

Firewall Settings

A firewall protects your network from the outside world. The D-Link DIR-665 offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

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

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

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

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

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

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

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

The screenshot displays the D-Link DIR-665 Firewall Settings page. The interface includes a navigation menu on the left with options like SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The main content area is titled 'FIREWALL SETTINGS' and contains 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'.
- Enable SPI:** A checkbox that is checked.
- NAT ENDPOINT FILTERING:** Contains two sections:
 - UDP Endpoint Filtering:** Radio buttons for 'Endpoint Independent', 'Address Restricted' (selected), and 'Port And Address Restricted'.
 - TCP Endpoint Filtering:** Radio buttons for 'Endpoint Independent' (selected), 'Address Restricted', and 'Port And Address Restricted'.
- ANTI-SPOOF CHECKING:** Includes 'Enable anti-spoof checking:' with an unchecked checkbox.
- DMZ HOST:** Includes a description of the DMZ option, a 'Note' about security risks, and an 'Enable DMZ Host:' checkbox (unchecked). Below it is a 'DMZ IP Address:' field with '0.0.0.0' and a 'Computer Name' dropdown menu.
- APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION:** Includes checkboxes for 'PPTP', 'IPSec (VPN)', 'RTSP', and 'SIP', all of which are checked.

On the right side, there is a 'Helpful Hints...' section with additional information and a 'More...' link.

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.

RTSP: Allows applications that use Real Time Streaming Protocol to receive streaming media from the internet. QuickTime and Real Player are some of the common applications using this protocol.

SIP: Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.

Routing

The Routing option is an advanced method of customizing specific routes of data through your network.

Destination IP: Enter the IP address of packets that will take this route.

Netmask: Enter the netmask of the route, please note that the octets must match your destination IP address.

Gateway: Enter your next hop gateway to be taken if this route is used.

Metric: The route metric is a value from 1 to 16 that indicates the cost of using this route. A value 1 is the lowest cost and 15 is the highest cost.

Interface: Select the interface that the IP packet must use to transit out of the router when this route is used.

Product Page: DIR-665 Hardware Version: A1 Firmware Version: 1.00

D-Link

DIR-665 // SETUP ADVANCED TOOLS STATUS SUPPORT

ROUTING :

This Routing page allows you to specify custom routes that determine how data is moved around your network.

Save Settings Don't Save Settings

32 -- ROUTE LIST

	Name	Destination IP	Metric	Interface
<input type="checkbox"/>	<input type="text"/>	<input type="text"/> 0.0.0.0	<input type="text"/> 1	<input type="text"/> WAN
	Netmask	gateway		
	<input type="text"/> 0.0.0.0	<input type="text"/> 0.0.0.0		
<input type="checkbox"/>	<input type="text"/>	<input type="text"/> 0.0.0.0	<input type="text"/> 1	<input type="text"/> WAN
	Netmask	gateway		
	<input type="text"/> 0.0.0.0	<input type="text"/> 0.0.0.0		
<input type="checkbox"/>	<input type="text"/>	<input type="text"/> 0.0.0.0	<input type="text"/> 1	<input type="text"/> WAN
	Netmask	gateway		
	<input type="text"/> 0.0.0.0	<input type="text"/> 0.0.0.0		
<input type="checkbox"/>	<input type="text"/>	<input type="text"/> 0.0.0.0	<input type="text"/> 1	<input type="text"/> WAN
	Netmask	gateway		
	<input type="text"/> 0.0.0.0	<input type="text"/> 0.0.0.0		

Helpful Hints..

Each route has a check box next to it, check this box if you want the route to be enabled.

The name field allows you to specify a name for identification of this route, e.g. "Network Z"

The destination IP address is the address of the host or network you wish to reach.

The netmask field identifies the portion of the destination IP in use.

The gateway IP address is the IP address of the router, if any, used to reach the specified destination.

[More...](#)

Advanced Wireless Settings

Transmit Power: Set the transmit power of the antennas.

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

RTS Threshold: This value should remain at its default setting of 2342. If inconsistent data flow is a problem, only a minor modification should be made.

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.

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

WMM Enable: Check box if you wish to enable this feature.

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.

Product Page: DIR-665 Hardware Version: A1 Firmware Version: 1.00

D-Link

DIR-665 // SETUP ADVANCED TOOLS STATUS SUPPORT

ADVANCED WIRELESS

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

Save Settings Don't Save Settings

ADVANCED WIRELESS SETTINGS

Transmit Power : High

Beacon Period : 100 (20..1000)

RTS Threshold : 2347 (0..2347)

DTIM Interval : 1 (1..255)

WLAN Partition :

WMM Enable :

Short GI :

Helpful Hints...

It is recommended that you leave these parameters at their default values. Adjusting them could limit the performance of your wireless network.

Use **802.11d** only for countries where it is required.

Enabling **WMM** can help control latency and jitter when transmitting multimedia content over a wireless connection.

[More...](#)

Advanced Network Settings

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

Internet Ping: Unchecking the box will not allow the DIR-665 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”.

Internet 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.

Product Page: DIR-665 Hardware Version: A1 Firmware Version: 1.00

D-Link

DIR-665 // 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 : Allow_All

WAN PORT SPEED

WAN Port Speed : 10/100/1000Mbps Auto

MULTICAST STREAMS

Enable Multicast Streams :

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.

Gateway Name: Enter a name for the DIR-665 router.

Enable Graphical Authentication: Enables a challenge-response test to require users to type letters or numbers from a distorted image displayed on the screen to prevent online hackers and unauthorized users from gaining access to your router's network settings.

Enable Remote Management: Remote management allows the DIR-665 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-665.

Example: `http://x.x.x.x:8080` whereas x.x.x.x is the Internet IP address of the DIR-665 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-665 web management interface. At the top, it displays 'Product Page: DIR-665', 'Hardware Version: A1', and 'Firmware Version: 1.00'. The D-Link logo is prominently displayed. Below the logo, there are navigation tabs: 'DIR-665', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'ADVANCED' tab is selected, and the 'ADMINISTRATOR SETTINGS' sub-tab is active. The page content is as follows:

- ADMINISTRATOR SETTINGS:** A message states: 'The '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. By default there is no password configured. It is highly recommended that you create a password to keep your router secure.' Below this message are two buttons: 'Save Settings' and 'Don't Save Settings'.
- ADMIN PASSWORD:** A section titled 'Please enter the same password into both boxes, for confirmation.' containing two input fields: 'Password' and 'Verify Password'.
- USER PASSWORD:** A section titled 'Please enter the same password into both boxes, for confirmation.' containing two input fields: 'Password' and 'Verify Password'.
- SYSTEM NAME:** A section with the label 'Gateway Name' and a text input field containing 'DIR-665'.
- ADMINISTRATION:** A section with several settings:
 - 'Enable Graphical Authentication':
 - 'Enable Remote Management':
 - 'Remote Admin Port': A text input field containing '8080'.
 - 'Remote Admin Inbound Filter': A dropdown menu set to 'Allow All'.
 - 'Detail': A text input field containing 'Allow All'.

On the right side of the page, there is a 'Helpful Hints...' section with the following text: 'For security reasons, it is recommended that you change the password for the Admin and User accounts. Be sure to write down the new and passwords to avoid having to reset the router in case they are forgotten. Enabling Remote Management, allows you or others to change the router configuration from a computer on the Internet. Choose a port to open for remote management. Select a filter that controls access as needed for this admin port. If you do not see the filter you need in the list of filters, go to the Advanced -- Inbound Filter screen and create a new filter. More...'

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**.

Product Page: DIR-665 Hardware Version: A1 Firmware Version: 1.00

D-Link

DIR-665 // SETUP ADVANCED TOOLS STATUS SUPPORT

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

TIME

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 NTP (Network Time Protocol) Server. Daylight Saving can also be configured to adjust the time when needed

Save Settings Don't Save Settings

TIME CONFIGURATION

Time : Friday, September 18, 2009 6:33:30 AM
Time Zone : (GMT-08:00) Pacific Time (US/Canada), Tijuana
Enable Daylight Saving :
Daylight Saving Dates :
DST Start : Mar 3rd Sun 1 am
DST End : Nov 2nd Sun 1 am

AUTOMATIC TIME CONFIGURATION

Enable NTP Server :
NTP Server Used : << Select NTP Server

SET THE DATE AND TIME MANUALLY

Date And Time : Year 2009 Month Sep Day 18
Hour 06 Minute 33 Second 27 AM
Copy Your Computer's Time Settings

Helpful Hints...
Good timekeeping is important for accurate logs and scheduled firewall rules.
More...

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).

Product Page: DIR-665 Hardware Version: A1 Firmware Version: 1.00

D-Link

DIR-665 // SETUP ADVANCED **TOOLS** STATUS SUPPORT

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

SYSLOG

The SysLog options allow you to send log information to a SysLog Server.

Save Settings Don't Save Settings

SYSLOG SETTINGS

Enable Logging To Syslog Server :

Syslog Server IP Address : 0.0.0.0 << Computer Name ▾

Helpful Hints...

A System Logger (syslog) is a server that collects in one place the logs from different sources. If the LAN includes a syslog server, you can use this option to send the router's logs to that server.

[More...](#)

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.

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**.

Product Page: DIR-665 Hardware Version: A1 Firmware Version: 1.00

D-Link

DIR-665 // SETUP ADVANCED TOOLS STATUS SUPPORT

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

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.

Save Settings Don't Save Settings

EMAIL NOTIFICATION

Enable Email Notification :

EMAIL SETTINGS

From Email Address :
To Email Address :
SMTP Server Address :
Enable Authentication :
Account Name : user
Password :
Verify Password :

EMAIL LOG WHEN FULL OR ON SCHEDULE

On Log Full :
On Schedule :
Schedule : Never
Detail : Never

Helpful Hints...
You may want to make the email settings similar to those of your email client program.
More...

System Settings

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

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

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

Reboot Device: Click to reboot the router.

Product Page: DIR-665 Hardware Version: A1 Firmware Version: 1.00

D-Link

DIR-665 // SETUP ADVANCED **TOOLS** STATUS SUPPORT

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

SYSTEM SETTINGS

The System Settings section allows you to reboot the device, or 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 have created.

The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.

SYSTEM SETTINGS

Save To Local Hard Drive:

Load From Local Hard Driver:

Restore To Factory Default:
Restore all settings to the factory defaults.

Reboots the Device:

Helpful Hints...

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 Online Now for Latest Firmware Version** 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 Options: 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.

Product Page: DIR-665 Hardware Version: A1 Firmware Version: 1.00

D-Link

DIR-665 // SETUP ADVANCED TOOLS STATUS SUPPORT

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

FIRMWARE

There may be new firmware for your DIR-665 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.

FIRMWARE INFORMATION

Current Firmware Version : 1.00
Current Firmware Date : Thu, 17, Sep, 2009
Check Online Now for Latest Firmware Version :

FIRMWARE UPGRADE

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.

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.

Helpful Hints...
Firmware updates are released periodically to improve the functionality of your router and to add features. If you run into a problem with a specific feature of the router, check if updated firmware is available for your router.
[More...](#)

DDNS

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

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

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

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

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

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

Timeout: Enter a time (in hours).

The screenshot shows the D-Link DIR-665 web interface. At the top, it displays 'Product Page: DIR-665', 'Hardware Version: A1', and 'Firmware Version: 1.00'. The D-Link logo is prominently displayed. Below the logo is a navigation bar with tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'DYNAMIC DNS' section is highlighted in orange. It contains an introductory text block explaining the DDNS feature and a link to sign up for D-Link's Free DDNS service at www.dlinkddns.com. Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. The 'DYNAMIC DNS SETTINGS' section is below, featuring a checked 'Enable Dynamic DNS' checkbox. The 'Server Address' field is set to 'dlinkddns.com(Free)' with a dropdown menu open showing options: 'Select Dynamic DNS Server', 'dlinkddns.com(Free)', 'dyndns.com(Custom)', and 'dyndns.com(Free)'. Other fields include 'Host Name', 'Username or Key', 'Password or Key', 'Verify Password or Key', and 'Timeout' (set to 576 hours). The 'Status' is currently 'Disconnected'.

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-665 web interface. At the top, it shows 'Product Page: DIR-665', 'Hardware Version: A1', and 'Firmware Version: 1.00'. The D-Link logo is prominently displayed. Below the logo is a navigation menu with tabs for 'DIR-665 //', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'TOOLS' tab is selected, and the 'PING TEST' option is highlighted in orange. The main content area is divided into three sections: a description of the Ping Test, a form for entering a host name or IP address with a 'ping' button, and a section for displaying ping results. A 'Helpful Hints...' sidebar on the right provides additional information about the Ping Test function.

DIR-665 //	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
ADMIN	PING TEST				Helpful Hints... "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. More...
TIME	Ping Test sends "ping" packets to test a computer on the Internet.				
SYSLOG	PING TEST Host Name or IP Address : <input type="text"/> <input type="button" value="ping"/>				
EMAIL SETTINGS	PING RESULT				
SYSTEM					
FIRMWARE					
DYNAMIC DNS					
SYSTEM CHECK					
SCHEDULES					

Schedules

Name: Enter a name for your new schedule.

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

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

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

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

Product Page: DIR-665 Hardware Version: A1 Firmware Version: 1.00

D-Link

DIR-665 // SETUP ADVANCED TOOLS STATUS SUPPORT

SCHEDULES

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

Save Settings Don't Save Settings

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.

[More...](#)

Device Information

This page displays the current information for the DIR-665. 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.

Product Page: DIR-665 Hardware Version:A1 Firmware Version:1.00

D-Link

DIR-665 // SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICE INFO

DEVICE INFORMATION

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

GENERAL

Time : Friday, September 18, 2009 6:39:01 AM
Firmware Version : 1.00 , Thu, 17, Sep, 2009

WAN

Connection Type: DHCP Client Disconnected

Cable Status : Disconnected
 Network Status : Disconnected
 Connection Up Time : N/A
 MAC Address : 00:18:e7:6a:24:f8
 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 :
 Advanced DNS : Disabled

LAN

MAC Address : 00:18:e7:6a:24:f7
 IP Address : 192.168.0.1
 Subnet Mask : 255.255.255.0
 DHCP Server : Enabled

WIRELESS LAN

Wireless Radio : Enabled
 MAC Address : 00:18:e7:6a:24:f7
 Network Name (SSID) : dlink
 Channel : 3
 Security Mode : disable

LAN COMPUTERS

IP Address	Name (if any)	MAC

IGMP MULTICAST MEMBERSHIPS

Multicast Group Address

WIRELESS

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

Log

The router automatically logs (records) events of possible interest in 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-655

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

Statistics

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DIR-665 on both the Internet and the LAN ports. The traffic counter will reset if the device is rebooted.

Product Page: DIR-665 Hardware Version: A1 Firmware Version: 1.00

D-Link

DIR-665 // SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICE INFO LOGS STATISTICS INTERNET SESSIONS ROUTING WIRELESS

TRAFFIC STATISTICS
Traffic Statistics display Receive and Transmit packets passing through your router.
Refresh Statistics Clear Statistics

LAN STATISTICS

Sent :	7466	Received :	3524
TX Packets Dropped :	0	RX Packets Dropped :	0
Collisions :	0	Errors :	0

WAN STATISTICS

Sent :	3	Received :	0
TX Packets Dropped :	0	RX Packets Dropped :	0
Collisions :	0	Errors :	0

WIRELESS STATISTICS

Sent :	3	Received :	1289
TX Packets Dropped :	0	RX Packets Dropped :	0
		Errors :	0

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

Internet Sessions

This screen displays details of the active internet sessions connected to your router.

Product Page: DIR-665 Hardware Version: A1 Firmware Version: 1.00

D-Link

DIR-665 // SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICE INFO LOGS STATISTICS INTERNET SESSIONS ROUTING WIRELESS

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

INTERNET SESSIONS

Local	NAT	Internet	Protocol	State	Dir	Time Out
-------	-----	----------	----------	-------	-----	----------

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

Routing

This screen displays the routing details configured from your router.

Product Page: DIR-665 Hardware Version: A1 Firmware Version: 1.00

D-Link

DIR-665 // SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICE INFO LOGS STATISTICS INTERNET SESSIONS ROUTING WIRELESS

ROUTING

Routing Table

This page displays the routing details configured for your router.

ROUTING TABLE

Deatination IP	NetMask	Gateway	Metric	Interface	Type	Creator
192.168.0.0	255.255.255.0	0.0.0.0	0	LAN	INTRANET	System
239.0.0.0	255.0.0.0	0.0.0.0	0	LAN	INTRANET	System
127.0.0.0	255.0.0.0	0.0.0.0	0	Local Loopback	INTRANET	System

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.

Product Page: DIR-665 Hardware Version: A1 Firmware Version: 1.00

D-Link

DIR-665 // SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICE INFO LOGS STATISTICS INTERNET SESSIONS ROUTING WIRELESS

WIRELESS

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

NUMBER OF WIRELESS CLIENTS : 0

MAC Address	IP Address	Mode	Rate	Signal(%)
-------------	------------	------	------	-----------


Helpful Hints...

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

[More...](#)

Support

Product Page: DIR-665 Hardware Version: A1 Firmware Version: 1.00



DIR-665 ///	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
MENU	SUPPORT MENU				
SETUP	<ul style="list-style-type: none"> • Setup • Advanced • Tools • Status 				
ADVANCED	SETUP HELP				
TOOLS	<ul style="list-style-type: none"> • Internet Connection • WAN • Wireless • Network Settings 				
STATUS	ADVANCED HELP				
	<ul style="list-style-type: none"> • Virtual Server • Port Forwarding • Application Rules • QoS Engine • Access Control • Website Filter • Network Filter • Firewall Settings • Inbound Filter • Advanced Wireless • Advanced Network • IPv6 				
	TOOLS HELP				
	<ul style="list-style-type: none"> • Admin • Time • Syslog • Email Settings • System • Firmware • Dynamic DNS • System Check • Schedules 				
	STATUS				
	<ul style="list-style-type: none"> • Device Info • Logs • Statistics • Internet Sessions 				

WIRELESS

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-665 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**.

Enter the SSID (Service Set Identifier) name for your network. You may also create a name using up to 32 characters. The SSID is also case sensitive. Select from the following choices:

- Automatically assign a network key
- Manually assign a network key

Click **Next** to continue.

The Setup is now complete. Keep the information provided for future reference. Click **Save** to finish.

WIRELESS SETTINGS

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

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

WIRELESS NETWORK SETUP WIZARD

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

[Wireless Connection Setup Wizard](#)

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

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

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

Network Name (SSID) :

Automatically assign a network key (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.

SETUP COMPLETE!

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

Wireless Network Name (SSID) : dlink
Wep Key Length : 128 bits
Default WEP Key to Use : 1
Authentication : Open
Wep Key : dd5ebf5ee70e86cbbb0826757

Enter the SSID (Service Set Identifier). The SSID is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive. If you selected to Manually assign a network key, click **Next** to continue.

Select a wireless security password between 8 and 63 characters.

Click **Next** to continue.

Your setup is now complete. Print the information provided or write on a piece of paper to configure the correct settings. Click **Save** to finish.

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

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

Network Name (SSID) :

Automatically assign a network key (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.

Prev Next Cancel Save

STEP 2: SET YOUR WIRELESS SECURITY PASSWORD

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

The WPA (Wi-Fi Protected Access) key must meet one of following guidelines:

- Between 8 and 63 characters (A longer WPA key is more secure than a short one)
- Exactly 64 characters using 0-9 and A-F

Wireless Security Password :

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

Prev Next Cancel

SETUP COMPLETE!

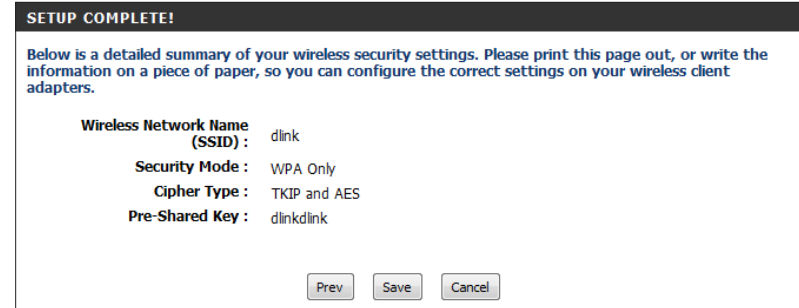
Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Wireless Network Name (SSID) : dlink
Security Mode : WPA Only
Cipher Type : TKIP and AES
Pre-Shared Key : dlinkdlink

Prev Save Cancel

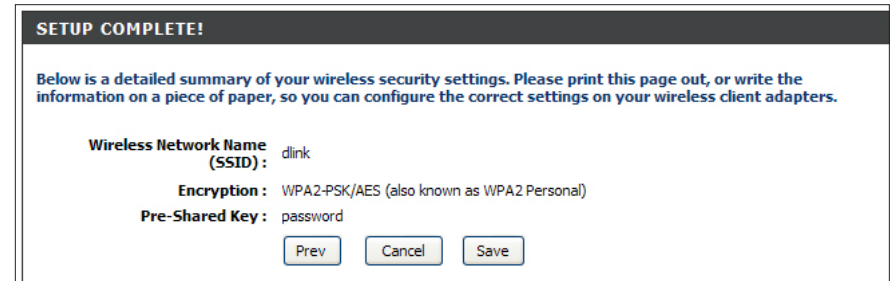
If you selected Better, the following screen will show you your Pre-Shared Key to enter on your wireless clients.

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



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

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



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

Wireless Device with WPS Wizard

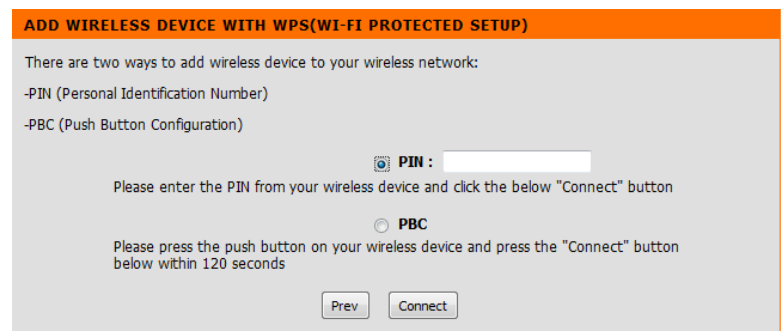
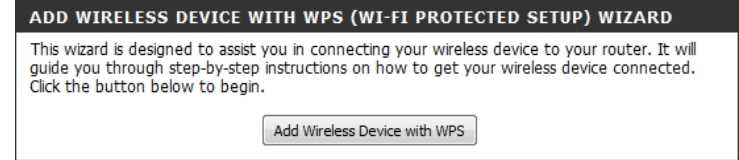
From the **Setup > Wireless Settings** screen, click **Add Wireless Device with WPS**.

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

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

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

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



Configure WPA-Personal (PSK)

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

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **WPA-Personal**.
3. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.
4. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).
5. 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.
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 on your adapter and enter the same passphrase as you did on the router.

WIRELESS SECURITY MODE

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

Security Mode :

WPA

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

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

WPA Mode :

Cipher Type :

Group Key Update Interval : (seconds)

PRE-SHARED KEY

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

Pre-Shared Key :

Configure WPA-Enterprise (RADIUS)

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

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **WPA-Enterprise**.
3. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.
4. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).
5. Next to *Authentication Timeout*, enter the amount of time before a client is required to re-authenticate (60 minutes is default).
6. Next to *RADIUS Server IP Address* enter the IP Address of your RADIUS server.
7. Next to *RADIUS Server Port*, enter the port you are using with your RADIUS server. 1812 is the default port.
8. Next to *RADIUS Server Shared Secret*, enter the security key.

WIRELESS SECURITY MODE

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

Security Mode :

WPA

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

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

WPA Mode :

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 :

9. 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.
10. Click **Advanced** to enter settings for a secondary RADIUS Server.
11. 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 :

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.

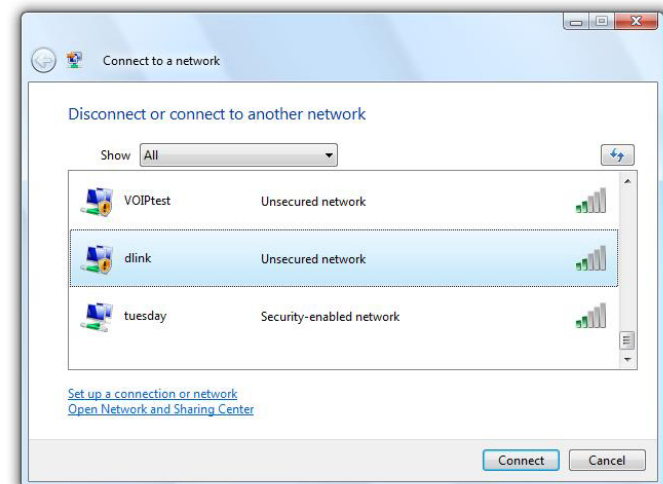
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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.

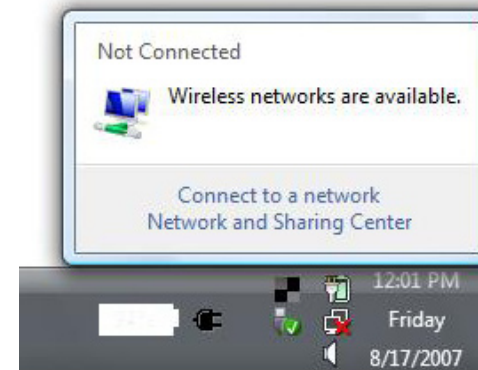
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



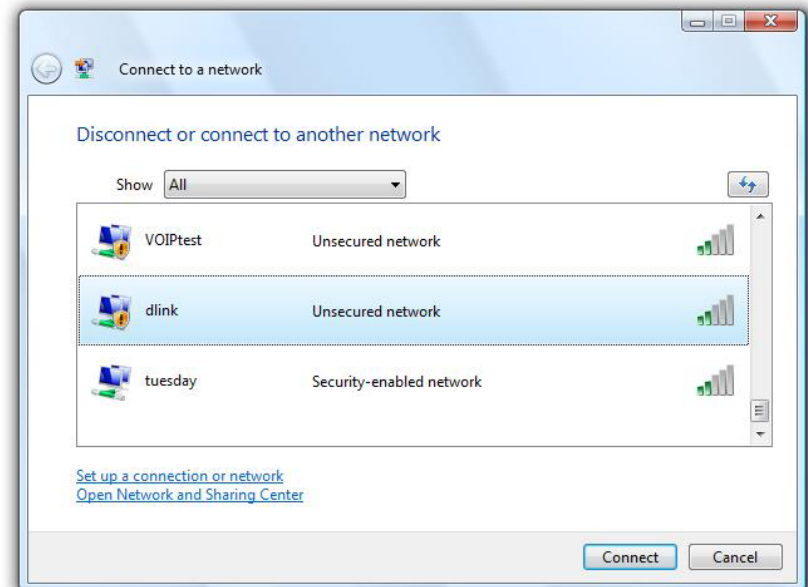
Configure Wireless Security

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**.

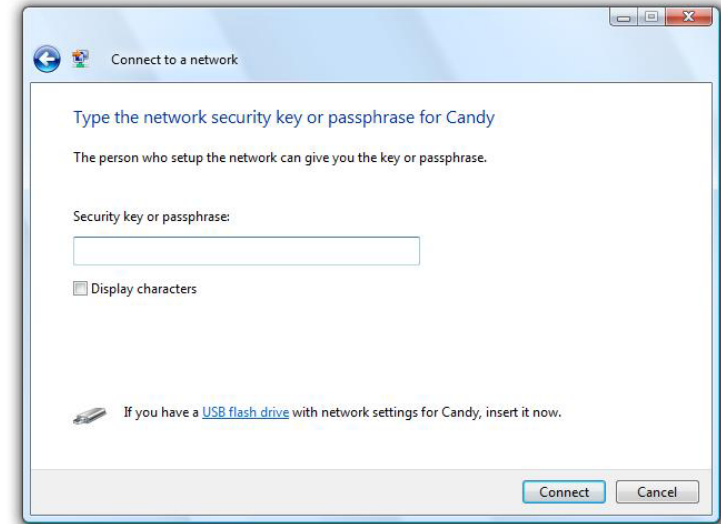


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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 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.

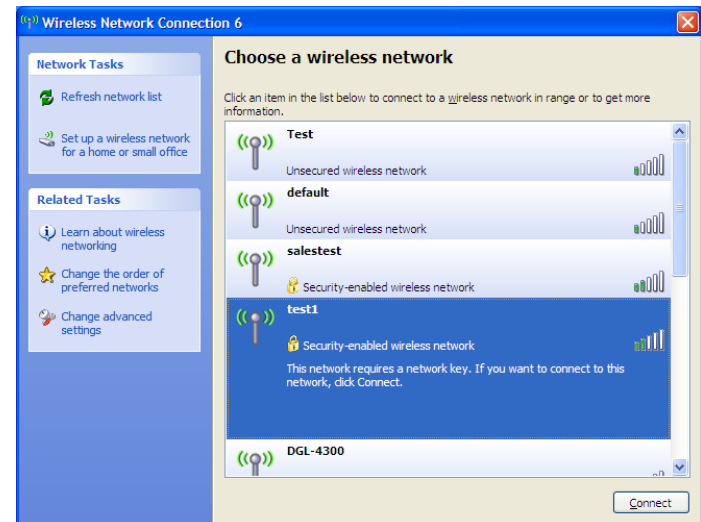
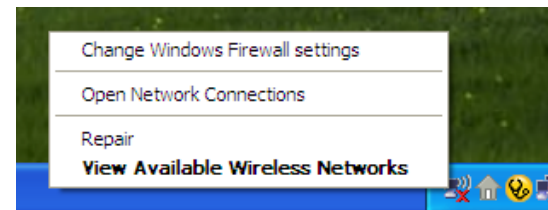
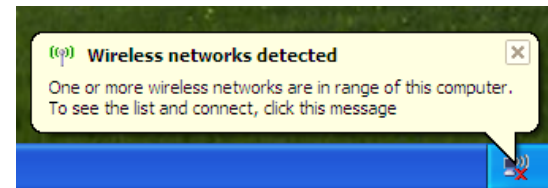
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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.

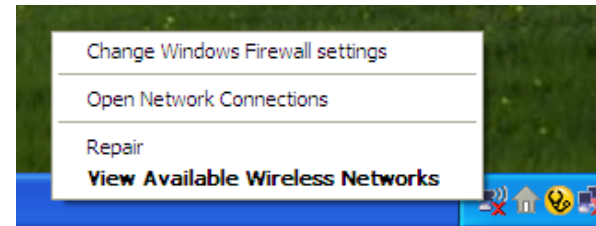
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



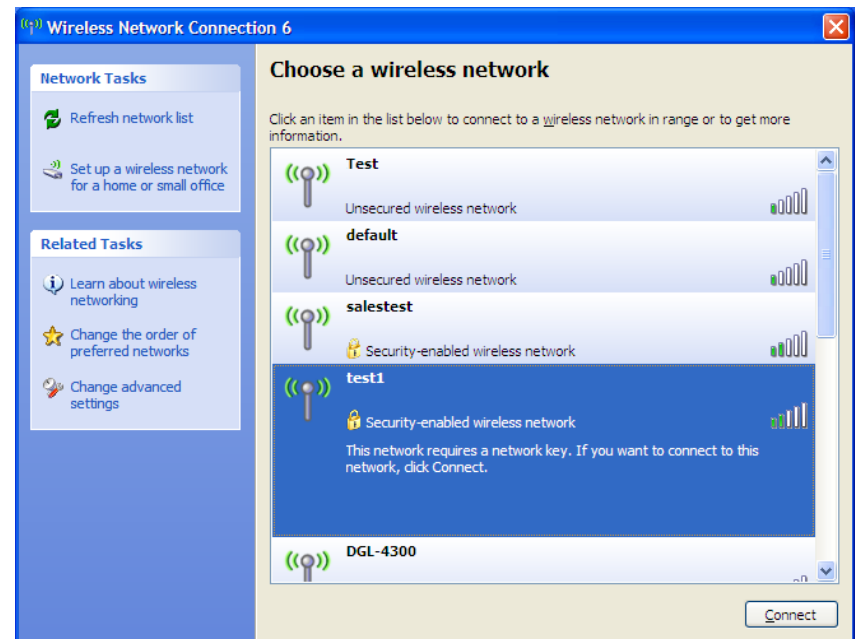
Configure WPA-PSK

It is recommended to enable 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 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**.

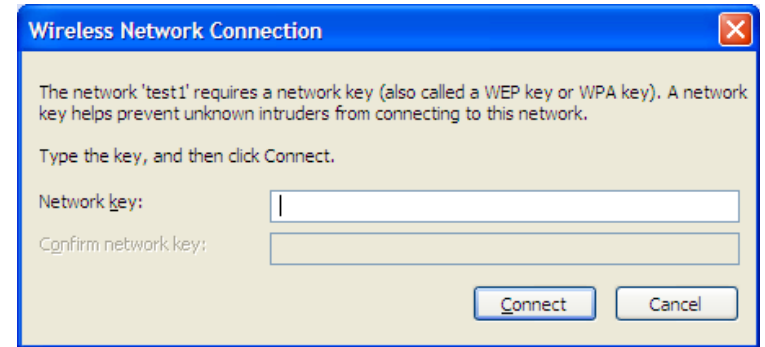


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

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



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-665. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

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

- Make sure you have an updated Java-enabled web browser. We recommend the following:
 - Internet Explorer 6.0 or higher
 - Netscape 8 or higher
 - Mozilla 1.7.12 (5.0) or higher
 - Opera 8.5 or higher
 - Safari 1.2 or higher (with Java 1.3.1 or higher)
 - Camino 0.8.4 or higher
 - Firefox 1.5 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:
 - Go to **Start > Settings > Control Panel**. Double-click the **Internet Options** Icon. From the **Security** tab, click the button to restore the settings to their defaults.
 - Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.
 - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
 - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your the web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

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

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

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

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

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

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

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

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

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

Example: **ping yahoo.com -f -l 1472**

```
C:\>ping yahoo.com -f -l 1482
Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

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

C:\>ping yahoo.com -f -l 1472
Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:
Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

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

C:\>
```

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

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

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

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