



User Manual

HSPA+ 3G VPN Router

DWR-755

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.

Manual Revisions

Revision	Date	Description
1.0	February 21, 2014	• Initial release

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.

Apple®, Apple logo®, Safari®, iPhone®, iPad®, iPod touch® and Macintosh® are trademarks of Apple Inc., registered in the U.S. and other countries. App StoreSM is a service mark of Apple Inc.

Chrome™ browser, Google Play™ and Android™ are trademarks of Google Inc.

Internet Explorer®, Windows® and the Windows logo are trademarks of the Microsoft group of companies.

Copyright © 2014 by D-Link Corporation, Inc.

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

The purpose of this product is to create a constant network connection for your devices. As such, it does not have a standby mode or use a power management mode. If you wish to power down this product, please simply unplug it from the power outlet.

Table of Contents

Preface	i	L2TP	18
Manual Revisions	i	3G	19
Trademarks	i	GRE Settings	21
Product Overview	1	Wireless Settings	22
Package Contents	1	Wireless Connection Setup Wizard	22
System Requirements	2	Manual Wireless Connection Setup	25
Introduction	3	Network Settings	30
Features	4	DHCP Server Settings	31
Hardware Overview	5	IPv6	32
Rear Panel	5	Static IPv6	33
Front Panel	6	LAN IPv6 Address Settings	34
LEDs	7	PPPoE	35
Installation	8	LAN IPv6 Link-Local Address	36
Before you Begin	8	6 to 4	37
Wireless Installation Considerations	9	6rd	38
Configuration	10	Autoconfiguration	39
Web-based Configuration Utility	10	Message Service	40
Setup	11	SMS Inbox	40
Internet Connection Setup Wizard	12	Create Message	41
Manual Internet Connection Setup	14	USSD	42
Static (assigned by ISP)	14	VPN Settings	43
Dynamic IP (DHCP)	15	VPN Setup Wizard	43
PPPoE	16	Manual VPN Setup	45
PPTP	17	VPN Dynamic IP	46
		Tunnel - IKE	48
		Tunnel - Manual	51

Advanced	53	Statistics	79
Virtual Server	53	Wireless	80
Application Rules	54	IPv6 Status	81
QoS Engine	55	Support	82
MAC Address Filter	56	Connecting a Wireless Client	83
URL Filter	57	WPS Button	83
Outbound Filter	58	Windows® 8	84
Inbound Filter	59	WPA/WPA2	84
SNMP	60	Windows® 7	86
Routing	61	WPA/WPA2	86
Advanced Wireless	62	WPS	89
Advanced Network	64	Windows Vista®	93
Network Scan	65	WPA/WPA2	94
DMZ	66	Windows® XP	96
Tools	67	WPA/WPA2	97
Admin	67	Troubleshooting	99
Time	68	Wireless Basics	103
Syslog	69	What is Wireless?	104
Email Settings	70	Tips	106
System	71	Wireless Modes	107
Firmware	72	Networking Basics	108
Dynamic DNS	73	Check your IP address	108
System Check	74	Statically Assign an IP address	109
Schedules	75	Technical Specifications	110
PIN Control	76		
Status	77		
Device Info	77		
Log	78		

Package Contents



DWR-755 HSPA+ 3G VPN Router



Ethernet Cable



Detachable Antenna



Power Adapter

If any of the above items are missing, please contact your reseller.

Note: *Using a power supply with a different voltage rating than the one included with the DWR-755 will cause damage and void the warranty for this product.*

System Requirements

Network Requirements	• An Ethernet-based cable or DSL modem • IEEE 802.11n, 802.11g, or 802.11b wireless clients • 10/100 Ethernet • A compatible (U)SIM card with service.* *Subject to services and service terms available from your carrier.
Web-based Configuration Utility Requirements	Computer with the following: • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter Browser Requirements: • Internet Explorer 6 or higher • Firefox 3.0 or higher • Safari 3.0 or higher • Chrome 2.0 or higher Windows® Users: Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.

Introduction

The D-Link DWR-755 is a 802.11n/g/b compliant device that delivers real world performance of up to 14x faster than an 802.11g wireless connection (also faster than a 100 Mbps wired Ethernet connection). Create a secure wireless network to share photos, files, music, video, printers, and network storage throughout your home. Connect the DWR-755 router to a cable or DSL modem and share your high-speed Internet access with everyone on the network. In addition, this router includes a Quality of Service (QoS) engine that keeps digital phone calls (VoIP) and online gaming smooth and responsive, providing a better Internet experience.

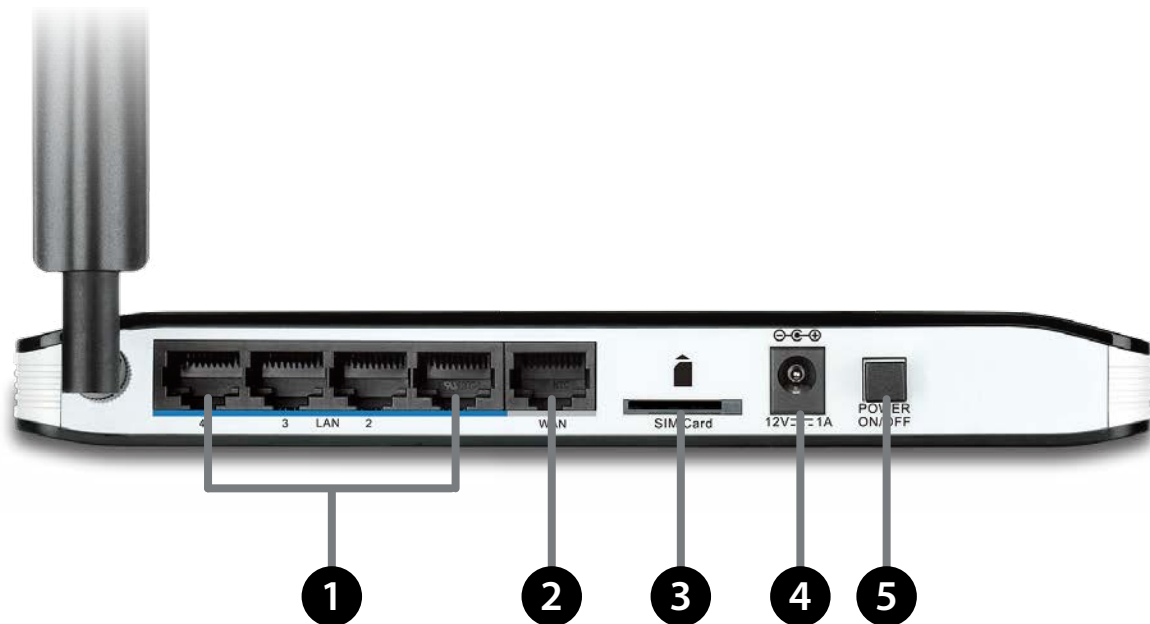
Features

- **Ultimate Performance** - The D-Link DWR-755 delivers real world performance of up to 14x faster than an 802.11g wireless connection so you can stream photos, music, and videos smoothly throughout your home.
- **Extended Whole Home Coverage** - Powered by Wireless N technology, this high performance router provides superior Whole Home Coverage while reducing dead spots. The router is designed for use in bigger homes and for users who demand higher performance networking. Add a Wireless N notebook or desktop adapter and stay connected to your network from virtually anywhere in your home.
- **Total Network Security** - The Wireless N router supports all of the latest wireless security features to prevent unauthorized access, be it from over the wireless network or from the Internet. Support for WPA/WPA2 standards ensures that you'll be able to use the best possible encryption method, regardless of your client devices. In addition, this router utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.
- **Quality of Service (QoS)** - For smooth, uninterrupted streaming, this router includes a Quality of Service (QoS) engine that prioritizes according to data type so your digital phone calls (VoIP) and online gaming stay smooth and responsive.

* Maximum wireless signal rate derived from IEEE Standard 802.11b, 802.11g and 802.11n 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 conditions will adversely affect wireless signal range.

Hardware Overview

Rear Panel



1	LAN Ports (1-4)	Connect Ethernet devices such as computers, switches, and NAS.
2	WAN Port	The auto MDI/MDIX Internet port connects to your cable or DSL modem via an Ethernet cable.
3	SIM	Accepts a standard (U)SIM card for 2G/3G connectivity.
4	Power Receptor	Connects to the included power adapter.
5	Power Switch	Turns the device on or off.

Hardware Overview

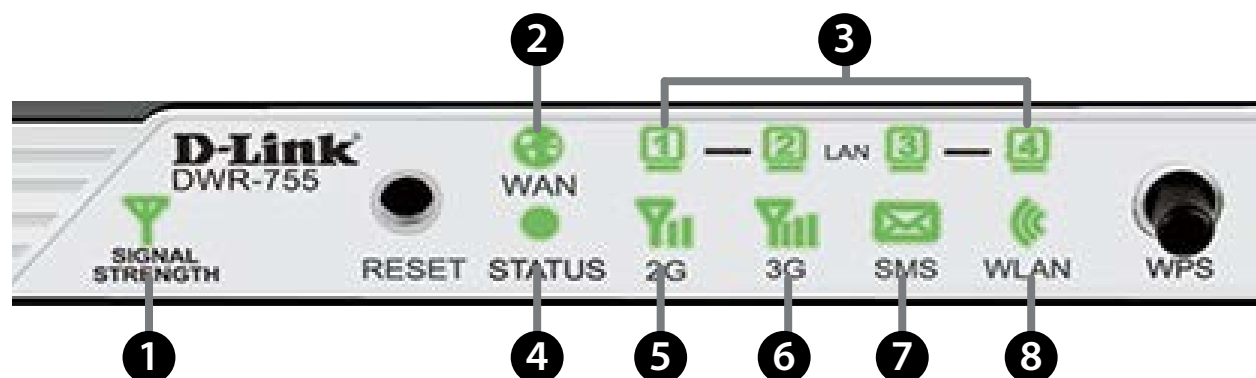
Front Panel



1	Reset	Press this button for 10 seconds with an unfolded paperclip to reset the device.
2	WPS	Press this button to initiate a new WPS connection. Refer to “Add Wireless Device with WPS” on page 24 for more details.

Hardware Overview

LEDs



1	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)
2	WAN	Solid Green: Ethernet connection has been established Blinking Green: Data is being transferred
3	LAN (1-4)	Solid Green: Ethernet connection has been established Blinking Green: Data is being transferred
4	Status	Blinking Green: Device is working
5	2G	Solid Green: EDGE or GPRS connection has been established Blinking Green: Data is being transferred via 2G
6	3G	Solid Green: UMTS/HSDPA/HSUPA/HSPA+ connection is established Blinking: Data is being transferred via 3G
7	SMS	Solid Green: SMS storage is full Blinking Green: There is an unread SMS
8	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.

Before you Begin

1. Ensure that your DWR-755 is disconnected and powered off.
2. Insert a standard (U)SIM card into the SIM card slot on the back of the router as indicated by the SIM card logo next to the slot. The gold contacts should face downwards.

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.

3. Connect the power adapter to the socket on the back panel of your DWR-755. Plug the other end of the power adapter into a wall outlet or power strip and turn the device on.
 - 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 DWR-755 performs initialization and Internet connection processes.

Wireless Installation Considerations

The D-Link wireless router lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

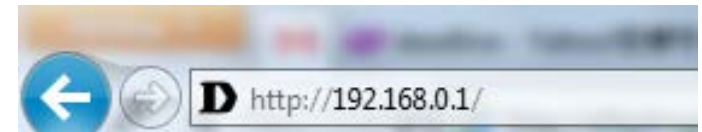
1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.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. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

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 (**http://192.168.0.1**).



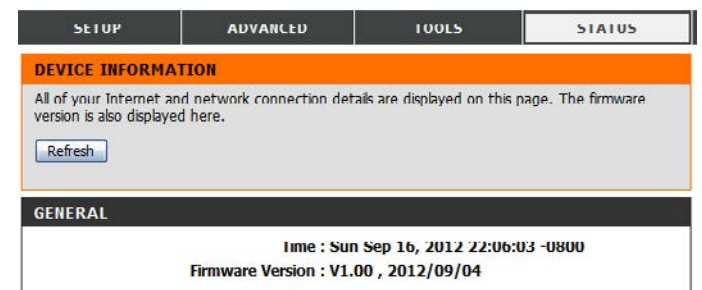
Type **Admin** and then enter the password. By default, the password is blank.

If you get a **Page Cannot be Displayed** error, please refer to “Troubleshooting” on page 56 for assistance.



The configuration utility will open to the **STATUS > DEVICE INFO** page. You can view different configuration pages by clicking on the categories at the top of the screen (SETUP/ADVANCED/TOOLS/STATUS/SUPPORT), and then selecting a configuration page from the bar on the left side.

The following pages will describe each section in detail, starting with the **SETUP** pages.



Setup

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 refer to “Manual Internet Connection Setup” on page 14.

SETUP	ADVANCED	TOOLS	STATUS
INTERNET CONNECTION			
There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection.			
INTERNET CONNECTION SETUP WIZARD			
If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your Router to the Internet, click on the button below.			
Internet Connection Setup Wizard			
Note : Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.			
MANUAL INTERNET CONNECTION OPTIONS			
If you would like to configure the Internet settings of your Router manually, then click on the button below.			
Manual Internet Connection Setup			

Internet Connection Setup Wizard

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

Click **Next** to continue.

Note: While using the wizard, you can click **Prev** to go back to the previous step, or you can click **Cancel** to close the wizard.

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

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

Select the Internet connection type you use. The connection types are explained on the following page. If you are unsure which connection type you should use, contact your Internet Service Provider (ISP).

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

Note: The DWR-755 has a WAN failover feature that allows the router to switch to a 2G/3G connection if the WAN connection is down or unavailable.

WELCOME TO THE SETUP WIZARD

It appears that you have already successfully connected your new router to the Internet. Click **Next** if you still want to secure the router with a password and set the time zone.

- Step 1: Set your Password
- Step 2: Select your Time Zone
- Step 3: Configure your Internet Connection
- Step 4: Save Settings and Connect

Prev Next Cancel Connect

STEP 1: SET YOUR PASSWORD

To secure your new networking device, please set and verify a password below:

Password :

Verify Password :

Prev Next Cancel Connect

STEP 2: SELECT YOUR TIME ZONE

Select the appropriate time zone for your location. This information is required to configure the time-based options for the router.

(GMT-08:00) Pacific Time (US & Canada)

Prev Next Cancel Connect

STEP 3: CONFIGURE YOUR INTERNET CONNECTION

Please select the Internet connection type below:

- ☒ **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.
- ☐ **Username / Password Connection (PPPoE)**
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.
- ☐ **Username / Password Connection (PPTP)**
PPTP client.
- ☐ **Username / Password Connection (L2TP)**
L2TP client.
- ☐ **3G Connection**
3G.
- ☐ **Static IP Address Connection**
Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

Prev Next Cancel Connect

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 "Dynamic IP (DHCP)" on page 15 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 "PPPoE" on page 16 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 "PPTP" on page 17 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 "L2TP" on page 18 for information about how to configure this type of connection. |
| 3G Connection: | Choose this connection if you have installed a SIM card into the DWR-755. See "3G" on page 19 for information about how to configure this type of connection. |
| Static IP Address
Connection: | Choose this option if your Internet Service Provider provided you with IP address information that has to be manually configured. See "Static (assigned by ISP)" on page 14 for information about how to configure this type of connection. |

After entering the requested information, click **Next** to continue.

Note: If you are not sure what connection type to use or what settings to enter, check with your Internet Service Provider.

This completes the Internet Connection Setup Wizard. Click **Connect** to save your changes and reboot the router.



Manual Internet Connection Setup

Static (assigned by ISP)

Select Static IP Address if all the Internet port's IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The router will not accept the IP address if it is not in this format. After modifying any settings, click **Save Settings** to save your changes.

Failover Internet Type Is: This will display the failover Internet type, if available.

IP Address: Enter the IP address assigned by your ISP.

Subnet Mask: Enter the Subnet Mask assigned by your ISP.

Default Gateway: Enter the Gateway assigned by your ISP.

DNS Servers: The DNS server information will be supplied by your ISP (Internet Service Provider.)

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

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** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

The screenshot shows the 'INTERNET CONNECTION TYPE' section with a dropdown menu set to 'Static IP' and 'Failover Internet Type' set to 'Disable (N/A)'. Below this is the 'STATIC IP ADDRESS INTERNET CONNECTION TYPE' section, which includes input fields for IP Address, Subnet Mask, Default Gateway, Primary DNS Server, and Secondary DNS Server. There is also an MTU field with a default value of 1500 and a 'Clone' button next to the MAC Address field.

INTERNET CONNECTION TYPE	
Choose the mode to be used by the router to connect to the Internet.	
My Internet Connection is	Static IP
Failover Internet Type is	Disable (N/A)

STATIC IP ADDRESS INTERNET CONNECTION TYPE	
Enter the static address information provided by your Internet Service Provider (ISP).	
IP Address :	
Subnet Mask :	
Default Gateway :	
Primary DNS Server :	
Secondary DNS Server :	
MTU :	(bytes) MTU default = 1500
MAC Address :	Clone

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. After modifying any settings, click **Save Settings** to save your changes.

Host Name: (Optional) Fill in the host name of your DNS server.

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

Secondary DNS Server: (Optional) Fill in with IP address of the 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** 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 the WAN IP address automatically when the lease time has expired.

The screenshot shows a web interface titled "DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE". Below the title is a blue instruction box: "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 configuration fields include: "Host Name:" with a text input; "Primary DNS Server:" with a text input; "Secondary DNS Server:" with a text input; "MTU:" with a text input and "(bytes) MTU default = 1500" text; "MAC Address:" with a text input and a "Clone" button; and "Auto-reconnect:" with a checked checkbox and the label "Enable".

PPPoE

Choose this Internet connection if your ISP provides you with a PPPoE account. After modifying any settings, click **Save Settings** to save your changes.

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: Re-type your password in this field.

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

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

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

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

MAC Address: MAC address of WAN interface. You can also copy MAC address of your PC to its WAN interface by clicking the **Clone** button.

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

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU.

Auto-reconnect: The device will automatically reconnect to your PPPoE connection automatically.

The screenshot shows a web-based configuration page titled "PPPoE". Below the title is a subtitle: "Enter the information provided by your Internet Service Provider (ISP)". The form contains the following fields and controls:

- Username :** A text input field.
- Password :** A text input field.
- Verify Password :** A text input field.
- Service Name :** A text input field with "(optional)" to its right.
- IP Address :** A text input field.
- Primary DNS Server :** A text input field with "(optional)" to its right.
- Secondary DNS Server :** A text input field with "(optional)" to its right.
- MAC Address :** A text input field with a "Clone" button to its right.
- Maximum Idle Time :** A numeric input field with "600" entered, followed by "seconds".
- MTU :** A numeric input field with "0" entered, followed by "(bytes) MTU default = 1492".
- Auto-reconnect :** A checkbox labeled "Enable".

PPTP

Choose PPTP (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. Click **Save Settings** to save your changes.

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: Re-enter your password for verification.

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 a PPTP connection when local users want to connect to the Internet, and disconnect if there is no traffic after the time period defined by the **Maximum Idle Time** setting.

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 titled "PPTP". Below the title is a subtitle: "Enter the information provided by your Internet Service Provider (ISP)". The form contains the following fields and options:

- Address Mode :** Two radio buttons: "Dynamic IP" (unselected) and "Static IP" (selected).
- PPTP IP Address :** A text input field.
- PPTP Subnet Mask :** A text input field.
- PPTP Gateway IP Address :** A text input field.
- PPTP Server IP Address :** A text input field.
- Username :** A text input field.
- Password :** A text input field.
- Verify Password :** A text input field.
- Reconnect Mode :** Two radio buttons: "Always-on" (selected) and "Connect-on-demand" (unselected).
- Maximum Idle Time :** A text input field containing the value "300", followed by the label "seconds".

L2TP

Choose this Internet connection if your ISP provides you with an L2TP account. After modifying any settings, click **Save Settings** to save your changes.

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: Re-type your password in this field.

Reconnect Mode: Choose **Always-on** when you want to establish L2TP connection all the time. If you choose **Connect-on-demand** the device will establish L2TP connection when local users want to use 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 0 or choose **Always-on** to disable this feature.

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

- Address Mode :** Radio buttons for ☐ Dynamic IP and ☒ Static IP.
- L2TP IP Address :** Text input field.
- L2TP Subnet Mask :** Text input field.
- L2TP Gateway IP Address :** Text input field.
- L2TP Server IP Address :** Text input field.
- Username :** Text input field.
- Password :** Text input field.
- Verify Password :** Text input field.
- Reconnect Mode :** Radio buttons for ☒ Always-on and ☐ Connect-on-demand.
- Maximum Idle Time :** A numeric input field set to 300, followed by the text "seconds".

3G

Choose this Internet connection if you already use a SIM card for 2G/3G Internet service from your mobile Internet service provider. The fields here may not be necessary for your connection. The information on this page should only be used if required by your service provider. After modifying any settings, click **Save Settings** to save your changes.

Dial Up Profile: Select **Auto-Detection** to have the router automatically detect the settings for your connection. Select **Manual** to enter the details of your connection manually.

Country/Telecom: Select your country and service provider to automatically fill in some of the required settings.

3G Network Choose between **WCDMA/HSPA** or **CDMA2000/EV-DO**.

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

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

Verify Password: Re-type your password.

Dialed Number: Enter the number to be dialed.

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

APN: Enter the APN information (optional).

Pin Code: Enter the PIN associated with your SIM card.

Reconnect Mode: Select **Auto** or **Manual** to determine whether the router should reconnect to your 3G/4G network automatically or manually.

- Maximum Idle Time:** Set the maximum time your connection can be idle before disconnecting. Set it to 0 or choose Auto in Reconnect Mode to disable this feature.
- Primary DNS Server:** Fill in if provided by your ISP. If not, keep the default value (optional).
- Secondary DNS Server:** Fill in if provided by your ISP. If not, keep the default value (optional).
- Keep Alive:** Select **Disable** or **Use Ping** depending on the settings required by your ISP. If you select Use Ping, set the ping interval and the IP address to ping.
- Bridge Ethernet Ports:** Activate this feature to use the Ethernet WAN port as an additional LAN port.

3G INTERNET CONNECTION TYPE

Enter the information provided by your Internet Service Provider (ISP).

Dial-Up Profile : ☐ Auto Detection ☒ Manual

Country :

Telecom :

3G Network :

Username : (optional)

Password : (optional)

Verify Password : (optional)

Dialed Number :

Authentication :

APN : (optional)

Pin Code :

Reconnect Mode : ☒ Auto ☐ Manual

Maximum Idle Time : seconds

Primary DNS Server :

Secondary DNS Server :

Keep Alive : ☒ Disable ☐ Use Ping

Bridge ethernet ports : ☐ Enable

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. Click **Save Settings** to apply changes.

- Name:** Choose a name for the GRE tunnel.
- Tunnel IP:** Enter the IP address for the tunnel.
- Peer IP:** Enter a Peer IP for the tunnel.
- Key:** Define a key.
- TTL:** Set the time to live for the GRE tunnel.
- Subnet:** Enter the subnet address.
- Enable:** Check this box to enable the individual GRE tunneling rule.
- Default Gateway:** Choose a gateway from the drop-down menu (if any).
- Refresh:** Update the information on current GRE tunnels.

GRE TUNNEL

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

Default Gateway: None

TUNNELS INFORMATION

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

Refresh

Wireless Settings

Wireless Connection Setup Wizard

This section will help you to manually configure the wireless settings of your router. Please note that changes made in this section may also need to be duplicated on your wireless devices and clients. The Wireless Settings page allows you to configure how your router connects to the Internet. There are several ways to set up your wireless connection. You can click on the **Wireless Connection Setup Wizard** button to start a wizard that will guide you through setting up your wireless settings. If you want to manually configure your settings, click the **Manual Wireless Connection Setup** button and skip to "Manual Wireless Connection Setup" on page 25. You can also set up a wireless connection to a device automatically, or configure your router automatically through Windows by clicking the **Wi-Fi Protected Setup** button. This is described in "Add Wireless Device with WPS" on page 24.

This wizard will guide you through a step-by-step process to configure your router's wireless settings.

Click **Next** to continue.

Note: While using the wizard, you can click **Prev** to go back to the previous page or you can click **Cancel** to close the wizard.

Enter a name (SSID) for your wireless network, then click **Next** to continue.

Select a level of wireless security to use, then click **Next** to continue.

WELCOME TO THE WIRELESS SECURITY SETUP WIZARD

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

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

Prev Next Cancel Save

STEP 1: NAME YOUR WIRELESS NETWORK

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

Wireless Network Name (SSID):

Prev Next Cancel Save

STEP 2: SECURE YOUR WIRELESS NETWORK

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

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

BEST : ☒ Select this option if your wireless adapters SUPPORT WPA2

BETTER : ☐ Select this option if your wireless adapters SUPPORT WPA

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

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

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

Note: All wireless adapters currently support WPA.

Prev Next Cancel Save

If you chose **BEST** or **BETTER**, select whether to use TKIP or AES encryption, then enter a password to use for your wireless network. It is recommended that you use AES if your wireless computers and devices support it, as it is more secure. Click **Next** to continue.

STEP 3: SET YOUR WIRELESS SECURITY PASSWORD

Once you have selected your security level - you will need to set a wireless security password. With this password, a unique security key will be generated.

Wireless Security Password : AES TKIP myPassword

Note: You will need to enter the unique security key generated into your wireless clients enable proper wireless communication - not the password you provided to create the security key.

If you chose **GOOD**, select whether to use a HEX or ASCII password, then enter a password to use for your wireless network. If you choose HEX, you will need to enter a 10 or 26 digit password using only hex characters (0-9, A-F). If you choose ASCII, the password must be 5 or 13 alphanumeric characters. Click **Next** to continue.

STEP 3: SET YOUR WIRELESS SECURITY PASSWORD

Once you have selected your security level - you will need to set a wireless security password. With this password, a unique security key will be generated.

Wireless Security Password : HEX ASCII 1234567890

Note: You will need to enter the unique security key generated into your wireless clients enable proper wireless communication - not the password you provided to create the security key.

This completes the Wireless Connection Setup Wizard. Click **Save** to save your changes and reboot the router.

SETUP COMPLETE!

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

Wireless Network Name (SSID) : myNetwork

Add Wireless Device with WPS

Wi-Fi Protected Setup (WPS) System is a simplified method for securing your wireless network during the initial setup as well as the “Add New Device” processes. The Wi-Fi Alliance (WFA) has certified it across different products as well as manufacturers. The process is just as easy as pressing a button for the Push-Button method or correctly entering the 8-digit code for the Pin Code method. The time reduction in setup and ease of use are quite beneficial, while the highest wireless Security setting of WPA2 is automatically used.

WPS: Enable the Wi-Fi Protected Setup feature.

AP PIN: A PIN is a unique number that can be used to add the router to an existing network or to create a new network. Pushing this button will generate a new, random PIN.

Config Mode: Choose either **Enrollee** or **Registrar** from the drop-down menu.

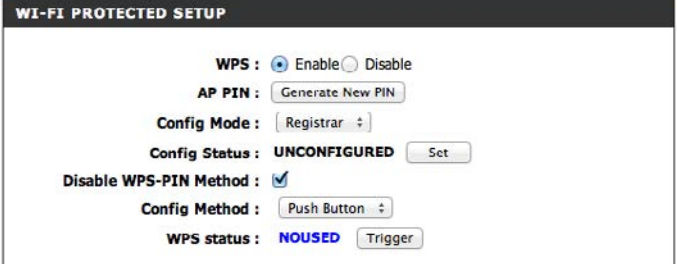
Config Status: Press **Set** to switch between **Configured** and **Unconfigured** states.

Disable WPS-PIN Method: Check this button to use the Push Button method only.

Config Method: Select **Push Button** or **PIN** method from the drop-down menu. For the Push Button method, to add a wireless client simply push the WPS button on the device and click Trigger. In order to use the PIN method you must know the wireless client's 8 digit PIN and click Trigger.

Note: Once you click **Trigger**, you will have a 120 second time limit to apply the settings to your wireless client(s) and successfully establish a connection.

WPS Status: Indicates whether WPS is **In Use** or **Not In Use**. The Trigger button will activate WPS for up to 120 seconds.



The screenshot shows the 'WI-FI PROTECTED SETUP' configuration interface. It includes the following elements: a 'WPS' toggle set to 'Enable'; an 'AP PIN' field with a 'Generate New PIN' button; a 'Config Mode' dropdown menu set to 'Registrar'; a 'Config Status' indicator showing 'UNCONFIGURED' with a 'Set' button; a 'Disable WPS-PIN Method' checkbox that is checked; a 'Config Method' dropdown menu set to 'Push Button'; and a 'WPS status' indicator showing 'NOUSED' with a 'Trigger' button.

Manual Wireless Connection Setup

This page lets you set up your wireless network and choose a wireless security mode. After modifying any settings, click **Save Settings** to save your changes.

Enable Wireless: Check this box to enable wireless access. When you enable 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: **B/G mixed:** Enable this mode if your network contains a mix of 802.11b and 802.11g devices.
N only: Enable this mode if your network only has 802.11n devices.
B/G/N mixed: Enable this mode if you have a mix of 802.11n, 802.11g, and 802.11b clients.

Auto Channel Scan: Enabling this feature will allow the router to automatically scan for the best wireless channel to use.

Wireless Channel: 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, or enable Auto Channel Scan for the router to automatically select the best channel.

Visibility Status: This setting determines whether the SSID will be **Visible** or **Invisible** to wireless clients looking for wireless networks. Setting this to **Invisible** can increase the security of your network by making it undetectable, but clients will need to manually enter the SSID of your network to connect.

SETUP	ADVANCED	TOOLS	STATUS																		
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 <table> <tr> <td>Enable Wireless :</td> <td>☒</td> <td></td> </tr> <tr> <td>Wireless Network Name :</td> <td> dlinkrouter </td> <td>(Also called the SSID)</td> </tr> <tr> <td>802.11 Mode :</td> <td>B/G/N mixed</td> <td></td> </tr> <tr> <td>Auto Channel Scan :</td> <td>☐</td> <td></td> </tr> <tr> <td>Wireless Channel :</td> <td>2.462 GHz - CH 11</td> <td></td> </tr> <tr> <td>Visibility Status :</td> <td>☒ Visible</td> <td>☐ Invisible</td> </tr> </table>				Enable Wireless :	☒		Wireless Network Name :	dlinkrouter	(Also called the SSID)	802.11 Mode :	B/G/N mixed		Auto Channel Scan :	☐		Wireless Channel :	2.462 GHz - CH 11		Visibility Status :	☒ Visible	☐ Invisible
Enable Wireless :	☒																				
Wireless Network Name :	dlinkrouter	(Also called the SSID)																			
802.11 Mode :	B/G/N mixed																				
Auto Channel Scan :	☐																				
Wireless Channel :	2.462 GHz - CH 11																				
Visibility Status :	☒ Visible	☐ Invisible																			

Security Mode: You can choose from 4 different security modes.

- **None:** No security will be used. This setting is not recommended.
- **WEP:** WEP encryption will be used. This setting is only recommended if your wireless devices do not support WPA or WPA2.
- **WPA-Personal:** WPA-PSK encryption will be used. This setting is recommended for most users.
- **WPA-Enterprise:** WPA-EAP encryption will be used. This setting is only recommended if you have a RADIUS authentication server. Otherwise, **WPA-Personal** should be used.

WIRELESS SECURITY MODE	
Security Mode :	None ▼

WEP

- Authentication:** Select whether to use **Open** or **Shared** authentication.
- WEP Encryption:** Select whether to use **64-bit** or **128-bit** encryption.
- Default WEP Key:** Select which WEP key (1-4) to use as the default key. This will also change the WEP Key text box to that WEP key for you to configure(1-4).
- WEP Key:** Set the WEP key/password for your wireless network. Based on whether you are using 64 or 128-bit encryption, and whether you are using a HEX or ASCII key, you will need to enter different numbers of characters for your key, as indicated below the WEP Key text box. ASCII keys may use letters and numbers only, and HEX keys may use numbers 0-9 and letters A-F only.

The screenshot shows the 'WIRELESS SECURITY MODE' configuration page. At the top, 'Security Mode' is set to 'WEP'. Below this, the 'WEP' section contains explanatory text about the standard and key entry requirements. It states that for 64-bit keys, 10 hex digits must be entered, and for 128-bit keys, 26 hex digits must be entered. It also mentions that a hex digit can be a number 0-9 or a letter A-F, and that for the most secure use, 'Shared Key' authentication should be selected. Below the text, there are four configuration options: 'Authentication' set to 'Open', 'WEP Encryption' set to '64Bit', 'Default WEP Key' set to 'WEP Key 1', and 'WEP Key' set to 'HEX' with a text box containing '1234567890'. A note below the text box indicates '(5 ASCII or 10 HEX)'.

WIRELESS SECURITY MODE

Security Mode : WEP

WEP

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

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

Authentication : Open

WEP Encryption : 64Bit

Default WEP Key : WEP Key 1

WEP Key : HEX 1234567890
(5 ASCII or 10 HEX)

WPA-Personal

- WPA Mode:** Select whether to use **WPA2 only** or **WPA only**. **WPA2 only** is the most secure, provided that all of your clients can support it.
- Cipher Type:** Select whether to use the **TKIP** or **AES** cipher. The **AES** cipher is the most secure, provided that all of your clients can support it.
- Network Key:** Enter the key/password you want to use for your wireless network. The key must be between 8 and 63 characters long, and may only contain letters and numbers.

The screenshot displays the 'WIRELESS SECURITY MODE' configuration page. At the top, 'Security Mode' is set to 'WPA-Personal'. Below this, the 'WPA' section provides detailed instructions on choosing between WPA and WPA2 modes based on client compatibility and security requirements. It specifies that WPA2 Only uses AES (CCMP) and is the most secure, while WPA Only uses TKIP for better compatibility. Below the text, 'WPA Mode' is set to 'WPA only' and 'Cipher Type' is set to 'AES'. The 'PRE-SHARED KEY' section at the bottom instructs the user to enter an 8- to 63-character alphanumeric pass-phrase. A text box shows a generated key: '7L9aetLadJ9L6u0L05343ed887475446L747fUz', with a note indicating it can be 8-63 ASCII or 64 HEX characters.

WIRELESS SECURITY MODE

Security Mode : WPA-Personal

WPA

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

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

WPA Mode : WPA only

Cipher Type : AES

PRE-SHARED KEY

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

Network Key : 7L9aetLadJ9L6u0L05343ed887475446L747fUz
(8~63 ASCII or 64 HEX)

WPA-Enterprise

WPA Mode: Select whether to use **WPA2 only** or **WPA only**. **WPA2 only** is the most secure, provided that all of your clients can support this security method.

Cipher Type: Select whether to use the **TKIP** or **AES** cipher. The **AES** cipher is the most secure, provided that all of your clients can support it.

RADIUS Server IP Address: Enter the IP address of your RADIUS server.

RADIUS Server Port: Enter the port used for your RADIUS server.

RADIUS Server Shared Secret: Enter the shared secret/password for your RADIUS server.

WIRELESS SECURITY MODE	
Security Mode :	WPA-Enterprise
WPA	
Use WPA or WPA2 mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use WPA2 Only mode. This mode uses AES(COMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use WPA Only . This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.	
To achieve better wireless performance use WPA2 Only security mode (or in other words AES cipher).	
WPA Mode :	WPA only
Cipher Type :	AES
EAP (802.1X)	
When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.	
RADIUS Server IP Address :	0.0.0.0
RADIUS server Port :	1812
RADIUS server Shared Secret :	

Network Settings

This section will help you to change the internal network settings of your router and to configure the DHCP Server settings. After modifying any settings, click **Save Settings** to save your changes.

ROUTER 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, once you click **Save Settings**, you will need to enter the new IP address in your browser to get back into the configuration utility.

Subnet Mask: Enter the subnet mask. The default subnet mask is 255.255.255.0.

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

ROUTER SETTINGS

Use this section to configure the internal network settings of your router. The IP address that is configured here is the IP address that you use to access the Web-based management interface. If you change the IP address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address :

192.168.0.1

Default Subnet Mask :

255.255.255.0

Local Domain Name :

DHCP Server Settings

The DWR-755 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 are automatically assigned to the clients on the network. After modifying any settings, click **Save Settings** to save your changes.

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

DHCP IP Address Range: Enter the range of IPs for the DHCP server to use to assign IP addresses to devices on your network. These values will represent the last octet of the IP addresses in the pool.

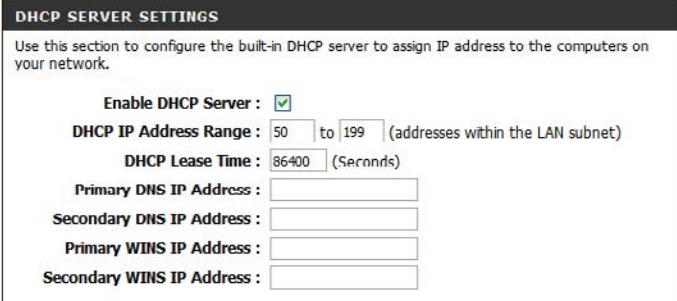
DHCP Lease Time: Enter the lease time for IP address assignments.

Primary DNS IP Address: Enter the primary DNS IP address that will be assigned to DHCP clients.

Secondary DNS IP Address: Enter the secondary DNS IP address that will be assigned to DHCP clients.

Primary WINS IP Address: Enter the primary WINS IP address that will be assigned to DHCP clients.

Secondary WINS IP Address: Enter the secondary WINS IP address that will be assigned 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 with a green box; 'DHCP IP Address Range' is set to '50' to '199' with a note '(addresses within the LAN subnet)'; 'DHCP Lease Time' is set to '86400' with a note '(Seconds)'; 'Primary DNS IP Address', 'Secondary DNS IP Address', 'Primary WINS IP Address', and 'Secondary WINS IP Address' are all empty input fields.

IPv6

There are several connection types to choose from: Static IPv6, LAN IPv6 Address, PPPoE, LAN IPv6 Link-Local, 6 to 4, 6rd, and Autoconfiguration. If you are unsure of your connection method, please contact your IPv6 Internet Service Provider (ISP).

Note: If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers has been removed or disabled.

SETUP	ADVANCED	TOOLS	STATUS
IPv6 Use this section to configure your IPv6 Connection Type. If you are unsure of your connection method, please contact your Internet Service Provider. Save Settings Don't Save Settings			
6 TO 4 SETTINGS Choose the mode to be used by the router to connect to the IPv6 Internet. IPv6 : ☐ Disable ☒ Enable IPv6 Connection : Static IPv6			
LAN IPv6 ADDRESS SETTINGS Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again. Enable DHCP-PD : ☒ LAN IPv6 Address : /64 LAN IPv6 Link-Local Address : /64			
LAN ADDRESS AUTOCONFIGURATION SETTINGS Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network. Enable Autoconfiguration : ☐ Autoconfiguration Type : SLAAC+Stateless DHCPv6 Router Advertisement Lifetime : seconds			

Static IPv6

- IPv6:** Tick to **Enable** IPv6 tunneling.
- IPv6 Connection:** Select **Static IPv6** from the drop-down menu.
- Remote IPv4 Address:** Enter the remote IPv4 address.
- Local IPv4 Address:** Enter the local IPv4 address.
- Default Gateway:** Enter the default gateway.
- DNS Addresses:** Enter the primary and secondary DNS addresses here.
- LAN IPv6 Address:** Enter the LAN IPv6 address.
- LAN IPv6 Link-Local Address:** Displays the LAN IPv6 link-local address.
- Enable Autoconfiguration:** Check to enable the autoconfiguration feature.
- Autoconfiguration Type:** Select **SLAAC + Stateless DHCPv6** or **Stateful (DHCPv6)**.
- Router Advertisement Lifetime:** Enter the IPv6 Address Lifetime (in seconds).
- DS-Lite Enable:** Tick to enable DS-Lite.
- DS-Lite Configuration:** Tick **Manual Configuration**.
- AFTR IPv6 Address:** Enter the AFTR IPv6 address supplied by your service provider.

6 TO 4 SETTINGS

Choose the mode to be used by the router to connect to the IPv6 Internet.

IPv6 : ☐ Disable ☒ Enable
IPv6 Connection :

ROUTER ADVERTISEMENT LIFETIME

Remote IPv4 Address :
Local IPv4 Address :
Default Gateway :
Primary DNS Address :
Secondary DNS Address :

LAN IPV6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Address : /64
LAN IPv6 Link-Local Address : /64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration : ☐
Autoconfiguration Type :
Router Advertisement Lifetime : seconds

DS-LITE

Enter the AFTR address information provided by your Internet Service Provider(ISP)..

DS-Lite Enable : ☐
DS-Lite Configuration : ☒ DS-Lite DHCPv6 Option ☐ Manual Configuration
AFTR IPv6 Address :

LAN IPv6 Address Settings

- IPv6:** Tick to **Enable** IPv6 tunneling.
- IPv6 Connection:** Select **LAN IPv6 Address Settings** from the drop-down menu.
- DNS Addresses:** Enter the primary and secondary DNS addresses here.
- Enable DHCP-PD:** Tick to enable DHCP-PD.
- LAN IPv6 Address:** Enter the LAN IPv6 address.
- LAN IPv6 Link-Local Address:** Displays the LAN IPv6 link-local address.
- Enable Autoconfiguration:** Check to enable the autoconfiguration feature.
- Autoconfiguration Type:** Select **SLAAC + Stateless DHCPv6** or **Stateful (DHCPv6)**.
- Router Advertisement Lifetime:** Enter the IPv6 address lifetime (in seconds).
- DS-Lite Enable:** Tick to enable DS-Lite.
- DS-Lite Configuration:** Tick **DS-Lite DHCPv6 Option** or **Manual Configuration**.
- AFTR IPv6 Address:** Enter the AFTR IPv6 address supplied by your service provider.

6 TO 4 SETTINGS

Choose the mode to be used by the router to connect to the IPv6 Internet.

IPv6 : ☐ Disable ☒ Enable

IPv6 Connection : LAN IPv6 Address Settings

IPv6 DNS SETTINGS

Use this section to configure your IPv6 Connection Type. If you are unsure of your connection method, please contact your Internet Service Provider. :

☒ When configuring the router to access the IPv6 internet be sure to choose the correct IPv6 Connection Type from the drop down menu. If you are unsure of which option to choose, contact your internet Service Provider (ISP.)

☐ Use the following DNS address

Primary DNS Address :

Secondary DNS Address :

LAN IPv6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.

Enable DHCP-PD : ☒

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : /64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration : ☐

Autoconfiguration Type : SLAAC+Stateless DHCPv6

Router Advertisement Lifetime : seconds

DS-LITE

Enter the AFTR address information provided by your Internet Service Provider (ISP)..

DS-Lite Enable : ☐

DS Lite Configuration : ☒ DS-Lite DHCPv6 Option ☐ Manual Configuration

AFTR IPv6 Address :

PPPoE

IPv6:	Tick to Enable IPv6 tunneling.
IPv6 Connection:	Select LAN IPv6 Address Settings from the drop-down menu.
LAN IPv6 Address:	Enter the LAN IPv6 address.
MTU:	You may need to change the Maximum Transmission Unit (MTU) for optimal performance.
DNS Addresses:	Enter the primary and secondary DNS addresses here.
Enable DHCP-PD:	Tick to enable DHCP-PD.
LAN IPv6 Address:	Enter the LAN IPv6 address.
LAN IPv6 Link-Local Address:	Displays the LAN IPv6 Link-local address.
Enable Autoconfiguration:	Check to enable the autoconfiguration feature.
Autoconfiguration Type:	Select SLAAC + Stateless DHCPv6 or Stateful (DHCPv6) .
Router Advertisement Lifetime:	Enter the IPv6 address lifetime (in seconds).

6 TO 4 SETTINGS

Choose the mode to be used by the router to connect to the IPv6 Internet.

IPv6 :

☐ Disable ☒ Enable

IPv6 Connection :

PPPoE

PPPOE SETTINGS

LAN IPv6 Address :

Password :

Local IPv6 Address :

MTU :

IPv6 DNS SETTINGS

Use this section to configure your IPv6 Connection Type. If you are unsure of your connection method, please contact your Internet Service Provider. :

☒ When configuring the router to access the IPv6 internet be sure to choose the correct IPv6 Connection Type from the drop down menu. If you are unsure of which option to choose, contact your internet Service Provider (ISP.)

☐ Use the following DNS address

Primary DNS Address :

Secondary DNS Address :

LAN IPV6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.

Enable DHCP-PD :

☒

LAN IPv6 Address :

/64

LAN IPv6 Link-Local Address :

/64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

☐

Autoconfiguration Type :

SLAAC+Stateless DHCPv6

Router Advertisement Lifetime :

seconds

LAN IPv6 Link-Local Address

- IPv6:** Tick to **Enable** IPv6 tunneling.
- IPv6 Connection:** Select **LAN IPv6 Link-Local Address** from the drop-down menu.
- Remote IPv4 Address:** Enter the remote IPv4 address.
- Local IPv4 Address:** Enter the local IPv4 address.
- Local IPv6 Address:** Enter the local IPv6 address.
- DNS Setting:** Choose to automatically obtain the DNS server address or to set manually.
- DNS Addresses:** Enter the primary and secondary DNS addresses here.
- LAN IPv6 Address:** Enter the LAN IPv6 address.
- LAN IPv6 Link-Local Address:** Displays the LAN IPv6 link-local address.
- Enable Autoconfiguration:** Check to enable the autoconfiguration feature.
- Autoconfiguration Type:** Select **SLAAC + Stateless DHCPv6** or **Stateful (DHCPv6)**.
- Router Advertisement Lifetime:** Enter the IPv6 address lifetime (in seconds).

6 TO 4 SETTINGS
 Choose the mode to be used by the router to connect to the IPv6 Internet.
 IPv6 : ☐ Disable ☒ Enable
 IPv6 Connection : LAN IPv6 Link-Local Address ▼

LAN ADDRESS AUTOCONFIGURATION SETTINGS
 Remote IPv4 Address :
 Local IPv4 Address :
 Local IPv6 Address : /64

IPv6 DNS SETTINGS
 DNS Setting : ☒ Obtain DNS Server address Automatically
 ☐ Use the following DNS address
 Primary DNS Address :
 Secondary DNS Address :

LAN IPv6 ADDRESS SETTINGS
 Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.
 LAN IPv6 Address : /64
 LAN IPv6 Link-Local Address : /64

LAN ADDRESS AUTOCONFIGURATION SETTINGS
 Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.
 Enable Autoconfiguration : ☐
 Autoconfiguration Type : SLAAC+Stateless DHCPv6 ▼
 Router Advertisement Lifetime : seconds

6 to 4

6 TO 4 SETTINGS

Choose the mode to be used by the router to connect to the IPv6 Internet.

IPv6 :

Disable

Enable

IPv6 Connection :

6 to 4

6 TO 4 SETTINGS

6 to 4 Address :

Primary DNS Address :

Secondary DNS Address :

LAN IPV6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Address :

/64

LAN IPv6 Link-Local Address :

/64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

☐

Autoconfiguration Type :

SLAAC | Stateless DHCPv6

Router Advertisement Lifetime :

seconds

IPv6: Tick **Enable** to activate IPv6 tunneling.

IPv6 Connection: Select **6 to 4** from the drop-down menu.

6 to 4 Address: Displays the IPv6 settings supplied by your Internet Service Provider (ISP).

Primary/Secondary DNS Address: Enter the primary and secondary DNS server addresses.

LAN IPv6 Address: Displays the LAN (local) IPv6 address for the router.

LAN Link-Local Address: Displays the router's LAN link-local address.

Enable Autoconfiguration: Check to enable the autoconfiguration feature.

Autoconfiguration Type: Select **Stateful (DHCPv6)** or **SLAAC+Stateless DHCPv6** autoconfiguration.

Router Advertisement Lifetime: Enter the IPv6 address lifetime (in seconds).

6rd

- IPv6:

Tick to **Enable** IPv6 tunneling.
- IPv6 Connection:

Select **6rd** from the drop-down menu.
- Remote IPv4 Address:

Enter the IPv4 (remote) address here.
- IPv4 Mask Length:

Enter the mask length of the IPv4 address.
- Remote Prefix:

Enter the remote prefix of the IPv4 address.
- Prefix Length:

Enter the length of the remote prefix.
- Primary/Secondary DNS Addresses:

Enter the DNS server addresses.
- LAN IPv6 Address:

Displays the LAN (local) IPv6 address for the router.
- LAN Link-Local Address:

Displays the router’s LAN link-local address.
- Enable Autoconfiguration:

Check to enable the autoconfiguration feature.
- Autoconfiguration Type:

Select **Stateful (DHCPv6)** or **SLAAC+Stateless DHCPv6** autoconfiguration.
- Router Advertisement Lifetime:

Enter the IPv6 address lifetime (in seconds).

6 TO 4 SETTINGS

Choose the mode to be used by the router to connect to the IPv6 Internet.

IPv6 :

☐ Disable ☒ Enable

IPv6 Connection :

6rd

6RD SETTINGS

Remote IPv4 Address :

IPv4 Mask Length :

Remote Prefix :

 ::

Prefix Length :

Primary DNS Address :

Secondary DNS Address :

LAN IPV6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your router. The LAN IPv6 Link Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Address :

/64

LAN IPv6 Link-Local Address :

/64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

☐

Autoconfiguration Type :

SLAAC+Stateless DHCPv6

Router Advertisement Lifetime :

 seconds

Autoconfiguration

- IPv6:** Tick to **Enable** IPv6 tunneling.
- IPv6 Connection:** Select **Autoconfiguration Type** from the drop-down menu.
- LAN Link-Local Address:** Displays the router’s LAN link-local address.

6 TO 4 SETTINGS

Choose the mode to be used by the router to connect to the IPv6 Internet.

IPv6 :

☐ Disable

☒ Enable

IPv6 Connection :

Autoconfiguration Type

LAN IPV6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Link Local Address :

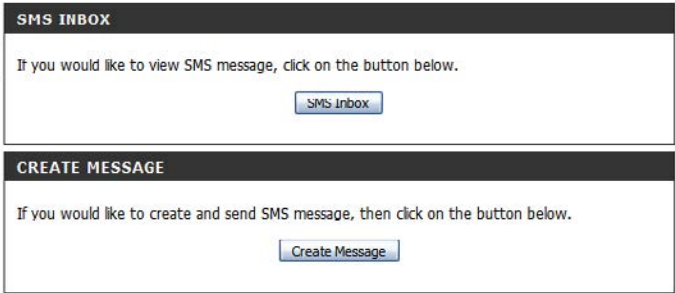
/64

Message Service

If your ISP provides SMS service, you can check and send messages from this page.

SMS Inbox: Click this button to view SMS messages that you have received.

Create Message: Click this button to create a new message to send.



SMS Inbox

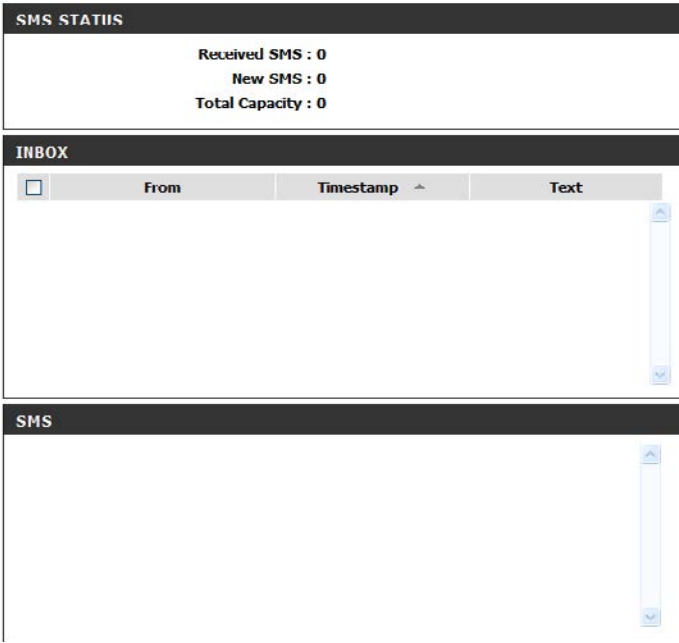
This page shows all messages that are stored on the SIM card. Select a message to display its contents in the SMS window. After you have read a message, you can delete it, or reply to the sender. Click the **Refresh** button to update the list.

Delete: Deletes the selected SMS message.

Reply: Opens a Create Message window to reply to the selected SMS message.

Forward: Opens a Create Message windows to forward the selected SMS message to another recipient.

Refresh: Click this button to check for new messages.



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 the message. Then click the **Send Message** button to send out the 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.

Send Message: Click this button to send the message.

Cancel: Click this button to clear the message.



The screenshot shows a web form titled "CREATE MESSAGE". On the left, there are labels: "Text message :", "The max. length of a message is 160 characters. :", and "Add '+' for international format of the phone number. :". To the right of "Text message :", there is a small input field with the placeholder "Enter Message...". Below this is a large text area for the message content. At the bottom right of the text area, it says "0 Current input text length :". At the very bottom of the form, there are two buttons: "Send message" and "Cancel".

USSD

You can use this page to send Unstructured Supplementary Service Data (USSD) codes used by your service provider to activate specific applications with an SMS message.

USSD: Enter an application activation code and click the **Send** button. This will allow you to activate applications by sending an SMS to your ISP.

USSD

USSD is a protocol used by GSM cellular telephones to communicate with the service provider's computers.

USSD

USSD :

Send

VPN Settings

VPN Setup Wizard

The DWR-755 allows you to set up VPN using the automated **VPN Setup Wizard** or using **Manual VPN Setup**. VPN settings are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin authentication, and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

This window explains the steps you will be guided through to set up an IPSec VPN tunnel.

Click **Next** to continue.

If there is a trusted subnet for remote gateway, select **Yes**, otherwise choose **No**.

Click **Next** to continue.

If you chose “yes” you will now need to enter the **Remote Subnet** and **Remote Netmask**.

Click **Next** to continue.

Enter the **Remote Gateway** address.

Click **Next** to continue.

WELCOME TO THE SETUP WIZARD

Gather following information for setting the configuration of an IPSec VPN tunnel:

- Step 1: Is there a trusted subnet (LAN) for remote gateway?
- Step 2: What is the IP address of remote gateway?
- Step 3: What is the pre-shared key?
- Step 4: What is the IKE Proposal?
- Step 5: What is the IPSec Proposal?

Prev Next Cancel

STEP 1: IS THERE A TRUSTED SUBNET (LAN) FOR REMOTE GATEWAY?

Is there a trusted subnet (LAN) for remote gateway?
If yes, what are the subnet address and netmask of LAN side of remote gateway?

☒ Yes
☐ No

Prev Next Cancel

STEP 2: SET THE IP ADDRESS OF REMOTE SUBNET AND NETMASK

Remote Subnet :

Remote Netmask :

Prev Next Cancel

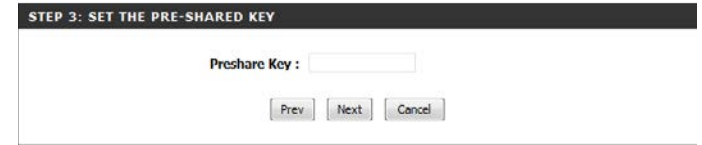
STEP 2: SET THE IP ADDRESS OF REMOTE GATEWAY

Remote Gateway :

Prev Next Cancel

Set your **Preshared Key**.

Click **Next** to continue.



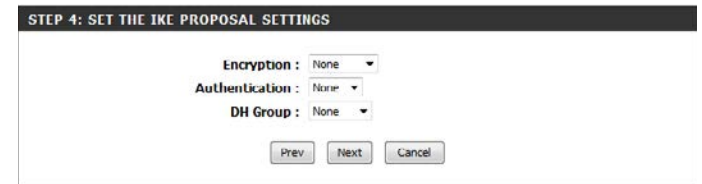
STEP 3: SET THE PRE-SHARED KEY

Preshare Key :

Prev Next Cancel

Set your IKE Proposal Settings by choosing your **Encryption**, **Authentication**, and **DH Group** settings from the drop-down menus.

Click **Next** to continue.

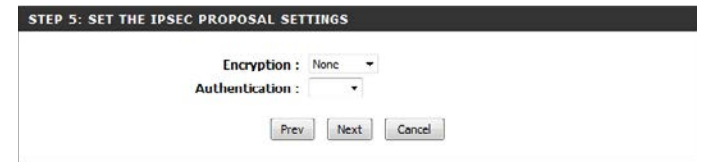


STEP 4: SET THE IKE PROPOSAL SETTINGS

Encryption : None ▾
Authentication : None ▾
DH Group : None ▾

Prev Next Cancel

Set the type of encryption and authentication of your IPsec proposal settings and click **Next**.



STEP 5: SET THE IPSEC PROPOSAL SETTINGS

Encryption : None ▾
Authentication : ▾

Prev Next Cancel

When setup is completed the name and security details will be displayed and the router will reboot.

Click **Save** to finish.



RESTART ROUTER

The device is rebooting...

Please **DO NOT POWER OFF** the device.

And please wait for 57 seconds...

Manual VPN Setup

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: Check this box to enable IPSec VPN function.

Netbios over IPSEC: Check this box to receive Netbios from Network Neighborhood.

NAT Traversal: Some NAT routers will block IPSec packets if it doesn't support IPSec passthrough. If you connect to another NAT router which doesn't support IPSec passthrough on the WAN side, you need to activate this option.

VPN Statistic: Check this box to enable VPN Statistic options.

Max Number of Tunnels: The device supports 1~10 tunnels.

VPN Dynamic IP Setting: Check this box to enable this features and click **More** to configure VPN Dynamic IP on a separate page. Please see the next page for more details.

Tunnel Settings: Tunnel details are displayed here. Click **More** to configure a new tunnel or click **Disconnect** to disconnect from an existing tunnel. Select the **Enable** checkbox to activate this rule. In tunnel settings page, you can click **More** under Action for detail tunnel setting.

XAUTH account: select it to store XAUTH account information such as user name and password.

PPTP client / PPTP Server: DWR-755 can act as either client or server under PPTP, click it to configure this setting.

L2TP client / L2TP Server: DWR-755 can act as either client or server under L2TP, click it to configure this setting.

VPN SETTINGS

VPN-IPSEC : ☒ Enabled

Netbios over IPSEC : ☐ Enabled

NAT Traversal : ☐ Enabled

VPN Statistic : ☐ Enabled

Max. number of tunnels : 40

DYNAMIC VPN SETTING

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

TUNNEL SETTINGS

ID	Tunnel Name	Remote Addr.	Gateway	Status	Action	Enable
1	Tunnel#1	255.255.255.0/0.0.0.255	224.52.45.2	Connecting...	More Disconnect	☒
2					More	☐
3					More	☐
4					More	☐
5					More	☐

[XAUTH account](#) [Refresh](#)

[PPTP Client](#) [PPTP Server](#) [L2TP Client](#) [L2TP Server](#)

VPN Dynamic IP

- Tunnel Name:** Enter a name for your VPN.
- Local Subnet/Netmask:** Enter the local (LAN) subnet and mask.
(ex. 192.168.0.0/24)
- Phase1/2 Key Life Time:** Enter the amount of time in seconds that the Phase 1 and Phase 2 keys should last.
- Encapsulation Protocol:** Choose either **ESP**, **AH** or **ESP + AH** from the drop-down menu.
- PFS Group:** **Enable** or **Disable** the PFS Group option using the drop-down menu. PFS is an additional security protocol.
- Preshare Key:** Manually enter an ASCII passphrase in box.
- Remote ID:** Choose from **Username**, **FQDN**, **User@FQDN**, or **Key ID** using the drop-down menu and then the ID in the box.
- Local ID:** Choose from **Username**, **FQDN**, **User@FQDN**, or **Key ID** using the drop-down menu and then the ID in the box.
- Dead Peer Detection (DPD):** Check this box to enable Dead Peer Detection, then enter the time in seconds in which a peer is determined to be no longer active. You may also enter a delay period in seconds.
- XAUTH:** Check this box to include additional username and password authentication requirements for the VPN. Select **Server Mode** or **None**. Then enter the user name and password if required by the remote VPN server endpoint configured in xAuth Server Mode.
- Set IKE Proposal:** Check this box to enable IKE Proposal.
- Set IPSEC Proposal:** Check this box to enable IPSec Proposal.

The screenshot shows the 'VPN DYNAMIC IP SETTING' configuration window. It contains the following fields and options:

- Tunnel Name :** Text input field.
- Local Subnet :** Text input field.
- Local Netmask :** Text input field.
- Phase1 Key Life Time :** Text input field followed by 'seconds'.
- Phase2 Key Life Time :** Text input field followed by 'seconds'.
- Encapsulation Protocol :** Drop-down menu with 'ESP' selected.
- PFS Group :** Drop-down menu with 'Disable' selected.
- Preshare Key :** Text input field.
- Remote ID :** Drop-down menu with 'Type: Username' selected, followed by an 'ID:' text input field.
- Local ID :** Drop-down menu with 'Type: Username' selected, followed by an 'ID:' text input field.
- Dead Peer Detection (DPD) :**
 - ☐ Enable
 - When enabled, it shows 'Timeout : 180 Second(s)' and 'Delay : 30 Second(s)'.
- XAUTH :**
 - ☒ None
 - ☐ Server
- Set IKE Proposal :** ☐ Enable
- Set IPSEC Proposal :** ☐ Enable

- IKE Proposal Settings:

Use this area to **Enable** IKE Proposals. Then determine the **Encryption** and **Authentication** types, as well as the **DH Group** from the drop-down menus.
- IPSEC Proposal Settings:

Use this area to **Enable** IPSec Proposals. Then determine the **Encryption** and **Authentication** types from the drop-down menus.

IKE PROPOSAL SETTINGS

ID	Encryption	Authentication	DH Group	Enable
1	DES	SHA1	Group1	☐
2	DES	SHA1	Group1	☐

IPSEC PROPOSAL SETTINGS

ID	Encryption	Authentication	Enable
1	DES	None	☐
2	DES	None	☐

Tunnel - IKE

Tick **Enabled**, choose **IKE** in the Method field, and configure your settings. When you are done, click **Save Settings** to apply changes.

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

Method: Choose either **IKE** from the drop-down menu.

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 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

VPN SETTINGS - TUNNEL 1

☒ Enabled

Tunnel Name : Tunnel#1

Method : IKE

Local Subnet : 192.168.0.0

Local Netmask : 255.255.255.0

Remote Subnet : 255.255.255.0

Remote Netmask : 0.0.0.255

Remote Gateway :

Phase1 Key Life Time : 28800 seconds

Phase2 Key Life Time : 28800 seconds

Encapsulation Protocol : ESP

PFS Group : Disable

Aggressive Mode : ☒ Enable

Preshare Key : adfaf

Connecting Type : Always on

Remote ID : Type: Username
ID:

Local ID : Type: Username
ID:

Dead Peer Detection (DPD) : ☒ Enable
 ▶ Timeout : 180 Second(s)
 ▶ Delay : 30 Second(s)

XAUTH : ☒ None
☐ Server
☐ Client
 ▶ Username :
 ▶ Password :

Set IKE Proposal : ☒ Enable

Set IPSEC Proposal : ☒ Enable

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.

Connecting Type: Choose **Always on** or **Manual** from the drop-down menu.

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. 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.

Dead Peer Detection (DPD): Check this box to enable Dead Peer Detection, then enter the time in seconds in which a peer is determined to be no longer active. You may also enter a delay period in seconds.

XAUTH: Check this box to include additional username and password authentication requirements for the VPN. Select **Server Mode** or **None**. Then enter the user name and password if required by the remote VPN server endpoint configured in xAuth Server Mode.

Set IKE Proposal: Check this box to enable IKE Proposal.

Set IPSEC Proposal: Check this box to enable IPSec Proposal.

VPN SETTINGS - TUNNEL 1

- ☒ Enabled
- Tunnel Name : Tunnel#1
- Method : IKE
- Local Subnet : 192.168.0.0
- Local Netmask : 255.255.255.0
- Remote Subnet : 255.255.255.0
- Remote Netmask : 0.0.0.255
- Remote Gateway :
- Phase1 Key Life Time : 28800 seconds
- Phase2 Key Life Time : 28800 seconds
- Encapsulation Protocol : ESP
- PFS Group : Disable
- Aggressive Mode : ☐ Enable
- Preshare Key : adfaf
- Connecting Type : Always on
- Remote ID : Type: Username ID:
- Local ID : Type: Username ID:
- Dead Peer Detection (DPD) : ☐ Enable
 - Timeout : 180 Second(s)
 - Delay : 30 Second(s)
- XAUTH : ☒ None ☐ Server ☐ Client
 - Username :
 - Password :
- Set IKE Proposal : ☒ Enable
- Set IPSEC Proposal : ☒ Enable

Encryption: Five algorithms can be selected: **DES**, **3DES**, **AES-128**, **AES-192**, and **AES-256**.

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

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

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

Encryption: Five algorithms can be selected: **DES**, **3DES**, **AES-128**, **AES-192**, and **AES-256**. However, when the encapsulation protocol is set to AH, the encryption algorithm is unnecessary.

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

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

IKE PROPOSAL SETTINGS				
ID	Encryption	Authentication	DH Group	Enable
1	DES	SHA1	Group1	☐
2	DES	SHA1	Group1	☐

IPSEC PROPOSAL SETTINGS			
ID	Encryption	Authentication	Enable
1	DES	None	☐
2	DES	None	☐

Tunnel - Manual

Tick **Enabled**, choose **MANUAL** in the Method field, and configure your settings. When you are done, click **Save Settings** to apply changes.

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

Method: Choose **Manual** from the drop-down menu.

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.

Encapsulation Protocol: Select **ESP** or **AH**.

Outbound SPI: SPI is an important parameter during hashing. Outbound SPI will be included in the outbound packet transmitted from local gateway. The value of outbound SPI should be set in hex formatted.

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

VPN SETTINGS - TUNNEL 1

☒ Enabled

Tunnel Name : Tunnel#1

Method : MANUAL

Local Subnet :

Local Netmask :

Remote Subnet :

Remote Netmask :

Remote Gateway :

Encapsulation Protocol : ESP

Outbound SPI : 0x

Inbound SPI : 0x

Encryption Algorithm : 3DES

Encryption Key :

Authentication Algorithm : SHA1

Authentication Key :

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**.

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

☒ Enabled

Tunnel Name : Tunnel#1

Method : MANUAL ▼

Local Subnet :

Local Netmask :

Remote Subnet :

Remote Netmask :

Remote Gateway :

Encapsulation Protocol : ESP ▼

Outbound SPI : 0x

Inbound SPI : 0x

Encryption Algorithm : 3DES ▼

Encryption Key :

Authentication Algorithm : SHA1 ▼

Authentication Key :

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

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: This identifies the rule.

Service Ports: Enter the public port(s) you want to open.

Server IP: Port: Enter the IP address and port of the computer on your local network that you want to forward the Service Ports to.

Enable: Check the box to enable the specified rule.

Schedule Rule #: Specify the schedule rule number. To create schedules, click on the **Add New Rule** button. For further information on schedules, please refer to "Schedules" on page 75.

ID	Service Ports	Server IP : Port	Enable	Schedule Rule#
1			☐	Add New Rule...
2			☐	Add New Rule...
3			☐	Add New Rule...
4			☐	Add New Rule...
5			☐	Add New Rule...
6			☐	Add New Rule...
7			☐	Add New Rule...
8			☐	Add New Rule...
9			☐	Add New Rule...
10			☐	Add New Rule...
11			☐	Add New Rule...
12			☐	Add New Rule...
13			☐	Add New Rule...
14			☐	Add New Rule...
15			☐	Add New Rule...
16			☐	Add New Rule...
17			☐	Add New Rule...
18			☐	Add New Rule...
19			☐	Add New Rule...
20			☐	Add New Rule...

Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, and Internet telephony. These applications may have difficulty working through NAT (Network Address Translation). Application Rules allow some of these applications to work with the DWR-755 by opening ports after detecting traffic being sent through a trigger port. After modifying any settings, click **Save Settings** to save your changes.

- Popular Applications:

Select from a list of popular applications. You can select a service, select a rule ID, then click the **Copy to** button to copy the default settings for that service to the specified rule ID.
- ID:

Specifies which rule to copy the selected **Popular application** settings to when you click the **Copy to** button.

APPLICATION RULES

- ID:

This identifies the rule.
- Trigger:

Enter the port to listen to in order to trigger the rule.
- Incoming Ports:

Specify the incoming port(s) to open when traffic comes over the Trigger port.
- Enable:

Check the box to enable the specified rule.

SETUP

ADVANCED

TOOLS

STATUS

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			☐

QoS Engine

The QoS engine improves your online gaming or streaming media experience by ensuring that your game or media 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. After modifying any settings, click **Save Settings** to save your changes.

QOS ENGINE SETUP

Enable QoS Packet Filter:

Select this box to enable the QoS feature.

Upstream Bandwidth:

Specify the maximum upstream bandwidth here (e.g. 400 Kbps).

Use Schedule Rule:

Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to "Schedules" on page 75.

QOS RULES

ID:

This identifies the rule.

Local IP : Ports:

Specify the local IP address(es) and port(s) for the rule to affect.

Remote IP : Ports:

Specify the remote IP address(es) and port(s) for the rule to affect.

QoS Priority:

Select what priority level to use for traffic affected by the rule: **Low, Normal, or High**.

Enable:

Check the box to enable the specified rule.

Use Rule #:

Specify the schedule rule number. To create a new schedule, click on the **Add New Rule** button. For more information about schedules, please refer to "Schedules" on page 75.

The screenshot shows the 'ADVANCED' tab of the configuration interface. The 'QOS ENGINE' section is highlighted in orange and contains a description of the engine's purpose and two buttons: 'Save Settings' and 'Don't Save Settings'. Below this is the 'QOS ENGINE SETUP' section, which includes a checkbox for 'Enable QoS Packet Filter', a text input for 'Upstream bandwidth' (set to kbps), and a 'Use schedule rule' dropdown menu currently set to '---ALWAYS ON---'. A 'Copy to' button and an 'ID' dropdown are also present. The 'QOS RULES' section at the bottom features a table with 8 rows. Each row has columns for ID, Local IP : Ports, Remote IP : Ports, QoS Priority (a dropdown menu), Enable (a checkbox), and Use Rule# (a button labeled 'Add New Rule...').

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1			High	☐	Add New Rule...
2			High	☐	Add New Rule...
3			High	☐	Add New Rule...
4			High	☐	Add New Rule...
5			High	☐	Add New Rule...
6			High	☐	Add New Rule...
7			High	☐	Add New Rule...
8			High	☐	Add New Rule...

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. After modifying any settings, click **Save Settings** to save your changes.

MAC FILTERING SETTINGS

- MAC Address Control:

Tick this box to enable MAC filtering.
- Connection Control:

Check the box to allow wireless and wired clients with **C** selected to connect to this device. You can also select to **allow** or **deny** connections from unspecified MAC addresses.
- Association Control:

Check the box to allow wireless clients with **A** selected can associate to the wireless LAN. You can also select to **allow** or **deny** connections from unspecified MAC addresses.

MAC FILTERING RULES

- ID:

This 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.
- C:

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

If this box is ticked, the rule will follow the association control setting specified in MAC filtering settings specified above.

SETUP

ADVANCED

TOOLS

STATUS

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 allow unspecified MAC addresses to associate.

DHCP clients

-- select one --

Copy to

ID

-- --

MAC FILTERING RULES

ID	MAC Address	C	A
1		☐	☐
2		☐	☐
3		☐	☐
4		☐	☐
5		☐	☐

Previous page

Next page

URL Filter

The URL filter allows you to set up a list of websites that will be blocked from users on your network. After modifying any settings, click **Save Settings** to save your changes.

URL Filtering: Check the box to enable URL filtering.

URL FILTERING RULES

ID: This identifies the rule.

URL: Enter URL that you would like to block. All URLs that begin with this URL will be blocked.

Enable: Check the box to enable the specified rule.

SETUP

ADVANCED

TOOLS

STATUS

URL FILTER

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

Save Settings

Don't Save Settings

URL FILTERING SETTING

URL Filtering : ☐ Enable

URL FILTERING RULES

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

Outbound Filter

The outbound filter enables you to control what packets are allowed to be sent out to the Internet. The outbound filter applies to all outbound packets. After modifying any settings, click **Save Settings** to save your changes.

OUTBOUND FILTER SETTING

- Outbound Filter:** Select this box to **Enable** outbound filtering.
- Use Schedule Rule:** Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to “Schedules” on page 75.

OUTBOUND FILTER RULES LIST

Here, you can select whether to **Allow** or **Deny** all outgoing traffic except for traffic that matches the listed rules.

- ID:** This identifies the rule.
- 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:** Check the box to enable the specified rule.
- Schedule Rule #:** Specify the schedule rule number. Click on the **Add New Rule** button to create a new schedule rule.
- Previous Page:** Go back to the previous filter page.
- Next Page:** Advance to the next filter page.

SETUP

ADVANCED

TOOLS

STATUS

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	:	:	☐	Add New Rule...
2	:	:	☐	Add New Rule...
3	:	:	☐	Add New Rule...
4	:	:	☐	Add New Rule...
5	:	:	☐	Add New Rule...
6	:	:	☐	Add New Rule...
7	:	:	☐	Add New Rule...
8	:	:	☐	Add New Rule...

Previous page

Next page

Inbound Filter

The inbound filter enables you to control what packets are allowed to come in to your network from the Internet. The inbound filter only applies to packets that are destined for Virtual Servers or DMZ hosts. After modifying any settings, click **Save Settings** to save your changes.

INBOUND FILTER SETTING

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

Use Schedule Rule: Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to “Schedules” on page 75.

INBOUND FILTER RULES LIST

Here, you can select whether to **Allow** or **Deny** all incoming traffic except for traffic that matches the listed rules.

ID: This identifies the rule.

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: Check the box to enable the specified rule.

Schedule Rule #: Specify the schedule rule number. Click on the **Add New Rule** button to create a new schedule rule.

Previous Page: Go back to the previous filter page.

Next Page: Advance to the next filter page.

SETUP

ADVANCED

TOOLS

STATUS

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.

Save Settings

Don't Save Settings

INBOUND FILTER SETTING

Inbound Filter : ☐ Enable

Use schedule rule ---ALWAYS ON---

Copy to

 ID -- --

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			☐	Add New Rule...
2			☐	Add New Rule...
3			☐	Add New Rule...
4			☐	Add New Rule...
5			☐	Add New Rule...
6			☐	Add New Rule...
7			☐	Add New Rule...
8			☐	Add New Rule...

Previous page

Next page

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 DWR-755. The DWR-755 supports SNMP v1 and v2c. After modifying any settings, click **Save Settings** to save your changes.

SNMP

SNMP Local: Select whether to **Enable** or **Disable** local SNMP administration.

SNMP Remote: Select whether to **Enable** or **Disable** remote 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 enable read/write access to the network using SNMP.

IP 1/2/3/4: Enter up to 4 IP addresses to use as trap targets for your network.

SNMP Version: Select the SNMP version of your system.

WAN Access IP Address: If you want to limit remote access SNMP access, enter the IP address of the remote computer you will use to access this device; all other IP addresses will be denied remote SNMP access.

