Schedules

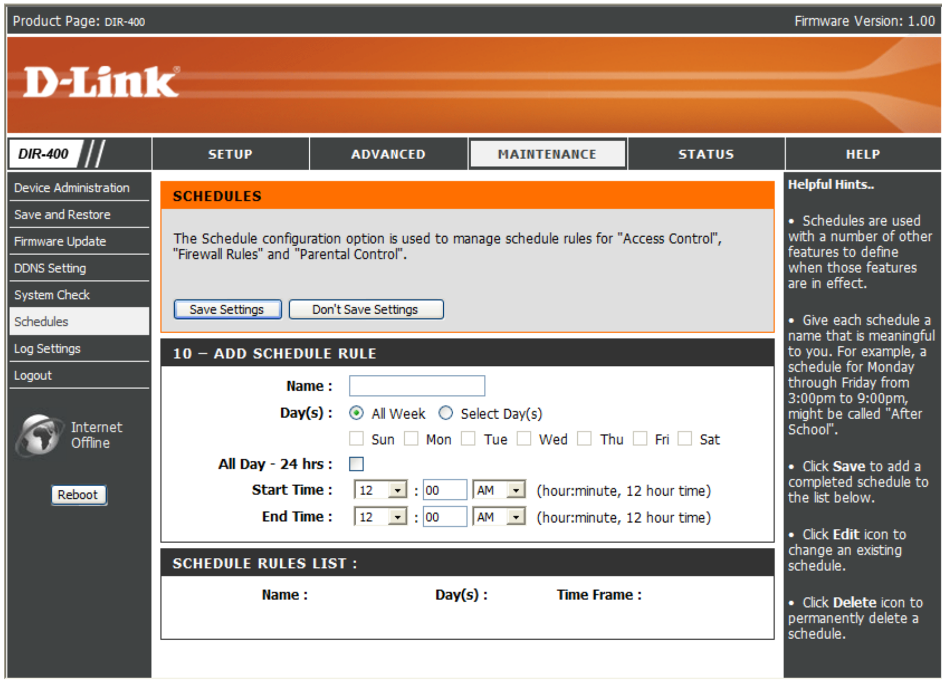
The Schedules screen allows the user to manage schedule rules for various firewall and parental control features. Once you have finished configuring or creating a schedule rule, click the **Save Settings** button at the top of the window.

Name: Enter a name for the new schedule rule.

Day(s): Choose All Week to have the schedule run every day, or choose Select Day(s) to have the schedule run only on particular days. If Select Day(s) is selected, please use the checkboxes directly below to specify the individual days.

All Day - 24 hrs: Tick this check box if the new schedule rule applies to the full 24-hour period for the days selected.

Start Time/ End Time: If the new schedule rule does not apply to the full 24-hour period, make sure the All Day - 24 hrs checkbox is unticked and enter a specific beginning and ending time for the schedule to run.



SCHEDULES

The Schedule configuration option is used to manage schedule rules for "Access Control", "Firewall Rules" and "Parental Control".

10 – ADD SCHEDULE RULE

Name :

Day(s) : ● All Week ○ Select Day(s)

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

All Day - 24 hrs : □

Start Time : 12 : 00 AM (hour:minute, 12 hour time)

End Time : 12 : 00 AM (hour:minute, 12 hour time)

SCHEDULE RULES LIST :

Name : **Day(s) :** **Time Frame :**

Helpful Hints..

- Schedules are used with a number of other features to define when those features are in effect.
- Give each schedule a name that is meaningful to you. For example, a schedule for Monday through Friday from 3:00pm to 9:00pm, might be called "After School".
- Click **Save** to add a completed schedule to the list below.
- Click **Edit** icon to change an existing schedule.
- Click **Delete** icon to permanently delete a schedule.

Log Settings

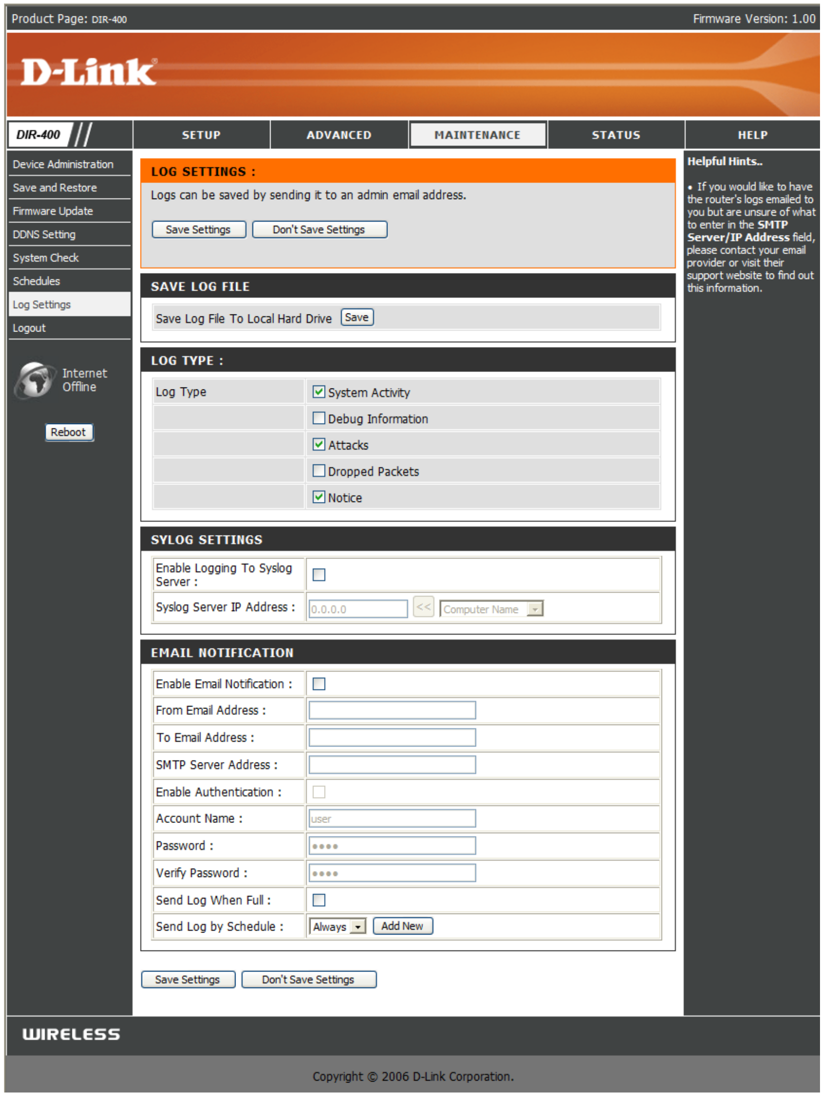
The system log displays chronological event log data specified by the router user. You can customize what data is logged and then save the log to disk. You can also send log information to a syslog server, or have the log sent to an e-mail address.

Save Log File: Click on the **Save** button link on this window to save the current log file to your local hard drive.

Log Type: Tick the checkbox(es) to specify what information will be logged: System Activity, Debug Information, Attacks, Dropped Packets, and Notice.

Enable Logging To Syslog Server: This allows the router to send log information to a syslog server, which can be used to monitor your router's activities. To enable this feature, tick the checkbox.

Enter the IP address of the server in this box. If the syslog server is internal to your network, you can use the dropdown box (Computer Name) to automatically enter the IP address of the computer acting as your syslog server. To do so, select a computer from the dropdown box, then click the **<<** button.



LOG SETTINGS :

Logs can be saved by sending it to an admin email address.

SAVE LOG FILE

Save Log File To Local Hard Drive

LOG TYPE :

Log Type	☑ System Activity
	□ Debug Information
	☑ Attacks
	□ Dropped Packets
	☑ Notice

SYLOG SETTINGS

Enable Logging To Syslog Server :	□
Syslog Server IP Address :	0.0.0.0 << Computer Name

EMAIL NOTIFICATION

Enable Email Notification :	□
From Email Address :	
To Email Address :	
SMTP Server Address :	
Enable Authentication :	□
Account Name :	user
Password :	••••
Verify Password :	••••
Send Log When Full :	□
Send Log by Schedule :	Always Add New

Helpful Hints..

- If you would like to have the router's logs emailed to you but are unsure of what to enter in the **SMTP Server/IP Address** field, please contact your email provider or visit their support website to find out this information.

Copyright © 2006 D-Link Corporation.

Log Settings - Email Notification

Email notification is a feature that sends the router log to a specified e-mail address. Log updates will be sent to the specified e-mail address automatically in 5 minute intervals, or when the log becomes full. You can also send logs according to a set schedule you can define.

Enable Email Notification: To enable e-mail notification, tick this checkbox.

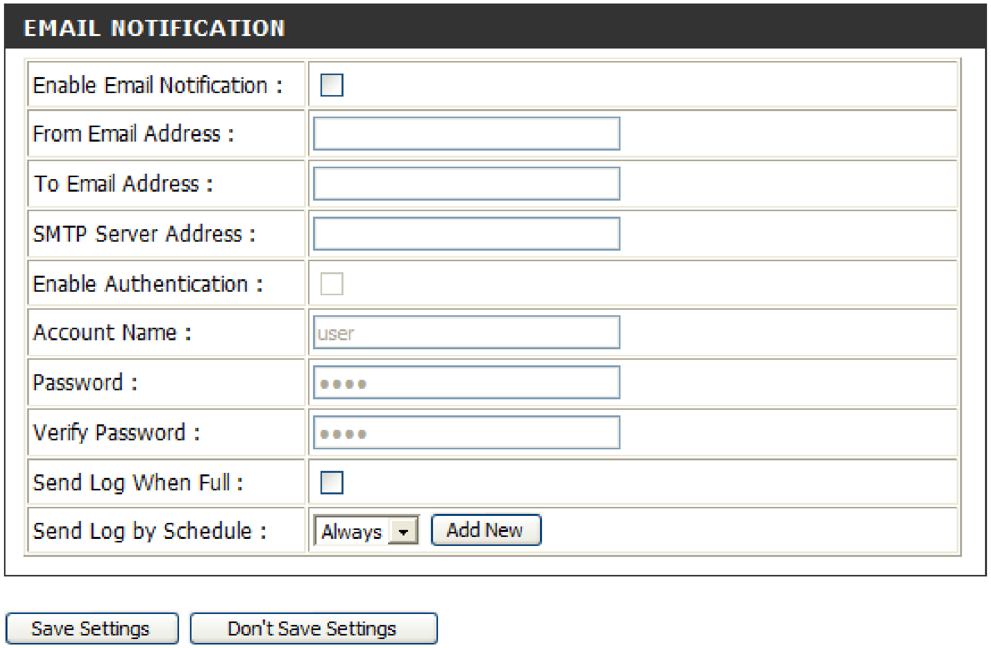
From Email Address: Enter the e-mail address you want to appear in the *From:* field when sending an e-mail of the log.

To Email Address: Enter the e-mail address you want the log to be sent to.

SMTP Server Address: Enter the name of the SMTP mail server that you want to use to send your e-mails through.

Enable Authentication: Tick this checkbox if your SMTP mail server requires authentication.

Account Name: If your SMTP server requires authentication, enter your account's user name in this box.



EMAIL NOTIFICATION

Enable Email Notification :	□
From Email Address :	
To Email Address :	
SMTP Server Address :	
Enable Authentication :	□
Account Name :	user
Password :	••••
Verify Password :	••••
Send Log When Full :	□
Send Log by Schedule :	Always ▾ Add New

Password / Verify Password: If your SMTP server requires authentication, enter your account's password in this box, and enter it again in the Verify Password box.

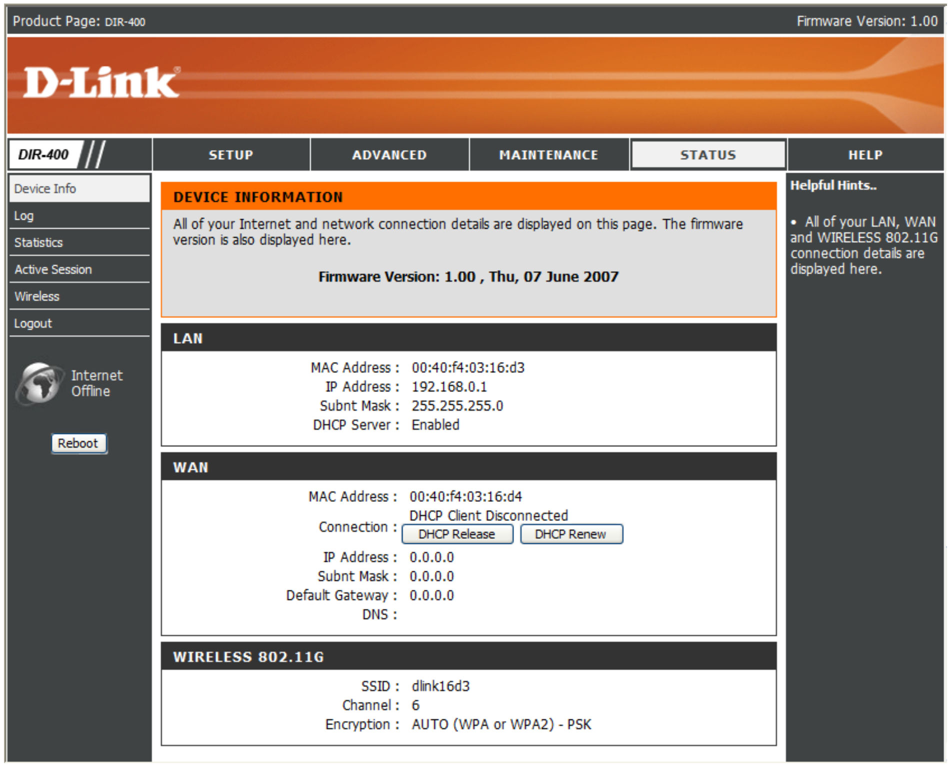
Send Log When Full: Ticking this box will set the router to e-mail the log only when the log becomes full. When this feature is enabled, you cannot use the Send Log by Schedule feature.

Send Log by Schedule: This lets you select a schedule that will be used to determine when router logs will be sent. During the time specified by your schedule, logs will be sent to your e-mail address in 5 minute intervals. To set a schedule, you must untick the Send Log When Full checkbox.

Device Information

This window displays the current information for the DIR-400. It will display LAN, WAN, and Wireless information.

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



DEVICE INFORMATION

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

Firmware Version: 1.00 , Thu, 07 June 2007

LAN

MAC Address : 00:40:f4:03:16:d3
IP Address : 192.168.0.1
Subnt Mask : 255.255.255.0
DHCP Server : Enabled

WAN

MAC Address : 00:40:f4:03:16:d4
Connection : DHCP Client Disconnected
IP Address : 0.0.0.0
Subnt Mask : 0.0.0.0
Default Gateway : 0.0.0.0
DNS :

WIRELESS 802.11G

SSID : dlink16d3
Channel : 6
Encryption : AUTO (WPA or WPA2) - PSK

Helpful Hints..

- All of your LAN, WAN and WIRELESS 802.11G connection details are displayed here.

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

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

Wireless 802.11G: Displays the wireless MAC address and your wireless settings such as SSID, Channel, and Encryption status.

Log

This window allows you to view a log of activities on the router. This is especially helpful for detecting unauthorized network usage.

First Page: View the first page of the log.

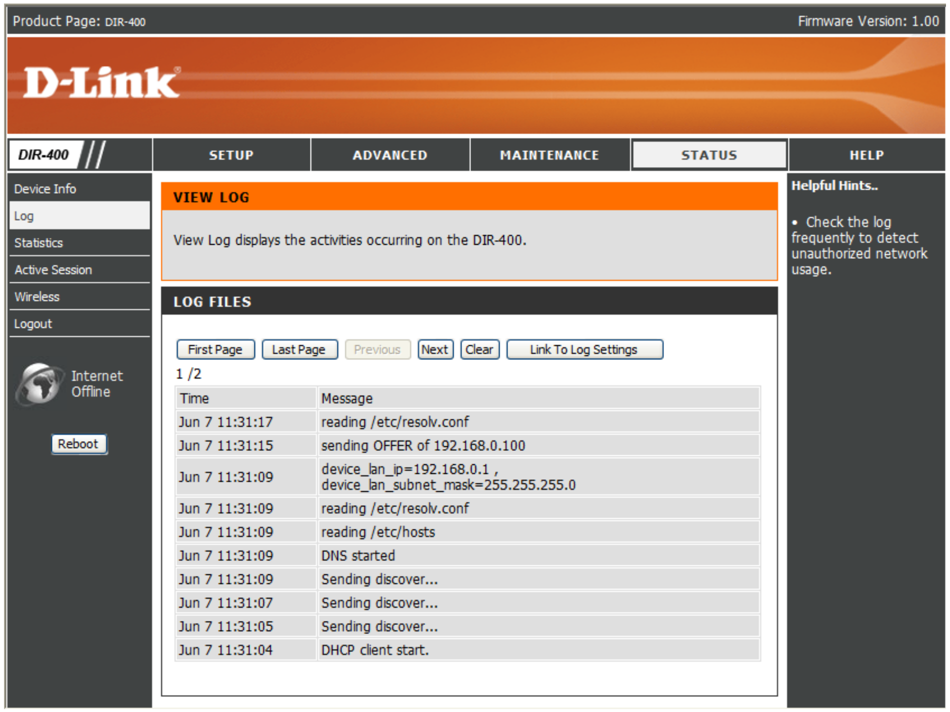
Last Page: View the last page of the log.

Previous: View the previous page.

Next: View the next page.

Clear: Clear the log.

Link to Log Settings: Click this button to go directly to the Log Settings window (**Maintenance** > **Log Settings**).



Product Page: DIR-400

Firmware Version: 1.00

VIEW LOG

View Log displays the activities occurring on the DIR-400.

LOG FILES

1 /2

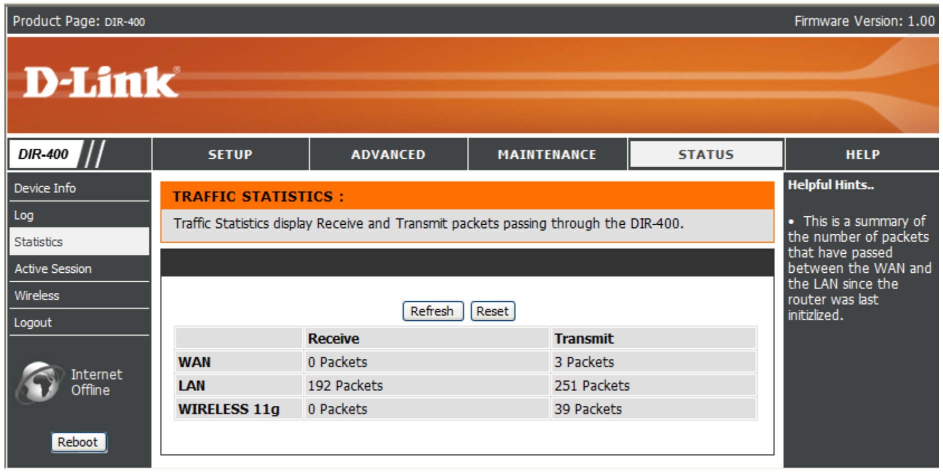
Time	Message
Jun 7 11:31:17	reading /etc/resolv.conf
Jun 7 11:31:15	sending OFFER of 192.168.0.100
Jun 7 11:31:09	device_lan_ip=192.168.0.1 , device_lan_subnet_mask=255.255.255.0
Jun 7 11:31:09	reading /etc/resolv.conf
Jun 7 11:31:09	reading /etc/hosts
Jun 7 11:31:09	DNS started
Jun 7 11:31:09	Sending discover...
Jun 7 11:31:07	Sending discover...
Jun 7 11:31:05	Sending discover...
Jun 7 11:31:04	DHCP client start.

Helpful Hints..

- Check the log frequently to detect unauthorized network usage.

Statistics

The window below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DIR-400 on both the WAN and the LAN ports. The traffic counter will reset if the device is rebooted.



TRAFFIC STATISTICS :

Traffic Statistics display Receive and Transmit packets passing through the DIR-400.

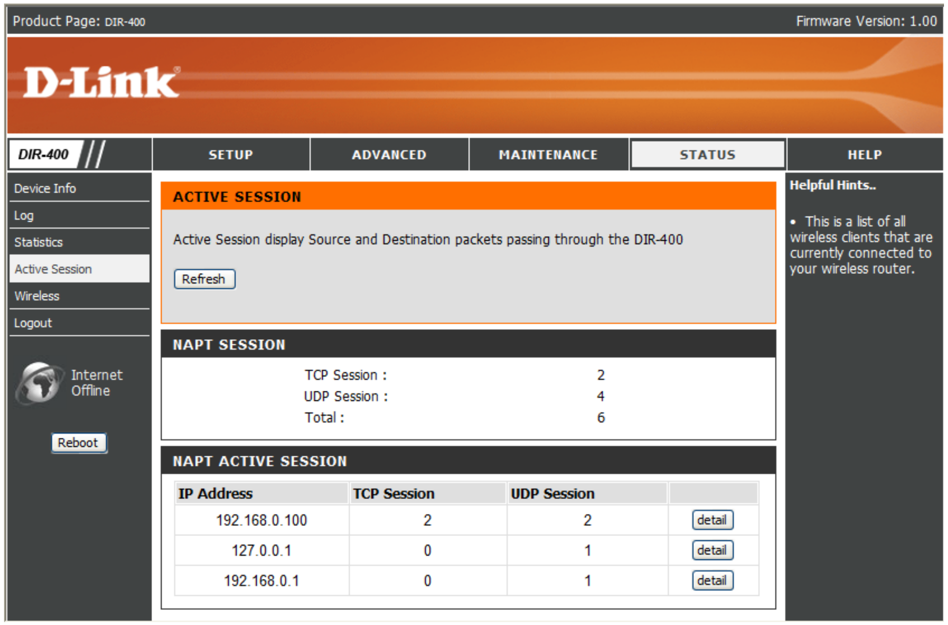
	Receive	Transmit
WAN	0 Packets	3 Packets
LAN	192 Packets	251 Packets
WIRELESS 11g	0 Packets	39 Packets

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 initizlized.

Active Session

The NAPT Active Session table displays a list of all active sessions between WAN computers and LAN computers.



ACTIVE SESSION

Active Session display Source and Destination packets passing through the DIR-400

NAPT SESSION

TCP Session :	2
UDP Session :	4
Total :	6

NAPT ACTIVE SESSION

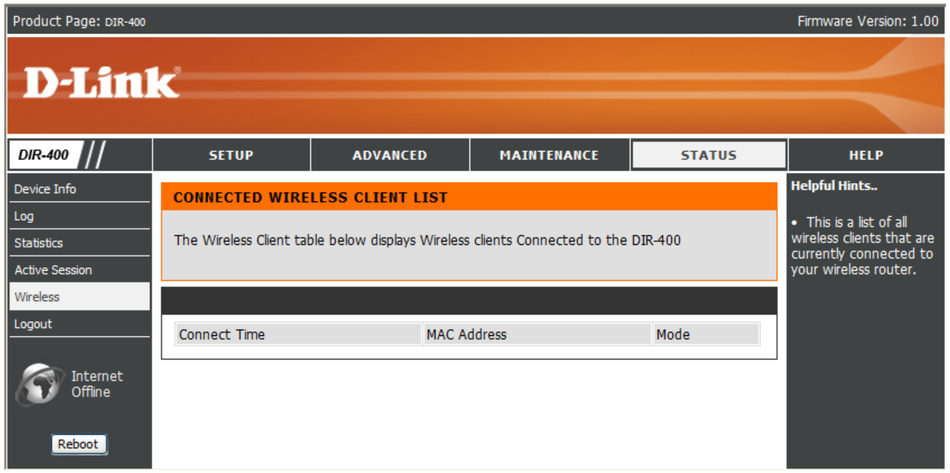
IP Address	TCP Session	UDP Session	
192.168.0.100	2	2	detail
127.0.0.1	0	1	detail
192.168.0.1	0	1	detail

Helpful Hints..

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

Wireless

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



CONNECTED WIRELESS CLIENT LIST

The Wireless Client table below displays Wireless clients Connected to the DIR-400

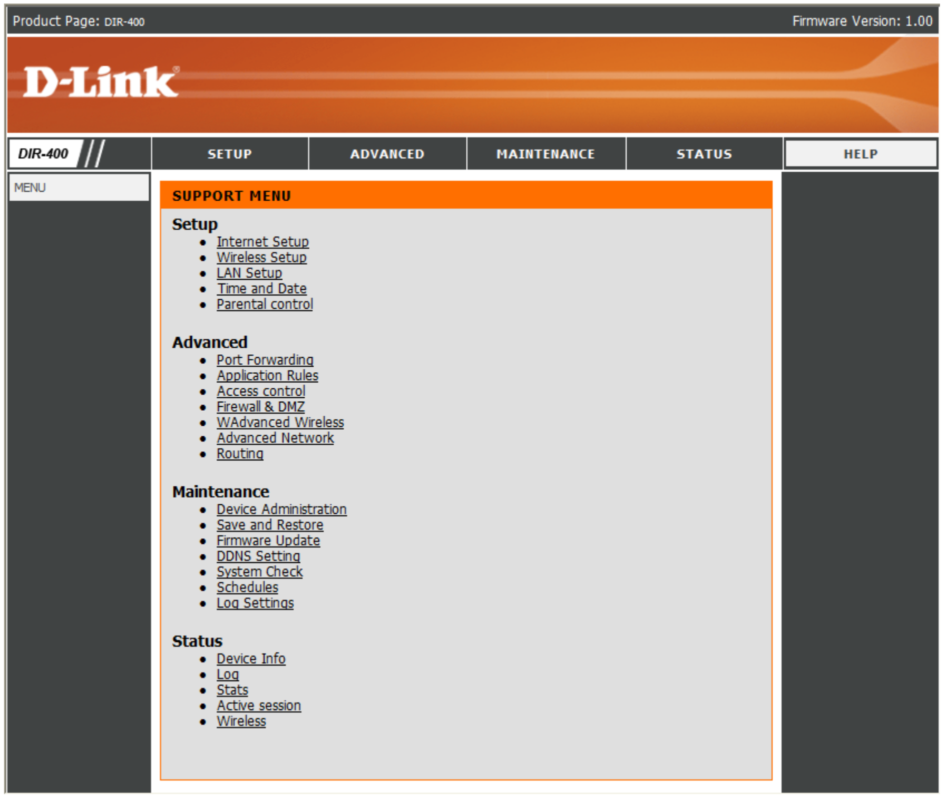
Connect Time	MAC Address	Mode

Helpful Hints..

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

Help

Click the desired hyperlink to view more information about how to use the router.



SUPPORT MENU

Setup

- Internet Setup
- Wireless Setup
- LAN Setup
- Time and Date
- Parental control

Advanced

- Port Forwarding
- Application Rules
- Access control
- Firewall & DMZ
- WAdvanced Wireless
- Advanced Network
- Routing

Maintenance

- Device Administration
- Save and Restore
- Firmware Update
- DDNS Setting
- System Check
- Schedules
- Log Settings

Status

- Device Info
- Log
- Stats
- Active session
- Wireless

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders.
The DIR-400 offers the following types of security:

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

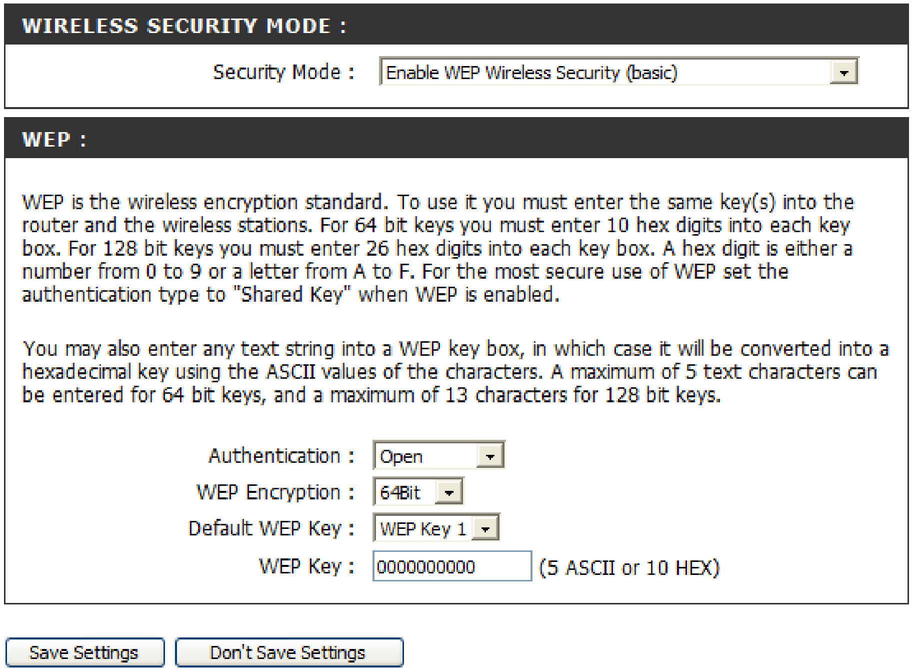
What is WEP?

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.

Configuring 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.



WIRELESS SECURITY MODE :

Security Mode : Enable WEP Wireless Security (basic)

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.

Authentication : Open

WEP Encryption : 64Bit

Default WEP Key : WEP Key 1

WEP Key : 0000000000 (5 ASCII or 10 HEX)

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 **Wireless Setup** on the left side.

2. Next to **Security Mode**, select *Enable WEP Wireless Security (basic)*.

3. Next to **Authentication**, select either *Shared Key or Open*. *Shared Key* is recommended as it provides greater security when WEP is enabled.

4. Select either *64Bit* or *128Bit* encryption from the drop-down menu next to **WEP Encryption**.

5. Next to **Default WEP Key**, select *WEP Key 1* and create your own WEP key. Make sure you enter this key exactly on all your wireless devices. You may enter up to four different keys either using *Hex* or *ASCII*. *Hex* is recommended (only letters A-F and numbers 0-9 are valid). In *ASCII* all numbers and letters are valid.

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.

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 two major improvements over WEP are:

- 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 the Advanced Encryption Standard (AES) instead of TKIP.

- User authentication, which is generally missing in WEP, is done 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.

Configuring WPA-PSK and WPA2-PSK

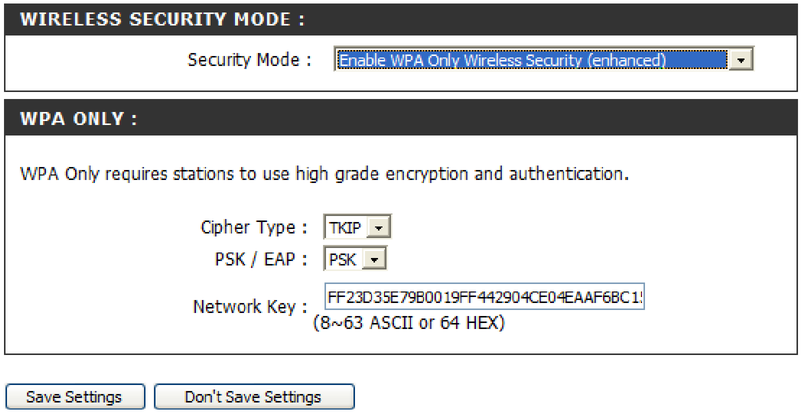
It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

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 **Wireless Setup** on the left side.

2. Next to **Security Mode**, select *Enable WPA Only Wireless Security (enhanced)* or *Enable WPA2 Only Wireless Security (enhanced)*.

3. Next to **Cipher Mode**, select *TKIP*, *AES*, or *Both*.

4. Next to **PSK/EAP**, select *PSK*.



WIRELESS SECURITY MODE :

Security Mode : Enable WPA Only Wireless Security (enhanced)

WPA ONLY :

WPA Only requires stations to use high grade encryption and authentication.

Cipher Type : TKIP

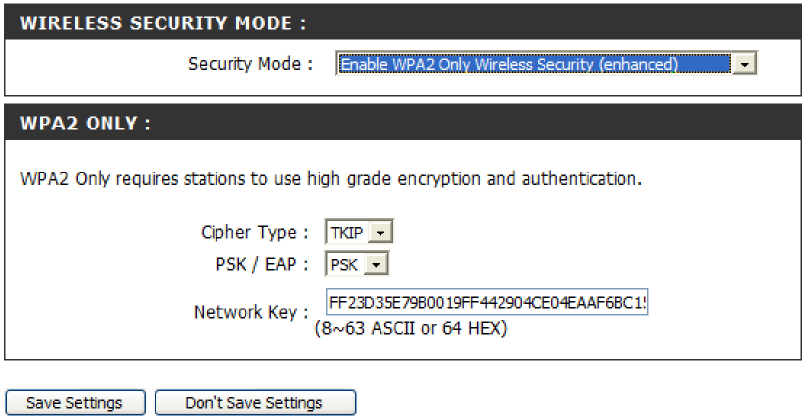
PSK / EAP : PSK

Network Key : FF23D35E79B0019FF442904CE04EAAF6BC1!

(8~63 ASCII or 64 HEX)

5. Next to **Network Key**, enter a key (passphrase). The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.

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 WPA-PSK or WPA2-PSK on your adapter and enter the same passphrase as you did on the router.



WIRELESS SECURITY MODE :

Security Mode : Enable WPA2 Only Wireless Security (enhanced)

WPA2 ONLY :

WPA2 Only requires stations to use high grade encryption and authentication.

Cipher Type : TKIP

PSK / EAP : PSK

Network Key : FF23D35E79B0019FF442904CE04EAAF6BC1!

(8~63 ASCII or 64 HEX)

Configuring WPA/WPA2-PSK

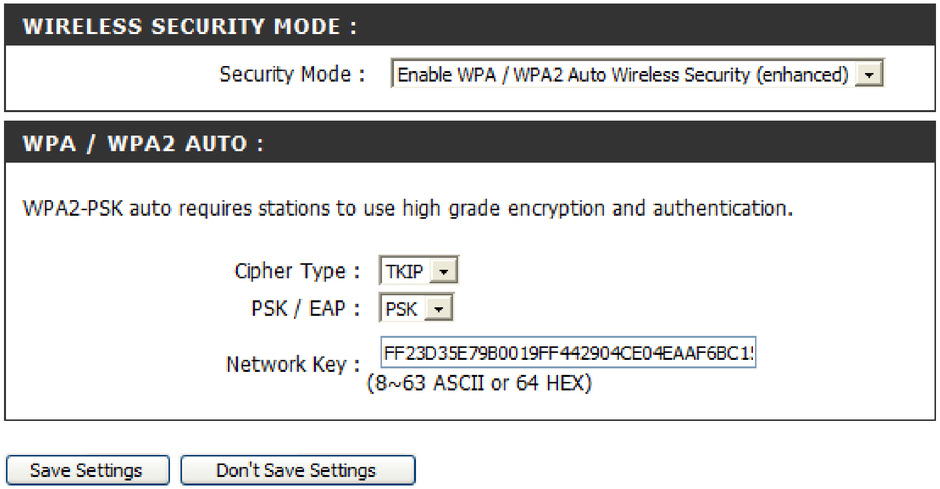
It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

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 **Wireless Setup** on the left side.

2. Next to **Security Mode**, select *Enable WPA/WPA2 Wireless Security (enhanced)*.

3. Next to **Cipher Mode**, select *TKIP*, *AES*, or *Both*.

4. Next to **PSK/EAP**, select *PSK*.



WIRELESS SECURITY MODE :

Security Mode : Enable WPA / WPA2 Auto Wireless Security (enhanced)

WPA / WPA2 AUTO :

WPA2-PSK auto requires stations to use high grade encryption and authentication.

Cipher Type : TKIP

PSK / EAP : PSK

Network Key : FF23D35E79B0019FF442904CE04EAAF6BC1

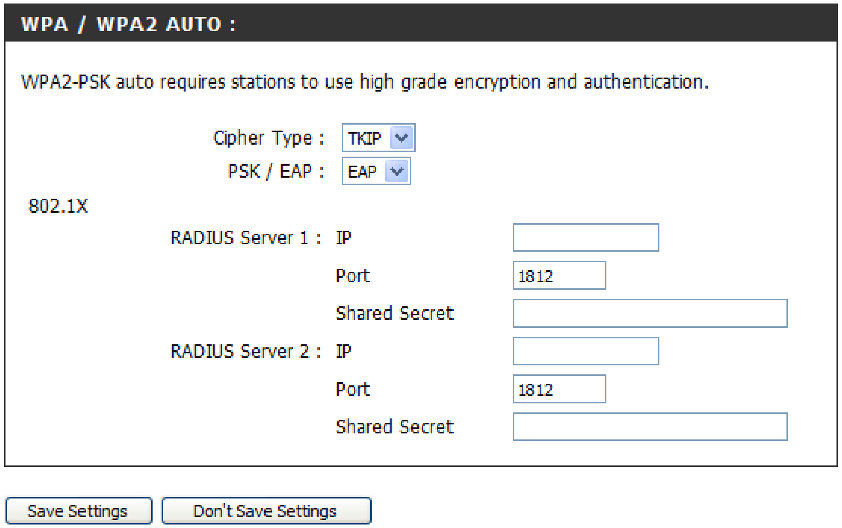
(8~63 ASCII or 64 HEX)

5. Next to **Network Key**, enter a key (passphrase). The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.

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 WPA/WPA2-PSK on your adapter and enter the same passphrase as you did on the router.

Configuring WPA, WPA2, & WPA/WPA2 (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.



WPA / WPA2 AUTO :

WPA2-PSK auto requires stations to use high grade encryption and authentication.

Cipher Type : TKIP
PSK / EAP : EAP

802.1X

RADIUS Server 1 : IP
Port 1812
Shared Secret

RADIUS Server 2 : IP
Port 1812
Shared Secret

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 **Wireless Settings** on the left side.

2. Next to **Security Mode**, select *Enable WPA Only Wireless Security (enhanced), Enable WPA2 Only Wireless Security (enhanced)*, or *Enable WPA/WPA2 Wireless Security (enhanced)*.

3. Next to **Cipher Type**, select *TKIP*, *AES*, or *Auto*.

4. Next to **PSK/EAP**, select *EAP*.

5. Next to **RADIUS Server 1** enter the **IP Address** of your RADIUS server.

6. Next to **Port**, enter the port you are using for your RADIUS server. *1812* is the default port.

7. Next to **Shared Secret**, enter the security key.

8. If you have a secondary RADIUS server, enter its IP address, port, and secret key.

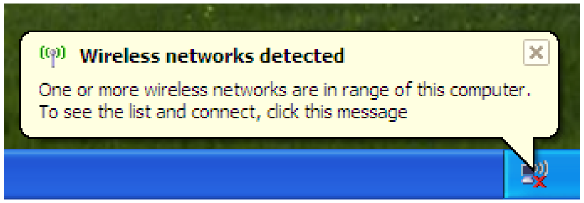
9. Click **Save Settings** to save your settings.

Note: When using EAP mode, you cannot have WPS enabled.

Connecting to a Wireless Network
Using Windows® XP

Windows® XP users may use XP's built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another 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.

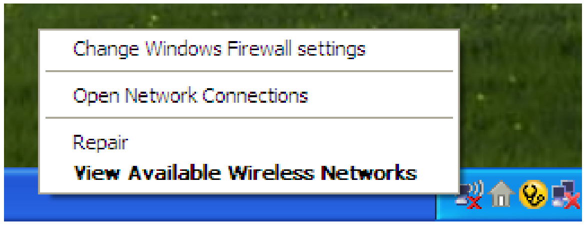


Wireless networks detected

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

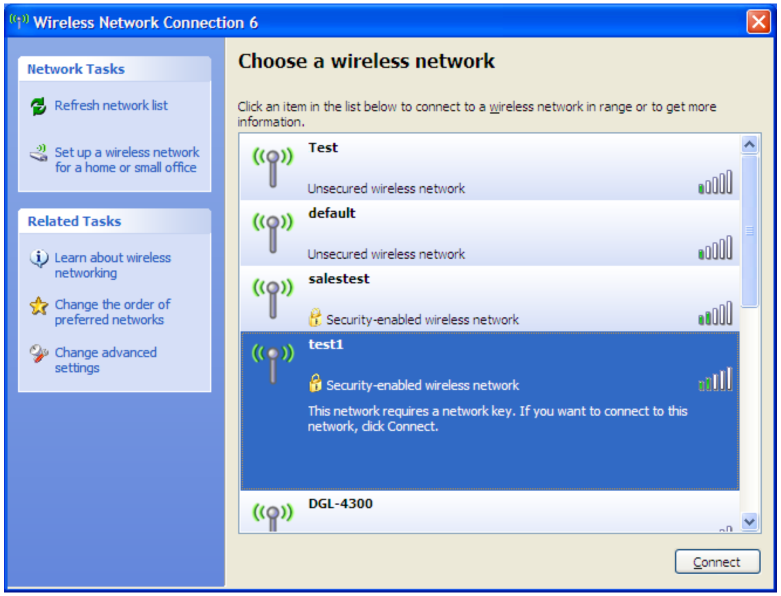
or

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 your 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

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

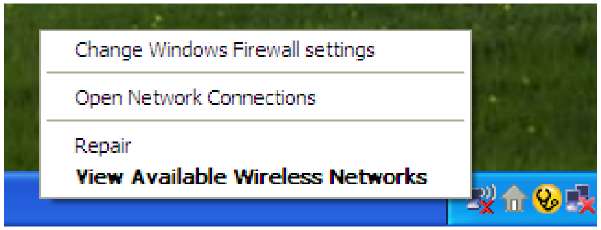
test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

DGL-4300

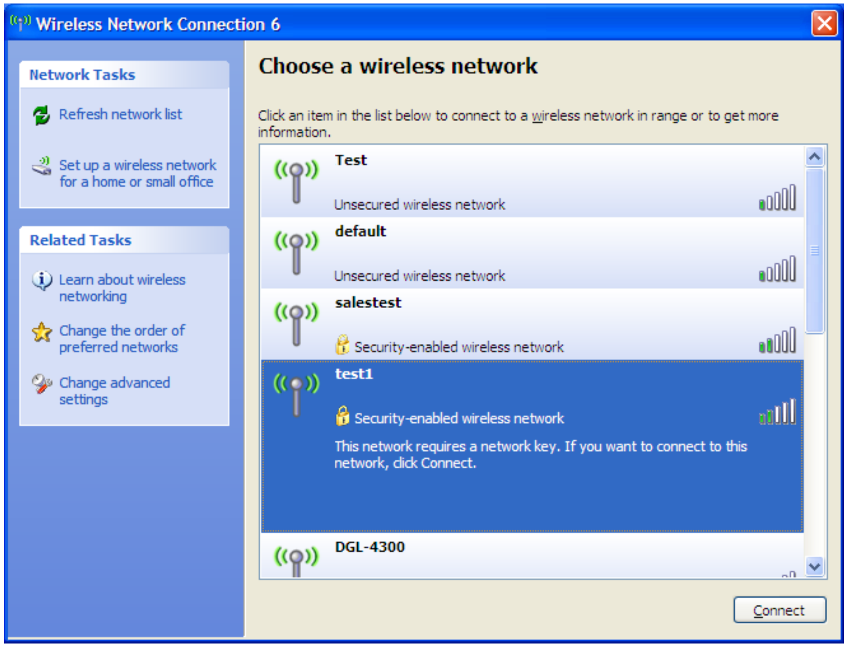
Configure WEP

It is recommended to enable WEP encryption 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
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

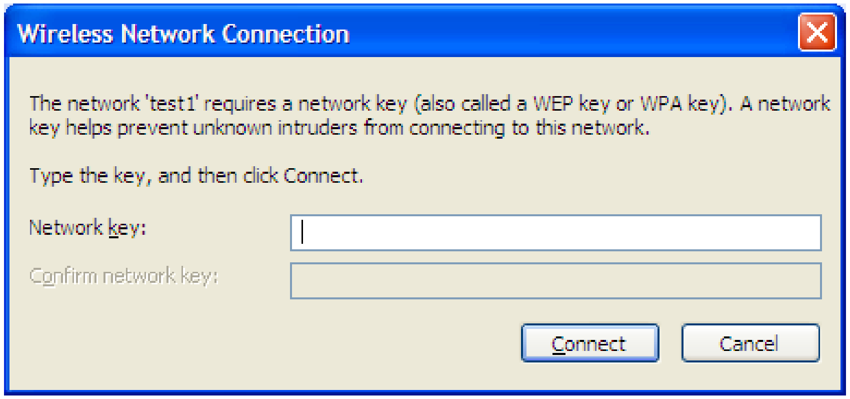
salestest
Security-enabled wireless network

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

DGL-4300

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.

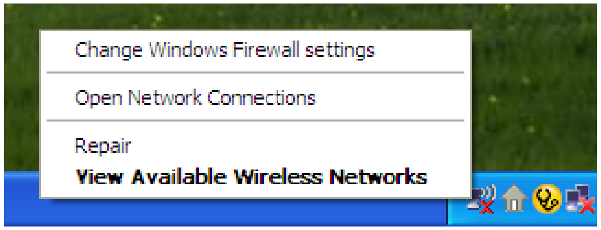
Network key:

Confirm network key:

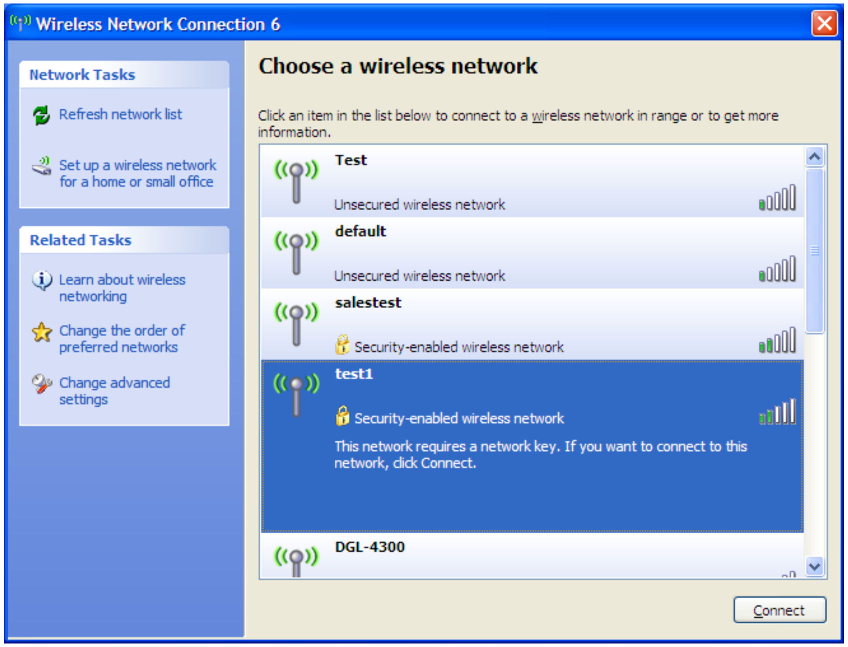
Configuring WPA-PSK

It is recommended to enable WPA-PSK encryption 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 WPA-PSK passphrase 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
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

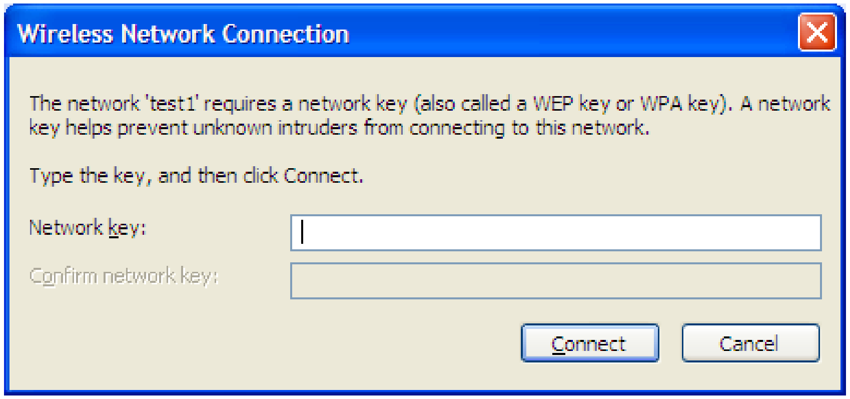
salestest
Security-enabled wireless network

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

DGL-4300

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.



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:

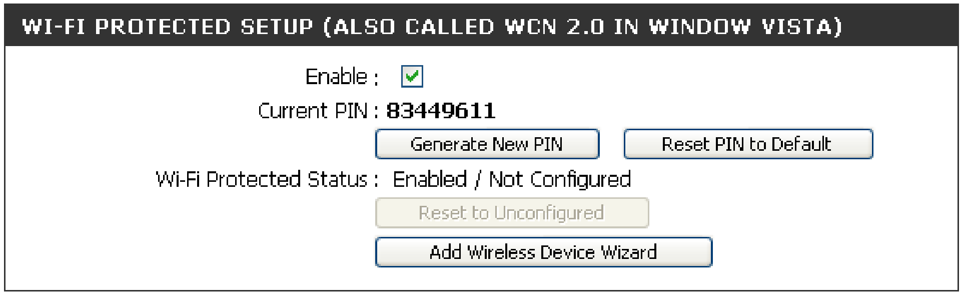
Setting Up Wi-Fi Protection (WCN 2.0 in Windows Vista)

The DIR-400 supports Wi-Fi protection, referred to as WCN 2.0 in Windows Vista. The instructions for setting this up depend on whether you are using Windows Vista or third party software to configure the router.

Initial Router Configuration for Wi-Fi Protection

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 use the traditional Ethernet approach.

If you are running Windows Vista, tick the Enable checkbox on the **Wireless Network** window. You can choose to use the Current PIN that is displayed on the **Wireless Network** window, randomly create a new PIN by clicking **Generate New PIN**, or click on **Reset PIN to Default** to use the default PIN.



WI-FI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOW VISTA)

Enable : ☑

Current PIN : 83449611

Wi-Fi Protected Status : Enabled / Not Configured

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

Setting Up a Configured Router

Once the router has been configured, you can use the push button on the router or in the third party software interface to invite a newcomer to join your Wi-Fi protected network. For maximum security, the software method is recommended. However, the push button method is ideal if there is no access to a GUI.

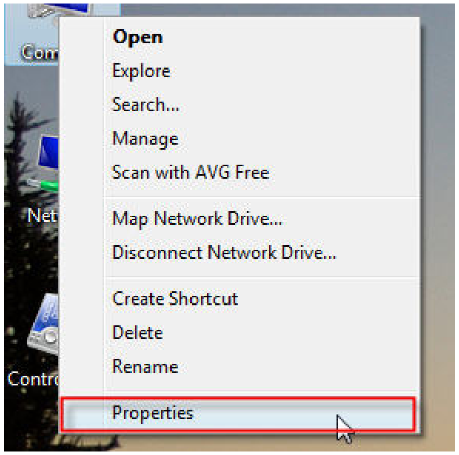
If you are using the router's Wi-Fi Security push button option, press the Wi-Fi Protected Setup button on the side of the router, then push the button on the client (or virtual button on the client's GUI) within 2 minutes. Next click **Finish**. The Client's software will then allow a newcomer to join your secure, Wi-Fi protected network.

If you are using third party software, run the appropriate Wi-Fi Protected System utility. You will be asked to either use the push button method or to manually enter the PIN. Follow the on-screen instructions to finish setting up your connection.

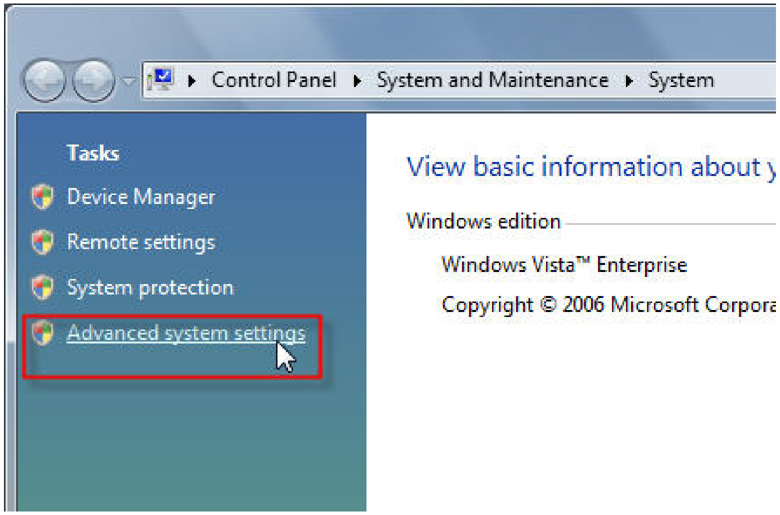
Changing the Computer Name and Joining a Workgroup

The following are step-by-step directions to change the computer name and join a workgroup.

1. Right-click on **Control Panel** and click on **Properties**.



2. Click on the **Advanced system settings** link.



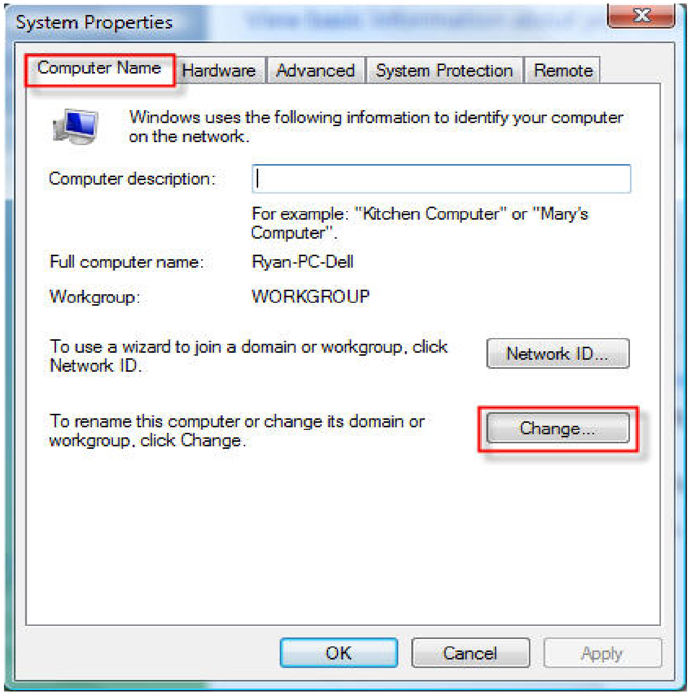
View basic information about y

Windows edition

Windows Vista™ Enterprise

Copyright © 2006 Microsoft Corpora

3. Click the **Computer Name** tab in the **System Properties** window and enter a description of your computer in the text box. When you are finished, click the **Change** button.


System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

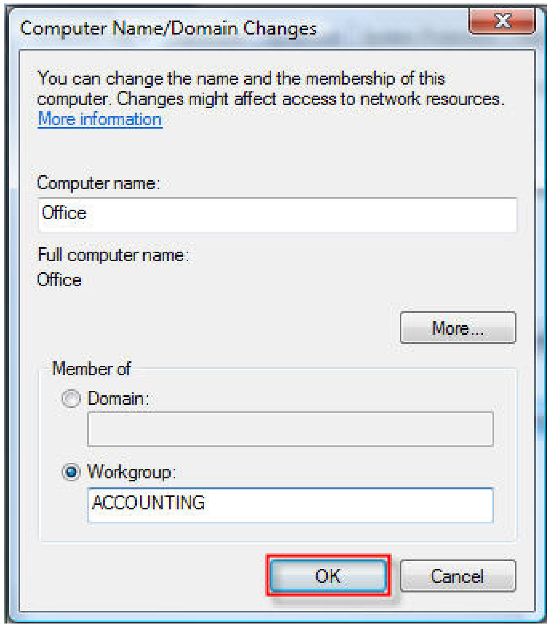
Full computer name: Ryan-PC-Dell

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

4. Go to the **Computer Name/Domain Changes** window and click the radio button next to the Workgroup you want to join. When you are finished, click the **OK** button.


Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources. More information

Computer name: Office

Full computer name: Office

Member of

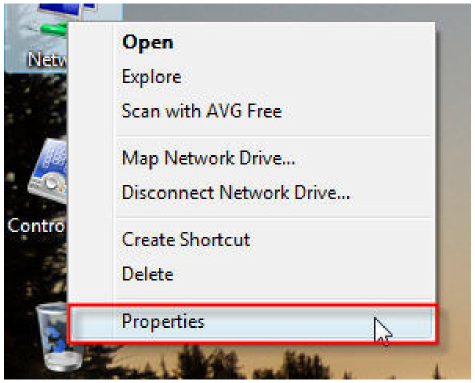
○ Domain:

● Workgroup: ACCOUNTING

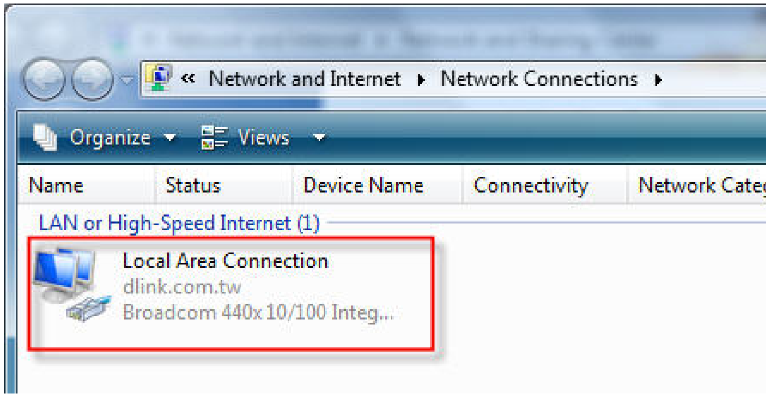
Configuring the IP Address in Vista

The following are step-by-step directions to configure the IP address in Windows Vista.

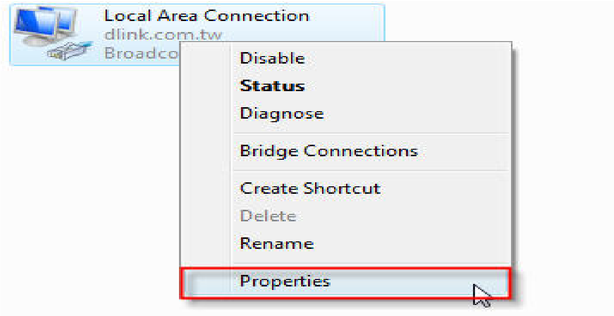
1. Right-click on **Network** and click on **Properties**.



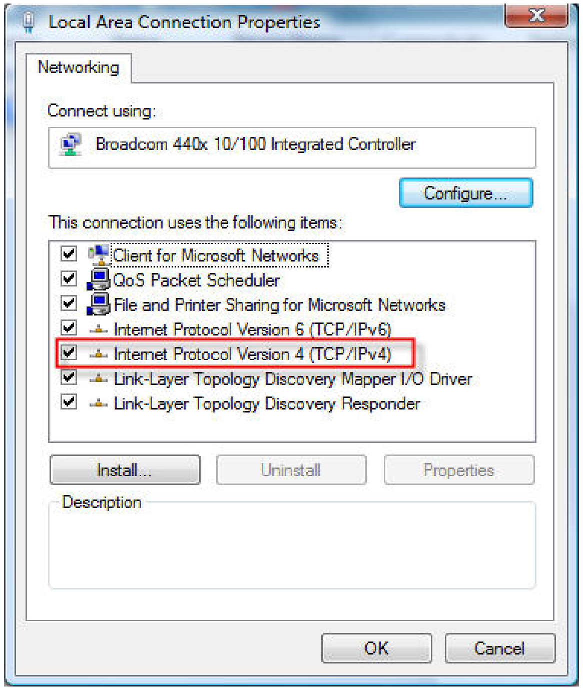
2. Go to the **Network and Internet** window and click the appropriate **Local Area Connection** icon.


« Network and Internet ▸ Network Connections ▸
Organize
Views
Name
Status
Device Name
Connectivity
Network Categ
LAN or High-Speed Internet (1)
Local Area Connection
dlink.com.tw
Broadcom 440x 10/100 Integ...

3. Right-click the **Local Area Connection** icon and then select **Properties** from the context menu.



4. Tick the **Internet Protocol Version 4 (TCP/IPv4)** checkbox in the **Networking** tab in the **Local Area Connection Properties** window, then click on the **Properties** button.


Local Area Connection Properties

Networking

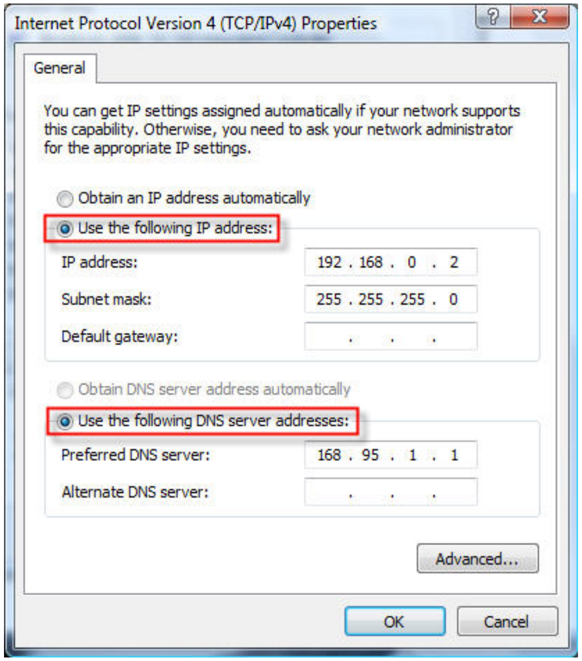
Connect using:

Broadcom 440x 10/100 Integrated Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

5. Click the “Use the following IP address” option in the **General** tab in the **Local Area Connection**’s **Properties** window and enter the desired IP address in the space offered. Then click the “Use the following DNS server adresses” option on the same tab and enter the desired DNS server information. Click **OK**, then **OK** again to exit the Properties windows.


Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

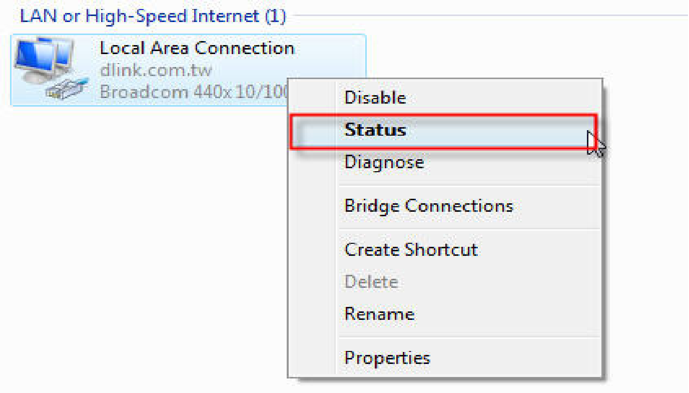
IP address:	192 . 168 . 0 . 2
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

○ Obtain DNS server address automatically

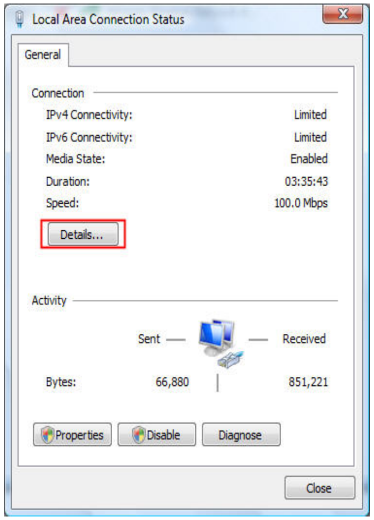
● Use the following DNS server addresses:

Preferred DNS server:	168 . 95 . 1 . 1
Alternate DNS server:	. . .

6. Right-click the **Local Area Connection** icon and then select **Status** from the drop-down menu.



7. Go to the **Local Area Connection Status** window and click the **Details** button.



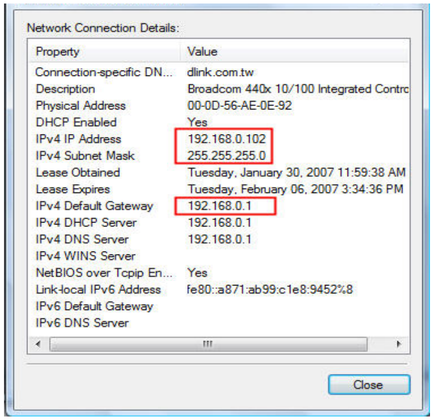
Connection

IPv4 Connectivity:	Limited
IPv6 Connectivity:	Limited
Media State:	Enabled
Duration:	03:35:43
Speed:	100.0 Mbps

Activity

	Sent	Received
Bytes:	66,880	851,221

8. Confirm your new settings on the **Network Connection Status** window. When you are finished, click the **Done** button.



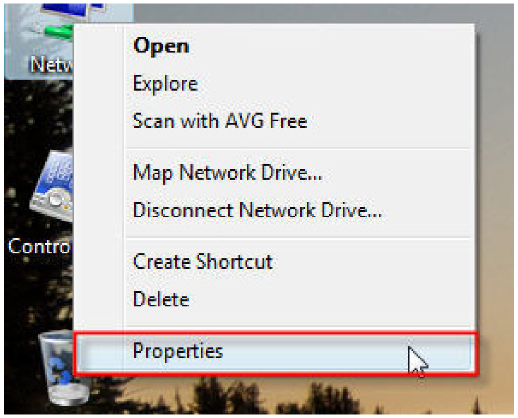
Network Connection Details:

Property	Value
Connection-specific DN...	dlink.com.tw
Description	Broadcom 440x 10/100 Integrated Contrc
Physical Address	00-0D-56-AE-0E-92
DHCP Enabled	Yes
IPv4 IP Address	192.168.0.102
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Tuesday, January 30, 2007 11:59:38 AM
Lease Expires	Tuesday, February 06, 2007 3:34:36 PM
IPv4 Default Gateway	192.168.0.1
IPv4 DHCP Server	192.168.0.1
IPv4 DNS Server	192.168.0.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::a871:ab99:c1e8:9452%8
IPv6 Default Gateway	
IPv6 DNS Server	

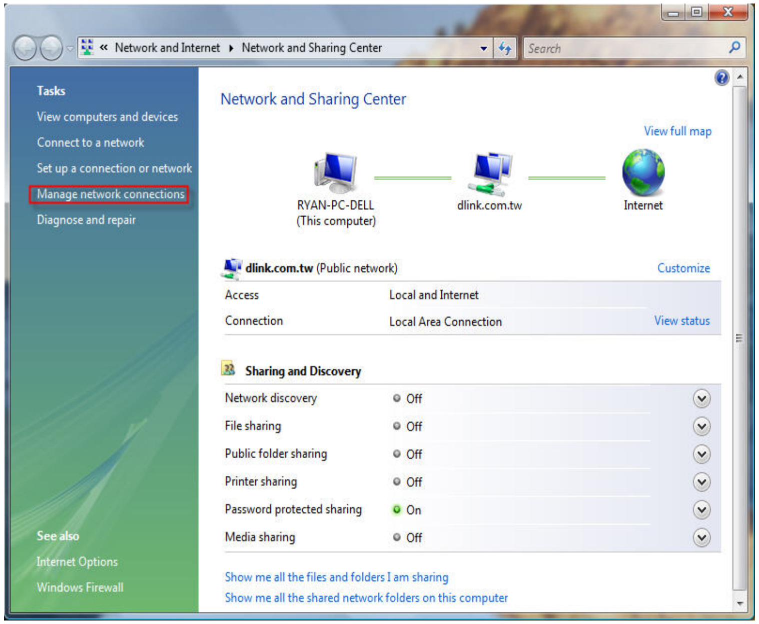
Connecting to a Secured Wireless Network (WEP, WPA-PSK & WPA2-PSK)

The following are step-by-step directions to set up a wireless connection.

1. Right-click on **Network** and click on **Properties**.



2. Click the **Manage network connections** link in the **Network and Sharing Center** window.



Network and Sharing Center

dlink.com.tw (Public network)

Access	Local and Internet
Connection	Local Area Connection

Sharing and Discovery

Network discovery	○ Off
File sharing	○ Off
Public folder sharing	○ Off
Printer sharing	○ Off
Password protected sharing	● On
Media sharing	○ Off

Show me all the files and folders I am sharing

Show me all the shared network folders on this computer