

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.

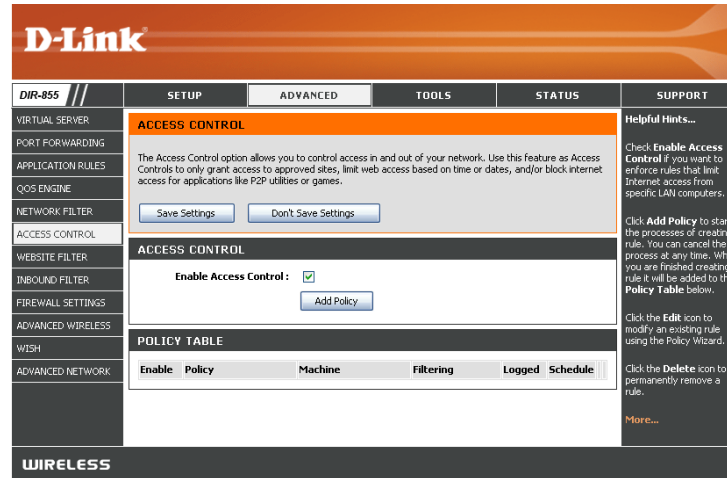
Clear: Click to remove the MAC address.

The screenshot shows the D-Link DIR-855 web interface. The top navigation bar includes 'DIR-855', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various settings categories: VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, QOS ENGINE, NETWORK FILTER, ACCESS CONTROL, WEBSITE FILTER, INBOUND FILTER, FIREWALL SETTINGS, ADVANCED WIRELESS, WISH, and ADVANCED NETWORK. The main content area is titled 'MAC ADDRESS FILTER' and contains the following text: 'The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.' Below this text are 'Save Settings' and 'Don't Save Settings' buttons. The section is titled '24 -- MAC FILTERING RULES' and includes a dropdown menu to 'Configure MAC Filtering below:' with 'Turn MAC Filtering OFF' selected. Below this is a table with two columns: 'MAC Address' and 'DHCP Client List'. The table contains five rows, each with an empty 'MAC Address' field, a '<<' button, a 'Computer Name' dropdown menu, and a 'Clear' button. To the right of the table is a 'Helpful Hints...' section with instructions on how to use the DHCP Client List and a 'More...' link.

Access Control

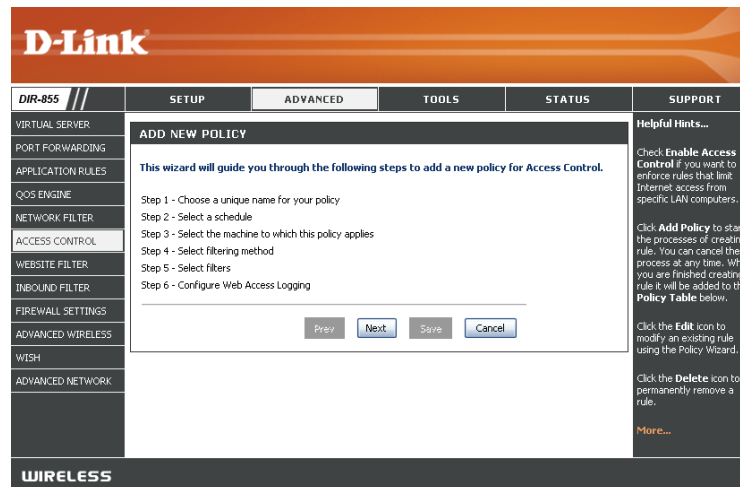
The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

Add Policy: 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.

The screenshot shows the 'STEP 1: CHOOSE POLICY NAME' screen. The 'Policy Name' field is empty. The 'Next' button is highlighted. The interface includes a sidebar with navigation options and a 'Helpful Hints...' section on the right.

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

The screenshot shows the 'STEP 2: SELECT SCHEDULE' screen. The 'Always' schedule is selected in the drop-down menu. The 'Next' button is highlighted. The interface includes a sidebar with navigation options and a 'Helpful Hints...' section on the right.

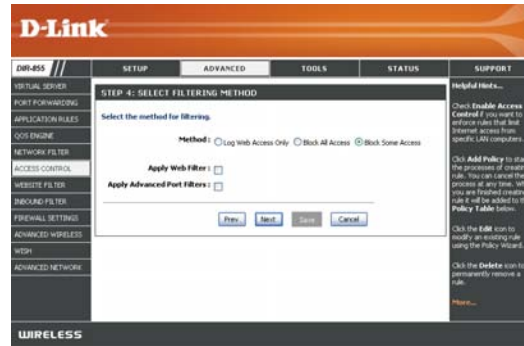
Enter the following information and then click **Next** to continue.

- 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.

The screenshot shows the 'STEP 3: SELECT MACHINE' screen. The 'IP Address' field is filled with '0.0.0.0'. The 'Next' button is highlighted. The interface includes a sidebar with navigation options and a 'Helpful Hints...' section on the right.

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.

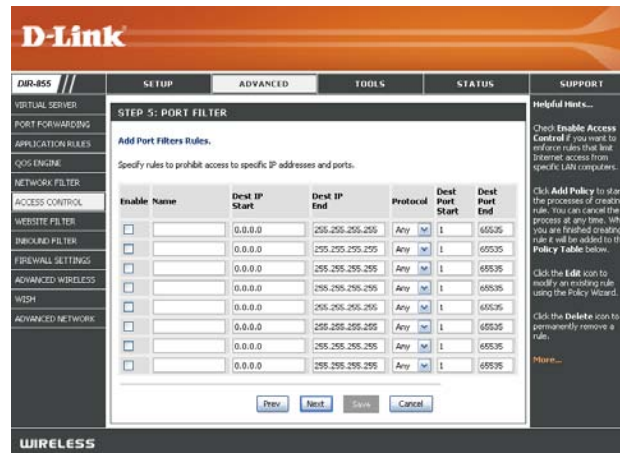
Dest IP Start - Enter the starting IP address.

Dest IP End - Enter the ending IP address.

Protocol - Select the protocol.

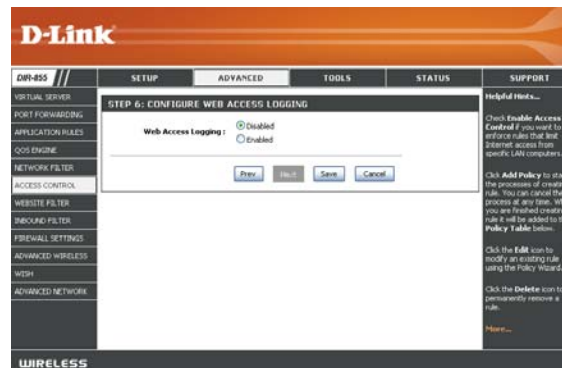
Dest Port Start - Enter the starting port number.

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 **Save Settings**. You must also select **Apply Web Filter** under the *Access Control* section (page 40).

Add Website Filtering Rule: Select **Allow** or **Deny**.

Website URL/ Domain: Enter the keywords or URLs that you want to allow or block. Click **Save Settings**.

The screenshot displays the D-Link DIR-855 web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration sections, with 'ACCESS CONTROL' selected and 'WEBSITE FILTER' highlighted. The main content area is titled 'WEBSITE FILTER' and contains the following information:

- WEBSITE FILTER** (Section Header)
- Description: "The Website Filter option allows you to set up a list of Web sites you would like to allow or deny through your network. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section."
- Buttons: "Save Settings" and "Don't Save Settings"
- 64 -- WEBSITE FILTERING RULES** (Section Header)
- Configuration: "Configure Website Filter below:" with a dropdown menu set to "DENY computers access to ONLY these sites".
- Button: "Clear the list below..."
- Table: A table with the header "Website URL/Domain" and four empty rows for input.

On the right side of the interface, there is a "Helpful Hints..." section with the text: "Create a list of Web Sites to which you would like to deny or allow through the network." and a note: "Use with **Advanced** → **Access Control**." followed by a "More..." link.

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.

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

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

Add: Click the **Add** 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.

D-Link

DIR-855 // SETUP ADVANCED TOOLS STATUS SUPPORT

INBOUND FILTER

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 for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Port Forwarding, or Remote Administration features.

ADD INBOUND FILTER RULE

Name :

Action :

Remote IP Range	Enable	Remote IP Start	Remote IP End
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255

INBOUND FILTER RULES LIST

Name	Action	Remote IP Range

Helpful Hints...

Give each rule a **Name** that is meaningful to you.

Each rule can either **Allow** or **Deny** access from the WAN.

Up to eight ranges of WAN IP addresses can be controlled by each rule. The checkbox by each IP range can be used to disable ranges already defined.

The starting and ending IP addresses are WAN-side address.

Click the **Add** or **Update** button to store a finished rule in the Rules List below.

Click the **Edit** icon in the Rules List to change a rule.

Click the **Delete** icon in the Rules List to permanently remove a rule.

[More...](#)

WIRELESS

Firewall Settings

A firewall protects your network from the outside world. The DIR-855 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.

Anti-Spoof Check: Enable this feature to protect your network from certain kinds of “spoofing” attacks.

Enable DMZ: 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.

DMZ 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 **Basic > DHCP** page so that the IP address of the DMZ machine does not change.

The screenshot displays the D-Link DIR-855 web interface for Firewall Settings. The left sidebar contains a navigation menu with options like VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, QOS ENGINE, NETWORK FILTER, ACCESS CONTROL, WEBSITE FILTER, INBOUND FILTER, FIREWALL SETTINGS (selected), ROUTING, ADVANCED WIRELESS, WISH, WI-FI PROTECTED SETUP, and ADVANCED NETWORK. The main content area is titled 'FIREWALL SETTINGS' and includes a 'Helpful Hints...' section on the right. The settings are organized into several sections:

- FIREWALL SETTINGS:** Includes a description: "The Firewall Settings allow you to set a single computer on your network outside of the router." and buttons for "Save Settings" and "Don't Save Settings".
- FIREWALL SETTINGS:** A sub-section with "Enable SPI" checked.
- NAT ENDPOINT FILTERING:** Contains two sections:
 - UDP Endpoint Filtering:** Radio buttons for "Endpoint Independent" (selected), "Address Restricted", and "Port And Address Restricted".
 - TCP Endpoint Filtering:** Radio buttons for "Endpoint Independent", "Address Restricted", and "Port And Address Restricted" (selected).
- ANTI-SPOOF CHECKING:** "Enable anti-spoof checking" is unchecked.
- DMZ HOST:** Includes a description of DMZ, a "Note" about security risks, "Enable DMZ" (unchecked), and a "DMZ IP Address" field set to "0.0.0.0" with a "Computer Name" dropdown menu.
- APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION:** "PPTP" and "IPSec (VPN)" are both checked.

The bottom of the page shows the "WIRELESS" section.

Application Level Gateway (ALG) Configuration

Here you can enable or disable ALG's. Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.

PPTP: Allows multiple machines on the LAN to connect to their corporate network using PPTP protocol.

IPSEC (VPN): Allows multiple VPN clients to connect to their corporate network using IPsec. Some VPN clients support traversal of IPsec through NAT. This ALG may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off. Please check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

Advanced Wireless Settings

802.11n/g (2.4GHz)

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 2346. 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.

ADVANCED WIRELESS SETTINGS

Wireless Band : 2.4GHz Band

Transmit Power : High

Beacon Period : (20..1000)

RTS Threshold : (0..2347)

Fragmentation Threshold : (256..2346)

DTIM Interval : (1..255)

802.11d Enable :

Wireless Isolation :

WMM Enable :

A-MPDU Aggregation :

Short GI :

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.

802.11d: 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.

Wireless Isolation: When checked, it will disable the ability for computers on the wireless network from seeing each other, but will allow you to see computers on the wired network.

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

A-MPDU Aggregation: Aggregated-MAC Packet Data Unit, is a group of MPDUs which built an PSDU (Physical Service Data Unit). It has lower overhead and provides robust recovery in case of loss.

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 Wireless Settings

802.11n/a (5GHz)

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 2342. 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.

802.11d: 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.

Wireless Isolation: When checked, it will disable the ability for computers on the wireless network from seeing each other, but will allow you to see computers on the wired network.

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

A-MPDU Aggregation: Aggregated-MAC Packet Data Unit, is a group of MPDUs which built an PSDU (Physical Service Data Unit). It will lower overhead and provides robust recovery in case of loss.

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 WIRELESS SETTINGS

Wireless Band : 5GHz Band

Transmit Power : High

Beacon Period : (20..1000)

RTS Threshold : (0..2347)

Fragmentation Threshold : (256..2346)

DTIM Interval : (1..255)

802.11d Enable :

Wireless Isolation :

WMM Enable :

A-MPDU Aggregation :

Short GI :

Extra Wireless Protection :

WISH Settings

WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications.

Enable WISH: Enable this option if you want to allow WISH to prioritize your traffic.

HTTP: Allows the router to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

Windows Media Center: Enables the router to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.

Automatic: When enabled, this option causes the router to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behaviour that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.

WISH Rules: A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required.

WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used.

The screenshot displays the WISH configuration interface for a D-Link DIR-855 router. The interface is organized into several sections:

- WISH:** A section with a description: "WISH (Wireless Intelligent Stream Handling) prioritizes the traffic of various wireless applications." It includes "Save Settings" and "Don't Save Settings" buttons.
- WISH:** A section where the "Enable WISH" checkbox is checked.
- PRIORITY CLASSIFIERS:** A section where three checkboxes are checked: "HTTP", "Windows Media Center", and "Automatic" (with a note: "(default if not matched by anything else)").
- 24 -- WISH RULES:** A table listing two rules. Each rule has a checkbox, a "Name" field, a "Priority" dropdown set to "Best Effort (BE)", and a "Protocol" dropdown set to "TCP". The first rule has "Host 1 IP Range" and "Host 2 IP Range" both set to "0.0.0.0 to 255.255.255.255", and "Host 1 Port Range" and "Host 2 Port Range" both set to "0 to 65535". The second rule has "Host 1 IP Range" set to "0.0.0.0 to 255.255.255.255" and "Host 1 Port Range" set to "0 to 65535".

On the right side of the interface, there is a "Helpful Hints..." section with the text: "Enable this option if you want to allow WISH to prioritize wireless traffic. For most applications, the priority classifiers ensure the right priorities, and specific WISH Rules are not required. More..."

Name: Create a name for the rule that is meaningful to you.

Priority: The priority of the message flow is entered here. The four priorities are defined as:

BK: Background (least urgent)

BE: Best Effort.

VI: Video

VO: Voice (most urgent)

Name	Priority	Protocol
	Best Effort (BE)	6 << TCP
<input type="checkbox"/> Host 1 IP Range	0.0.0.0 to 255.255.255.255	Host 1 Port Range 0 to 65535
Host 2 IP Range	0.0.0.0 to 255.255.255.255	Host 2 Port Range 0 to 65535

Protocol: The protocol used by the messages.

Host IP Range: The rule applies to a flow of messages for which one computer's IP address falls within the range set here.

Host Port Range: The rule applies to a flow of messages for which host's port number is within the range set here.

Advanced Network Settings

Enable UPnP: 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-855 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 Ping Inbound Filter: Select from the drop-down menu if you would like to apply the Inbound Filter to the WAN ping. Refer to page 44 for more information regarding Inbound Filter.

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.

D-Link

DIR-855 // SETUP ADVANCED TOOLS STATUS SUPPORT

ADVANCED NETWORK

If you are not familiar with these Advanced Network settings, please read the help section before attempting to modify these settings.

Save Settings Don't Save Settings

UPNP

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

Enable UPnP:

WAN PING

If you enable this feature, the WAN port of your router will respond to ping requests from the Internet that are sent to the WAN IP Address.

Enable WAN Ping Respond:

WAN Ping Inbound Filter: Allow All

Details : Everyone allowed

WAN PORT SPEED

WAN Port Speed: Auto 10/100Mbps

MULTICAST STREAMS

Enable Multicast Streams:

WIRELESS

Helpful Hints...

UPnP helps other UPnP LAN hosts interoperate with the router. Leave the UPnP option enabled as long as the LAN has other UPnP applications.

For added security, it is recommended that you disable the WAN Ping Respond option. Ping is often used by malicious Internet users to locate active networks or PCs.

The WAN speed is usually detected automatically. If you are having problems connecting to the WAN, try selecting the speed manually.

If you are having trouble receiving multicast streams from the Internet, make sure the Multicast Streams option is enabled.

More...

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.

System Name: Enter a name for the DIR-855 router.

Remote Management: Remote management allows the DIR-855 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-855. Example: http://x.x.x.x:8080 whereas x.x.x.x is the Internet IP address of the DIR-855 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 **Delete** icon to remove the rule.

The screenshot shows the D-Link DIR-855 web management interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The main content area is titled "ADMINISTRATOR SETTINGS" and contains the following sections:

- ADMINISTRATOR SETTINGS:** A text box explaining that 'admin' and 'user' accounts can access the management interface. The admin has read/write access and can change passwords, while the user has read-only access. Below this text are two buttons: "Save Settings" and "Don't Save Settings".
- ADMIN PASSWORD:** A section with the instruction "Please enter the same password into both boxes, for confirmation." It contains two input fields: "Password:" and "Verify Password:".
- USER PASSWORD:** A section with the instruction "Please enter the same password into both boxes, for confirmation." It contains two input fields: "Password:" and "Verify Password:".
- SYSTEM NAME:** A section with the label "Gateway Name:" and a text input field containing "D-Link DIR-855".
- ADMINISTRATION:** A section with the following options:
 - Enable Remote Management:** A checkbox that is currently unchecked.
 - Remote Admin Port:** A text input field containing "8080".
 - Remote Admin Inbound Filter:** A dropdown menu set to "Allow All".
 - Details:** A text input field containing "Everyone allowed".

On the right side of the interface, there is a "Helpful Hints..." section with several tips, including one about security recommendations for password changes and another about enabling Remote Management.

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.

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.

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**. You can also click **Copy Your Computer's Time Settings**.

The screenshot displays the D-Link DIR-855 web interface for Time Configuration. The top navigation bar includes 'DIR-855', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists menu items: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'TIME' and contains the following sections:

- Time Configuration:** A text box explaining the purpose of the section and two buttons: 'Save Settings' and 'Don't Save Settings'.
- TIME CONFIGURATION:**
 - Current Router Time: Saturday, January 31, 2004 2:50:54 PM
 - Time Zone: (GMT-08:00) Pacific Time (US/Canada), Tijuana
 - Enable Daylight Saving:
 - Daylight Saving Offset: +1:00
 - Daylight Saving Dates:

DST Start	Month	Week	Day of Week	Time
Apr	1st	Sun	2 am	
DST End	Oct	5th	Sun	2 am
- AUTOMATIC TIME CONFIGURATION:**
 - Enable NTP Server:
 - NTP Server Used: << Select NTP Server
- SET THE DATE AND TIME MANUALLY:**
 - Date And Time:

Year	2004	Month	Jan	Day	31	Hour	2	Minute	50	Second	45	PM
------	------	-------	-----	-----	----	------	---	--------	----	--------	----	----
 - Copy Your Computer's Time Settings

The right sidebar contains 'Helpful Hints...' with text about timekeeping and a 'More...' link.

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.

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).

The screenshot displays the D-Link DIR-855 web management interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration sections: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'SYSLOG' and contains the following information:

- A heading 'SYSLOG' with a sub-heading 'SYSLOG SETTINGS'.
- A descriptive text: 'The SysLog options allow you to send log information to a SysLog Server.'
- Two buttons: 'Save Settings' and 'Don't Save Settings'.
- A checkbox labeled 'Enable Logging To Syslog Server' which is checked.
- A text field for 'Syslog Server IP Address' containing '0.0.0.0' and a dropdown menu set to 'Computer Name'.

On the right side of the interface, there is a 'Helpful Hints...' section with text explaining that a System Logger (syslog) is a server that collects logs from different sources and that if the LAN includes a syslog server, the router's logs can be sent to it. A 'More...' link is also present.

Email Settings

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

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

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

To Email Address: Enter the email address where you want the email sent.

SMTP Server Address: Enter the SMTP server address for sending email. 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 email.

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 email when the log is full.

On Schedule: Selecting this option will send the logs via email 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**.

The screenshot shows the D-Link DIR-855 web interface. The top navigation bar includes 'DIR-855', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options: ADMIN, TIME, SYSLOG, EMAIL SETTINGS (highlighted), SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'EMAIL SETTINGS' and contains the following sections:

- Email Settings:** A descriptive text box stating: "The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address." Below this are two buttons: "Save Settings" and "Don't Save Settings".
- ENABLE:** A section with a single checkbox labeled "Enable Email Notification" which is checked.
- EMAIL SETTINGS:** A section with several input fields:
 - From Email Address: [text input]
 - To Email Address: [text input]
 - SMTP Server Address: [text input]
 - Enable Authentication:
 - Account Name: [text input]
 - Password: [text input]
 - Verify Password: [text input]
- EMAIL LOG WHEN FULL OR ON SCHEDULE:** A section with checkboxes for "On Log Full" and "On Schedule", both of which are unchecked. Below these is a "Schedule" dropdown menu currently set to "Never", with a "Details" field showing ":Never".

The bottom of the page features a "WIRELESS" section header.

System Settings

This section allows you to manage the router's configuration settings, reboot the router, and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.

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.

The screenshot displays the D-Link DIR-855 web interface. The top navigation bar includes 'DIR-855', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'SYSTEM SETTINGS' and contains the following sections:

- Save Settings To Local Hard Drive:** A button labeled 'Save Configuration'.
- Load Settings From Local Hard Drive:** A text input field, a 'Browse...' button, and buttons for 'Restore Configuration from File' and 'Cancel'.
- Restore To Factory Default Settings:** A button labeled 'Restore all Settings to the Factory Defaults'.
- Reboot The Device:** A button labeled 'Reboot the Device'.

On the right side, there is a 'Helpful Hints...' section with the following text: 'Once your router is configured the way you want it, you can save the configuration settings to a configuration file. You might need this file so that you can load your configuration later in the event that the router's default settings are restored. To save the configuration, click the **Save Configuration** button. [More...](#)'

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 Upgrade: Click on **Check Now** to find out if there is an updated firmware; if so, download the new firmware to your hard drive.

Browse: 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.

Notifications Check **Automatically Check Online for Latest Firmware Version** to have the router check automatically to see if there is a new firmware upgrade.

Check **Email Notification of Newer Firmware Version** to have the router send an email when there is a new firmware available.

The screenshot displays the D-Link DIR-855 web interface. The top navigation bar includes 'DIR-855', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'FIRMWARE' and contains the following sections:

- FIRMWARE:** A message stating, 'There may be new firmware for your DIR-855 to improve functionality and performance. To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button below to start the firmware upgrade.' Below this message are two buttons: 'Save Settings' and 'Don't Save Settings'.
- FIRMWARE INFORMATION:** Displays 'Current Firmware Version : 1.00' and 'Current Firmware Date : 2007/10/17'. It includes a 'Check Online Now for Latest Firmware Version : [Check Now]' button.
- FIRMWARE UPGRADE:** Contains a red note: 'Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Tools → System screen.' Below the note, it states: 'To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.' There is an 'Upload : [text box] [Browse...]' field and an 'Upload' button.
- FIRMWARE UPGRADE NOTIFICATION OPTIONS:** Includes two checkboxes: 'Automatically Check Online for Latest Firmware Version : ' and 'Email Notification of Newer Firmware Version : '.

The bottom of the interface features a 'WIRELESS' section.

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.

Enable Dynamic DNS: 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.

Timeout: Enter a time (in hours).

The screenshot shows the D-Link DIR-855 web interface. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'DYNAMIC DNS' section is highlighted in orange. The main content area contains the following text and fields:

DYNAMIC DNS

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 your host name to connect to your game server no matter what your IP address is.

Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com.

Buttons: Save Settings, Don't Save Settings

DYNAMIC DNS

Enable Dynamic DNS:

Server Address: << Select Dynamic DNS Server >>

Host Name: (e.g.: me.mydomain.net)

Username or Key:

Password or Key:

Verify Password or Key:

Timeout: (hours)

Status: Disconnect

The sidebar on the right contains 'Helpful Hints...' and 'More...' links.

System Check

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.

The screenshot displays the D-Link DIR-855 web interface. At the top, the D-Link logo is visible. Below it, a navigation menu includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The TOOLS tab is selected, and the PING TEST tool is active. The interface shows a sidebar with various configuration options, a main content area with a PING TEST section containing a text input field for 'Host Name or IP Address' and 'Ping'/'Stop' buttons, and a PING RESULT section. A 'Helpful Hints...' section on the right provides instructions on how to use the ping test.

DIR-855	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
ADMIN	PING TEST				Helpful Hints...
TIME	Ping Test sends "ping" packets to test a computer on the Internet.				"Ping" checks whether a computer on the Internet is running and responding. Enter either the IP address of the target computer or enter its fully qualified domain name.
SYSLOG	PING TEST				More...
EMAIL SETTINGS	Host Name or IP Address : <input type="text"/> <input type="button" value="Ping"/> <input type="button" value="Stop"/>				
SYSTEM	PING RESULT				
FIRMWARE	Enter a host name or IP address above and click 'Ping'				
DYNAMIC DNS					
SYSTEM CHECK					
SCHEDULES					
WIRELESS					

Schedules

Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.

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

D-Link

DIR-855 // SETUP ADVANCED TOOLS STATUS SUPPORT

ADMIN
TIME
SYSLOG
EMAIL SETTINGS
SYSTEM
FIRMWARE
DYNAMIC DNS
SYSTEM CHECK
SCHEDULES

SCHEDULES

The Schedule configuration option is used to manage schedule rules for various firewall and parental control features.

Save Settings Don't Save Settings

ADD SCHEDULE RULE

Name:

Day(s): All Week Select Day(s)

Sun Mon Tue Wed Thu Fri Sat

All Day - 24 hrs:

Start Time: 0 : 0 AM (hour:minute, 12 hour time)

End Time: 0 : 0 AM (hour:minute, 12 hour time)

Save Clear

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 the **Edit** icon to change an existing schedule.

Click the **Delete** icon to permanently delete a schedule.

More...

WIRELESS

Device Information

This page displays the current information for the DIR-855. 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.

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.

The screenshot shows the D-Link DIR-855 web interface. The main content area is titled "DEVICE INFORMATION" and contains the following sections:

- GENERAL:**
 - Time: Saturday, January 31, 2004 11:53:58 AM
 - Firmware Version: 1.00, 2007/10/17
- WAN:**
 - Connection Type: DHCP Client
 - QoS Engine: Active
 - Cable Status: Disconnected
 - Network Status: Disconnected
 - Connection Up Time: N/A
 - Buttons: Release, Renew
 - MAC Address: 00:03:64:00:01:23
 - IP Address: 0.0.0.0
 - Subnet Mask: 0.0.0.0
 - Default Gateway: 0.0.0.0
 - Primary DNS Server: 0.0.0.0
 - Secondary DNS Server: 0.0.0.0
- LAN:**
 - MAC Address: 00:03:64:00:01:24
 - IP Address: 192.168.0.1
 - Subnet Mask: 255.255.255.0
 - DHCP Server: Enabled
- WIRELESS LAN (2.4GHz Band):**
 - Wireless Band: 2.4GHz Band
 - Wireless Radio: Enabled
 - MAC Address: 00:19:5E:0E:0B:52
 - Network Name (SSID): dlk
 - Channel: 1
 - Security Mode: Disabled
 - WISH: Active
 - Wi-Fi Protected Setup: Enabled/Not Configured
- WIRELESS LAN (5GHz Band):**
 - Wireless Band: 5GHz Band
 - Wireless Radio: Enabled
 - MAC Address: 00:1B:1F:F2:01:00
 - Network Name (SSID): dlk_media
 - Channel: 157
 - Security Mode: Disabled
 - WISH: Active
 - Wi-Fi Protected Setup: Enabled/Not Configured
- LAN COMPUTERS:**

IP Address	Name (if any)	MAC
192.168.0.100	BLA00-53	00:0F:60:5A:e7:de
192.168.0.199	BLA00-56	00:1c:cc:39:59:b1

Log

The router automatically logs (records) events of possible interest in its 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 email address configured in the **Tools > Email** screen.

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

D-Link

DIR-855 // SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICE INFO LOGS STATISTICS INTERNET SESSIONS WIRELESS WISH SESSIONS

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

Apply Log Settings Now

LOG DETAILS

Refresh Clear Email Now Save Log

[INFO] Sat Jan 31 11:54:25 2004 Log viewed by IP address 192.168.0.156
 [INFO] Sat Jan 31 11:22:36 2004 Allowed configuration authentication by IP address 192.168.0.156
 [INFO] Sat Jan 31 11:22:23 2004 Latest firmware version 1.0 is available
 [INFO] Sat Jan 31 11:22:23 2004 Firmware upgrade server support.dlink.com is at IP address 64.7.210.130
 [INFO] Sat Jan 31 11:22:23 2004 Starting WAN Services
 [INFO] Sat Jan 31 11:22:23 2004 Estimated rate of link is 996 kbps
 [INFO] Sat Jan 31 11:21:59 2004 Lease 192.168.0.156 renewed by client 0011092A9411
 [INFO] Sat Jan 31 11:21:59 2004 Assigned new lease 192.168.0.156 to client 0011092A9411
 [WARN] Sat Jan 31 11:21:59 2004 Lease expired 192.168.0.156 - was reassigned because a client specifically requested this address
 [INFO] Sat Jan 31 11:21:53 2004 Initialization complete, starting DHCP server
 [INFO] Sat Jan 31 11:21:51 2004 Estimating speed of WAN interface
 [INFO] Sat Jan 31 11:21:51 2004 WAN interface is up. Connection to Internet established with IP Address 192.168.111.65 and default gateway 192.168.111.1
 [INFO] Sat Jan 31 11:21:51 2004 Obtained IP Address using DHCP. IP address is 192.168.111.65
 [INFO] Sat Jan 31 11:21:51 2004 DHCP Server Parameter 15 was added to the parameter database
 [INFO] Sat Jan 31 11:21:50 2004 DHCP Server Parameter 19 was added to the parameter database
 [INFO] Sat Jan 31 11:21:50 2004 DHCP Server Parameter 3 was added to the parameter database
 [INFO] Sat Jan 31 11:21:50 2004 DHCP Server Parameter 1 was added to the parameter database
 [INFO] Sat Jan 31 11:21:48 2004 Bringing up WAN using DHCP
 [INFO] Sat Jan 31 11:21:48 2004 WAN interface cable has been connected
 [INFO] Sat Jan 31 11:21:46 2004 DHCP Server Parameter 6 was added to the parameter database
 [INFO] Sat Jan 31 11:21:46 2004 LAN interface is up
 [INFO] Sat Jan 31 11:21:46 2004 LAN Ethernet Carrier Detected
 [INFO] Sat Jan 31 11:21:46 2004 Device initialized
 [INFO] Sat Jan 31 11:21:46 2004 Wireless Link is up
 [INFO] Sat Jan 31 11:21:46 2004 Stored configuration to non-volatile memory
 [INFO] Sat Jan 31 11:21:45 2004 No Internet access policy is in effect. Unrestricted Internet access allowed to everyone
 [INFO] Thu Jan 01 00:00:00 1970 Loaded configuration from non-volatile memory

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...

WIRELESS

Stats

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DIR-855 on both the Internet, LAN ports and both the 802.11n/g and 802.11a wireless bands. The traffic counter will reset if the device is rebooted.

DIR-855	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT						
DEVICE INFO LOGS STATISTICS INTERNET SESSIONS WIRELESS WISH SESSIONS	TRAFFIC STATISTICS Traffic Statistics display Receive and Transmit packets passing through your router. <input type="button" value="Refresh Statistics"/> <input type="button" value="Clear Statistics"/>				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. More...						
	LAN STATISTICS <table border="0"> <tr> <td>Sent : 6181</td> <td>Received : 3222</td> </tr> <tr> <td>TX Packets Dropped : 4</td> <td>RX Packets Dropped : 0</td> </tr> <tr> <td>Collisions : 0</td> <td>Errors : 0</td> </tr> </table>				Sent : 6181	Received : 3222	TX Packets Dropped : 4	RX Packets Dropped : 0	Collisions : 0	Errors : 0	
Sent : 6181	Received : 3222										
TX Packets Dropped : 4	RX Packets Dropped : 0										
Collisions : 0	Errors : 0										
	WAN STATISTICS <table border="0"> <tr> <td>Sent : 0</td> <td>Received : 0</td> </tr> <tr> <td>TX Packets Dropped : 0</td> <td>RX Packets Dropped : 0</td> </tr> <tr> <td>Collisions : 0</td> <td>Errors : 0</td> </tr> </table>				Sent : 0	Received : 0	TX Packets Dropped : 0	RX Packets Dropped : 0	Collisions : 0	Errors : 0	
Sent : 0	Received : 0										
TX Packets Dropped : 0	RX Packets Dropped : 0										
Collisions : 0	Errors : 0										
	WIRELESS STATISTICS – 2.4GHZ BAND <table border="0"> <tr> <td>Sent : 338</td> <td>Received : 41</td> </tr> <tr> <td>TX Packets Dropped : 0</td> <td>RX Packets Dropped : 0</td> </tr> <tr> <td></td> <td>Errors : 4</td> </tr> </table>				Sent : 338	Received : 41	TX Packets Dropped : 0	RX Packets Dropped : 0		Errors : 4	
Sent : 338	Received : 41										
TX Packets Dropped : 0	RX Packets Dropped : 0										
	Errors : 4										
	WIRELESS STATISTICS – 5GHZ BAND <table border="0"> <tr> <td>Sent : 381</td> <td>Received : 0</td> </tr> <tr> <td>TX Packets Dropped : 0</td> <td>RX Packets Dropped : 0</td> </tr> <tr> <td></td> <td>Errors : 0</td> </tr> </table>				Sent : 381	Received : 0	TX Packets Dropped : 0	RX Packets Dropped : 0		Errors : 0	
Sent : 381	Received : 0										
TX Packets Dropped : 0	RX Packets Dropped : 0										
	Errors : 0										
WIRELESS											

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.

D-Link

DIR-855 //

SETUP **ADVANCED** **TOOLS** **STATUS** **SUPPORT**

INTERNET SESSIONS

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

Local	NAT	Internet	Protocol	State	Dir	Priority	Time Out

Helpful Hints...

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

[More...](#)

WIRELESS

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.

The screenshot shows the D-Link DIR-855 web interface. The top navigation bar includes 'DIR-855', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists 'DEVICE INFO', 'LOGS', 'STATISTICS', 'INTERNET SESSIONS', 'WIRELESS', and 'WISH SESSIONS'. The main content area is titled 'WIRELESS' and contains the following information:

View the wireless clients that are connected to your wireless router.

NUMBER OF WIRELESS CLIENTS – 2.4GHZ BAND: 0

MAC Address	IP Address	Mode	Rate	Signal (%)
No clients listed.				

NUMBER OF WIRELESS CLIENTS – 5GHZ BAND: 0

MAC Address	IP Address	Mode	Rate	Signal (%)
No clients listed.				

Helpful Hints... This is a list of all wireless clients that are currently connected to your wireless router. [More...](#)

WISH

The WISH details page displays full details of wireless clients that are connected when WISH is enabled.

The screenshot shows the D-Link DIR-855 web interface. The top navigation bar includes 'DIR-855', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists 'DEVICE INFO', 'LOGS', 'STATISTICS', 'INTERNET SESSIONS', 'WIRELESS', and 'WISH SESSIONS'. The main content area is titled 'WISH SESSIONS' and contains the following information:

The WISH Sessions page displays full details of active local wireless sessions through your router when WISH has been enabled. A WISH session is a conversation between a program or application on a wirelessly connected LAN-side computer and another computer, however connected.

WISH SESSIONS

Originator	Target	Protocol	State	Priority	Time Out
No sessions listed.					

Helpful Hints... This is a list of all active conversations involving wireless clients in the local network. [More...](#)

Support

The screenshot displays the D-Link DIR-855 web interface. At the top, the D-Link logo is visible. Below it, a navigation bar contains tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The SUPPORT tab is currently selected. On the left side, a vertical menu lists various sections: MENU, SETUP, ADVANCED, TOOLS, STATUS, and GLOSSARY. The main content area is titled 'SUPPORT MENU' and contains several sections of help links:

- SUPPORT MENU**
 - [Setup](#)
 - [Advanced](#)
 - [Tools](#)
 - [Status](#)
 - [Glossary](#)
- SETUP HELP**
 - [Internet Connection](#)
 - [WAN](#)
 - [Wireless](#)
 - [Network Settings](#)
- ADVANCED HELP**
 - [Virtual Server](#)
 - [Port Forwarding](#)
 - [Application Rules](#)
 - [QOS ENGINE](#)
 - [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](#)

At the bottom of the interface, the word 'WIRELESS' is displayed in a dark bar.

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-855 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:

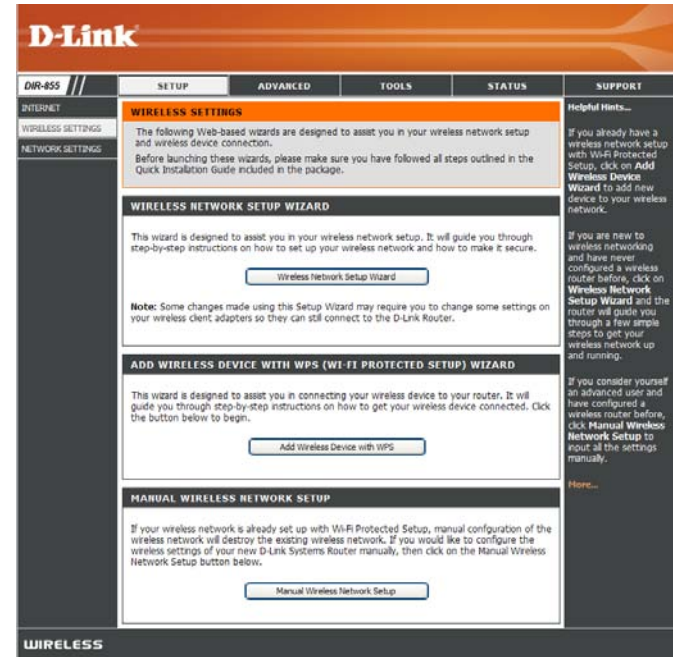
- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead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

To run the security wizard, click on Setup at the top and then click **Launch Wireless Security Setup Wizard**.



Check the **Manually set 5GHz band Network Name...** box to manually set your desired wireless network name for the 5GHz band.

Type your desired wireless network name (SSID).

Automatically: Select this option to automatically generate the router's network key and click **Next**.

Manually: Select this option to manually enter your network key and click **Next**.

Check the **“Use WPA encryption...”** box to use WPA.

STEP 1: WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

Give your network a name, using up to 32 characters.

Network Name (SSID) 2.4GHz Band :

Manually set 5GHz band Network Name (SSID)

Network Name (SSID) 5GHz Band :

Automatically assign a network key for both 2.4GHz and 5GHz band (Recommended)
To prevent outsiders from accessing your network, the router will automatically assign a security (also called WEP or WPA key) to your network.

Manually assign a network key
Use this options if you prefer to create our own key.

Use WPA encryption instead of WEP(WPA is stronger than WEP and all D-Link wireless client adapters support WPA)

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

If you selected **Automatically**, the summary window will display your settings. Write down the security key and enter this on your wireless clients. Click **Save** to save your settings.

SETUP COMPLETE!

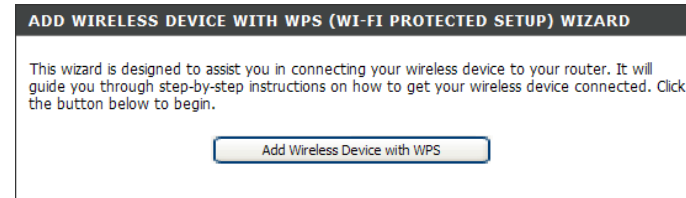
Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Wireless Network Name (SSID) : dlink
Wep Key Length : 128 bits
Default WEP Key to Use : 1
Authentication : Both
Wep Key : 6494971F655A79EA71AC7268F0

Wireless Network Name (SSID) : dlink_media
Wep Key Length : 128 bits
Default WEP Key to Use : 1
Authentication : Both
Wep Key : 6494971F655A79EA71AC7268F0

Add Wireless Device with WPS Wizard

From the **Basic > Wizard** screen, click **Add Wireless Device with WPS**.



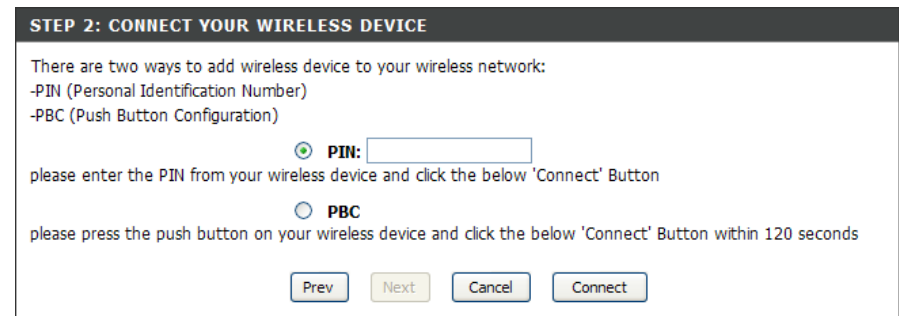
Select **Auto** to add a wireless client using WPS (Wi-Fi Protected Setup). Once you select **Auto** and click **Connect**, you will have a 120 second time limit to apply the settings to your wireless client(s) and successfully establish a connection.

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**.
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 two wireless security modes including: WPA-Personal, and WPA-Enterprise. 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

WPA requires stations to use high grade encryption and authentication. For legacy compatibility, use **WPA or WPA2** mode. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. In this mode, legacy stations are not allowed access with WPA security. The AES cipher will be used across the wireless network to ensure best security.

WPA Mode :

Cipher Type :

Group Key Update Interval : (seconds)

PRE-SHARED KEY

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**.
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 two wireless security modes including: WPA-Personal, and WPA-Enterprise. 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

WPA requires stations to use high grade encryption and authentication. For legacy compatibility, use **WPA** or **WPA2** mode. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. In this mode, legacy stations are not allowed access with WPA security. The AES cipher will be used across the wireless network to ensure best security.

WPA Mode :

Cipher Type :

Group Key Update Interval : (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 : (minutes)

RADIUS server IP Address :

RADIUS server Port :

RADIUS server Shared Secret :

MAC Address Authentication :

[Advanced >>](#)

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 : (minutes)

RADIUS server IP Address :

RADIUS server Port :

RADIUS server Shared Secret :

MAC Address Authentication :

[<< Advanced](#)

Optional backup RADIUS server :

Second RADIUS server IP Address :

Second RADIUS server Port :

Second RADIUS server Shared Secret :

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.

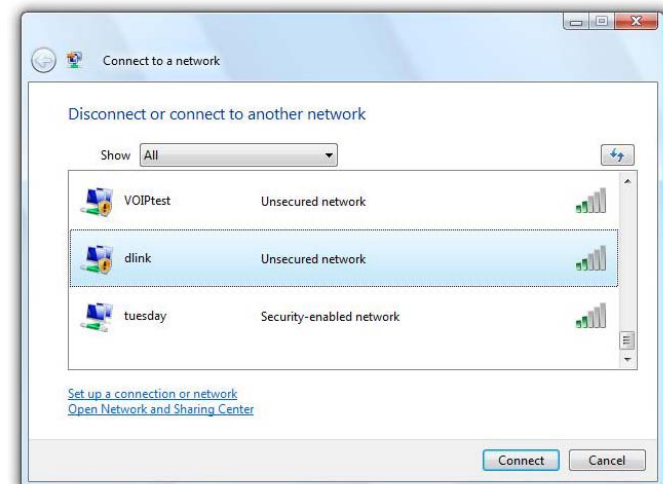
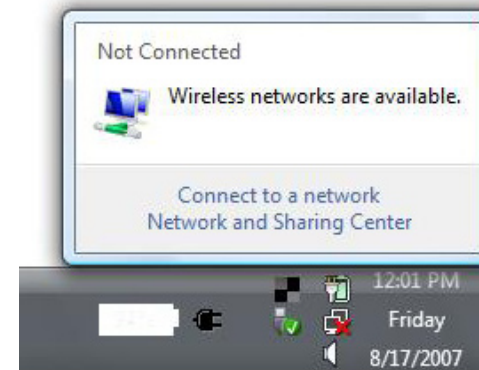
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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.

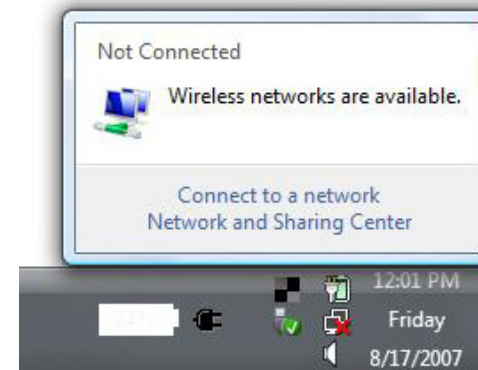
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



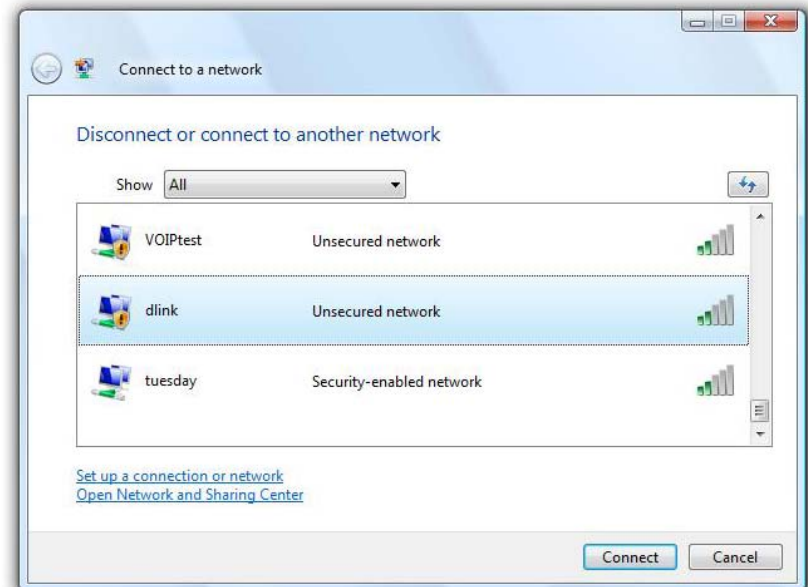
Configure Wireless Security

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**.

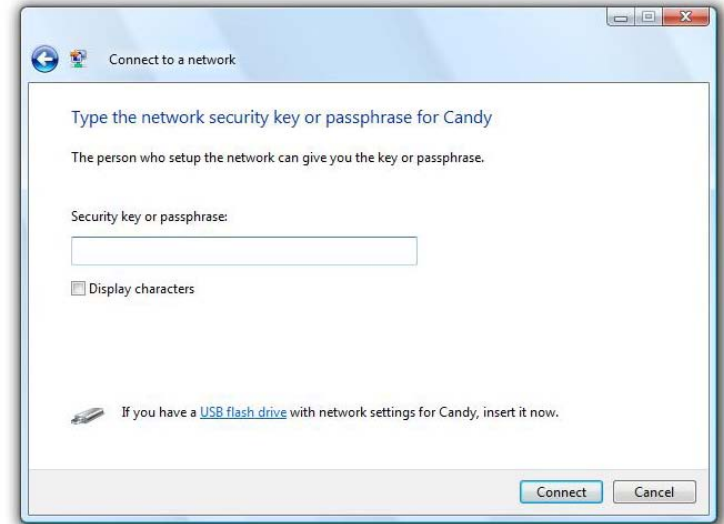


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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.



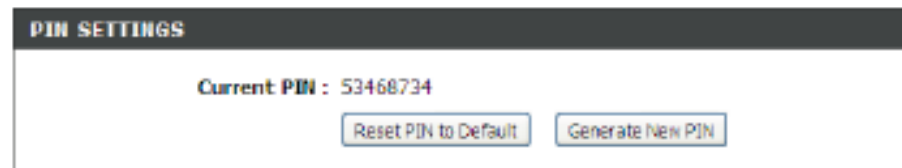
Connect Using WCN 2.0 in Windows Vista™

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.

For additional information, please refer to page 47.



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.

Connect to a Wireless Network 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.

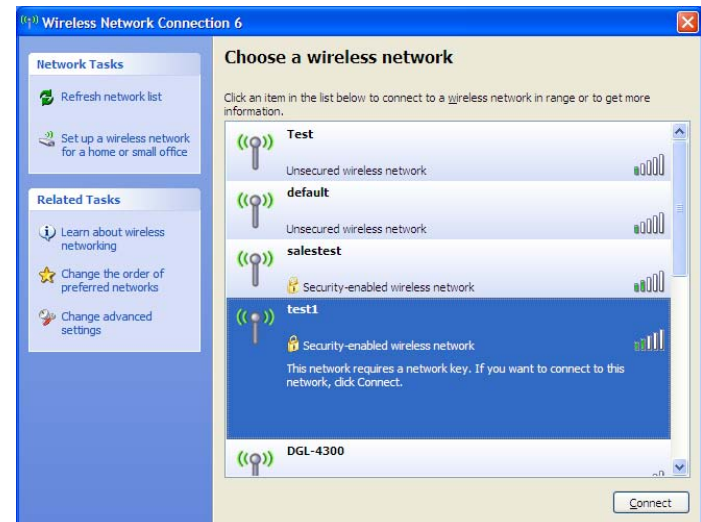
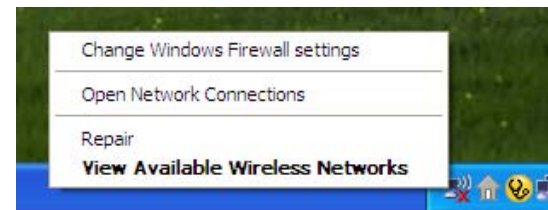
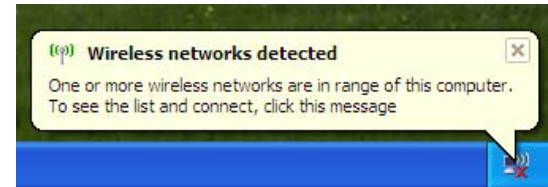
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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.

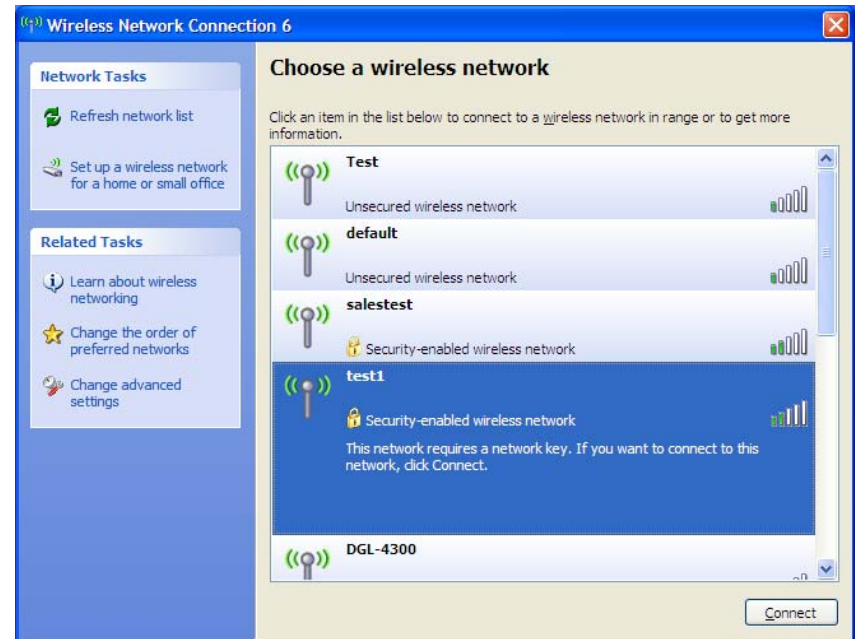
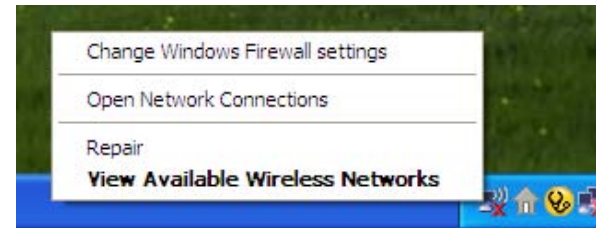
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



Configure WPA-PSK

It is recommended to enable WPA 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 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.

