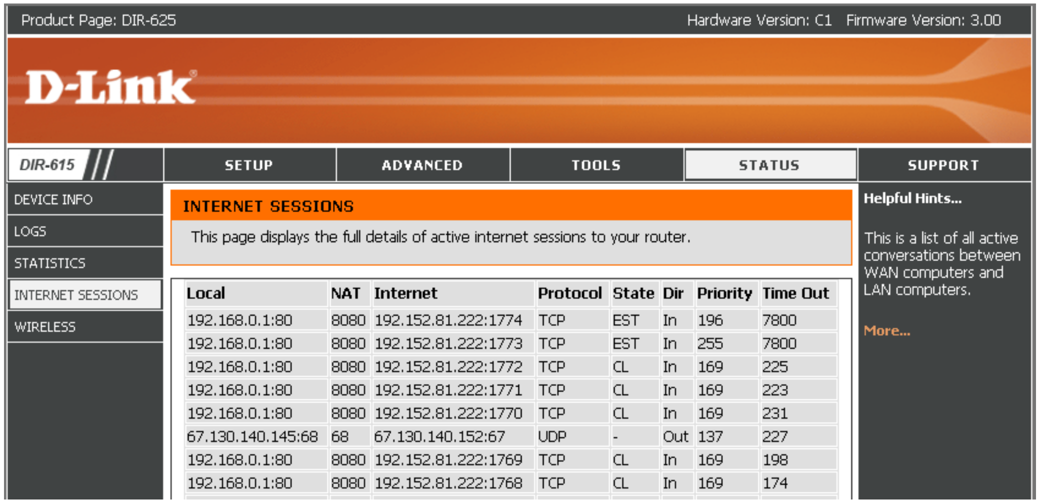
The Internet Sessions page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.

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

NAT: The port number of the LAN-side application as viewed by the WAN-side application.

Internet: The IP address and, where appropriate, port number of the application on the Internet.

Protocol: The communications protocol used for the conversation.



INTERNET SESSIONS

This page displays the full details of active internet sessions to your router.

Local	NAT	Internet	Protocol	State	Dir	Priority	Time Out
192.168.0.1:80	8080	192.152.81.222:1774	TCP	EST	In	196	7800
192.168.0.1:80	8080	192.152.81.222:1773	TCP	EST	In	255	7800
192.168.0.1:80	8080	192.152.81.222:1772	TCP	CL	In	169	225
192.168.0.1:80	8080	192.152.81.222:1771	TCP	CL	In	169	223
192.168.0.1:80	8080	192.152.81.222:1770	TCP	CL	In	169	231
67.130.140.145:68	68	67.130.140.152:67	UDP	-	Out	137	227
192.168.0.1:80	8080	192.152.81.222:1769	TCP	CL	In	169	198
192.168.0.1:80	8080	192.152.81.222:1768	TCP	CL	In	169	174

Helpful Hints...

This is a list of all active conversations between WAN computers and LAN computers.

State: State for sessions that use the TCP protocol:

NO: None -- This entry is used as a placeholder for a future connection that may occur.
SS: SYN Sent -- One of the systems is attempting to start a connection.
EST: Established -- the connection is passing data.
FW: FIN Wait -- The client system has requested that the connection be stopped.
CW: Close Wait -- The server system has requested that the connection be stopped.
TW: Time Wait -- Waiting for a short time while a connection that was in FIN Wait is fully closed.
LA: Last ACK -- Waiting for a short time while a connection that was in Close Wait is fully closed.
CL: Closed -- The connection is no longer active but the session is being tracked in case there are any retransmitted packets still pending.

The direction of initiation of the conversation:

Out - Initiated from LAN to WAN.
In - Initiated from WAN to LAN.

Dir: The preference given to outbound packets of this conversation by the QoS Engine logic. Smaller numbers represent higher priority.

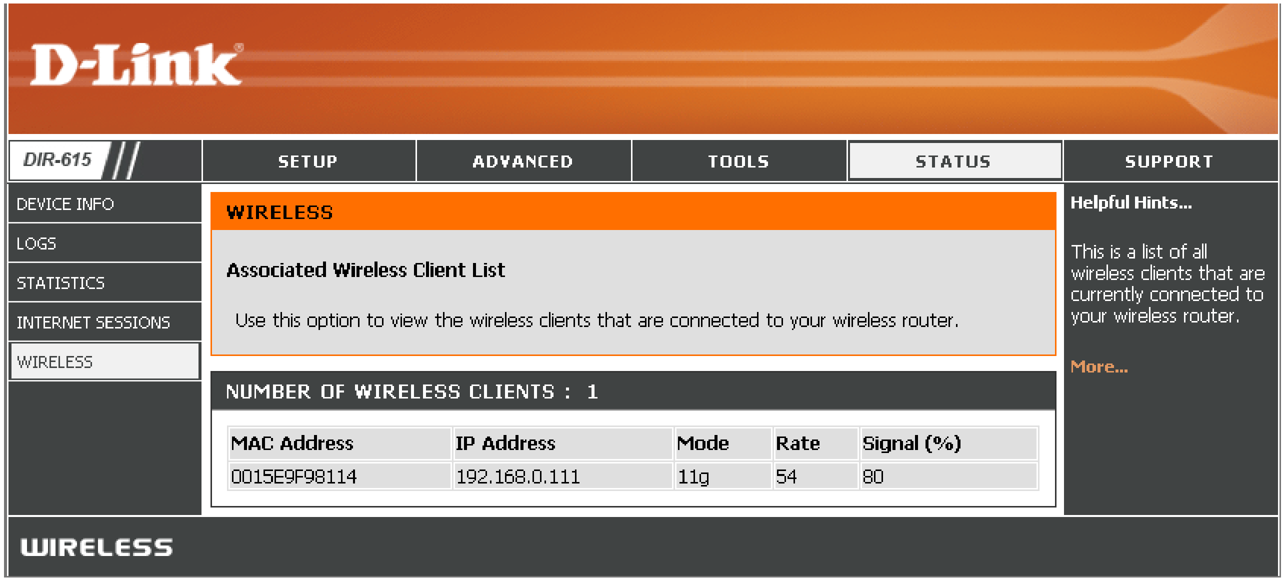
Priority: The number of seconds of idle time until the router considers the session terminated. The initial value of Time Out depends on the type and state of the connection.

Time Out:

300 seconds - UDP connections.
240 seconds - Reset or closed TCP connections. The connection does not close instantly so that lingering packets can pass or the connection can be re-established.
7800 seconds - Established or closing TCP connections.

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.



WIRELESS

Associated Wireless Client List

Use this option to view the wireless clients that are connected to your wireless router.

NUMBER OF WIRELESS CLIENTS : 1

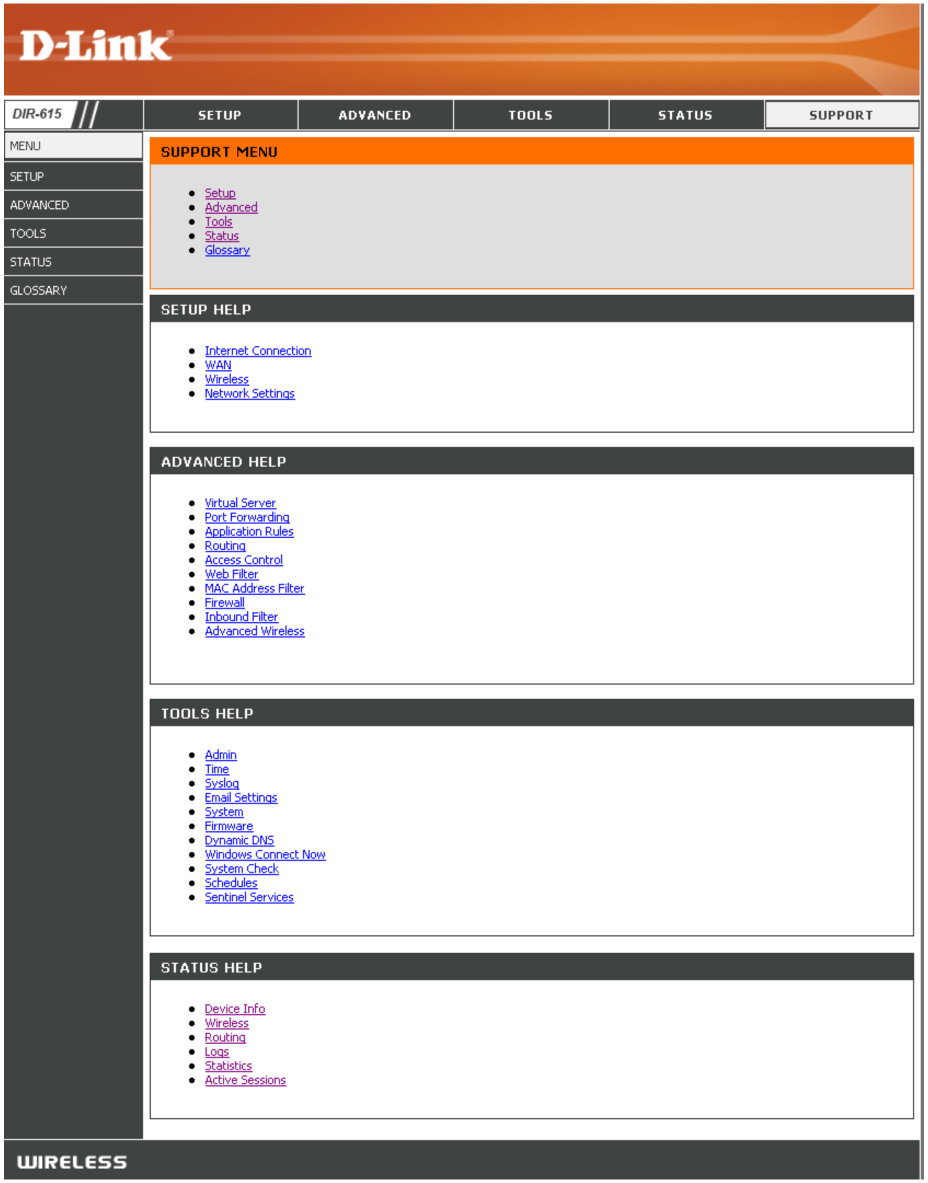
MAC Address	IP Address	Mode	Rate	Signal (%)
0015E9F98114	192.168.0.111	11g	54	80

Helpful Hints...

This is a list of all wireless clients that are currently connected to your wireless router.

WIRELESS

Support



SUPPORT MENU

- Setup
- Advanced
- Tools
- Status
- Glossary

SETUP HELP

- Internet Connection
- WAN
- Wireless
- Network Settings

ADVANCED HELP

- Virtual Server
- Port Forwarding
- Application Rules
- Routing
- Access Control
- Web Filter
- MAC Address Filter
- Firewall
- Inbound Filter
- Advanced Wireless

TOOLS HELP

- Admin
- Time
- Syslog
- Email Settings
- System
- Firmware
- Dynamic DNS
- Windows Connect Now
- System Check
- Schedules
- Sentinel Services

STATUS HELP

- Device Info
- Wireless
- Routing
- Logs
- Statistics
- Active Sessions

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-615 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WEP (Wired Equivalent Privacy)
- WPA2-PSK(Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

What is WEP?

WEP stands for Wired Equivalent Privacy. It is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. WEP provides security by encrypting data over your wireless network so that it is protected as it is transmitted from one wireless device to another.

To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange – alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.

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.

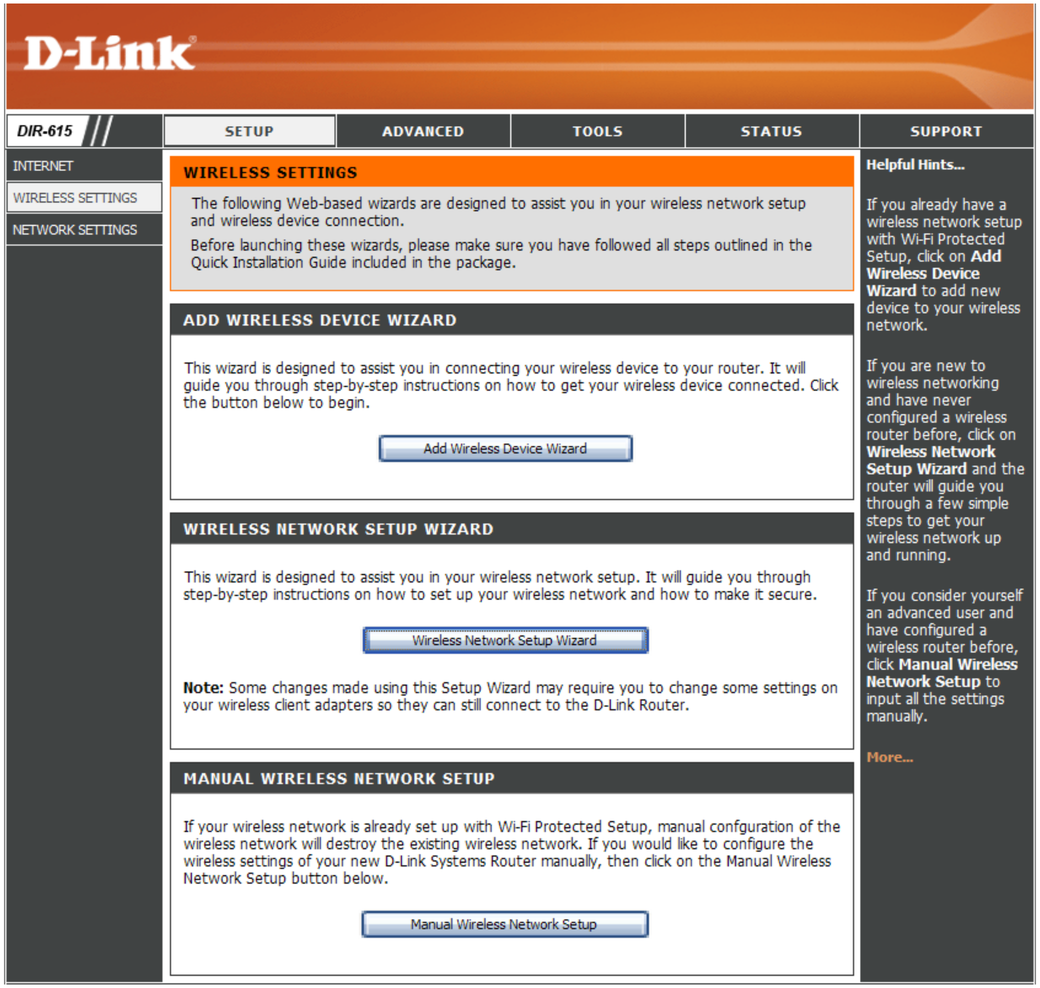
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key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

To run the security wizard, browse to the Setup page and then click the **Launch Wireless Security Setup Wizard**



WIRELESS SETTINGS

The following Web-based wizards are designed to assist you in your wireless network setup and wireless device connection.

Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

ADD WIRELESS DEVICE WIZARD

This wizard is designed to assist you in connecting your wireless device to your router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

WIRELESS NETWORK SETUP WIZARD

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the D-Link Router.

MANUAL WIRELESS NETWORK SETUP

If your wireless network is already set up with Wi-Fi Protected Setup, manual confguration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your new D-Link Systems Router manually, then click on the Manual Wireless Network Setup button below.

Helpful Hints...

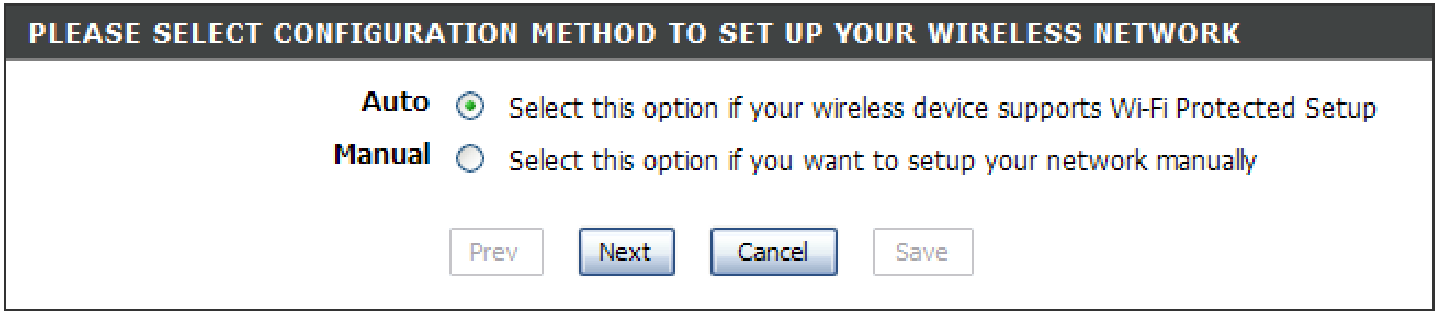
If you already have a wireless network setup with Wi-Fi Protected Setup, click on **Add Wireless Device Wizard** to add new device to your wireless network.

If you are new to wireless networking and have never configured a wireless router before, click on **Wireless Network Setup Wizard** and the router will guide you through a few simple steps to get your wireless network up and running.

If you consider yourself an advanced user and have configured a wireless router before, click **Manual Wireless Network Setup** to input all the settings manually.

Auto: Select to auto generate your wireless security settings. This option can be used when using a wireless adapter that supports Wi-Fi Protected Setup.

Manual: Select this option to run the wireless setup wizard which will guide you to configure your wireless settings. Skip to page 73.



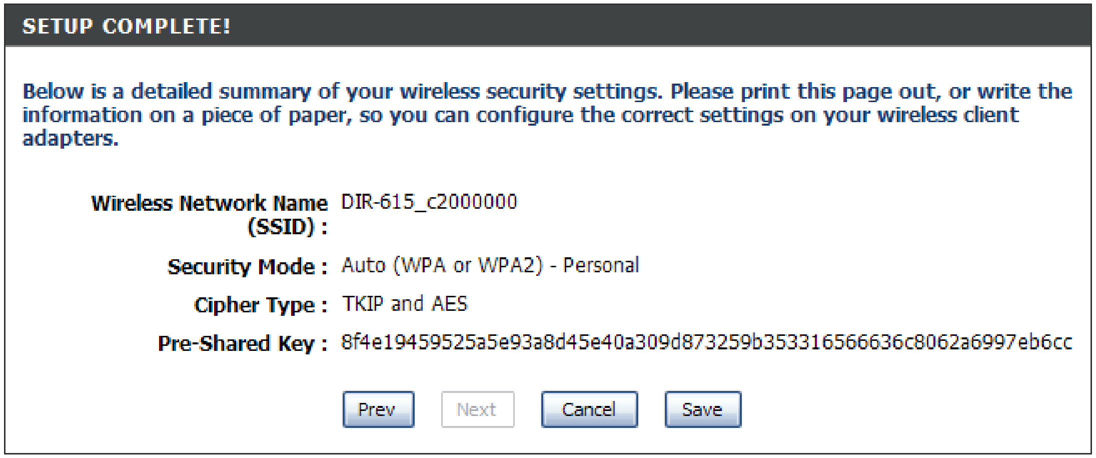
PLEASE SELECT CONFIGURATION METHOD TO SET UP YOUR WIRELESS NETWORK

Auto ● Select this option if your wireless device supports Wi-Fi Protected Setup

Manual ○ Select this option if you want to setup your network manually

Wireless Wizard - Auto

The router has automatically generated your wireless settings. Please write down and keep this information for your reference. Click **Save**.

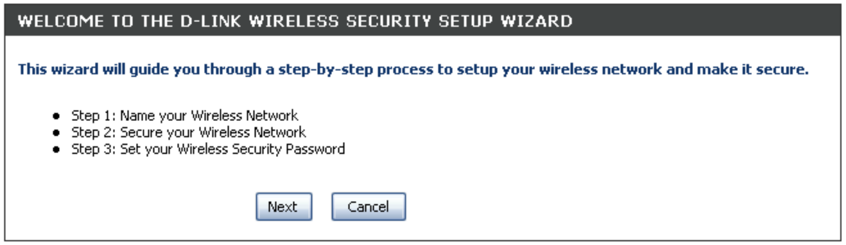


SETUP COMPLETE!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Wireless Network Name (SSID) :	DIR-615_c2000000
Security Mode :	Auto (WPA or WPA2) - Personal
Cipher Type :	TKIP and AES
Pre-Shared Key :	8f4e19459525a5e93a8d45e40a309d873259b353316566636c8062a6997eb6cc

Click **Next** to continue.

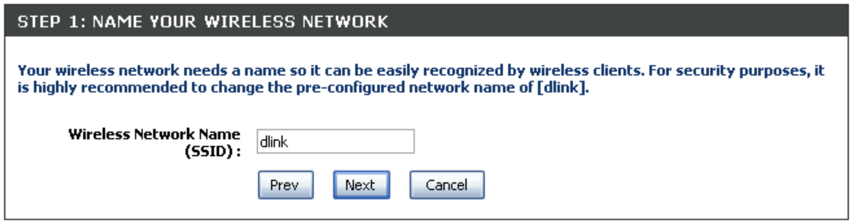


WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

This wizard will guide you through a step-by-step process to setup your wireless network and make it secure.

- Step 1: Name your Wireless Network
- Step 2: Secure your Wireless Network
- Step 3: Set your Wireless Security Password

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.



STEP 1: NAME YOUR WIRELESS NETWORK

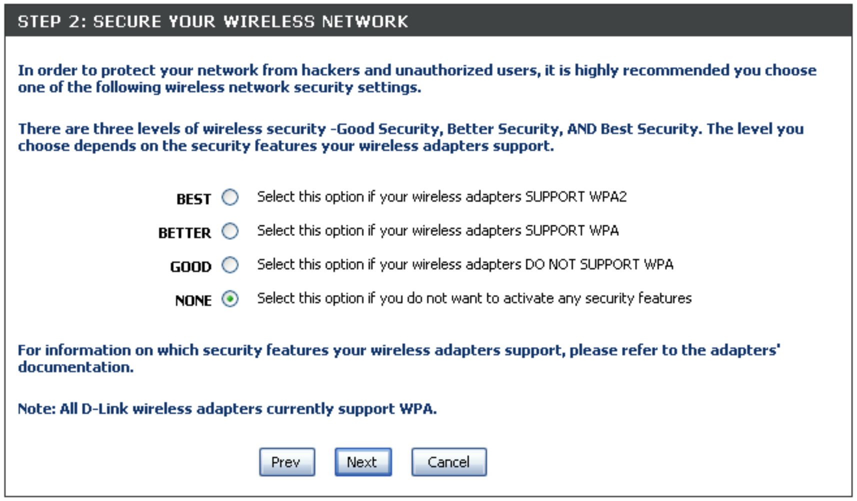
Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name of [dlink].

Wireless Network Name (SSID) : dlink

Select the level of security for your wireless network:

- Best - WPA2 Authentication
- Better - WPA Authentication
- Good - WEP Encryption
- None - No security

Click **Next** to continue.



STEP 2: SECURE YOUR WIRELESS NETWORK

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

There are three levels of wireless security -Good Security, Better Security, AND Best Security. The level you choose depends on the security features your wireless adapters support.

BEST ○ Select this option if your wireless adapters SUPPORT WPA2

BETTER ○ Select this option if your wireless adapters SUPPORT WPA

GOOD ○ Select this option if your wireless adapters DO NOT SUPPORT WPA

NONE ● Select this option if you do not want to activate any security features

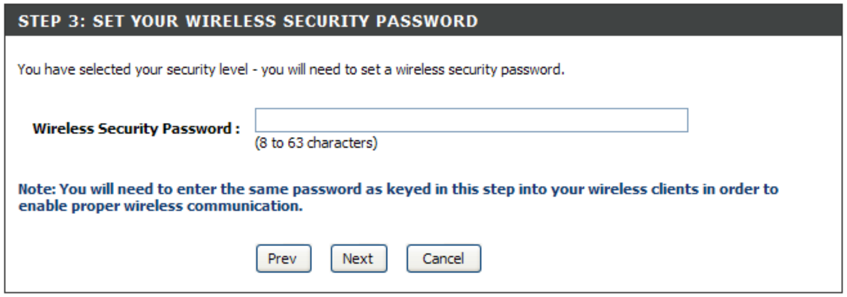
For information on which security features your wireless adapters support, please refer to the adapters' documentation.

Note: All D-Link wireless adapters currently support WPA.

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.



STEP 3: SET YOUR WIRELESS SECURITY PASSWORD

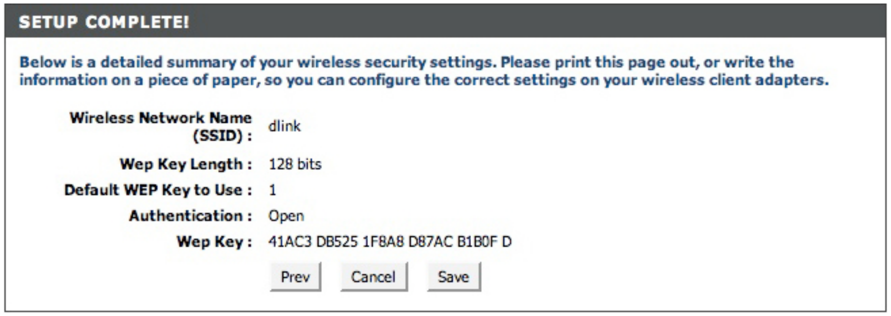
You have selected your security level - you will need to set a wireless security password.

Wireless Security Password : (8 to 63 characters)

Note: You will need to enter the same password as keyed in this step into your wireless clients in order to enable proper wireless communication.

If you selected Good, the following screen will show you your WEP key to enter on your wireless clients.

Click **Save** to finish the Security Wizard.



SETUP COMPLETE!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Wireless Network Name (SSID) : dlink

Wep Key Length : 128 bits

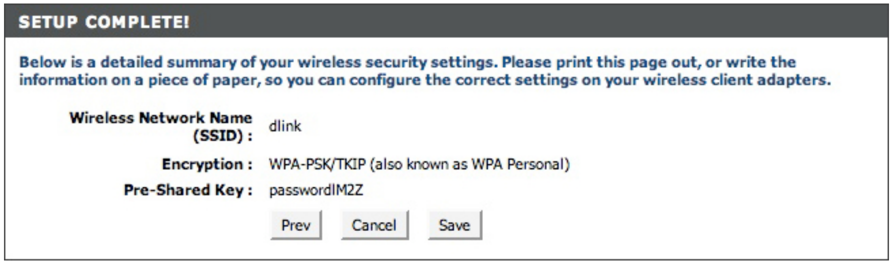
Default WEP Key to Use : 1

Authentication : Open

Wep Key : 41AC3 DB525 1F8A8 D87AC B1B0F D

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.



SETUP COMPLETE!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

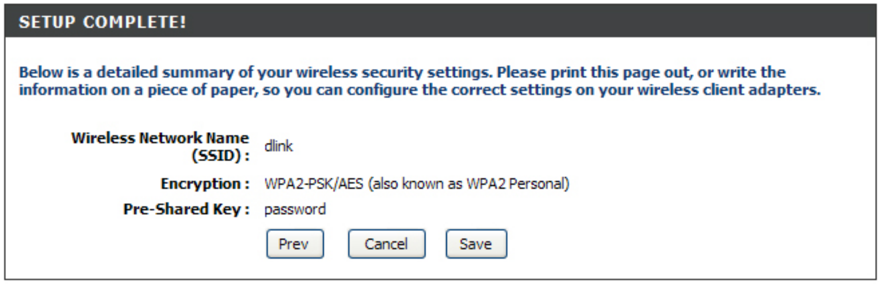
Wireless Network Name (SSID) : dlink

Encryption : WPA-PSK/TKIP (also known as WPA Personal)

Pre-Shared Key : passwordIM2Z

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.



SETUP COMPLETE!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Wireless Network Name (SSID) : dlink

Encryption : WPA2-PSK/AES (also known as WPA2 Personal)

Pre-Shared Key : password

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

Configure WEP

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 **WEP**.

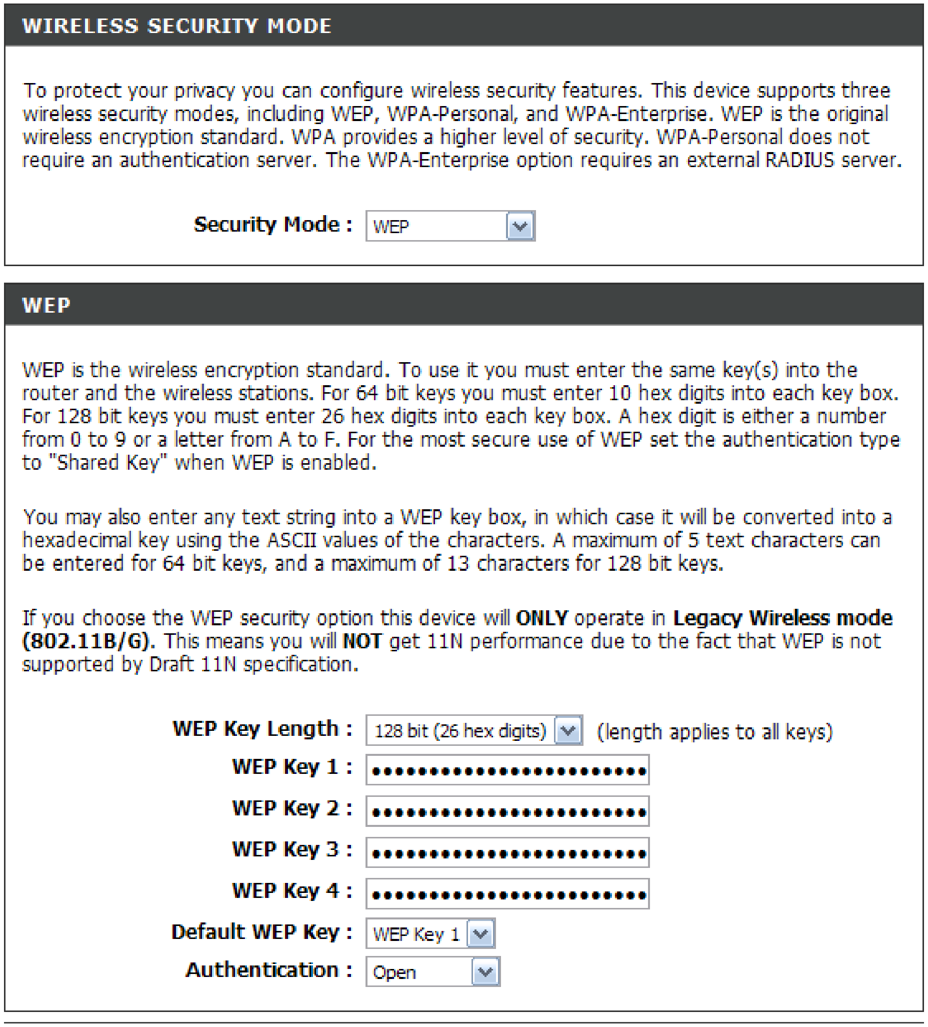
3. Next to *WEP Key Length*, select the level of encryption (64 or 128-bit).

   Hex - (recommended) Letters A-F and numbers 0-9 are valid.

4. Next to *WEP Key 1*, enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to 4 different keys.

5. Next to *Authentication*, select **Shared Key**.

6. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the router.



WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WEP

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G).** This means you will **NOT** get 11N performance due to the fact that WEP is not supported by Draft 11N specification.

WEP Key Length : 128 bit (26 hex digits) (length applies to all keys)
WEP Key 1 : ••••••••••••••••••••••••••
WEP Key 2 : ••••••••••••••••••••••••••
WEP Key 3 : ••••••••••••••••••••••••••
WEP Key 4 : ••••••••••••••••••••••••••
Default WEP Key : WEP Key 1
Authentication : Open

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**.

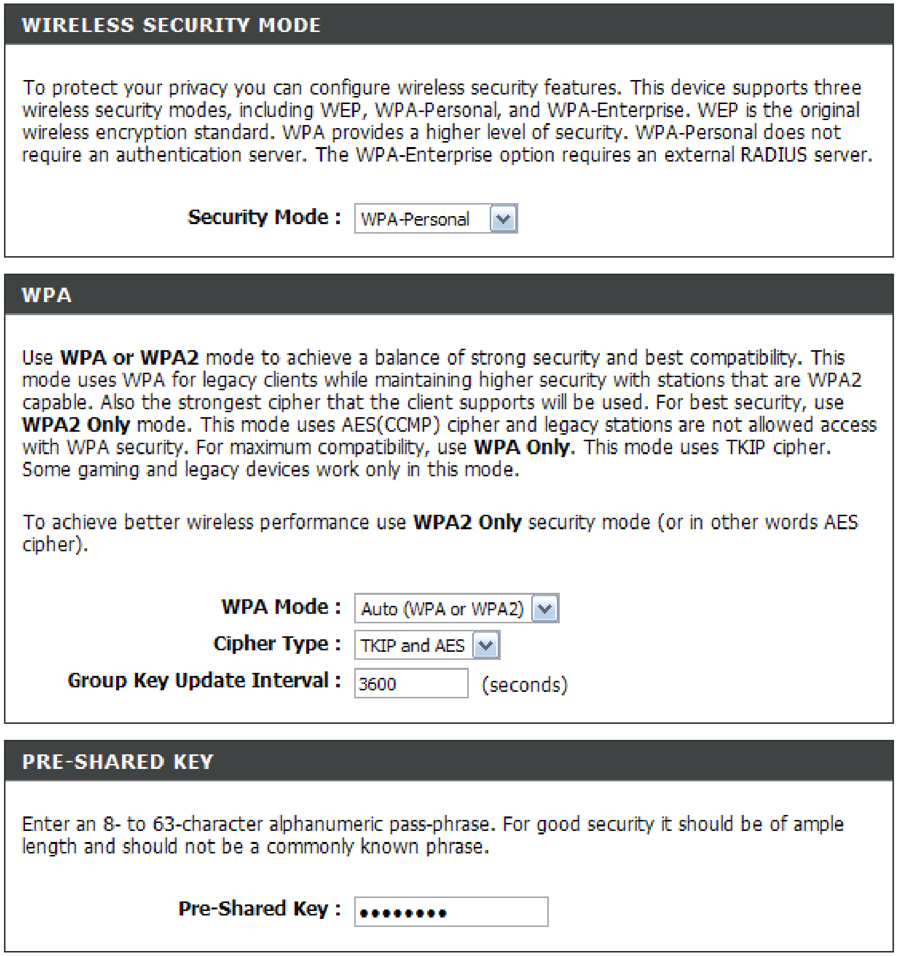
3. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.

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.



WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WPA-Personal

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto (WPA or WPA2)

Cipher Type : TKIP and AES

Group Key Update Interval : 3600 (seconds)

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key : ••••••••

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**.

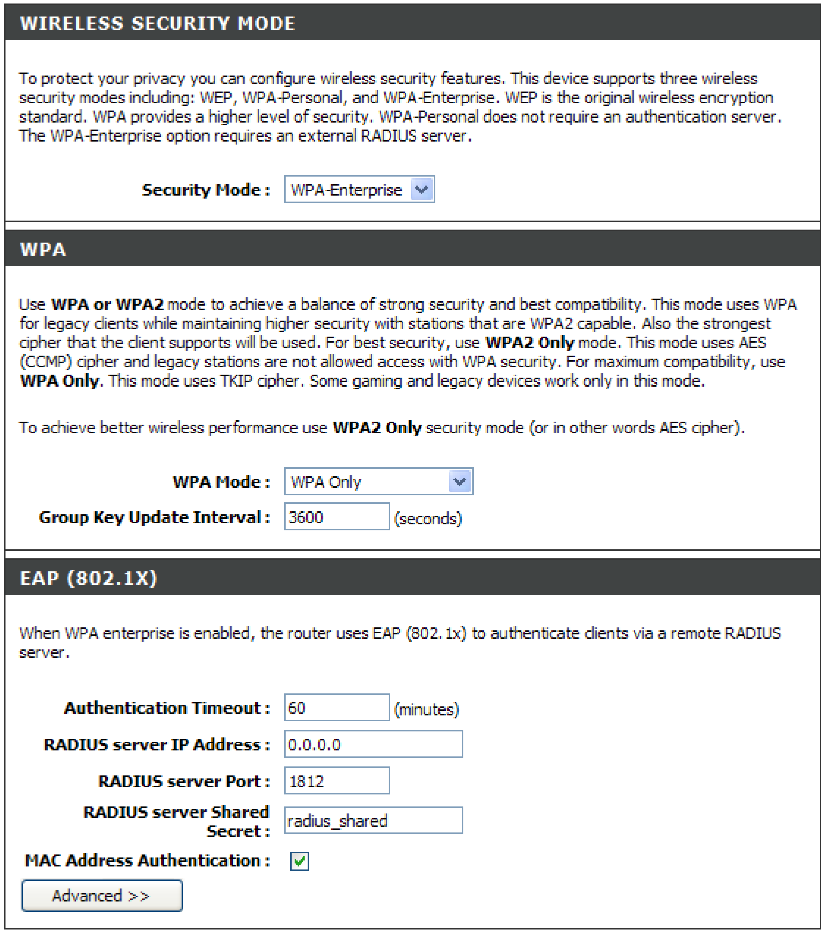
3. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.

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.



WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WPA-Enterprise

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES (CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : WPA Only

Group Key Update Interval : 3600 (seconds)

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 : ☑

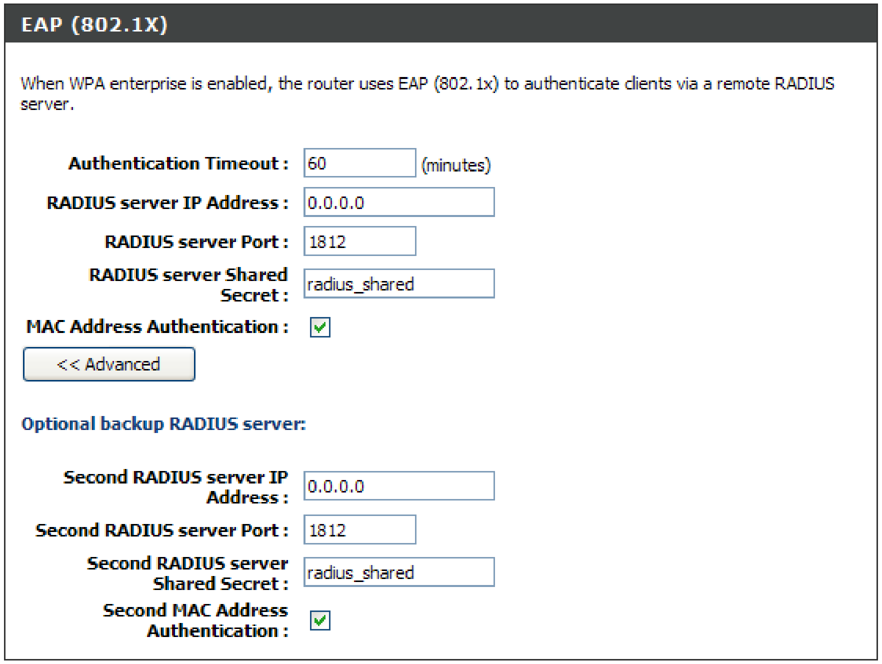
8. Next to *RADIUS Server Port*, enter the port you are using with your RADIUS server. 1812 is the default port.

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

10. If the *MAC Address Authentication* box is selected then the user will need to connect from the same computer whenever logging into the wireless network.

11. Click **Advanced** to enter settings for a secondary RADIUS Server.

12. Click **Apply Settings** to save your settings.



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 :	☑

Optional backup RADIUS server:

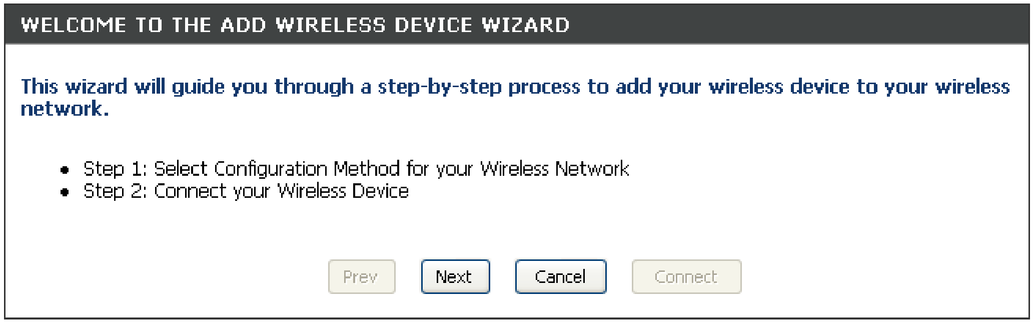
Second RADIUS server IP Address :	0.0.0.0
Second RADIUS server Port :	1812
Second RADIUS server Shared Secret :	radius_shared
Second MAC Address Authentication :	☑

Connect to a Wireless Network

Add Wireless Device Wizard

This feature allows you to add any wireless devices that support Wi-Fi Protected Setup (WPS).

Click **Next**.

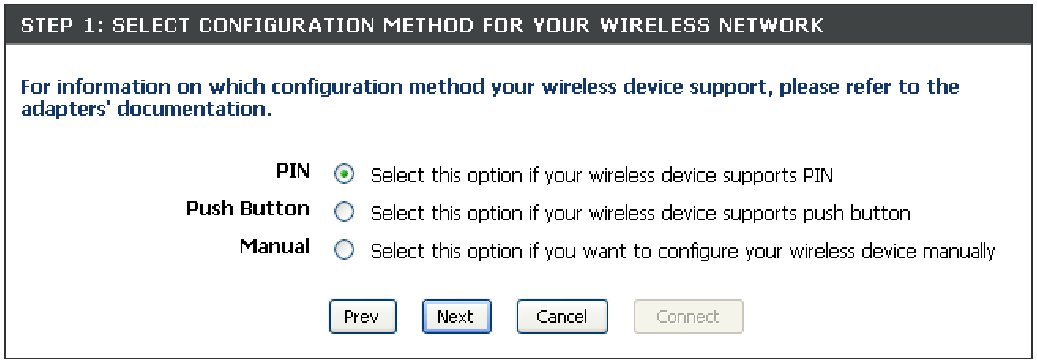


WELCOME TO THE ADD WIRELESS DEVICE WIZARD

This wizard will guide you through a step-by-step process to add your wireless device to your wireless network.

- Step 1: Select Configuration Method for your Wireless Network
- Step 2: Connect your Wireless Device

Select the method you would like to use for adding a new wireless device onto your wireless network.



STEP 1: SELECT CONFIGURATION METHOD FOR YOUR WIRELESS NETWORK

For information on which configuration method your wireless device support, please refer to the adapters' documentation.

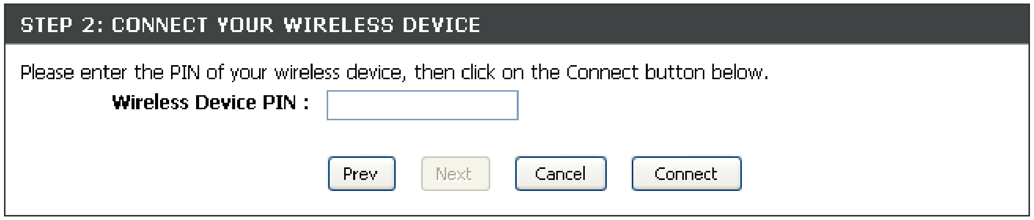
PIN ● Select this option if your wireless device supports PIN

Push Button ○ Select this option if your wireless device supports push button

Manual ○ Select this option if you want to configure your wireless device manually

PIN: PIN requires you to enter your wireless device's PIN information.

Enter the wireless device's PIN information in the box and click on **Connect**.



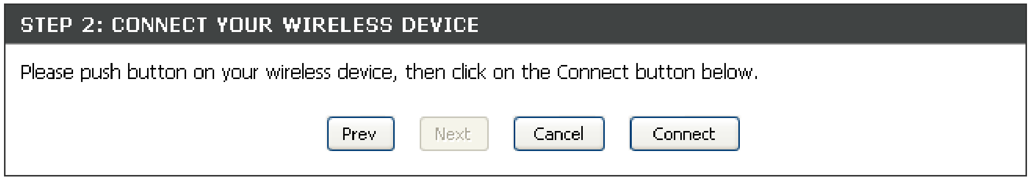
STEP 2: CONNECT YOUR WIRELESS DEVICE

Please enter the PIN of your wireless device, then click on the Connect button below.

Wireless Device PIN :

Push Button: Push button allows you to connect a wireless device onto your wireless network through button press method.

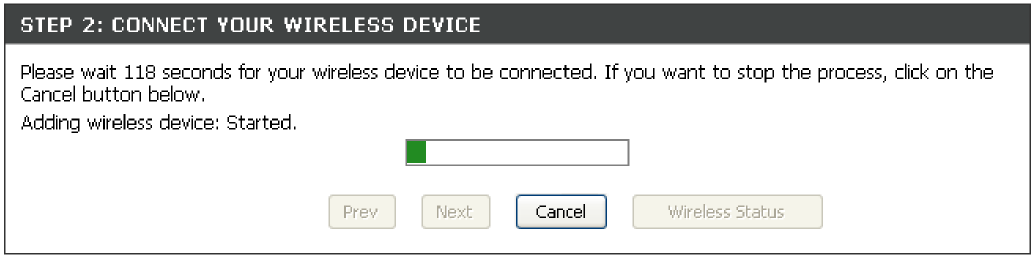
Click on **Connect** button when you are ready.



STEP 2: CONNECT YOUR WIRELESS DEVICE

Please push button on your wireless device, then click on the Connect button below.

To successfully add a new wireless device, you would have to enter either the PIN information or the button must be pressed within 120 seconds.

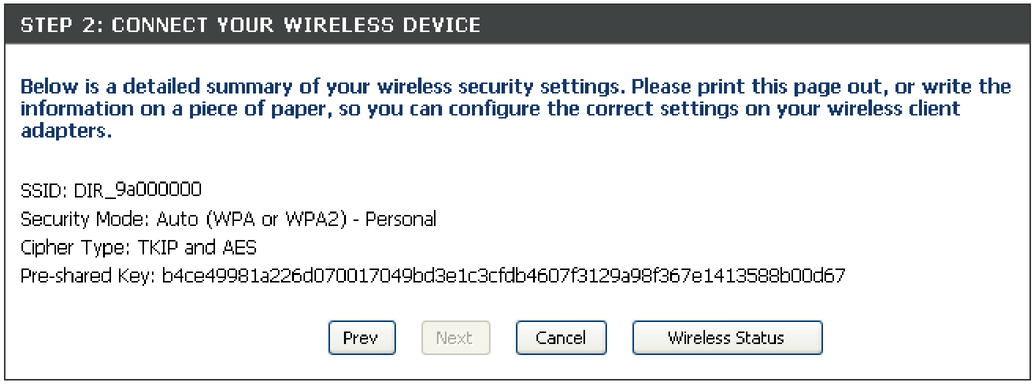


STEP 2: CONNECT YOUR WIRELESS DEVICE

Please wait 118 seconds for your wireless device to be connected. If you want to stop the process, click on the Cancel button below.

Adding wireless device: Started.

Manual: Use this option if you uncertain if your wireless device support WPS, it will display your current wireless settings.



STEP 2: CONNECT YOUR WIRELESS DEVICE

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

SSID: DIR_9a000000

Security Mode: Auto (WPA or WPA2) - Personal

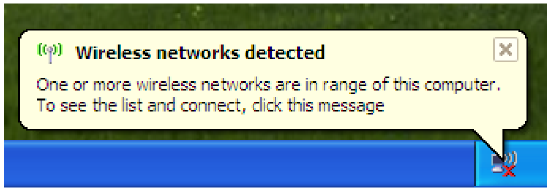
Cipher Type: TKIP and AES

Pre-shared Key: b4ce49981a226d070017049bd3e1c3cfdb4607f3129a98f367e1413588b00d67

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.

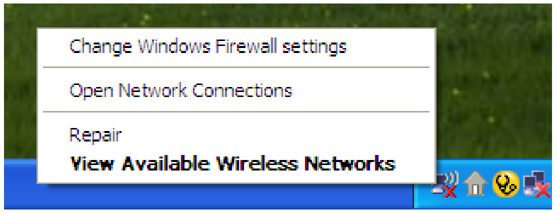


Wireless networks detected

One or more wireless networks are in range of this computer. To see the list and connect, click this message

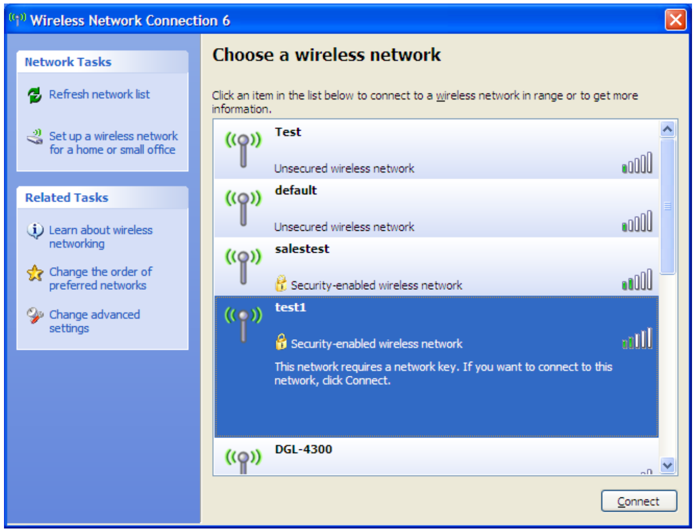
or

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


Change Windows Firewall settings
Open Network Connections
Repair
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.


Wireless Network Connection 6
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Test
Unsecured wireless network

default
Unsecured wireless network

salestest
Security-enabled wireless network

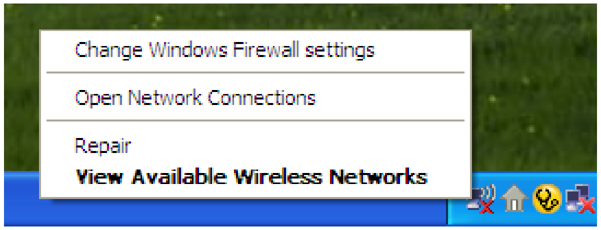
test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

DGL-4300

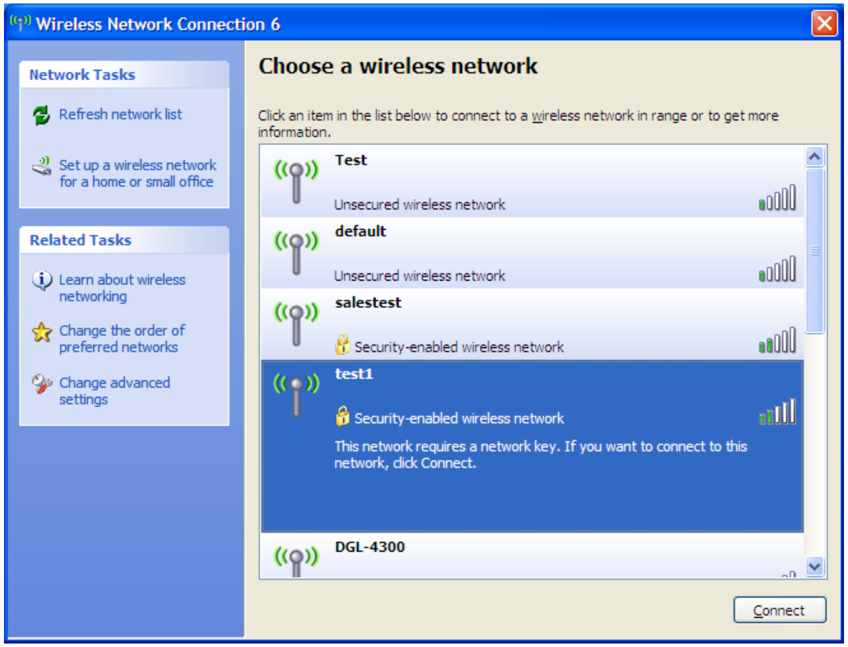
Configure WEP

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**.


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks

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

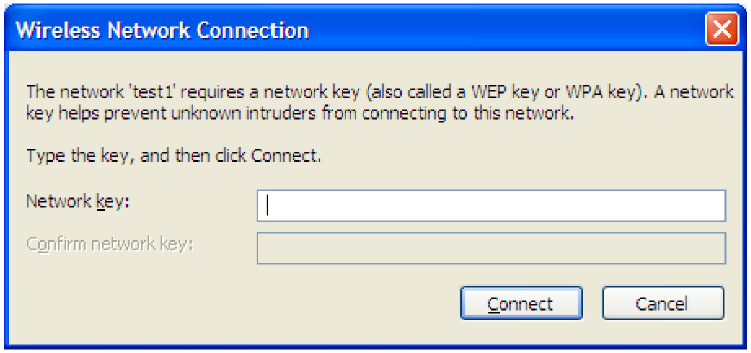

Wireless Network Connection 6
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Test
Unsecured wireless network
default
Unsecured wireless network
salestest
Security-enabled wireless network
test1
Security-enabled wireless network
DGL-4300
Connect

Click an item in the list below to connect to a wireless network in range or to get more information.

This network requires a network key. If you want to connect to this network, click Connect.

3. The **Wireless Network Connection** box will appear. Enter the same WEP key 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 WEP settings are correct. The WEP key must be exactly the same as on the wireless router.



Wireless Network Connection

The network 'test1' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

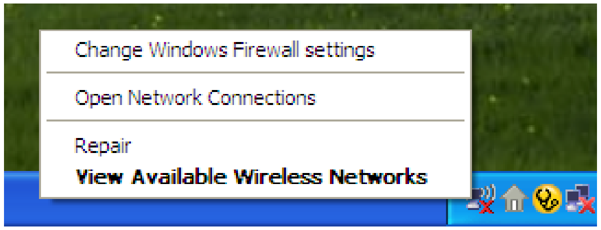
Network key:

Confirm network key:

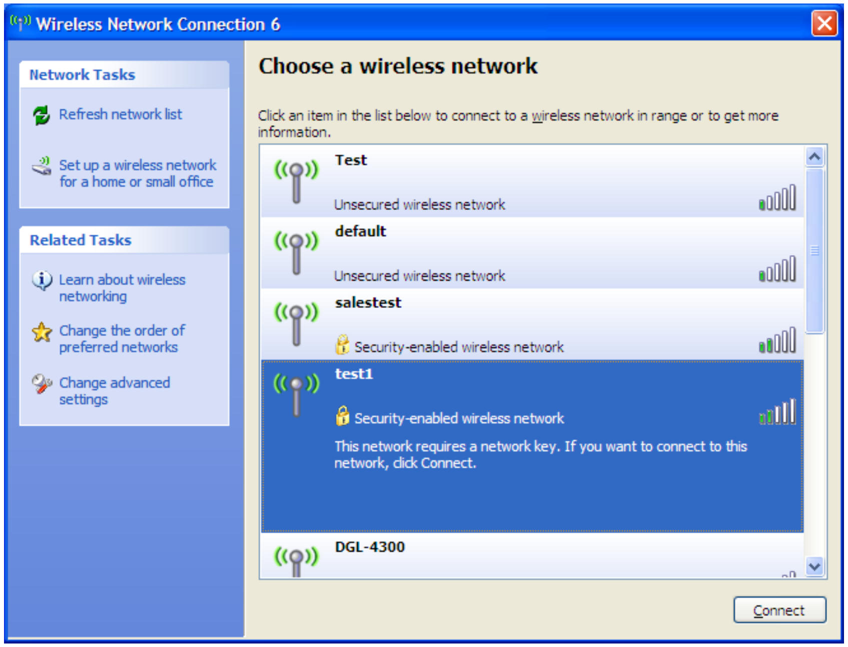
Configure WPA-PSK

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**.


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks

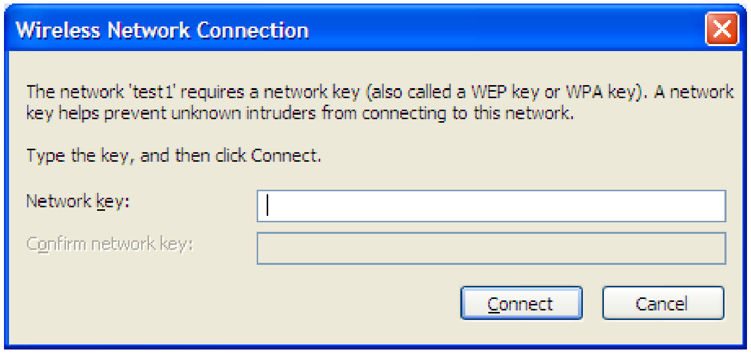
2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.


Wireless Network Connection 6
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Test
Unsecured wireless network
default
Unsecured wireless network
salestest
Security-enabled wireless network
test1
Security-enabled wireless network
DGL-4300
Connect

Click an item in the list below to connect to a wireless network in range or to get more information.

This network requires a network key. If you want to connect to this network, click Connect.

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



Wireless Network Connection

The network 'test1' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key:

Confirm network key:

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-615. 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).

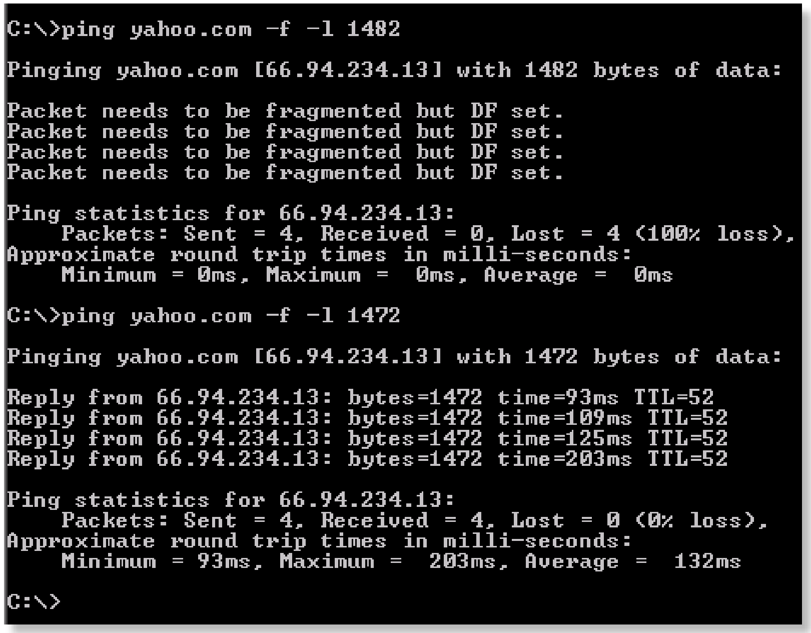
Note: AOL DSL+ users must use MTU of 1400.

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**



```
C:\>ping yahoo.com -f -l 1482

Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:

Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ping yahoo.com -f -l 1472

Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:

Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum =  203ms, Average =  132ms

C:\>
```

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.