

USER MANUAL

DIR-455U

VERSION 1.0



Preface

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

Trademarks

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

Copyright © 2009 by D-Link Systems, Inc.

All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from D-Link Systems, Inc.

Table of Contents

Preface	i	L2TP	19
Trademarks	i	3G	20
Product Overview	1	Static IP	21
Package Contents	1	GRE Settings	22
System Requirements	1	Wireless Settings	24
Introduction	2	Network Settings	26
Hardware Overview	3	Router Settings	26
Rear Panel	3	DHCP Server Settings	27
Front Panel	4	VPN Settings	28
LEDs	5	Tunnel 1 - IKE	30
Installation	6	Tunnel 1 - Manual Key	34
Connect to Your Network	6	Tunnel 1 - Manual Key	36
Connect a Telephone	7	Message Service	39
Wireless Installation Considerations	8	Virtual Server	41
Configuration	9	Application Rules	42
Web-based Configuration Utility	9	QoS Engine	43
Setup Wizard	10	MAC Address Filter	44
Internet Connection Setup Wizard	10	URL Filter	45
Manual Internet Connection Setup	14	Outbound Filter	46
Internet Connection	15	Inbound Filter	47
Internet Connection Type	15	SNMP	48
Dynamic IP (DHCP)	16	Routing	49
PPPoE	17	Advanced Wireless	50
PPTP	18	Advanced Network	51
		Admin	52
		Time	53

Syslog	54	Wireless Basics	81
E-mail Settings.....	55	What is Wireless?	82
System.....	56	Tips.....	84
Firmware	57	Wireless Modes	85
Dynamic DNS	58	Networking Basics	86
System Check.....	59	Check your IP address	86
Schedules	60	Statically Assign an IP address	87
Device Information.....	61	Technical Specifications.....	88
Logs	62		
Statistics	63		
Wireless	64		
Support	65		
Wireless Security.....	66		
What is WEP?	66		
Configure WEP	67		
What is WPA?	68		
Configure WPA-PSK	69		
Configure WPA (RADIUS).....	70		
Connect to a Wireless Network.....	71		
Using Windows Vista™	71		
Configure Wireless Security	72		
Using Windows® XP.....	74		
Configure WEP	75		
Configure WPA-PSK.....	77		
Troubleshooting	79		

Package Contents

- D-Link DIR-455U Mobile Router
- Power Adapter
- Ethernet Cable
- RJ-11 Telephone Cable
- Manual and Warranty on CD
- 3G external Antenna



Note: Using a power supply with a different voltage rating than the one included with the DIR-455U will cause damage and void the warranty for this product.

System Requirements

- A compatible (U)SIM card with service.*
- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer Version 6.0 or Netscape Navigator™ Version 6.0 and above (for configuration)

*Subject to services and service terms available from your carrier.

Introduction

The D-Link HSUPA 3.75G Mobile Communication Router allows users to access worldwide mobile broadband networks. Once connected, users can transfer data, stream media, send SMS messages, and make mobile phone calls. Simply insert your UMTS/HSUPA SIM card, and share your 3.75G Internet connection through a secure 802.11g wireless network or using any of the four 10/100 Ethernet ports.

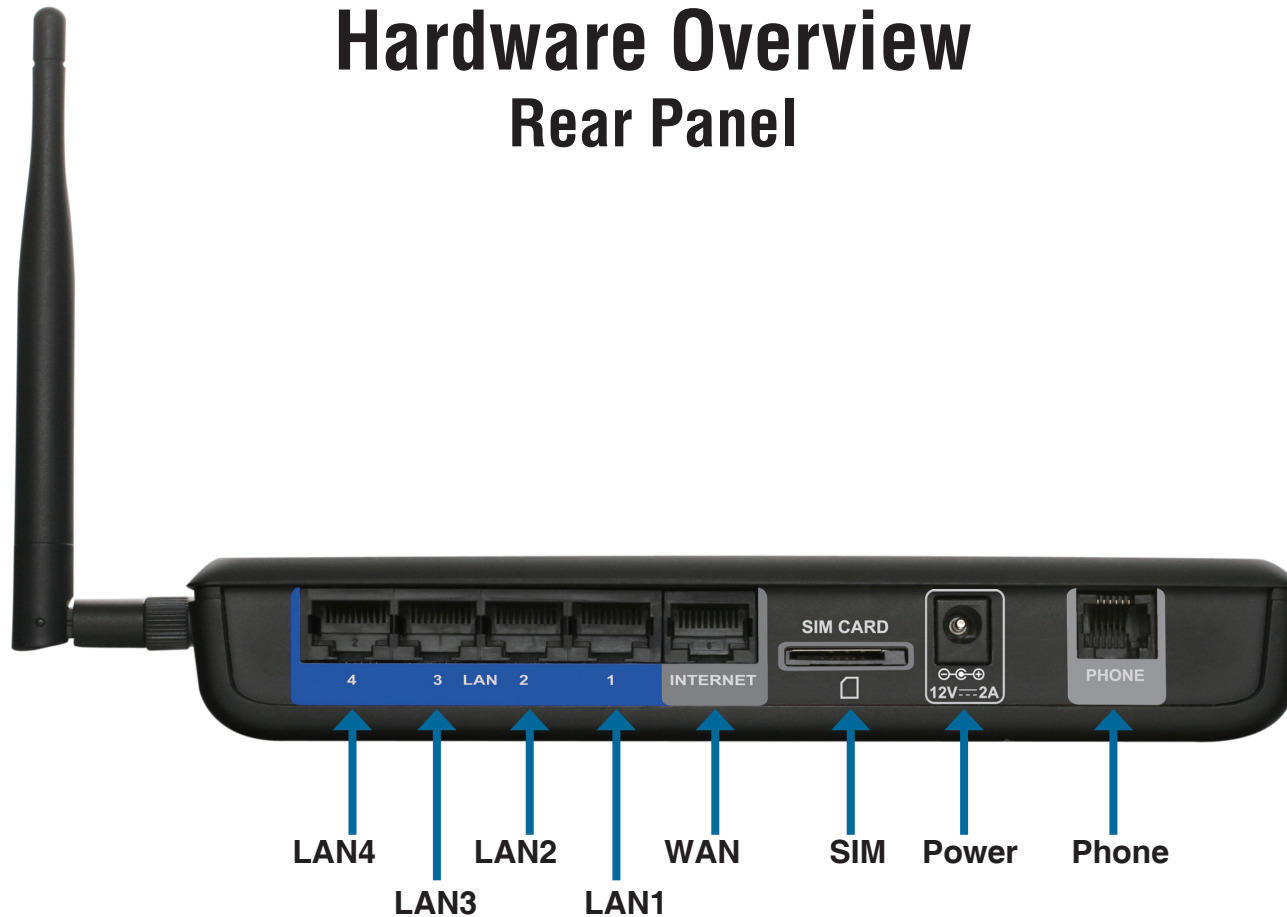
While accessing your 3.75G Internet connection, you will still have the ability to answer incoming mobile calls and respond to SMS messages. An RJ-11 jack allows you to attach a standard analog phone for high-quality mobile calls over a GSM network. Enjoy the comfort and convenience of your favorite office phone anywhere you go.

Keep your wireless network safe with WPA/WPA2 wireless encryption. The DIR-455U utilizes dual-active firewalls (SPI and NAT) to prevent potential attacks across the Internet, and supports up to five concurrent IPSec VPN tunnels.

The 3.75G Mobile Communication Router can be installed quickly and easily almost anywhere. This router is great for situations where an impromptu wireless network must be set up, or wherever conventional network access is unavailable. The DIR-455U can even be installed in buses, trains, or boats, allowing passengers to check e-mail or chat online while commuting.

Hardware Overview

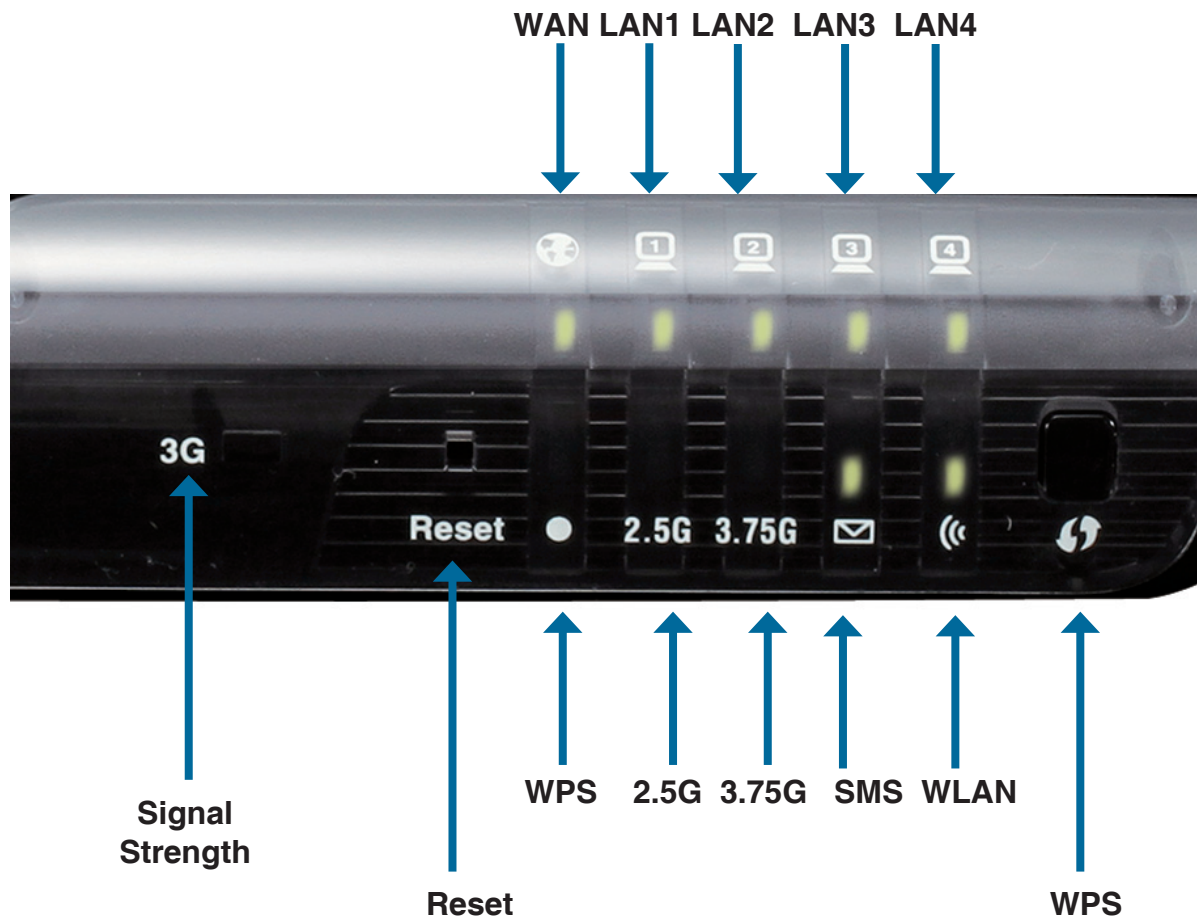
Rear Panel



Port	Function
LAN 1-4 (RJ-45)	Insert an Ethernet cable connected to a network device such as a desktop or notebook computer.
WAN (RJ-45)	Insert a standard CAT5 Ethernet cable connected to a DSL/ Cable modem or router.
SIM	Insert a standard (U)SIM card into this slot.
Power	Insert the provided DC power adapter into this socket.
Phone (RJ-11)	Insert an RJ-11 telephone cable connected to a standard landline telephone.

Hardware Overview

Front Panel



Button Name	Function
Reset	Hold this button down to reset the device.
WPS	Press this button to initiate a new WPS connection.

Hardware Overview

LEDs

LED Name	Function
WAN	Solid Green: Ethernet connection has been established Blinking Green: Data is being transferred
LAN 1-4	Solid Green: Ethernet connection has been established Blinking Green: Data is being transferred
Signal Strength	Blinking Red: No SIM card / signal or unverified PIN code Solid Red: Signal strength is at level one (weak) Solid Amber: Signal strength is at level two or three (medium) Solid Green: Signal strength is at level four or five (strong)
WPS	Slow Blinking Green: WPS is functioning normally Fast Blinking Green: WPS is functioning in PBC mode
2.5G	Solid Green: EDGE or GPRS connection has been established Blinking Green: Data is being transferred via 2G/2.5G
3.75G	Solid Green: UMTS/HSUPA/HSUPA connection is established Blinking: Data is being transferred via 3G
SMS	Solid Green: Lights up when an SMS has been received
WLAN	Solid Green: WLAN is active and available Blinking Green: Data is being transferred via WLAN

Installation

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

Connect to Your Network

Note: Ensure that your DIR-455U Mobile Router is disconnected and powered **off** before performing the installation steps below.

1. Insert a standard (U)SIM card into the **SIM** card slot on the back of the router with the gold contacts facing downwards.
2. Insert your Internet/WAN network cable into the **INTERNET** port on the back of the router.

Note: The 3.5G connection can also be used as a backup WAN. Once a backup is configured, the router will automatically use 3.75G for the Internet connection if the Ethernet WAN is not available.

3. Insert the Ethernet cable into the LAN Port 1 on the back panel of the DIR-455U Mobile Router, and an available Ethernet port on the network adapter in the computer you will use to configure the unit.

Note: The DIR-455U Mobile Router LAN Ports are “Auto-MDI/MDIX.” Therefore, patch or crossover Ethernet cables can be used.

4. Connect the power adapter to the socket on the back panel of your DIR-455U Mobile Router. Plug the other end of the power adapter into a wall outlet or power strip.
 - a. The **Status LED** will light up to indicate that power has been supplied to the router.
 - b. The LEDs on the front panel will flash on and off as the DIR-455U Mobile Router performs initialization and Internet connection processes.
 - c. After a few moments, if a connection has been established, the following LEDs will turn solid green: Power, Status, WAN, WLAN, and LAN Port 1 (or whichever port(s) your Ethernet cable has been connected to).

Caution! Always unplug/power down the router before installing or removing the SIM card. Never insert or remove the SIM card while the router is in use.

Connect a Telephone

A standard RJ-11 jack on the back of the router allows you to connect a standard analog telephone for voice calls.

Simply plug the phone cable into the jack labeled **PHONE**.

You can then use your handset to dial out as you typically would with a standard landline.

Your attached phone will also ring for any incoming voice calls.



Wireless Installation Considerations

The DIR-455U can be accessed using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the quantity, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or office. The key to maximizing the wireless range is to follow these basic guidelines:

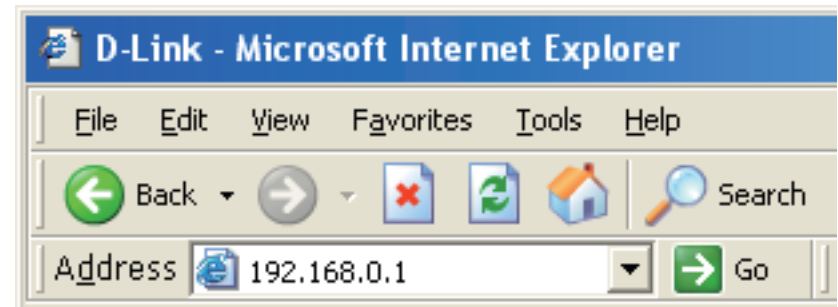
1. Minimize the number of walls and ceilings between the D-Link router and other network devices. Each wall or ceiling can reduce your adapter's range from 3 to 90 feet (1 to 30 meters).
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick. Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
3. Try to position access points, wireless routers, and computers so that the signal passes through open doorways and drywall. Materials such as glass, metal, brick, insulation, concrete and water can affect wireless performance. Large objects such as fish tanks, mirrors, file cabinets, metal doors and aluminum studs may also have a negative effect on range.
4. If you are using 2.4GHz cordless phones, make sure that the 2.4GHz phone base is as far away from your wireless device as possible. The base transmits a signal even if the phone is not in use. In some cases, cordless phones, X-10 wireless devices, and electronic equipment such as ceiling fans, fluorescent lights, and home security systems may dramatically degrade wireless connectivity.

Configuration

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

Web-based Configuration Utility

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



Type **Admin** and then enter the password. By default, the password is blank.

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

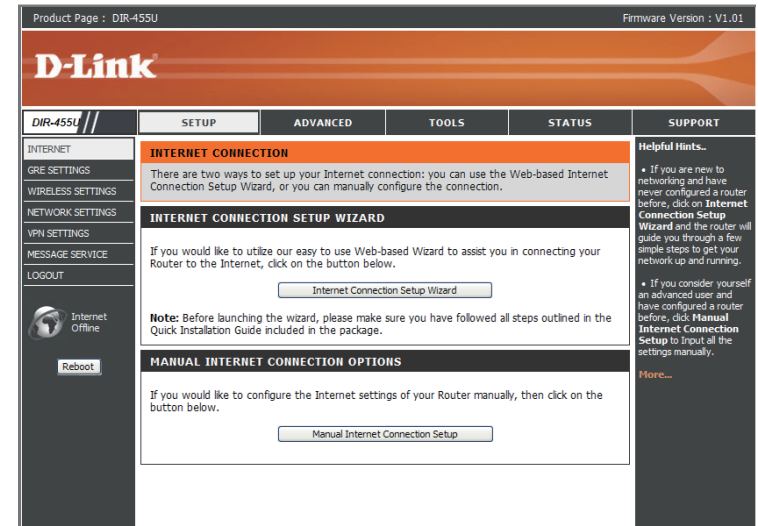
A screenshot of the D-Link router's login page. The page has an orange header with the word 'LOGIN' in white. Below the header, it says 'Log in to the router:'. There are two input fields: 'User Name : admin' and 'Password :'. A 'Log In' button is to the right of the password field.

Setup Wizard

The setup wizard guides you through the initial setup of your router. There are two ways to setup your Internet connection. You can use the Web-based **Internet Connection Setup Wizard** or you can manually configure using the **Manual Internet Connection Setup** wizard.

Click **Internet Connection Setup Wizard** to begin.

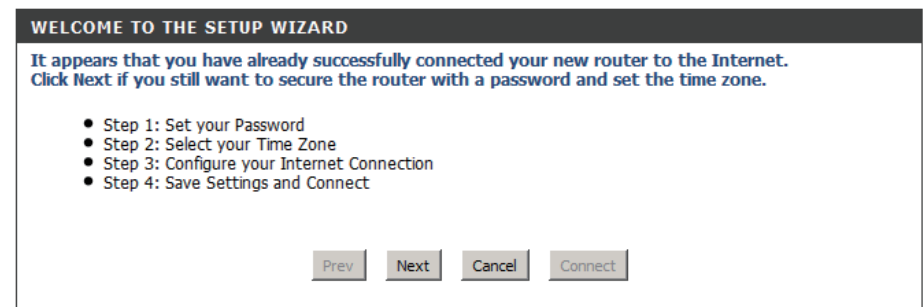
If you want to enter your settings without running the wizard, click **Manual Internet Connection Setup** and skip to page 13.



Internet Connection Setup Wizard

This wizard will guide you through a step-by-step process to configure your D-Link router to connect to the Internet.

Click **Next** to continue.



Create a new password and then click **Next** to continue.

Click **Prev** to go back to the previous page or click **Cancel** to close the wizard.

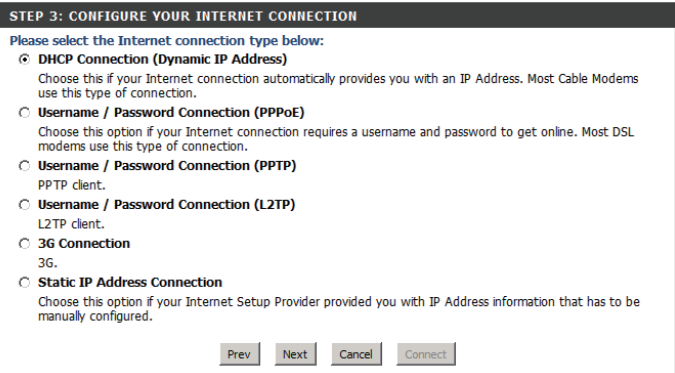
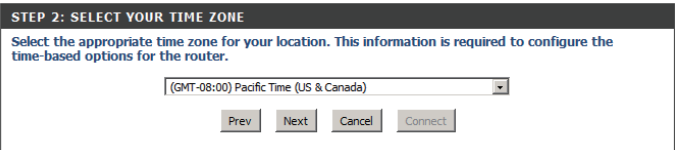
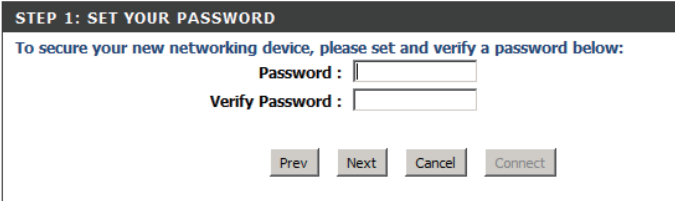
Select your time zone from the drop-down box and then click **Next** to continue.

Click **Prev** to go back to the previous page or click **Cancel** to close the wizard.

Select the Internet connection type. The connection types are explained on the following page. If you are unsure of the correct connection type, you may have to contact your Internet Service Provider (ISP).

Click **Prev** to go back to the previous page or click **Cancel** to close the wizard.

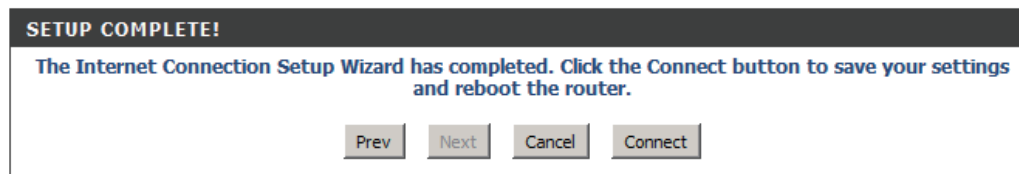
Note: The DIR-455U supports several kinds of WAN interfaces, allowing you to assign either a WAN or a WWAN(3.75G) connection as the Backup WAN. If the Primary WAN is down or unavailable, configure the Backup WAN to **Enable**, and all the traffic will be routed through Backup WAN. This feature is called **WAN Failover**. You can use WAN Failover if you need redundancy to your Internet connection or any other network.



The subsequent configuration pages will differ depending on the selection you make on this page.

- DHCP Connection (Dynamic IP Address):** Choose this if your Internet connection automatically provides you with an IP Address. Most cable modems use this type of connection. See page 16 for information about how to configure this type of connection.
- Username / Password Connection (PPPoE):** Choose this option if your Internet connection requires a username and password to connect. Most DSL modems use this style of connection. See page 17 for information about how to configure this type of connection.
- Username / Password Connection (PPTP):** Choose this option if your Internet connection requires Point-to-Point Tunneling Protocol (PPTP). See page 18 for information about how to configure this type of connection.
- Username / Password Connection (L2TP):** Choose this option if your Internet connection requires Layer 2 Tunneling Protocol (L2TP). See page 19 for information about how to configure this type of connection.
- 3G Connection:** Choose this connection if you have installed a SIM card into the DIR-455U. See page 20 for information about how to configure this type of connection.
- Static IP Address Connection:** Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured. See page 21 for information about how to configure this type of connection.

You have completed the **Setup Wizard**.



Click **Connect** to save your settings.

A popup will appear, to confirm your settings.

Click **OK** to save your settings.

Manual Internet Connection Setup

Click **Manual Internet Connection Setup** to begin.

If you want to configure your router to connect to the Internet using the wizard, click **Internet Connection Setup Wizard** and refer to page 9.

Product Page : DIR-455UFirmware Version : V1.01

D-Link

DIR-455U

SETUP

ADVANCED

TOOLS

STATUS

SUPPORT

INTERNET

GRE SETTINGS

WIRELESS SETTINGS

NETWORK SETTINGS

VPN SETTINGS

MESSAGE SERVICE

LOGOUT

Internet Offline

Reboot

INTERNET CONNECTION

Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, and 3G. If you are unsure of your connection method, please contact your Internet Service Provider.

Note: If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

Save Settings Don't Save Settings

INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is :

Dynamic IP (DHCP)

Host Name :

Dlink

Auto-Backup ☐ Enable checking wired-WAN alive
Internet host

*Please input an IP address on the internet.

DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE

Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password.

Primary DNS Server :

0.0.0.0

Helpful Hints..

- Internet Connection:** When configuring the router to access the Internet, be sure to choose the correct **Internet Connection Type** from the drop down menu. If you are unsure of which option to choose, please contact your Internet Service Provider (ISP).
- Support:** If you are having trouble accessing the Internet through the router, double check any settings you have entered on this page and verify them with your ISP if needed.

More...

D-Link DIR-455U User Manual

14

Internet Connection

Internet Connection Type

Several different Internet Connection types can be selected depending upon the specifications of your Internet Service Provider (ISP).

My Internet Connection is: Select the Internet Connection type specified by your Internet Service Provider (ISP). The corresponding settings will be displayed below. Please see the following pages for details on how to configure these different connection types.

Auto-Backup: When this box is checked, the selected connection will act as a backup for the 3.75G connection.

Internet Host: Enter the IP address of the Internet host to be used as the backup connection.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // SETUP ADVANCED TOOLS STATUS SUPPORT

INTERNET
GRE SETTINGS
WIRELESS SETTINGS
NETWORK SETTINGS
VPN SETTINGS
MESSAGE SERVICE
LOGOUT

Internet Offline
Reboot

INTERNET CONNECTION

Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, and 3G. If you are unsure of your connection method, please contact your Internet Service Provider.

Note: If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

Save Settings Don't Save Settings

INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : Dynamic IP (DHCP)

Host Name : Dlink

Auto-Backup ☐ Enable checking wired-WAN alive

Internet host

*Please input an IP address on the internet.

DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE

Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password.

Primary DNS Server : 0.0.0.0

Helpful Hints..

- Internet Connection:** When configuring the router to access the Internet, be sure to choose the correct **Internet Connection Type** from the drop down menu. If you are unsure of which option to choose, please contact your **Internet Service Provider (ISP)**.
- Support:** If you are having trouble accessing the Internet through the router, double check any settings you have entered on this page and verify them with your ISP if needed.

More...

Dynamic IP (DHCP)

This section will help you to obtain IP Address information automatically from your ISP. Use this option if your ISP didn't provide you with IP Address information and/or a username and password.

Host Name: (Optional) Required by some ISPs.

Primary DNS Server: (Optional) Fill in with IP address of primary DNS server.

Secondary DNS Server: (Optional) Fill in with IP address of secondary DNS server.

MTU (Maximum Transmission Unit): You may need to change the Maximum Transmission Unit (MTU) for optimal performance. The default value is 1500.

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

Auto-reconnect: This feature enables this product to renew WAN IP address automatically when the lease time is expiring.

The screenshot shows a web interface titled "DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE". Below the title is a note: "Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password." The form contains several input fields and buttons: "Host Name" with "ROUTER" entered; "Primary DNS Server" with "0.0.0.0" entered; "Secondary DNS Server" with "0.0.0.0" entered and "(optional)" text to the right; "MTU" with "1500" entered and "(bytes) MTU default = 1500" text to the right; "MAC Address" with "00-21-9B-57-2A-9C" entered, followed by "Save" and "Restore MAC" buttons; and "Auto-reconnect" with an unchecked checkbox and "Enable" text. At the bottom are "Save Settings" and "Don't Save Settings" buttons.

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

PPPoE

Choose this Internet connection if your ISP provides you PPPoE account.

Username: The username/account name that your ISP provides to you for PPPoE dial-up.

Password: Password that your ISP provides to you for PPPoE dial-up.

Verify Password: Fill in with the same password in Password field.

Service Name: (Optional) Fill in if provided by your ISP.

IP Address: (Optional) Fill in if provided by your ISP. If not, keep the default value.

Primary DNS Server: (Optional) Fill in if provided by your ISP. If not, keep the default value.

Secondary DNS Server: (Optional) Fill in if provided by your ISP. If not, keep the default value.

MAC Address: MAC address of WAN interface. You can also copy MAC address of your PC to its WAN interface by pressing **Clone Your PC's MAC** button. The **Restore MAC** button will reset the router to its default MAC address.

Maximum Idle Time: The amount of time of inactivity before disconnecting established PPPoE session. Set it to zero or enable Auto-reconnect will disable this feature.

Maximum Transmission Unit (MTU): The default setting of PPPoE is 1492.

Auto-reconnect: The device will dial-up PPPoE connection automatically.

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

The screenshot shows the PPPoE configuration page. At the top, it says "PPPoE" and "Enter the information provided by your Internet Service Provider (ISP)". Below this are several input fields: Username, Password, Verify Password, Service Name (optional), IP Address (0.0.0.0), Primary DNS Server (0.0.0.0 optional), Secondary DNS Server (0.0.0.0 optional), MAC Address (00-00-00-00-01-00) with "Save" and "Restore MAC" buttons, Maximum Idle Time (300 seconds), MTU (1492 bytes) with a note "MTU default = 1492", and Auto-reconnect (checkbox) with "Enable" text. At the bottom are "Save Settings" and "Don't Save Settings" buttons.

PPTP

Choose this Internet connection if your ISP provides you PPTP account.

Address Mode: Choose Static IP only if your ISP assigns you an IP address. Otherwise, please choose Dynamic IP.

PPTP IP Address: Enter the information provided by your ISP. (Only applicable for Static IP PPTP.)

PPTP Subnet Mask: Enter the information provided by your ISP. (Only applicable for Static IP PPTP.)

PPTP Gateway IP Address: Enter the information provided by your ISP. (Only applicable for Static IP PPTP.)

PPTP Server IP Address: IP address of PPTP server.

Username: User/account name that your ISP provides to you for PPTP dial-up.

Password: Password that your ISP provides to you for PPTP dial-up.

Verify Password: Fill in with the same password in Password field.

Reconnect Mode: Choose **Always-on** when you want to establish PPTP connection all the time. If you choose **Connect-on-demand**, the device will establish PPTP connection when local users want to surf Internet, and disconnect if no traffic after time period of Maximum Idle Time.

Maximum Idle Time: The time of no activity to disconnect your PPTP session. Set it to zero or choose Always-on to disable this feature.

The screenshot shows a web-based configuration page for PPTP. At the top, it says 'PPTP' and 'Enter the information provided by your Internet Service Provider (ISP)'. Below this, there are several configuration fields:

- Address Mode:** Two radio buttons, 'Dynamic IP' and 'Static IP'. 'Static IP' is selected.
- PPTP IP Address:** A text box containing '0.0.0.0'.
- PPTP Subnet Mask:** A text box containing '255.255.255.0'.
- PPTP Gateway IP Address:** A text box containing '0.0.0.0'.
- PPTP Server IP Address:** An empty text box.
- Username:** An empty text box.
- Password:** An empty text box.
- Verify Password:** An empty text box.
- Reconnect Mode:** Two radio buttons, 'Always-on' and 'Connect-on-demand'. 'Connect-on-demand' is selected.
- Maximum Idle Time:** A text box containing '300' followed by the unit 'seconds'.

At the bottom right, there are two buttons: 'Save Settings' and 'Don't Save Settings'.

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

L2TP

Choose this Internet connection if your ISP provides you L2TP account.

Address Mode: Choose Static IP only if your ISP assigns you an IP address. Otherwise, please choose Dynamic IP.

L2TP IP Address: Enter the information provided by your ISP. (Only applicable for Static IP L2TP.)

L2TP Subnet Mask: Enter the information provided by your ISP. (Only applicable for Static IP L2TP.)

L2TP Gateway IP Address: Enter the information provided by your ISP. (Only applicable for Static IP L2TP.)

L2TP Server IP Address: IP address of L2TP server.

Username: User/account name that your ISP provides to you for L2TP dial-up.

Password: Password that your ISP provides to you for L2TP dial-up.

Verify Password: Fill in with the same password in Password field.

Reconnect Mode: Choose Always-on when you want to establish L2TP connection all the time. Choose Connect-on-demand the device will establish L2TP connection when local users want to surf Internet, and disconnect if no traffic after time period of Maximum Idle Time.

Maximum Idle Time: The time of no activity to disconnect your L2TP session. Set it to zero or choose Always-on to disable this feature.

The screenshot shows the L2TP configuration window with the following fields and values:

- Address Mode:** ☐ Dynamic IP ☒ Static IP
- L2TP IP Address:** 0.0.0.0
- L2TP Subnet Mask:** 255.255.255.0
- L2TP Gateway IP Address:** 0.0.0.0
- L2TP Server IP Address:** (empty)
- Username:** (empty)
- Password:** (empty)
- Verify Password:** (empty)
- Reconnect Mode:** ☐ Always-on ☒ Connect-on-demand
- Maximum Idle Time:** 300 seconds

At the bottom, there are two buttons: "Save Settings" and "Don't Save Settings".

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

3G

Choose this Internet connection if you already apply a SIM card for 3G Internet service from Telecom company. The fields here may not be necessary for your connection. The information on this page is only be used when your service provider requires.

Account/Profile Name: Fill in a name to indicate the following 3G configuration.

Username: (Optional) Fill in only if requested by ISP.

Password: (Optional) Fill in only if requested by ISP.

Dialed Number: Enter the number to be dialed.

Authentication: PAP, CHAP, or Auto detection. The default authentication method is Auto.

APN: (Optional) Enter the APN information.

PIN: Enter the PIN associated with your SIM card.

Reconnect Mode: Auto or Manual. Connect to 3G network automatically or manually.

Maximum Idle Time: The time of no activity to disconnect established 3G session. Set it to zero or choose Auto in Reconnect Mode to disable this feature.

Primary DNS Server: (Optional) Fill in if provided by your ISP. If not, keep the default value.

Secondary DNS Server: (Optional) Fill in if provided by your ISP. If not, keep the default value.

Keep Alive: Disable or Use LCP Echo Request. It depends on ISP requirement.

Bridge Ethernet Ports: Activate this feature to change Ethernet WAN port to LAN port.

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Static IP

Choose this Internet connection if your ISP assigns you a static IP address.

IP Address: Enter the IP address assigned to your network connection.

Subnet Mask: Enter the subnet mask.

Default Gateway: Enter the default gateway.

Primary DNS Server: Enter the primary DNS server.

Secondary DNS Server: Enter the secondary DNS server.

MTU: You may need to change the Maximum Transmission Unit (MTU) for optimal performance. The default value is 1500.

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

The screenshot shows a configuration window titled "STATIC IP ADDRESS INTERNET CONNECTION TYPE". Below the title is a subtitle: "Enter the static address information provided by your Internet Service Provider (ISP)". The form contains several input fields: "IP Address" (0.0.0.0), "Subnet Mask" (255.255.255.0), "Default Gateway" (0.0.0.0), "Primary DNS Server" (0.0.0.0), and "Secondary DNS Server" (0.0.0.0). Below these is the "MTU" field (1500) with a note "(bytes) MTU default = 1500". At the bottom is the "MAC Address" field (00-00-00-00-01-00) and a "Restore MAC" button. At the very bottom of the window are two buttons: "Save Settings" and "Don't Save Settings".

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

GRE Settings

This page allows you to set up GRE Tunnels and view information about the amount of data transmitted and received. Generic Routing Encapsulation (GRE) is an IP packet encapsulation protocol used when IP packets must be sent from one network to another.

GRE TUNNEL

- Name:** Enter a name for the GRE tunnel.
- Tunnel IP:** Specify the IP address of the tunnel.
- Peer IP:** Enter the target Peer IP.
- Key:** Enter a Key. The key can be a maximum of 7 characters long.
- TTL:** Time to Live (TTL) specifies how long the tunnel will remain alive. Valid values range from 1 to 255.
- Subnet:** Specify the subnet used by the tunnel.
- Enable:** Select this box to enable the tunnel.
- Default Gateway:** You may specify any one of the 8 available tunnels as default or simple choose “none”.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // SETUP ADVANCED TOOLS STATUS SUPPORT

INTERNET
GRE SETTINGS
WIRELESS SETTINGS
NETWORK SETTINGS
VPN SETTINGS
MESSAGE SERVICE
LOGOUT

Internet Offline
Reboot

GRE SETTINGS

Save Settings Don't Save Settings

GRE TUNNEL

ID	Name	Tunnel IP	Peer IP	Key	TTL	Subnet	Enable
1					0		☐
2					0		☐
3					0		☐
4					0		☐
5					0		☐
6					0		☐
7					0		☐
8					0		☐

Default Gateway: None

TUNNELS INFORMATION

Tunnel Name	Transmitted Packets	Transmitted Bytes	Received Packets	Received Bytes
Tunnel 1	0	0	0	0
Tunnel 2	0	0	0	0
Tunnel 3	0	0	0	0
Tunnel 4	0	0	0	0
Tunnel 5	0	0	0	0
Tunnel 6	0	0	0	0
Tunnel 7	0	0	0	0
Tunnel 8	0	0	0	0

Refresh

Save Settings Don't Save Settings

Helpful Hints...
+ GRE Settings
More...

TUNNELS INFORMATION

Tunnel Name: Displays the name of the tunnel.

Transmitted Packets: Displays the total number of packets transmitted through the tunnel.

Transmitted Bytes: Displays the total number of bytes transmitted through the tunnel.

Received Packets: Displays the total number of packets received.

Displays the total number of bytes received.

Received Bytes: Click Refresh to update the information in the table.

Refresh: Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // SETUP ADVANCED TOOLS STATUS SUPPORT

INTERNET
GRE SETTINGS
WIRELESS SETTINGS
NETWORK SETTINGS
VPN SETTINGS
MESSAGE SERVICE
LOGOUT

Internet
Offline
Reboot

GRE SETTINGS

Save Settings Don't Save Settings

GRE TUNNEL

ID	Name	Tunnel IP	Peer IP	Key	TTL	Subnet	Enable
1				0			☐
2				0			☐
3				0			☐
4				0			☐
5				0			☐
6				0			☐
7				0			☐
8				0			☐

Default Gateway: None

TUNNELS INFORMATION

Tunnel Name	Transmitted Packets	Transmitted Bytes	Received Packets	Received Bytes
Tunnel 1	0	0	0	0
Tunnel 2	0	0	0	0
Tunnel 3	0	0	0	0
Tunnel 4	0	0	0	0
Tunnel 5	0	0	0	0
Tunnel 6	0	0	0	0
Tunnel 7	0	0	0	0
Tunnel 8	0	0	0	0

Refresh

Save Settings Don't Save Settings

Helpful Hints...
GRE Settings
More...

Wireless Settings

This section will help you to manually configure the wireless settings of your router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

WIRELESS NETWORK SETTINGS

Enable Wireless: Select this checkbox to enable wireless access. When you set this option, the following parameters take effect.

Wireless Network Name: Also known as the SSID (Service Set Identifier), this is the name of your Wireless Local Area Network (WLAN). Enter a name using up to 32 alphanumeric characters. The SSID is case-sensitive.

802.11 Mode: **Mixed mode:** Enable this mode if your network contains a mix of 802.11b and 802.11g devices.

G mode: Enable this mode if your network has only 802.11g devices. If you have both 802.11b and 802.11g wireless clients, disable this mode.

Auto Channel Scan: A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may experience interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // SETUP ADVANCED TOOLS STATUS SUPPORT

WIRELESS NETWORK

Use this section to configure the wireless settings for this device. Please note that changes made on this section may also need to be duplicated on your wireless client.

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2.

Save Settings Don't Save Settings

WIRELESS NETWORK SETTINGS

Enable Wireless : ☒

Wireless Network Name : default (Also called the SSID)

802.11 Mode : Mixed mode

Auto Channel Scan : ☐

Wireless Channel : 2.462 GHz - CH 11

Visibility Status : ☒ Visible ☐ Invisible

WIRELESS SECURITY MODE

Security Mode : None

Save Settings Don't Save Settings

Helpful Hints..

- Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.
- Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device.
- If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this

Wireless Channel: Indicates the channel setting for the DIR-455U. By default the channel is set to 11. This can be changed to fit the channel setting for an existing wireless network or to customize your wireless network. Click **Auto Channel Scan** to automatically select the channel that it will operate on. This option is recommended because the router will choose the channel with the least amount of interference.

Visibility Status:

Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by DIR-455U. The SSID of your router will not be seen by Site Survey utilities. Therefore while setting up your wireless clients, you will have to manually enter your SSID to connect to the router.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // SETUP ADVANCED TOOLS STATUS SUPPORT

INTERNET
GRE SETTINGS
WIRELESS SETTINGS
NETWORK SETTINGS
VPN SETTINGS
MESSAGE SERVICE
LOGOUT

Internet Offline
Reboot

WIRELESS NETWORK

Use this section to configure the wireless settings for this device. Please note that changes made on this section may also need to be duplicated on your wireless client.

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2.

Save Settings Don't Save Settings

WIRELESS NETWORK SETTINGS

Enable Wireless : ☒

Wireless Network Name : HOME (Also called the SSID)

802.11 Mode : Mixed mode

Auto Channel Scan : ☐

Wireless Channel : 2.462 GHz - CH 11

Visibility Status : ☒ Visible ☐ Invisible

WIRELESS SECURITY MODE

Security Mode : None

Helpful Hints..

- Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.

Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device.

If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that

WIRELESS SECURITY MODE

Security Mode: This device supports three wireless security modes, **WEP**, **WPA-Personal**, **WPA-Enterprise** or **None**. WEP is the original wireless encryption standard. WPA provides a higher level of security and WPA-Personal does not require an authentication server. When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

Radius Server IP: IP address of RADIUS server.

Radius Port: The port used for RADIUS server. The default port is 1812.

Radius Shared Key: Key value shared by RADIUS server and this device.

Please refer to **Section 4 - Wireless Security** for more information on security and encryption.

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Network Settings

Router Settings

This section will help you to change the internal network settings of your router and to configure the DHCP Server settings.

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

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

Default Subnet Mask: Enter the **Subnet Mask** of the router. The default subnet mask is **255.255.255.0**.

Local Domain Name: Enter the local domain name for your network.

The screenshot displays the D-Link DIR-455U web-based configuration utility. The top navigation bar includes links for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar shows a menu with options like INTERNET, GIGABIT SETTINGS, WIRELESS SETTINGS, NETWORK SETTINGS (highlighted), VPN SETTINGS, MESSAGE SERVICE, and LOGOUT. The main content area is divided into two sections: NETWORK SETTING and DHCP SERVER SETTINGS. The NETWORK SETTING section includes a description of the settings and a note about the optional nature of the section. Below this, the ROUTER SETTINGS section contains input fields for Router IP Address (192.168.0.1), Default Subnet Mask (255.255.255.0), and Local Domain Name. The DHCP SERVER SETTINGS section includes a checkbox for Enable DHCP Server (checked), a range for DHCP IP Address (30 to 199), a lease time of 1440 minutes, and fields for Primary and Secondary DNS and WINS IP addresses. Both sections have 'Save Settings' and 'Don't Save Settings' buttons at the bottom.

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

DHCP Server Settings

The DIR-455U has a built-in DHCP (Dynamic Host Control Protocol) server. The DHCP server assigns IP addresses to devices on the network that request them. By default, the DHCP Server is enabled on the device. The DHCP address pool contains a range of IP addresses, which is automatically assigned to the clients on the network.

Enable DHCP Server: Select this box to enable the DHCP server on your router.

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

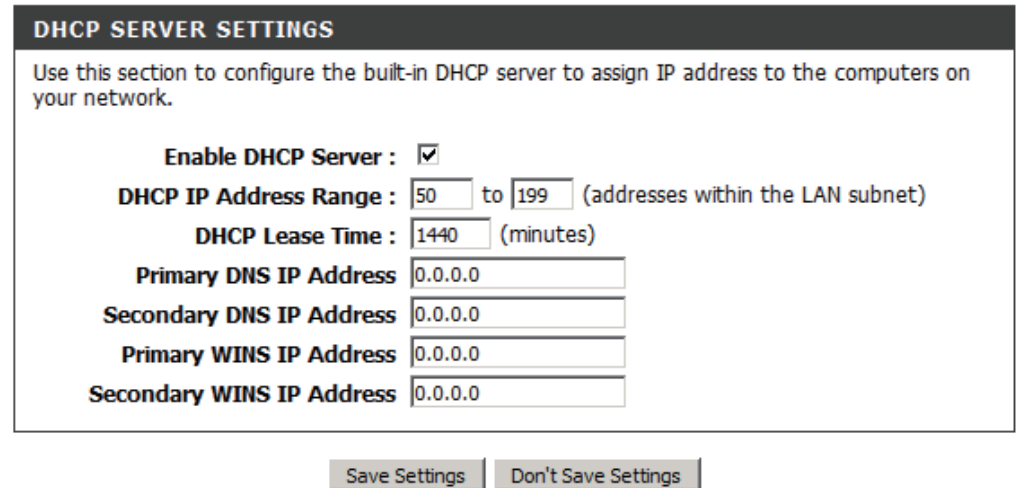
DHCP Lease Time: The time period for the IP address lease. Enter the Lease time in minutes.

Primary DNS IP Address: Primary DNS IP Address: assign a primary DNS Server to DHCP clients.

Secondary DNS IP Address: Secondary DNS IP Address: assign a DNS Server to DHCP clients.

Primary WINS IP Address: Primary WINS IP Address: assign a primary WINS Server to DHCP clients.

Secondary WINS IP Address: Secondary WINS IP Address: assign a WINS Server to DHCP clients.



The screenshot shows the 'DHCP SERVER SETTINGS' page. At the top, it says 'Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.' Below this, there are several settings: 'Enable DHCP Server' is checked; 'DHCP IP Address Range' is set to 50 to 199 with a note '(addresses within the LAN subnet)'; 'DHCP Lease Time' is set to 1440 minutes; 'Primary DNS IP Address' is 0.0.0.0; 'Secondary DNS IP Address' is 0.0.0.0; 'Primary WINS IP Address' is 0.0.0.0; and 'Secondary WINS IP Address' is 0.0.0.0. At the bottom right, there are two buttons: 'Save Settings' and 'Don't Save Settings'.

DHCP SERVER SETTINGS	
Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.	
Enable DHCP Server :	☒
DHCP IP Address Range :	50 to 199 (addresses within the LAN subnet)
DHCP Lease Time :	1440 (minutes)
Primary DNS IP Address	0.0.0.0
Secondary DNS IP Address	0.0.0.0
Primary WINS IP Address	0.0.0.0
Secondary WINS IP Address	0.0.0.0

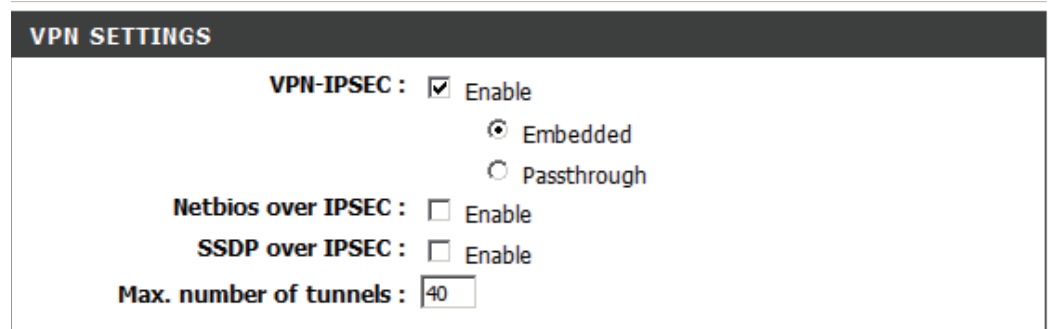
Save Settings Don't Save Settings

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

VPN Settings

This section will help you create and configure your **VPN** settings. The router supports IPsec as the Server Endpoint. IPsec (Internet Protocol Security) is a set of protocols defined by the IETF (Internet Engineering Task Force) to provide IP security at the network layer.

VPN-IPSEC: Select it to enable IPsec VPN function. Choosing “Embedded” to allow this device establishing VPN tunnel with remote VPN gateways. You can also choose “Passthrough” to let local PCs establish VPN tunnel with remote VPN gateways.



VPN SETTINGS

VPN-IPSEC : ☒ Enable
☒ Embedded
☐ Passthrough

Netbios over IPSEC : ☐ Enable

SSDP over IPSEC : ☐ Enable

Max. number of tunnels :

Netbios over IPSEC: Computers running Microsoft Windows can communicate with other computer by using NetBIOS. Users can access remote network resources by browsing the My Network Places.

SSDP over IPSEC: Computers running Microsoft Windows can communicate with other computer by using SSDP. The device will send SSDP data to the remote IPsec network if this option is enabled.

Max Number of Tunnels: Since VPN function requires signification processing power for encryption, too many concurrent VPN tunnels will greatly degrade the performance of the network. This value indicates the maximum number of VPN tunnels can be established at the same time.

Tunnel Name: Indicate a tunnel name of this VPN configuration.

Method: Two options can be selected: **IKE** or **Manual**.

Click the **More** button to continue settings, and select the **Enable** checkbox to activate this rule.

TUNNEL SETTINGS

ID	Tunnel Name	Method	Action	Enable
1	Tunnel#1	IKE	More	☒
2		IKE	More	☐
3		IKE	More	☐
4		IKE	More	☐
5		IKE	More	☐

Previous page

Next page

XAUTH account

Save Settings

Don't Save Settings

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Tunnel 1 - IKE

Tunnel Name: Indicate a tunnel name for this VPN configuration.

Local Subnet: The subnet of the VPN gateway's local network. It can be a host, a partial subnet or a whole subnet.

Local Netmask: Local netmask combined with local subnet to form a subnet domain.

Remote Subnet: The subnet of the remote VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.

Remote Netmask: The netmask of the remote VPN gateway's local network.

Remote Gateway: The WAN IP address of remote VPN gateway.

Phase 1 Key Life Time: The phase 1 key life time of the dedicated VPN tunnel between both end gateways (in seconds). Its value can range from 300 seconds to 172,800 seconds.

Phase 2 Key Life Time: The phase 2 key life time of the dedicated VPN tunnel between both end gateways (in seconds). Its value can range from 300 seconds to 172,800 seconds.

Encapsulation Protocol: ESP, AH, or ESP+AH.

PFS: Configures perfect forward secrecy for connections created with this IPsec transport profile by assigning a Diffie-Hellman prime modulus group.

VPN SETTINGS - TUNNEL 1 - IKE

Tunnel Name :	Tunnel-1
Local Subnet :	0.0.0.0
Local Netmask :	255.255.255.0
Remote Subnet :	0.0.0.0
Remote Netmask :	0.0.0.0
Remote Gateway :	
Phase1 Key Life Time	0 second
Phase2 Key Life Time	0 second
Encapsulation Protocol :	AH
PFS Group	Disable
Aggressive Mode :	☐ Enable
Preshare Key :	
Remote ID :	(optional)
Local ID :	(optional)
Keep Alive :	☐ Enable
	0.0.0.0 Remote IP
	0 Idle Time(Seconds, from 30~240)
XAUTH :	☒ None
	☐ Client
	username password
	☐ Server
Set IKE Proposal :	☐ Enable
Set IPSEC Proposal :	☐ Enable

PFS Group: Three groups can be selected: None, Group 1, Group 2, Group 5.

None: No PFS group

Group 1: 768-bit Diffie-Hellman prime modulus

Group 2: 1024-bit Diffie-Hellman prime modulus

Group 5: 1536-bit Diffie-Hellman prime modulus

Aggressive Mode: Enabling this mode will accelerate the initial tunnel setup, but the device will suffer from less security in the meantime. Hosts at both ends of the tunnel must support this mode so as to establish the tunnel properly.

Preshared Key: The first key that supports IKE mechanism of both VPN gateway and VPN client host for negotiating further security keys. The pre-shared key must be same on both VPN gateways and clients.

Remote ID: The Type and the Value must be the same as the Type and the Value of the Local ID of the remote VPN gateway.

Local ID: The Type and the Value must be the same as the Type and the Value of the Remote ID of the remote VPN gateway.

Keep Alive (Ping IP Address): Input the IP address of remote host that exist in the remote side of the VPN tunnel (Ex. You can input the LAN IP address of remote VPN gateway). The device will start to Ping the remote host when there is no traffic within the VPN tunnel. If the device is no longer receiving an ICMP response from remote host, it will terminate the VPN tunnel automatically.

VPN SETTINGS - TUNNEL 1 - IKE

Tunnel Name :	Tunnel-1
Local Subnet :	0.0.0.0
Local Netmask :	255.255.255.0
Remote Subnet :	0.0.0.0
Remote Netmask :	0.0.0.0
Remote Gateway :	
Phase1 Key Life Time	0 second
Phase2 Key Life Time	0 second
Encapsulation Protocol :	AH
PFS Group	Disable
Aggressive Mode :	☐ Enable
Preshare Key :	
Remote ID :	(optional)
Local ID :	(optional)
Keep Alive :	☐ Enable
	0.0.0.0 Remote IP
	0 Idle Time(Seconds, from 30~240)
XAUTH :	☒ None
	☐ Client
	username password
	☐ Server
Set IKE Proposal :	☐ Enable
Set IPSEC Proposal :	☐ Enable

xAuth (Extended Authentication): With the xAuth feature, the VPN client (or initiator) needs to provide additional user information to the remote VPN server (or VPN gateway) for extended authentication. Otherwise, the VPN server will reject the connection request from VPN clients due to an unknown user, even though the pre-shared key is correct. This function is suitable for remote mobile VPN clients. Not only can you configure a VPN rule with a pre-shared key for all remote users, you can also designate that a user is only permitted to establish a VPN connection with the VPN server.

xAuth - None: Disables Extended Authentication (xAuth).

xAuth - Client Mode: Select this checkbox if the device behaves as a VPN client, and will send user information to remote VPN server for extended authentication. You must input a correct user name and password to pass authentication. Please note that remote VPN servers without xAuth will reject your connect request if you have activated this feature.

xAuth - Server Mode: Select this checkbox if the router should behave as a VPN server, and will verify the legality of user information from the VPN client. The user information that is provided by a VPN client needs to match the user information that is in the user database of the VPN server. Click the **XAUTH account** button to edit the local user database. Please note that only VPN clients with xAuth can establish VPN connection with the device if this checkbox has been selected.

Set IKE Proposal: Select this box to enable IKE proposals.

Set IPSec Proposal: Select this box to enable IPSec proposals.

VPN SETTINGS - TUNNEL 1 - IKE

Tunnel Name :	Tunnel-1		
Local Subnet :	0.0.0.0		
Local Netmask :	255.255.255.0		
Remote Subnet :	0.0.0.0		
Remote Netmask :	0.0.0.0		
Remote Gateway :			
Phase1 Key Life Time	0	second	
Phase2 Key Life Time	0	second	
Encapsulation Protocol :	AH		
PFS Group	Disable		
Aggressive Mode :	☐ Enable		
Preshare Key :			
Remote ID :		(optional)	
Local ID :		(optional)	
Keep Alive :	☐ Enable		
	0.0.0.0	Remote IP	
	0	Idle Time(Seconds, from 30~240)	
XAUTH :	☒ None ☐ Client ☐ Server		
	username	password	
Set IKE Proposal :	☐ Enable		
Set IPSec Proposal :	☐ Enable		

IKE PROPOSAL SETTINGS

DH Group: Three groups can be selected: group 1 (MODP768), group 2 (MODP1024), and group 5 (MODP1536).

Encryption Algorithm: Three algorithms can be selected: 3DES, DES, and AES.

Authentication Algorithm: Two algorithms can be selected: SHA1 and MD5.

Enable: Select this checkbox to enable the IKE Proposal with this rule.

IKE PROPOSAL SETTINGS				
ID	Encrypt_Algorithm	Auth_Algorithm	DH_Group	Enable
1				☐
2				☐

IPSEC PROPOSAL SETTINGS

Encryption Algorithm: Three algorithms can be selected: 3DES, DES and AES. However, when the encapsulation protocol is set to AH, the encryption algorithm is unnecessary.

Authentication Algorithm: Two algorithms can be selected: SHA1 and MD5.

IPSEC PROPOSAL SETTINGS			
ID	Encrypt_Algorithm	Auth_Algorithm	Enable
1			☐
2			☐

Tunnel 1 - Manual Key

Choose **MANUAL** in the Method field, and press the **More** button to continue following configuration.

Tunnel Name: Indicate a tunnel name for this VPN configuration.

Local Subnet: The subnet of the VPN gateway's local network. It can be a host, a partial subnet or a whole subnet.

Local Netmask: Local netmask combined with local subnet to form a subnet domain.

Remote Subnet: The subnet of the remote VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.

Remote Netmask: The netmask of the remote VPN gateway's local network.

Remote Gateway: The WAN IP address of remote VPN gateway.

Life Time: The unit of life time is based on the value of Life Time Unit. The value of unit is second, the value of life time represents the life time of dedicated VPN tunnel between both end gateways. Its value ranges from 300 seconds to 172,800 seconds.

Encapsulation Protocol: Select ESP or AH.

Local SPI: SPI is an important parameter during hashing. Local SPI will be included in the outbound packet transmitted to WAN side of local gateway. The value of local SPI should be set in hex format.

Remote SPI: Remote SPI will be included in the inbound packet transmitted from WAN side of remote gateway. It will be used to de-hash the coming packet and check its integrity. The value of remote SPI should be set in hex format.

Encryption Algorithm: Two algorithms can be selected: 3DES and DES. When the encapsulation protocol is set to AH, the encryption algorithm is unnecessary.

Encryption Key: The encryption key is used by the encryption algorithm. Its length is 8 bytes if encryption algorithm is DES or 24 bytes if 3DES. The key value should be set in hex format.

Authentication Algorithm: Two algorithms can be selected: SHA1 and MD5. But “None” also can be selected here for non-hashing operation.

Authentication Key: This authentication key is used by the authentication algorithm. Its length is 16 bytes if authentication algorithm is MD5 or 20 bytes if SHA1. Its length will be 0 if no authentication algorithm is chosen. The key value should be set in hex format.

VPN SETTINGS - TUNNEL 1 - MANUAL KEY

Tunnel Name :	Tunnel-1
Local Subnet :	0.0.0.0
Local Netmask :	255.255.255.0
Remote Subnet :	0.0.0.0
Remote Netmask :	0.0.0.0
Remote Gateway :	
Life Time :	0 second
Encapsulation Protocol :	ESP
Method :	MANUAL
Local SPI :	0x0000
Remote SPI :	0x0000
Encryption Algorithm :	3DES
Encryption Key :	
Authentication Algorithm :	NONE
Authentication Key :	

Tunnel 1 - Manual Key

VPN Dynamic IP Setting: VPN Dynamic IP Setting: Enable it when you need remote mobile hosts to build secure VPN tunnel with the gateway. Click “More” button to continue the settings.

DYNAMIC VPN SETTING

VPN Dynamic IP Setting : ☐ Enable [More](#)

Tunnel Name: Indicate a tunnel name of this VPN configuration.

Local Subnet: The subnet of the VPN gateway's local network. It can be a host, a partial subnet or a whole subnet.

Local Netmask: Local netmask combined with local subnet form a subnet domain.

Phase 1 Key Life Time: The phase 1 key life time of the dedicated VPN tunnel between both end gateways (in seconds). Its value can range from 300 seconds to 172,800 seconds.

DYNAMIC VPN SETTINGS

Tunnel Name :

Local Subnet :

Local Netmask :

Phase1 Key Life Time second

Phase2 Key Life Time second

Encapsulation Protocol :

PFS group :

Preshare Key :

remote ID : (optional)

local ID : (optional)

XAUTH : ☒ None ☐ Server

Set IKE Proposal : ☐ Enable

Set IPSEC Proposal : ☐ Enable

Phase 2 Key Life Time: The phase 2 key life time of the dedicated VPN tunnel between both end gateways (in seconds). Its value can range from 300 seconds to 172,800 seconds.

Encapsulation Protocol: ESP, AH, or ESP+AH.

PFS: Configures perfect forward secrecy for connections created with this IPSec transport profile by assigning a Diffie-Hellman prime modulus group.

PFS Group: Three groups can be selected: None, Group 1, Group 2, Group 5.

None: No pfs group is used.

Group 1: Uses a 768-bit Diffie-Hellman prime modulus group.

Group 2: Uses a 1024-bit Diffie-Hellman prime modulus group.

Group 5: Uses a 1536-bit Diffie-Hellman prime modulus group.

Preshared Key: The first key that supports IKE mechanism of both VPN gateway and VPN client host for negotiating further security keys. The pre-shared key must be same on both VPN gateways and clients.

Remote ID: The Type and the Value must be the same as the Type and the Value of the Local ID of the remote VPN gateway.

Local ID: The Type and the Value must be the same as the Type and the Value of the Remote ID of the remote VPN gateway.

Extended Authentication: With the xAuth feature, the VPN client (or initiator) needs to provide additional user information to remote VPN server (or VPN gateway) for extended authentication. The VPN server would reject the connect request from VPN clients because of the unknown user, even though the pre-shared key is correct. This function is suitable to remote mobile VPN clients. You can configure a VPN rule with a pre-shared key for all remote users using, but you can also designate only someone is permitted to establish VPN connection with VPN server.

xAuth - None: Disables Extended Authentication (xAuth).

xAuth - Server Mode: Select this checkbox if the device behaves as a VPN server, and will verify the legality of user information from VPN client. The user information that is provided by VPN client needs to match to user information that is in local user database of VPN server. You can press “XAUTH account” button to edit local user database. Please note that only VPN clients with xAuth can establish VPN connection with the device if this checkbox has been selected.

Set IKE Proposal: Select this checkbox to enable IKE proposals.

Set IPSec Proposal: Select this checkbox to enable IPSec proposals

IKE PROPOSAL SETTINGS

DH Group: DH Group: Three groups can be selected: group 1 (MODP768), group 2 (MODP1024), and group 5 (MODP1536).

Encryption Algorithm: Three algorithms can be selected: 3DES, DES, and AES.

Authentication Algorithm: Two algorithms can be selected: SHA1 and MD5.

Enable: Select this checkbox to enable the IKE Proposal with this rule.

IKE PROPOSAL SETTINGS				
ID	DH_Group	Encrypt_Algorithm	Auth_Algorithm	Enable
1				☐
2				☐

IPSEC PROPOSAL SETTINGS

Encryption Algorithm: Three algorithms can be selected: 3DES, DES and AES. However, when the encapsulation protocol is set to AH, encryption algorithm is unnecessary.

Authentication Algorithm: Two algorithms can be selected: SHA1 and MD5.

IPSEC PROPOSAL SETTINGS			
ID	Encrypt_Algorithm	Auth_Algorithm	Enable
1			☐
2			☐

Message Service

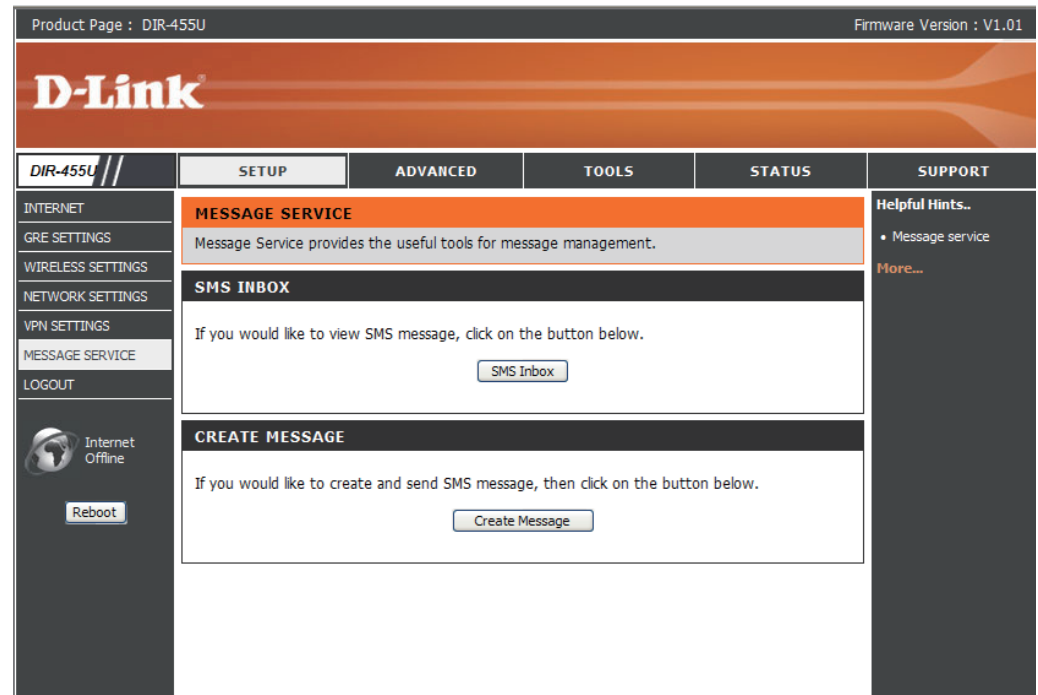
If your ISP provide **SMS** service, you can create new messages, and manage your messages from this page.

SMS INBOX

SMS Inbox: Click this button to view any SMS message that you may have received.

CREATE MESSAGE

Create Message: Click this button to create a message.



CREATE MESSAGE

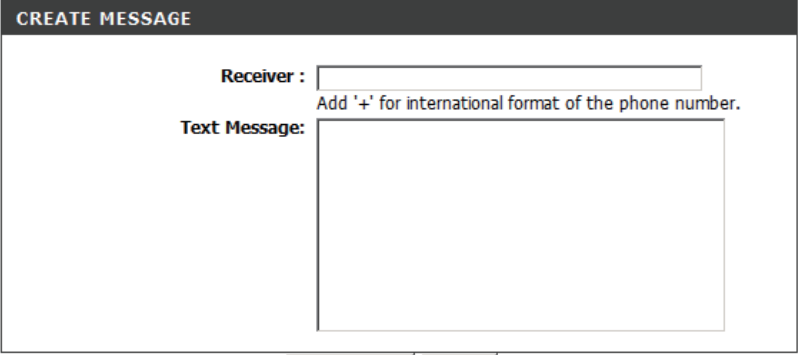
This page allows you to send an SMS to your contacts. Just fill in the phone number of the recipient, and type the content of message. Then push the “Send Message” button to send out this message. If you would like to add more than one recipient, you must put a semicolon (;) between each of the phone numbers.

Receiver: Type the phone number of the recipient.

Text Message: Type the message that you would like to send.

Sent Message: Click this button to send the message.

Cancel: Click this button to cancel message input.



The screenshot shows a web interface titled "CREATE MESSAGE". It features a "Receiver:" label followed by a text input field. Below the input field is a hint: "Add '+' for international format of the phone number." To the left of a larger text area is the label "Text Message:". At the bottom right of the form are two buttons: "Send message" and "Cancel".

INBOX

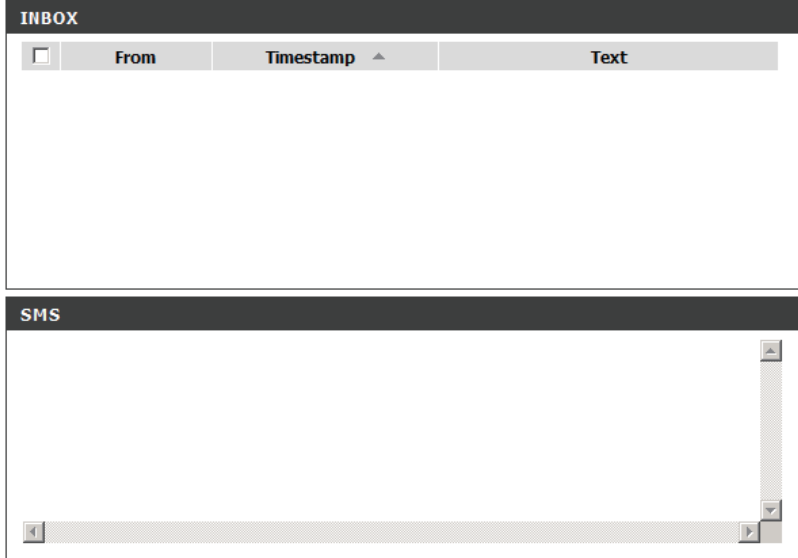
This page shows all messages that are stored on the SIM card. Selecting a message, and the content will be shown in the SMS window. After you read it, you can delete it, or reply to the sender. Push the “Refresh” button to update the list.

SMS

Delete Message: Deletes the selected SMS message.

Reply Message: Replies to the selected SMS message.

Refresh: Click this button to check for new messages.



The screenshot shows two sections of a web interface. The top section is titled "INBOX" and contains a table with columns: a checkbox, "From", "Timestamp" (with an upward arrow), and "Text". The bottom section is titled "SMS" and contains a large text area for displaying the content of a selected message. At the bottom right of the interface are three buttons: "Delete message", "Reply message", and "Refresh".

Virtual Server

The device can be configured as a virtual server so that users can access services such as Web or FTP via the public (WAN) IP address of the router.

Well-known Services: This contains a list of pre-defined services.

Copy to: Copies the rule to the line of the specified ID.

Use schedule rule: You may select **Always On** or choose the number of a schedule rule that you have defined.

VIRTUAL SERVERS LIST

ID: Identifies the virtual server.

Server IP: Port: Enter the last digits of the IP address of the computer on your local network that you want to allow the incoming service. In the next box, enter the port number that you would like to open.

Enable: Select this box to enable the rule.

Schedule Rule #: Specify the schedule rule number.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // SETUP ADVANCED TOOLS STATUS SUPPORT

VIRTUAL SERVER

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

Save Settings Don't Save Settings

Well known services -- select one -- Copy to ID --

Use schedule rule ---ALWAYS ON---

VIRTUAL SERVERS LIST

ID	Service Ports	Server IP : Port	Enable	Schedule Rule#
1		192.168.0. :	☐	0
2		192.168.0. :	☐	0
3		192.168.0. :	☐	0
4		192.168.0. :	☐	0
5		192.168.0. :	☐	0
6		192.168.0. :	☐	0
7		192.168.0. :	☐	0
8		192.168.0. :	☐	0
9		192.168.0. :	☐	0
10		192.168.0. :	☐	0
11		192.168.0. :	☐	0
12		192.168.0. :	☐	0

Save Settings Don't Save Settings

Internet Offline Reboot

Helpful Hints...

- You can select your computer from the list of DHCP clients in the Computer Name drop down menu, or enter the IP address manually of the computer you would like to open the specified port to.
- This feature allows you to open a range of ports to a computer on your network. To do so, enter the first port in the range you would like to open on the router in the first box under Public Port and last part of the range in the second one. After that you enter the first port in the range that the internal server uses in the first box under Private Port and the last part of the range in the second.
- To open a single port using this feature, simply enter the same number in both boxes.

More...

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). **Applications Rules** allow some of these applications work with the DIR-455U.

APPLICATION RULES

Popular Applications: Select from a list of popular applications.

Copy to ID: Copies the predefined application rule to the line of the specified ID.

ID: Identifies the rule.

Trigger: The name of the trigger.

Incoming Ports: Specify the incoming port for the trigger rule.

Enable: Select this box to enable the rule.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // SETUP ADVANCED TOOLS STATUS SUPPORT

APPLICATION RULES

This option is used to open single or multiple ports on your router when the router senses data sent to the Internet on a 'trigger' port or port range. Special Applications rules apply to all computers on your internal network.

Save Settings Don't Save Settings

Popular applications -- select one -- Copy to ID --

APPLICATION RULES

ID	Trigger	Incoming Ports	Enable
1			☐
2			☐
3			☐
4			☐
5			☐
6			☐
7			☐
8			☐
9			☐
10			☐
11			☐
12			☐

Save Settings Don't Save Settings

Helpful Hints..

- Check the Application Name drop down menu for a list of pre-defined applications that you can select from. If you select one of the pre-defined applications, click the arrow button next to the drop down menu to fill out the appropriate fields.

More...

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

QoS Engine

The **QoS Engine** improves your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web. For best performance, use the Automatic Classification option to automatically set the priority for the applications.

QoS ENGINE SETUP

QoS Packet Filter: Select this box to enable the QoS Packet Filter.

Upstream Bandwidth: Specify the maximum upstream bandwidth here (e.g. 400 kbps).

Downstream Bandwidth: Specify the maximum downstream bandwidth here (e.g. 400 kbps).

QoS RULES

ID: Identifies the rule.

Local IP : Ports: Specify the local IP address and then specify the port after the colon.

Remote IP : Ports: Specify the remote IP address and then the port after the colon.

QoS Priority: Select **Low**, **Normal**, or **High**.

Enable: Select a checkbox to enable the particular QoS rules individually.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // SETUP ADVANCED TOOLS STATUS SUPPORT

QoS ENGINE

Use this section to configure QoS Engine. The QoS Engine improves your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web. For best performance, use the Automatic Classification option to automatically set the priority for your applications.

Save Settings Don't Save Settings

QoS ENGINE SETUP

QoS Packet Filter : ☐ Enable

Upstream bandwidth : 0 kbps

Downstream bandwidth : 0 kbps

QoS RULES

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable
1			Low	☐
2			Low	☐
3			Low	☐
4			Low	☐
5			Low	☐
6			Low	☐
7			Low	☐
8			Low	☐

Save Settings Don't Save Settings

Internet Offline

Reboot

Helpful Hints..

- Gives a user the capability to control network traffic with different priority.

More...

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

MAC Address Filter

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.

MAC FILTERING SETTINGS

MAC Address Control: Select this box to enable Mac Filtering.

Connection Control: Wireless and wired clients with **C** selected can connect to this device and **allow/deny** connections from unspecified MAC addresses.

Association Control: Wireless clients with **A** selected can associate to the wireless LAN; and **allow/deny** connections from unspecified MAC addresses.

MAC FILTERING RULES

ID: Identifies the rule.

MAC Address: Specify the MAC Address of the computer to be filtered.

IP Address: Specify the last section of the IP address.

Wake On LAN: Click **Trigger** to configure Wake On LAN.

C: If this box is selected, the rule will follow the connection control setting specified in MAC filtering settings.

A: If this box is selected, the rule will follow the connection control setting specified in MAC filtering settings.

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U

SETUP ADVANCED TOOLS STATUS SUPPORT

MAC ADDRESS FILTER

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.

Save Settings Don't Save Settings

MAC FILTERING SETTINGS

MAC Address Control : ☐ Enable

☐ **Connection control :** Wireless and wired clients with **C** checked can connect to this device; and **allow** unspecified MAC addresses to connect.

☐ **Association control :** Wireless clients with **A** checked can associate to the wireless LAN; and **deny** unspecified MAC addresses to associate.

DHCP clients -- select one -- Copy to ID --

MAC FILTERING RULES

ID	MAC Address	IP Address	Wake On Lan	C	A
1		192.168.0.	Trigger	☐	☐
2		192.168.0.	Trigger	☐	☐
3		192.168.0.	Trigger	☐	☐
4		192.168.0.	Trigger	☐	☐

Previous page Next page

Save Settings Don't Save Settings

Helpful Hints...

- MAC Address Control** allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.
- Connection control:** Connection control allows you to allow or deny the wired and wireless clients to connect to this device and the Internet. Check Connection control to enable the controlling.
- If a client is denied to connect to this device, it means that the client can't access the Internet and some network resources. Choose **allow** or **deny** to allow or deny clients whose MAC addresses are not listed in the **Control table**.
- Association control:** The Association process is the exchange of information between wireless clients and this device to establish a link between them. A wireless client is capable of transmitting and receiving data to this device only after the association process is successfully completed.

URL Filter

URL Filter allows you to set up a list of Web-sites that will be blocked from users on your network.

URL Filtering: Select this box to enable URL Filtering.

URL FILTERING RULES

ID: Identifies the rule.

URL: Enter URL that you would like to block.

Enable: Click to enable the specific URL filter.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U //

- VIRTUAL SERVER
- APPLICATION RULES
- QOS ENGINE
- MAC ADDRESS FILTER
- URL FILTER**
- OUTBOUND FILTER
- INBOUND FILTER
- SNMP
- ROUTING
- ADVANCED WIRELESS
- ADVANCED NETWORK
- LOGOUT

Internet Offline

Reboot

SETUP
ADVANCED
TOOLS
STATUS
SUPPORT

URL FILTER

URL Blocking will block LAN computers to connect to pre-defined Websites.

URL FILTERING SETTING

URL Filtering : ☐ Enable

URL FILTERING RULES

ID	URL	Enable
1		☐
2		☐
3		☐
4		☐
5		☐

Helpful Hints..

- Create a list of Web Sites to which you would like to deny or allow through the network.

[More...](#)

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Outbound Filter

Outbound Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets.

OUTBOUND FILTER SETTING

Outbound Filter: Select this box to **Enable** the filter.

Use Schedule Rule: You may select **Always On** or choose the number of a schedule rule that you have defined.

Copy to ID: Copies the predefined filter to the specified ID

OUTBOUND FILTER RULES LIST

ID: Identifies the filter.

Source IP : Ports: Specify the local IP address and then specify the port after the colon.

Destination IP : Ports: Specify the remote IP address and then the port after the colon.

Enable: Select this box to enable the filter.

Schedule Rule #: Specify the schedule rule number.

Previous Page: Go back to the previous filter page.

Next Page: Advance to the next filter page.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // SETUP ADVANCED TOOLS STATUS SUPPORT

OUTBOUND FILTER

Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets.

Save Settings Don't Save Settings

OUTBOUND FILTER SETTING

Outbound Filter : ☐ Enable

Use schedule rule ---ALWAYS ON--- Copy to ID --

OUTBOUND FILTER RULES LIST

☒ Allow all to pass except those match the following rules.
☐ Deny all to pass except those match the following rules.

ID	Source IP:Ports	Destination IP:Ports	Enable	Schedule Rule#
1			☐	0
2			☐	0
3			☐	0
4			☐	0
5			☐	0
6			☐	0
7			☐	0
8			☐	0

Previous page Next page

Save Settings Don't Save Settings

Helpful Hints..

- Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, Inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:
- 1. Allow all to pass except those match the specified rules.
- 2. Deny all to pass except those match the specified rules.
- You can specify 8 rules for each directions: inbound or outbound. For each rule, you can define the following:
 - Source IP address
 - Source port address
 - Destination IP address
 - Destination port address
 - Protocol: TCP or UDP or both.

More...

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Inbound Filter

Inbound Filter enables you to control what packets are allowed to pass the router. Inbound filter only applies to packets that are destined for Virtual Servers or DMZ hosts.

INTBOUND FILTER SETTING

Inbound Filter: Select this box to **Enable** the filter.

Use Schedule Rule: You may select **Always On** or choose the number of a schedule rule that you have defined.

Copy to ID: Copies the predefined filter to the specified ID

INBOUND FILTER RULES LIST

ID: Identifies the filter.

Source IP : Ports: Specify the local IP address and then specify the port after the colon.

Destination IP : Ports: Specify the remote IP address and then the port after the colon.

Enable: Select this box to enable the filter.

Schedule Rule #: Specify the schedule rule number.

Previous Page: Go back to the previous filter page.

Next Page: Advance to the next filter page.

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U

- VIRTUAL SERVER
- APPLICATION RULES
- QOS ENGINE
- MAC ADDRESS FILTER
- URL FILTER
- OUTBOUND FILTER
- INBOUND FILTER**
- SNMP
- ROUTING
- ADVANCED WIRELESS
- ADVANCED NETWORK
- LOGOUT

Internet
Offline

Reboot

SETUP
ADVANCED
TOOLS
STATUS
SUPPORT

INBOUND FILTER

Packet Filter enables you to control what packets are allowed to pass the router. Inbound filter applies on packets that destined to Virtual Servers or DMZ host only.

INBOUND FILTER SETTING

Inbound Filter : ☐ Enable

Use schedule rule : ---ALWAYS ON---

INBOUND FILTER RULES LIST

☒ Allow all to pass except those match the following rules.
☐ Deny all to pass except those match the following rules.

ID	Source IP:Ports	Destination IP:Ports	Enable	Schedule Rule#
1			☐	0
2			☐	0
3			☐	0
4			☐	0
5			☐	0
6			☐	0
7			☐	0
8			☐	0

Helpful Hints..

- Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, Inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:
- 1. Allow all to pass except those match the specified rules.
- 2. Deny all to pass except those match the specified rules.
- You can specify 8 rules for each directions: inbound or outbound. For each rule, you can define the following:
 - -Source IP address
 - -Source port address
 - -Destination IP address
 - -Destination port address
 - -Protocol: TCP or UDP or both.

More...

SNMP

SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol that reports activity on each network device to the administrator of the network. SNMP can be used to monitor traffic and statistics of the DIR-455U. The DIR-455U supports SNMP v1 or v2c.

SNMP

SNMP Local: Select **Enabled** to allow local SNMP administration. Select **Disabled** to disallow local SNMP administration.

SNMP Remote: Select **Enabled** to allow local SNMP administration. Select **Disabled** to disallow local SNMP administration.

Get Community: Enter the password **public** in this field to allow “Read only” access to network administration using SNMP. You can view the network, but no configuration is possible with this setting.

Set Community: Enter the password **private** in this field to gain “Read and Write” access to the network using SNMP software.

IP 1, IP 2, IP 3, IP 4: Enter up to 4 IP addresses of any trap targets on your network.

SNMP Version: Select the SNMP version of your system.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // SETUP ADVANCED TOOLS STATUS SUPPORT

SNMP

Use Simple Network Management Protocol(SNMP) for management purposes.

Save Settings Don't Save Settings

SNMP

SNMP Local : ☐ Enabled ☒ Disabled

SNMP Remote : ☐ Enabled ☒ Disabled

Get Community :

Set Community :

IP 1 :

IP 2 :

IP 3 :

IP 4 :

SNMP Version : ☒ V1 ☐ V2c

Save Settings Don't Save Settings

Reboot

Helpful Hints..

- SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol that reports activity on each network device to the administrator of the network. SNMP can be used to monitor traffic and statistics of the device.

[More...](#)

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Routing

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

RIP SETTING

RIP: Select this box to enable routing.

Ripv1: Protocol in which the IP address is routed through the internet.

RIPv2: Enhanced version of RIPv1 with added features such as Authentication, Routing Domain, Next Hop Forwarding, and Subnet-mask Exchange.

ROUTING RULES

ID: Identifies the rule.

Destination: Enter in the IP of the specified network that you want to access using the static route.

Subnet Mask: Enter in the subnet mask to be used for the specified net work.

Gateway: Enter in the gateway IP address to the specified network.

Hop: Enter in the amount of hops it will take to reach the specified network.

Note: In a transmission path, each link is terminated at a network device such as a router or gateway. The number of hops equals the number of routers or gateways that data must pass through before reaching the destination.

Enable: Select this box to enable the rule.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U

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

RIP SETTING

RIP : ☐ Enable ☐ RIPv1 ☐ RIPv2

ROUTING RULES

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1					☐
2					☐
3					☐
4					☐
5					☐
6					☐
7					☐
8					☐

Save Settings Don't Save Settings

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 2'
- 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

Advanced Wireless contains settings which can negatively affect the performance of your router if configured improperly. Do not change these settings unless you are already familiar with them or have been instructed to make the change by one of our support personnel.

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

Transmit Power: Set the transmit power of the antennas.

RTS Threshold: This value should remain at its default setting of 2347. If inconsistent data flow is a problem, only a minor modification should be made.

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

WMM Capable: WMM (Wi-Fi Multimedia) is QoS (Quality of Service) system for your wireless network. Enable this option to improve the quality of video and voice applications for your wireless clients.

TX Rates: Select the basic transfer rates based on the speed of wireless adapters on your wireless network. It is strongly recommended to keep this setting to **Auto**.

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // 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

Beacon Interval : 100 (msec, range:1~1000, default: 100)

Transmit Power : 100%

RTS Threshold : 2347 (1~2347, default: 2347)

Fragmentation : 2346 (256~2346, default: 2346, even number only)

DTIM Interval : 3 (range: 1~255, default: 3)

WMM Capable : ☐ Enable ☒ Disable

TX Rates : Auto

Save Settings Don't Save Settings

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...](#)

Internet Offline

Reboot

Advanced Network

Advanced Network contains settings which can change the way the router handles certain types of traffic. We recommend that you do not change any of these settings unless you are already familiar with them or have been instructed to make the change by one of our support personnel.

UPNP

Enable UPnP: Click **Enable UPNP** to use the Universal Plug and Play (UPnP™) feature. UPNP provides compatibility with networking equipment, software and peripherals.

WAN PING

Enable WAN Ping Respond: Select the box to allow the WAN port to be “pinged.” Blocking the Ping option may provide some extra security from hackers.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // 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 : ☒

Save Settings Don't Save Settings

Internet Offline

Reboot

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.

[More...](#)

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Admin

The **Admin** page allows you to change the Administrator password and enable Remote Management. Admin has read/write access while the user has read-only access. Only the admin has the ability to change both admin and user account passwords.

ADMINISTRATOR

Admin Password: Enter and confirm the password that the admin account will use to access the router's management interface.

REMOTE MANAGEMENT

Remote Management: Remote management allows the DIR-455U to be configured from the Internet using a web browser. A username and password is still required to access the Web-Management interface. Usually 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.

IP Allowed to Access: Enter the Internet IP address of the PC that has access to the Broadband Router. If you enter an asterisk (*) in this field, then anyone will be able to access the Router. Adding an asterisk (*) into this field could present a security risk and is not recommended.

Port: This is the port number used to access the router. Example: 8080 is the port used for the Web-Management interface.

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

The screenshot shows the D-Link DIR-455U web management interface. The top bar indicates 'Product Page : DIR-455U' and 'Firmware Version : V1.01'. The main navigation menu includes 'DIR-455U', 'ADMIN', 'TIME', 'SYSLOG', 'EMAIL SETTINGS', 'SYSTEM', 'FIRMWARE', 'DYNAMIC DNS', 'SYSTEM CHECK', 'SCHEDULES', and 'LOGOUT'. The 'ADMIN' section is selected, showing 'ADMINISTRATOR SETTINGS' and 'REMOTE MANAGEMENT'.

ADMINISTRATOR SETTINGS

To help secure your network, we recommend that you should choose a new password.

Save Settings Don't Save Settings

ADMINISTRATOR (THE DEFAULT LOGIN NAME IS ("admin"))

Login Name :

New Password :

Confirm Password :

REMOTE MANAGEMENT

Enable Remote Management : ☐ Enabled

IP Allowed to Access :

Port :

Save Settings Don't Save Settings

Helpful Hints...

- 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.

[More...](#)

Time

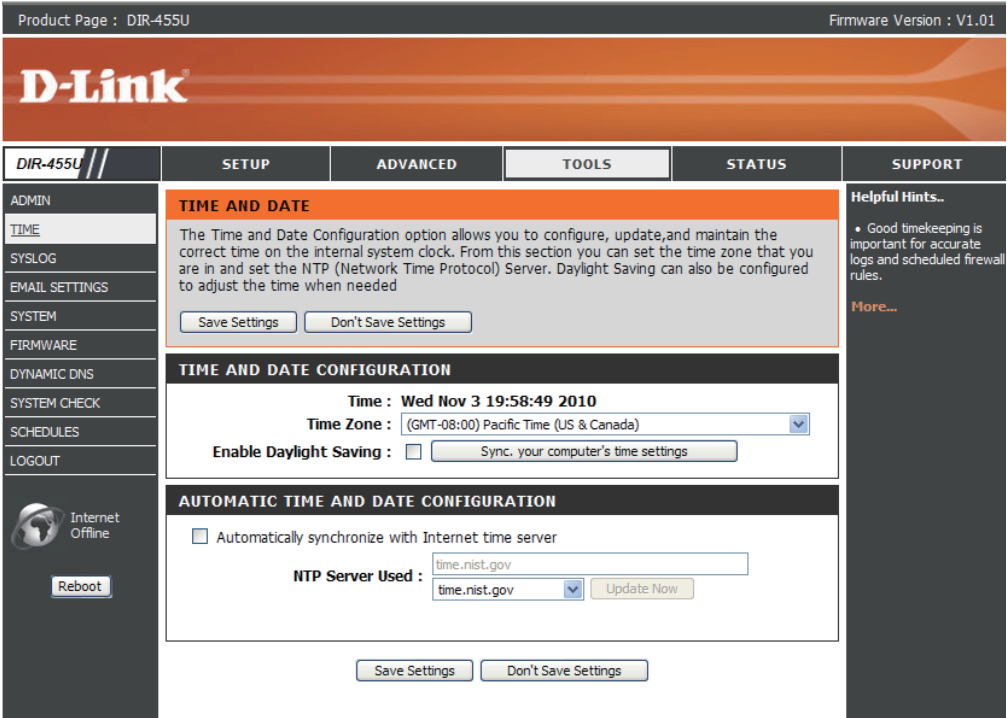
This section will help you set the time zone that you are in and the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to adjust the time when needed.

Time Zone: Select the appropriate **Time Zone** from the drop-down box.

Enable Daylight Saving: Select this checkbox to enter a start date and an end date for daylight saving time.

Automatic Time and Date Configuration: The Network Time Protocol (NTP) synchronizes the computer's clock over a network.

Set the Time and Date Manually: Manually enter the values for **Year, Month, Day, Hour, Minute, and Second.**



Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Syslog

The DIR-455U 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: Select this box to send the router logs to a Syslog Server.

Syslog Server IP Address: Enter the address of the Syslog server that will be used to send the logs. You may also select your computer from the drop-down box (only if you want to receive an IP address from the router via DHCP).

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

E-mail Settings

E-mail Settings allows you to send the system log files, router alert messages, and firmware update notifications to an e-mail address.

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

SMTP Sever IP and Port: Enter the SMTP server IP address followed by a colon and the port number (e.g. 123.123.123.1:25).

Send E-mail Alert to: Enter the e-mail address where you would like the e-mail sent to.

E-mail Subject: Enter a subject for the e-mail.

Test E-mail Alert: Click this button to send a test e-mail using the settings specified on this page.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // SETUP ADVANCED TOOLS STATUS SUPPORT

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

Internet Offline
Reboot

EMAIL SETTINGS

Send system log to a dedicated host or email to specific receipts

Save Settings Don't Save Settings

EMAIL SETTINGS

Enable Email Notification : ☐

SMTP Server IP and Port

Send E-mail alert to

E-mail Subject

Test E-mail alert

Save Settings Don't Save Settings

Helpful Hints..

- You may want to make the email settings similar to those of your email client program.

More...

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

System

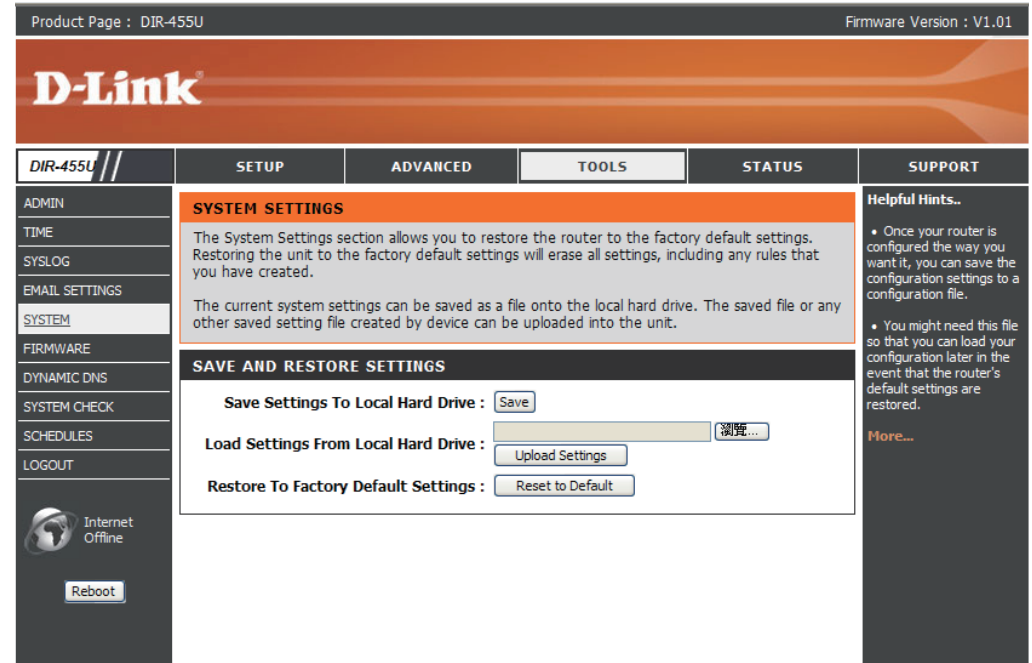
Here, you can save the current system settings onto the local hard drive.

Save To Local Hard Drive: Use this option to save your current router configuration settings to a file and onto your computer. Click **Save** to open a file dialog, and then select a location and file name for the settings.

Load From Local Hard Drive: Use this option to load the previously saved router configuration settings. Browse to find the saved file and then click **Upload Settings** to transfer those settings to the router.

Restore To Factory Default: This option will restore all settings back to their defaults. Any settings that have not been backed up will be lost, including any rules that you have created.

Reboots the DIR-455U: Click to reboot your router.



Firmware

Here, you can upgrade the firmware of your Router. Make sure the firmware you want to use is on the local hard drive of the computer and then click **Browse** to upload the file. 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.

Current Firmware Version: Displays your current firmware version.

Browse: After you have downloaded the new firmware, click **Browse** to locate the firmware on your computer.

Click **Upload** to start the firmware upgrade.

Product Page : DIR-455U

Firmware Version : V1.01

DIR-455U //

SETUP

ADVANCED

TOOLS

STATUS

SUPPORT

ADMIN

TIME

SYSLOG

EMAIL SETTINGS

SYSTEM

FIRMWARE

DYNAMIC DNS

SYSTEM CHECK

SCHEDULES

LOGOUT

Internet Offline

Reboot

FIRMWARE UPGRADE

There may be new firmware for your DIR-455U 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 Save Settings below to start the firmware upgrade.

FIRMWARE INFORMATION

Current Firmware Version : V1.01

Current Firmware Date : 2010/10/20

FIRMWARE UPGRADE

Note! Do not power off the unit when it is being upgraded.

The upgrade procedure takes about 180 seconds.

When the upgrade is done successfully, the unit will be restarted automatically.

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.

Upload :

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...

Dynamic DNS

The DDNS feature allows you to host a server (Web, FTP, or Game Server) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address.

Sign up for D-Link's free DDNS service at www.dlinkddns.com.

Enable Dynamic DNS: Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP Address. Select this box to enable DDNS.

Provider: Select your DDNS provider from the drop-down box.

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

Username / E-mail: Enter the **Username** for your DDNS account.

Password / Key: Enter the **Password** for your DDNS account.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // SETUP ADVANCED TOOLS STATUS SUPPORT

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

Internet Offline
Reboot

DYNAMIC DNS

The Dynamic DNS 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.

Save Settings Don't Save Settings

DYNAMIC DNS

DDNS : ☒ Disable ☐ Enable

Provider : DynDNS.org(Dynamic) ▼

Host Name :

Username / E-mail :

Password / Key :

Save Settings Don't Save Settings

Helpful Hints..

- To use this feature, you must first have a Dynamic DNS account from one of the providers in the drop down menu.

More...

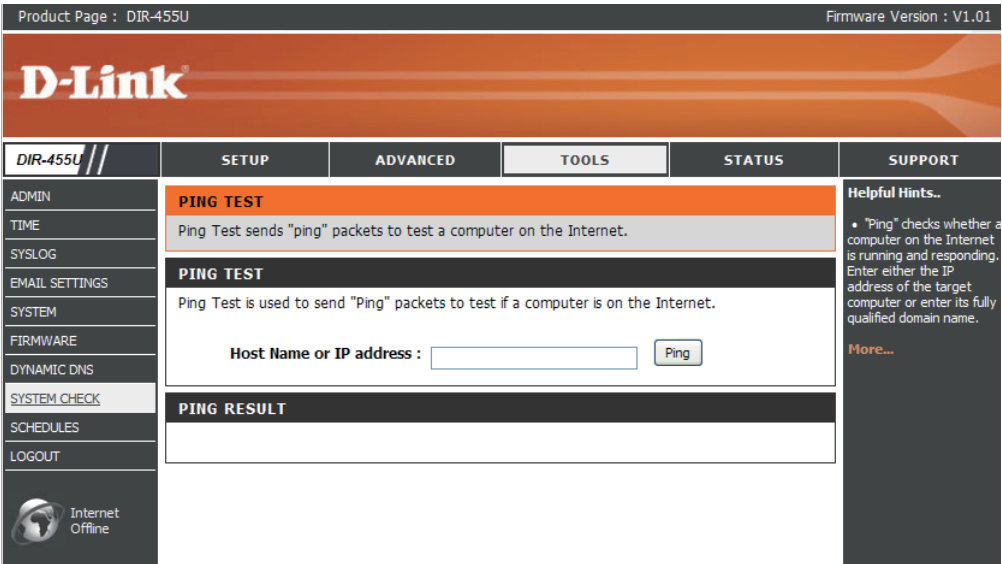
Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

System Check

This useful diagnostic utility can be used to check if a computer is connected to the network. It sends ping packets and listens for responses from the specific host.

Host Name or IP Address: Enter a host name or the IP address that you want to ping (Packet Internet Groper) and click **Ping**.

PING Result: The status of your Ping attempt will be displayed in the Ping Result box.



Schedules

This section allows you to manage schedule rules for various firewall and parental control features.

Add New Rule.... Click this button to specify the start time, end time, and name of the rule.

Edit: Edit the rule's start and end time.

Delete: Delete the rule.

Name of Rule 1: Enter a name for your new schedule.

Start Time (hh:mm): Enter the time at which you would like the schedule to become active.

End Time (hh:mm): Select the time at which you would like the schedule to become inactive.

Click **Save Settings** to save your changes, or click **Don't Save Settings** to discard your changes.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // SETUP ADVANCED **TOOLS** STATUS SUPPORT

SCHEDULES

The Schedule configuration option is used to manage schedule rules for "Virtual Server", "Outbound Filter" and "Inbound Filter".

Save Settings Don't Save Settings

SCHEDULE RULE

Enable Schedule : ☐

Rule#	Rule Name	Action
Add New Rule...		

Save Settings Don't Save Settings

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** to change an existing schedule.
- Click **Delete** icon to permanently delete a schedule.

[More...](#)

SCHEDULE RULE SETTING

Name of Rule 1 :

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Sunday	:	:
Monday	:	:
Tuesday	:	:
Wednesday	:	:
Thursday	:	:
Friday	:	:
Saturday	:	:
Every Day	:	:

Back

Device Information

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

General: Displays the current time and firmware version.

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

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

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

LAN Computers: Displays the list of DHCP clients.

DIR-455U //

ADMIN

TIME

SYSLOG

EMAIL SETTINGS

SYSTEM

FIRMWARE

DYNAMIC DNS

SYSTEM CHECK

SCHEDULES

LOGOUT

Internet Offline

Reboot

SETUP

ADVANCED

TOOLS

STATUS

SUPPORT

SCHEDULES

The Schedule configuration option is used to manage schedule rules for "Virtual Server", "Outbound Filter" and "Inbound Filter".

Save Settings Don't Save Settings

SCHEDULE RULE SETTING

Name of Rule 1 :

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Sunday	:	:
Monday	:	:
Tuesday	:	:
Wednesday	:	:
Thursday	:	:
Friday	:	:
Saturday	:	:
Every Day	:	:

Back

Save Settings Don't Save Settings

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...

Logs

Here, you can view logs and define events that you want to view. This router also has an internal syslog server, so you can send the log files to a computer that is running a syslog utility.

Product Page : DIR-455U Firmware Version : V1.01

D-Link

DIR-455U // SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICE INFO LOG STATISTICS WIRELESS LOGOUT

DEVICE INFORMATION

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

[Refresh](#)

GENERAL

Time : 2010年11月3日 下午 08:03:24
Firmware Version : V1.01, 2010/10/20

WAN

Connection Type : 3G
Service Type : N/A
Network Status : Disconnected
Connection Time : N/A
Signal Strength : (N/A)
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
DNS Server : 0.0.0.0

LAN

MAC Address : 1C-AF-F7-57-6D-6D
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WIRELESS LAN

MAC Address : 1C-AF-F7-57-6D-5F
Wireless : Enabled
SSID : default
Security : None
Channel : 11
802.11 Mode : Mixed mode
Wi-Fi Protected Setup : Disabled

LAN COMPUTERS

IP Address	Name	MAC
192.168.0.50	Merry-NB	00-18-F3-C8-BD-71

Helpful Hints...
• All of your LAN, WAN and WIRELESS connection details are displayed here.
[More...](#)

Internet Offline
[Refresh](#)

Statistics

Here you can view the packets transmitted and received passing through your router on both WAN and LAN ports. The traffic counter will reset if the device is rebooted.

Product Page : DIR-455U

Firmware Version : V1.01

DIR-455U //

SETUP

ADVANCED

TOOLS

STATUS

SUPPORT

DEVICE INFO

LOG

STATISTICS

WIRELESS

LOGOUT

Internet Offline

Reboot

VIEW LOG

View Log displays the activities occurring on the DIR-455U.

Refresh

Clear

Link To Log Settings

SYSTEM LOG

Time	Message
Nov 3 19:48:05	chat[3520]: alarm
Nov 3 19:48:05	chat[3520]: Failed
Nov 3 19:48:05	pppd: Connect script failed
Nov 3 19:48:05	pppd: pppd exit status = 8
Nov 3 19:48:07	pppd: Exit.
Nov 3 19:48:17	start: Start to open 3G connect
Nov 3 19:48:34	start: Try to set value CGATT to 1
Nov 3 19:48:51	pppd: Connecting with
Nov 3 19:48:51	chat[3614]: abort on (BUSY)
Nov 3 19:48:51	chat[3614]: abort on (NO CARRIER)
Nov 3 19:48:51	chat[3614]: abort on (ERROR)

Helpful Hints..

- Check the log frequently to detect unauthorized network usage.

More...

Wireless

This table displays a list of wireless clients that are connected to your wireless router. It also displays the connection time and MAC address of the connected wireless clients.

Product Page : DIR-455U

Firmware Version : V1.01



DIR-455U

SETUP

ADVANCED

TOOLS

STATUS

SUPPORT

DEVICE INFO

LOG

STATISTICS

WIRELESS

LOGOUT

 Internet Offline

Reboot

TRAFFIC STATISTICS

Traffic Statistics display Receive and Transmit packets passing through the DIR-455U.

Refresh

WAN STATISTICS INFORMATION

Statistics	Inbound	Outbound
Octets	0	0
Unicast Packets	0	0
Multicast Packets	0	0
Drops	0	0
Error	0	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...

Support

Product Page : DIR-455U

Firmware Version : V1.01

DIR-455U //

SETUP

ADVANCED

TOOLS

STATUS

SUPPORT

DEVICE INFO

LOG

STATISTICS

WIRELESS

LOGOUT

Internet Offline

Reboot

WIRELESS CLIENT LIST

View the wireless clients that are connected to the router. (A client might linger in the list for a few minutes after an unexpected disconnect.)

Refresh

WIRELESS CLIENT TABLE

IP Address	MAC Address
------------	-------------

Helpful Hints..

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

More...

Wireless Security

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

DIR-455U offers the following types of security:

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

What is WEP?

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

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

Configure WEP

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

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **Enable WEP Security**.
3. Next to *Authentication*, select **Open** or **Shared Key**.
4. Select either **64-bit** or **128-bit** encryption from the drop-down box next to *WEP Encryption*.
5. Next to *Key Type*, select either **Hex** or **ASCII**.

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

ASCII - All numbers and letters are valid.
6. Next to *Key 1*, enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to 4 different keys.
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 WEP on your adapter and enter the same WEP key as you did on the router.

WEP :

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

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

Authentication :	Open
WEP Encryption :	64Bit
Key Type :	HEX
Default WEP Key :	WEP Key 1
WEP Key 1 :	0000000000
WEP Key 2 :	0000000000
WEP Key 3 :	0000000000
WEP Key 4 :	0000000000

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.

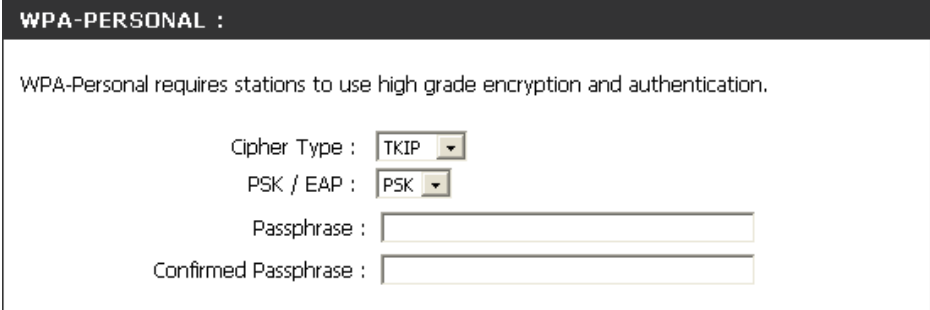
WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

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.

Configure WPA-PSK

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

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **Enable WPA-Personal Security** or **Enable WPA2-Personal Security**.
3. Next to *Cipher Mode*, select **TKIP**, **AES**, or **Auto**.
4. Next to *PSK/EAP*, select **PSK**.
5. Next to *Passphrase*, enter a key (passphrase). The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.
6. Enter the passphrase again next to *Confirmed Passphrase*.
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 (or WPA2-PSK) on your adapter and enter the same passphrase as you did on the router.



WPA-PERSONAL :

WPA-Personal requires stations to use high grade encryption and authentication.

Cipher Type :

PSK / EAP :

Passphrase :

Confirmed Passphrase :

Configure WPA (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 **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **Enable WPA-Personal Security** or **Enable WPA2-Personal Security**.
3. Next to *Cipher Mode*, select **TKIP**, **AES**, or **Auto**.
4. Next to *PSK/EAP*, select **EAP**.
5. Next to *RADIUS Server 1* enter the IP Address of your RADIUS server.
6. Next to *Port*, enter the port you are using with your RADIUS server. 1812 is the default port.
7. Next to *Shared Secret*, enter the security key.
8. If you have a secondary RADIUS server, enter its IP address, port, and secret key.
9. Click **Apply Settings** to save your settings.

WPA-PERSONAL :

WPA-Personal requires stations to use high grade encryption and authentication.

Cipher Type :

PSK / EAP :

802.1X

RADIUS Server 1 : IP

Port

Shared Secret

RADIUS Server 2 : IP

Port

Shared Secret

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.

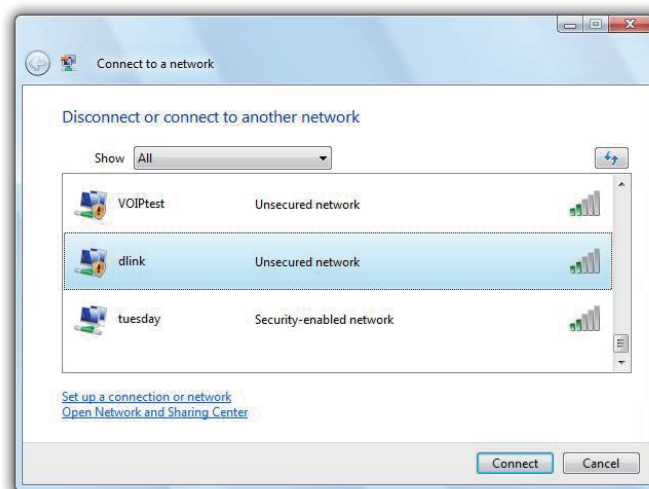
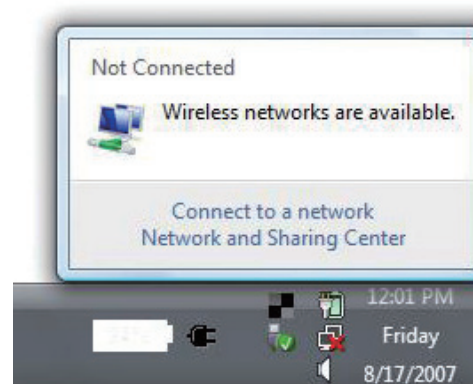
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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.

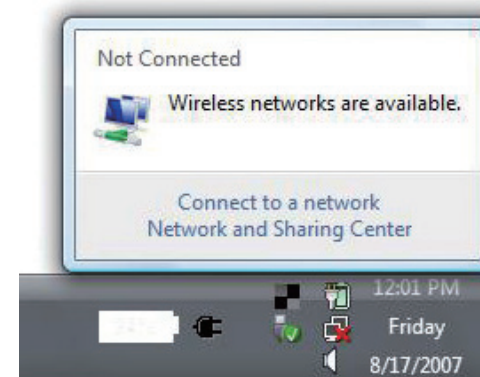
If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



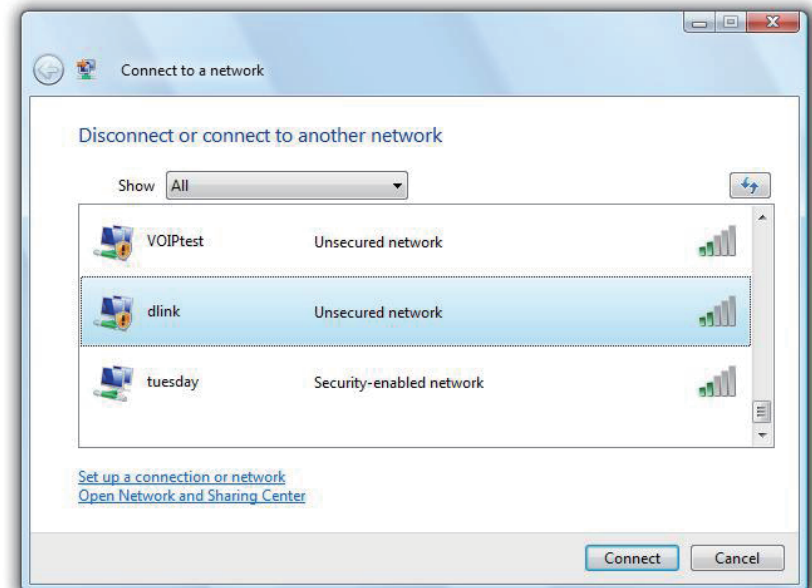
Configure Wireless Security

It is recommended to enable wireless security (WEP/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**.

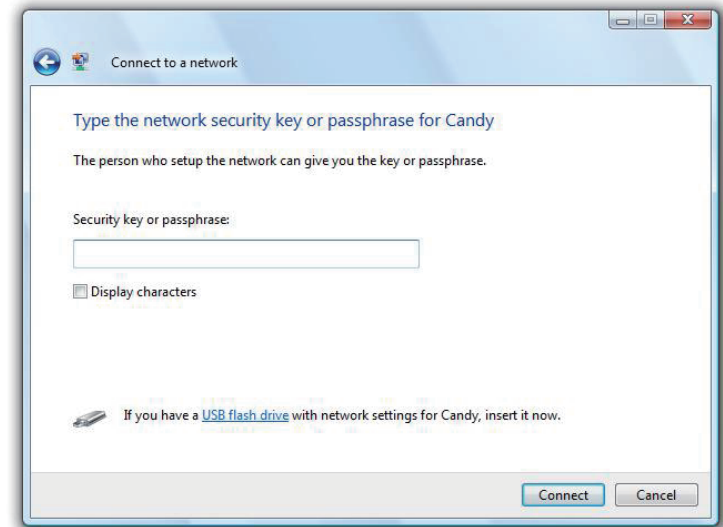


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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.

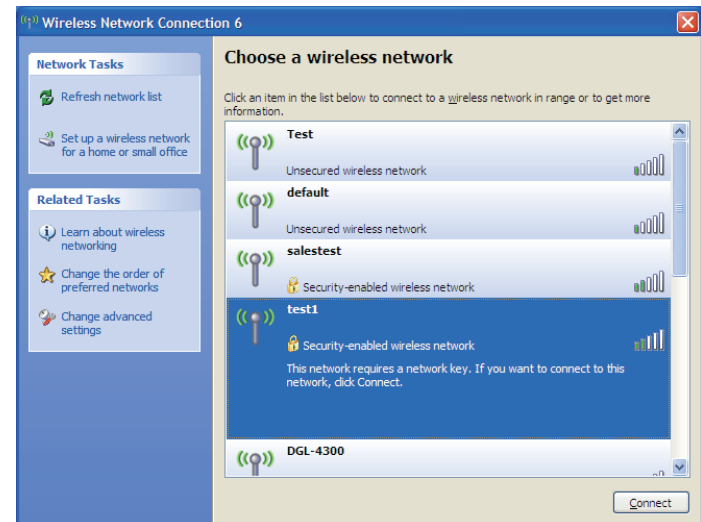
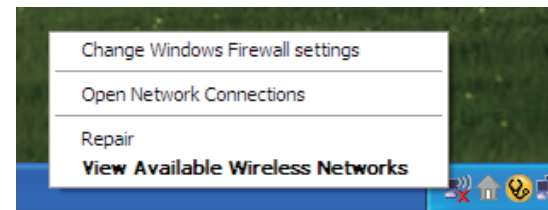
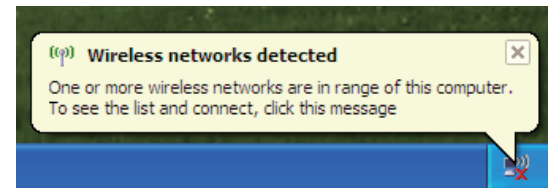
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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.

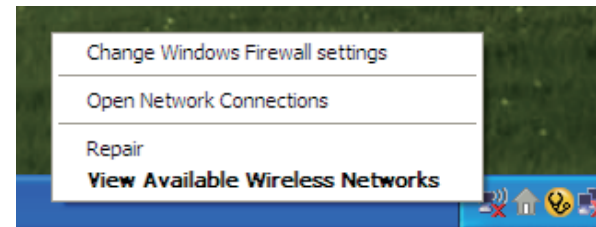
If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



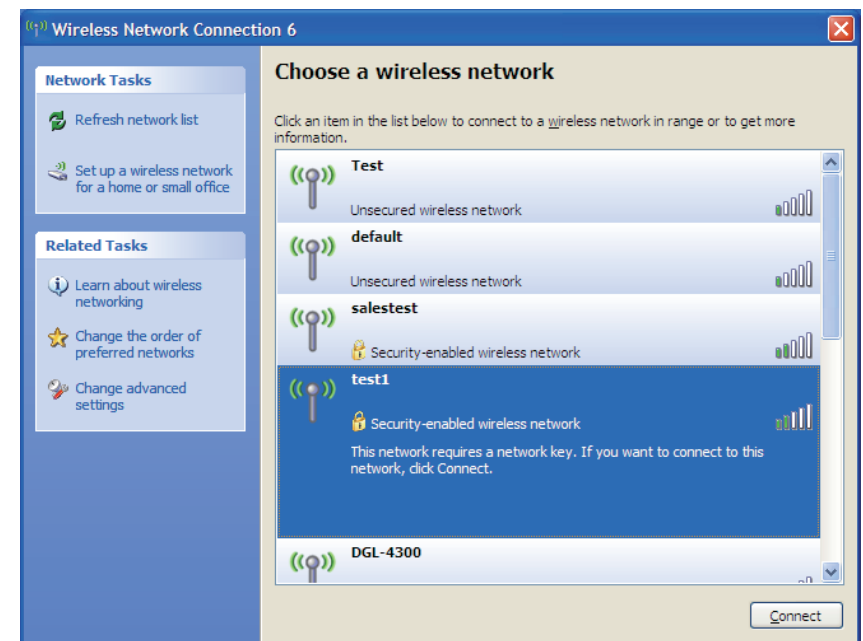
Configure WEP

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

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

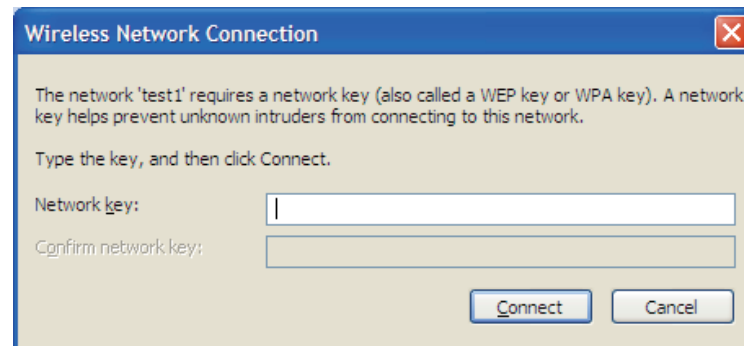


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the same WEP key that is on your router and click **Connect**.

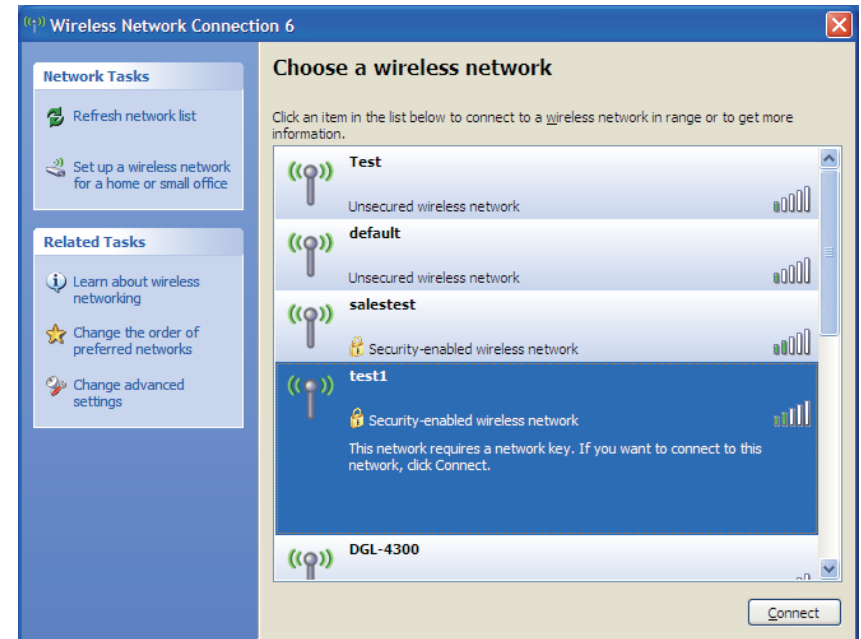
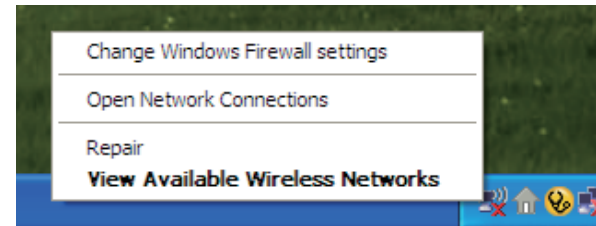
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP settings are correct. The WEP key must be exactly the same as on the wireless router.



Configure WPA-PSK

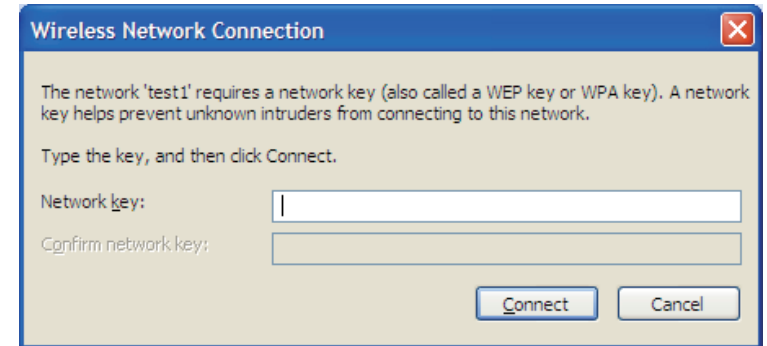
It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

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.



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-455U. 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.

Wireless Basics

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

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

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

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

What is Wireless?

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

Why D-Link Wireless?

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

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

Who uses wireless?

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

Home

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

Small Office and Home Office

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

Where is wireless used?

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

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

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

Tips

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

Centralize your Router or Access Point

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

Eliminate Interference

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

Security

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

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more WNA-2330 wireless network Cardbus adapters.

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

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

Networking Basics

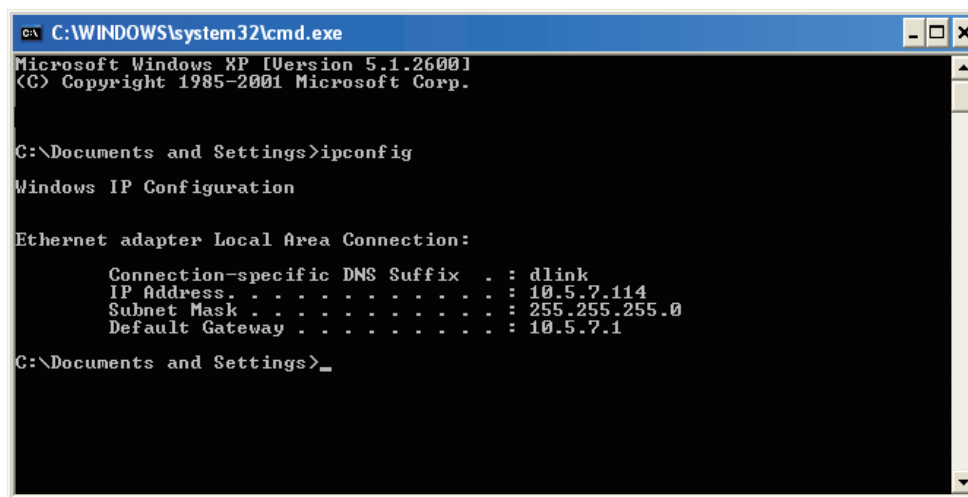
Check your IP address

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

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

At the prompt, type ***ipconfig*** and press **Enter**.

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



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600.1]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : dlink
    IP Address. . . . . : 10.5.7.114
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.5.7.1

C:\Documents and Settings>
```

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

Statically Assign an IP address

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

Step 1

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

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

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

Step 2

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

Step 3

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

Step 4

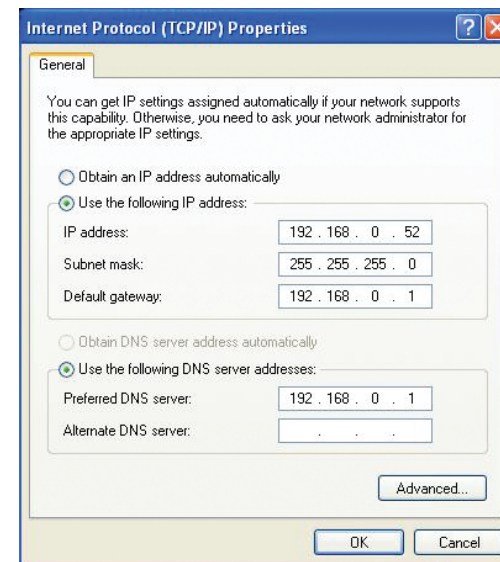
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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

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

Step 5

Click **OK** twice to save your settings.



Technical Specifications

GSM Band (GSM/GPRS/EDGE)

- 850 / 900 / 1800 / 1900 MHz
- Power Class 4 (850 / 900 MHz)
- Power Class 1 (1800 / 1900 MHz)

UMTS/HSUPA/HSDPA Band *

- 850 / 1900 / 2100 MHz
- Power Class 3

Data Rates **

- 6/9/11/12/18/24/36/48/54Mbps in 802.11g mode
- 1/2/5.5/11Mbps in 802.11b mode

Standards

- 802.11g
- 802.11b
- 802.3
- 802.3u

Wireless Security

- 64/128-bit WEP (Wired Equivalent Privacy)
- WPA & WPA2 (Wi-Fi Protected Access)

Firewall

- Network Address Translation (NAT)
- Stateful Packet Inspection (SPI)

VPN

- L2TP/PPTP/IPSEC VPN Pass-through
- 5 Dedicated IPsec tunnels

Antenna

- 2 Internal antennas
- 1 External Antenna

Ports

- 4 x LAN (RJ-45)
- 1 x WAN (RJ-45)
- 1 x Phone (RJ-11)

USIM Slot

- Standard 6-pin SIM card interface

LED Status Indicators

- WPS
- WAN
- LAN
- WLAN
- 2G/2.5G
- 3.5G/3.75G
- SMS
- Signal

Dimensions (L x W x H)

- 184 x 125 x 30 mm

Operating Temperature

- 0° to 40°C (32° to 104°F)

Operating Humidity

- 10%-90% (Non-condensing)

Certification

- CE
- FCC

* Supported frequency band is dependent upon regional hardware version.

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