



VDSL/ADSL2+/Fibre Ready Wireless AC1200 4-Port Modem Router

DSL-G2562DG



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
1.25	October 28, 2020	Final 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.

AppleR, Apple logoR, SafariR, iPhoneR, iPadR, iPod touchR and MacintoshR 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 ExplorerR, WindowsR and the Windows logo are trademarks of the Microsoft group of companies.

Copyright c 2018 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.

D-Link Building Networks for People

Preface	. 2
Product Overview	. 7
Package Contents	. 7
System Requirements	. 8
Introduction	. 9
Features	10
Hardware Overview	11
Back Panel	11
Top Panel	12
LEDs	13
	13
Installation	15
Before you begin	
	15
Before you begin	15 16
Before you begin Wireless Installation Considerations	15 16 17
Before you begin Wireless Installation Considerations Manual Setup	15 16 17 17
Before you begin Wireless Installation Considerations Manual Setup Hardware Installation	15 16 17 17 18
Before you begin Wireless Installation Considerations Manual Setup Hardware Installation Getting Started	15 16 17 17 18 18
Before you begin Wireless Installation Considerations Manual Setup Hardware Installation Getting Started Quick Setup	15 16 17 17 18 18 23
Before you begin	15 16 17 17 18 18 23 23
Before you begin Wireless Installation Considerations Manual Setup Hardware Installation Getting Started Quick Setup Configuration Log in	15 16 17 17 18 18 23 23 24

Network	25
Ethernet	27
Dongle	27
xDSL	28
LAN	29
Network	29
Ethernet	29
WLAN	30
DHCP Client	30
Statistics	31
WAN	
LAN	31
WLAN	
xTM	
xDSL	33
ARP	
Route	35
VoIP	35
Voice Status	35
Basic Setup	
WAN Interface	
ATM	
PTM	



Ethernet	37
Dongle	37
WAN Service	38
LAN	56
IPv4 Configuration	56
Reserved IP Address Settings	57
IPv6 Configuration	58
Wireless	59
Wireless Basic Configuration 2.4GHz	59
Wireless Basic Configuration 5GHz	60
Wireless Security Setting	61
Advanced Setup	62
WAN	62
xDSL Configuration	62
WAN - Ethernet Mode Configuration	62
LAN	63
LAN - Ethernet Mode Configuration	63
Wireless	64
Wireless Advanced Configuration 2.4GHz	64
Wireless Advanced Configuration 5GHz	66
Wireless MAC Filter	68
WPS Settings 2.4GHz	69
WPS Settings 5GHz	70

WDS Settings	71
Channel Information	72
NAT	73
Virtual Server	73
Virtual Server Settings	73
Port Triggering	75
Port Triggering Setting	75
Multi-NAT	76
Multi-NAT Edit	76
DMZ Settings	77
ALG Settings	77
Security	
IP Filtering	
Port Filter Rule Settings	79
MAC Filter	79
DDoS Protection	
Parental Control	
Access Time Restriction	
Access Time Restriction Configuration	
URL & IP Filter	
Access Time Restriction Configuration	
Routing	85
Static Route	85



Static Route Setting	85
Dynamic Route Setting	87
IPv6 Static Route	
IPv6 Static Route Setting	
IPv6 Dynamic Route	
Quality of Service	89
QoS Queue	
Classification List	
Classification Traffic Base	
Classification Traffic Base Settings	
QoS TCP Flags	
Bandwidth Limit	
Port Bandwidth Limit Configuration	
IP Bandwidth Limit Configuration	
IP Tunnel	
IPv4 In IPv6	
6 in 4 Tunnel Configuration	
Generic Routing Encapsulation	
GRE Setting	
Applications	
Storage Service	
Storage Device Info	
Storage Service - File Sharing Service Setup	

Storage Service - FTP Service Setup	
Storage Service - FTP Client Settings	100
Storage Service - TFTP Service Setup	100
Printer Service Setup	101
Multimedia Share Setup	101
Multimedia Share Setup	101
DNS	102
DDNS Settings	102
UPnP	103
Multicast	104
IGMP Settings	104
MLD Settings	105
SNMP Settings	106
VOIP	107
Basic Setup	107
Advance VoIP Setup	109
Media Settings	110
Fax Settings	110
Voice Service	111
Line Settings	112
Digital Map	112
Basic Call Control	113
CID	113



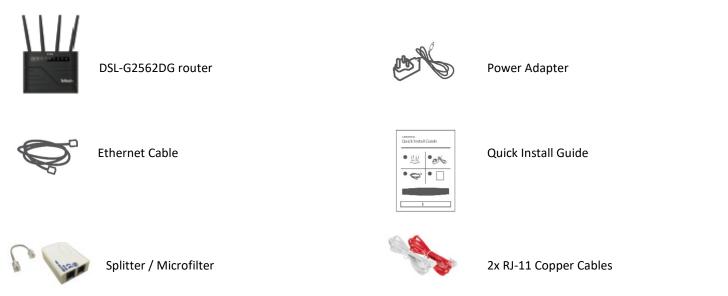
CDR
VPN
IPsec 115
L2TP
L2TP LAC Tunnel Setting119
L2TP LNS Tunnel Settings 120
VPN Lite
Management
Reboot
Settings122
Backup
DHCP Option 66 Files 123
Update Settings
Restore Default Settings 123
Update Software
Account Management - Passwords124

Logs 1	24
Log Level1	24
Logs1	25
Service Control1	26
Access Control IP Address Configuration1	26
Internet Time1	27
xDSL Diag1	29
Tools1	30
Ping1	30
Trace1	30
Connect a Wireless Client to your Router1	31
Troubleshooting1	38
Wireless Basics	41



Product Overview

Package Contents



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

Note: Using a power supply other than the one included with the DSL-G2562DG may cause damage and void the warranty for this product.



System Requirements

Network Requirements

- An active account with an Internet Service Provider using one of the following connection types:
- A Mobile connection using a SIM card
- A broadband device connected using the WAN port

Web-based Configuration Utility Requirements Computer with the following:

- Windows[®], Macintosh, or Linux-based operating system
- An installed Ethernet adapter

Browser Requirements:

- Internet Explorer 10 or higher
- Microsoft EDGE Browser 20 or higher
- Firefox 11 or higher
- Safari 5 or higher
- Chrome 17 or higher

Windows[®] Users: Make sure you have the latest version of Java installed. Visit version of Java installed. Visit <u>www.java.com</u> to download the latest version.



Introduction

The D-Link DSL-G2562DG VDSL/ADSL2+/Fibre Ready Wireless AC1200 4-Port Modem Router with VOIP share your internet connection over blazing-fast Wireless AC. Equipped with advanced AC beamforming technology to maximize the speed and range of your wireless signal to significantly outperform 802.11n and other older, non-beamforming capable 802.11ac devices. It also has a Gigabit WAN port, two USB ports, and four Gigabit ports to provide speeds up to 10 times faster than standard 10/100 ports. Enjoy uninterrupted Internet service thanks to 3G/4G failover protection, the WAN port to connect to Ethernet based networks while the USB slots allows for mobile broadband connection. With the addition of Advanced Quality of Service (QoS), data streams are separated, which helps organize and prioritize your network traffic so your video streaming, gaming, and VoIP calls run smoother over both your wired and wireless network.

The DSL-G2562DG DSL-G2562DG VDSL/ADSL2+/Fibre Ready Wireless AC1200 4-Port Modem Router with VOIP provides incredible speeds, smart antenna technology, fast ports. It also features a clean design and easy installation options.



Features

Faster Wireless Networking -The DSL-G2562DG is dual-band capable and equipped with four antennas to provide wireless speeds of up to 1200 Mbps* for your wireless devices. It operates on both the 2.4 GHz and 5GHz bands to allow separation of traffic so users can participate in high-bandwidth activities, such as video streaming, online gaming, and real-time audio, without affecting low-priority traffic like email and web surfing.

• Compatible with 802.11n/g/b/a devices - The DSL-G2562DG is still fully compatible with the 802.11n, 802.11g, and 802.11a standards, so it can connect with existing 802.11n, 802.11g, 802.11b, and 802.11a wireless devices.

• Advanced Firewall Features - The web-based user interface allows you to configure a number of advanced network management features including:

- Content Filtering Easily apply content filtering based on MAC address, URL, and/or domain name.
- Scheduling The wireless features can be scheduled to be active on a schedule you define.
- Multiple/Concurrent VPN Sessions The DSL-G2562DG can pass through VPN sessions. It supports multiple and concurrent IPsec and PPTP sessions, so users behind the DSL-G2562DG can access encrypted corporate networks.

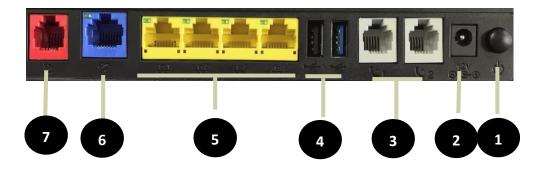
• User-friendly Setup Wizard - Through its easy-to-use web-based user interface, the DSL-G2562DG lets you control what information is accessible to those on the wireless network, whether from the Internet, or from your company's server. Configure your router to your specific settings within minutes.

* Maximum wireless signal rate derived from IEEE Standard 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac 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

Back Panel

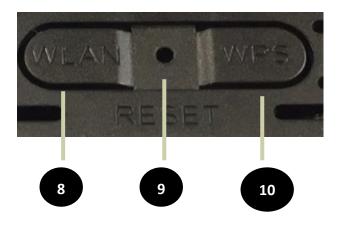


1.	Power Button	Press to switch router ON/OFF	
2.	Power Connector	Connector for the supplied power adapter.	
3.	FXS POTS ports	Connect your Analogue phone.	
4.	USB ports	Connect your 3G/4G Compatible dongle or External USB device	
5.	Ethernet Ports	Connects to Ethernet devices such as computers.	
6.	WAN Port	Connects to Ethernet WAN devices such as Fibre ONT.	
7.	DSL Port	Connect to DSL Line	



Hardware Overview

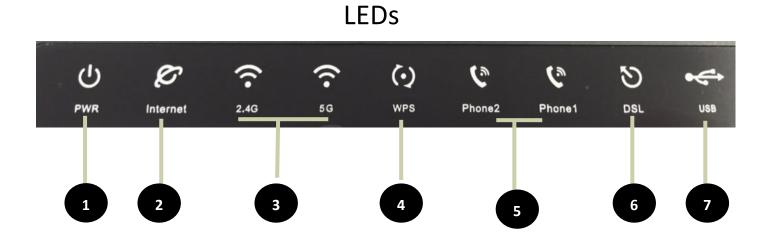
Top Panel



8.	WLAN	Press the button to switch the Wi-Fi ON/OFF
9.	Reset Button	Press and Hold the Reset button for 25 seconds to reset the DSL-G2562DG
10.	WPS Button	Press to start the WPS process and automatically create an encrypted connection to a WPS client.



Hardware Overview



1.	Power	Solid Blue	Device is powered on.
2.	2. Internet Solid Blue		There is internet is connected.
		Blinking Blue	The internet is properly connected and data is being transmitted.
		Red	Internet is not working or incorrect PPPoE details configured.
		OFF	No connection or Cable not connected properly.
		OFF	Nothing is connected to the Ethernet port.
3.		Blinking Blue	Enabled and data is being transmitted.



	Wi-Fi	Solid Blue	Enabled and no data is being transmitted.
	2.4Ghz/5Ghz	OFF	Wi-Fi is turned OFF
4.	WPS	Blinking Blue	WPS pairing mode active.
		Solid Blue	WPS enabled, paired with WPS client
		OFF	WPS disabled.
5.	Phone 1/Phone 2	Solid Blue	SIP account configured
		Blinking Blue	Phone active
		OFF	SIP account not configured or incorrectly configured
6.	DSL	Solid Blue	DSL line connected properly and sync to DSL network
		Blinking Blue	DSL training trying to sync to DSL line
		OFF	DSL line not connected or no connection on DSL line
7	USB	Solid Blue	USB storage device connected
		OFF	No USB device connected or USB not detected.



Installation

This section will walk 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, attic, or garage.

Note: This installation section is written for users who are setting up their home Internet service with the DSL-G2562DG FIBRE / LTE WI-FI AC1200 DUAL BAND ROUTER with VOIP for the first time. If you are replacing an existing modem and/or router, you may need to modify these steps.

Before you begin

- Make sure to have your DSL/Fibre service information provided by your Internet Service Provider handy. This information is likely to include your PPP (PPPoE) account's Username and Password. Your ISP may also supply you with additional WAN configuration settings which are necessary to establish a connection. This information may include the connection type (DHCP IP, Static IP, PPPoE, PPPoA, ATM or PTM) and/or ATM PVC details.
- If you are connecting a considerable amount of networking equipment, it may be a good idea to take the time to label each cable or take a picture of your existing setup before making any changes.
- We suggest setting up your DSL-G2562DG from a single device and verifying that it is connected to the Internet before connecting additional devices.



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 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:

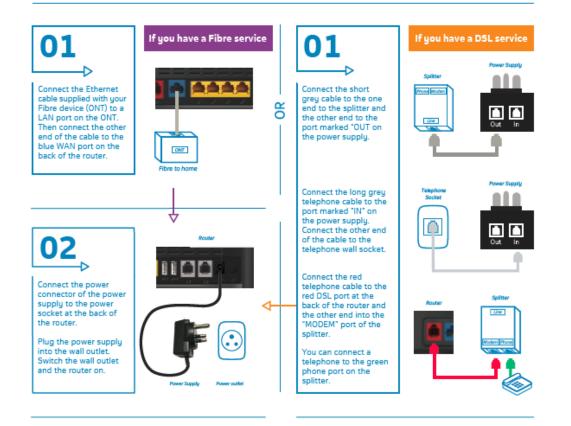
- 1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
- 2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
- 3. Building materials make a difference. A solid metal door or aluminium 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.



Manual Setup

Hardware Installation

Start Here





Getting Started

To set up the Internet connection without using the Quick Setup Wizard on the router, refer to Basic Setup on page 36

To connect to the web interface of the router and get started setting it up, refer to **Configuration on page**.

Quick Setup

Step 1

The Quick Setup menu is used to set up the Internet connection on the DSL-G2562DG. This is the first step in the Quick Setup tool and allows you to choose the connection type.

Step 1: Select Interface

Type: Please select which WAN interface to use: ADSL/VDSL or ETH. Your ISP should inform you of what method you use to connect to the Internet.

Click Next to continue.

Quick Setup

step1 -> step2 -> step3 -> step4 -> step5 -> step6 -> step7 -> step8 -> step9

Please select which WAN interface to use:ADSL,VDSL or Ethernet WAN,

then click the 'test' button to detect if the hardware interface is correctly connected.

Select Interface Type: ADSL/VDSL -





Step 2 Auto detecting

If you are on an DSL line you will need to use PPPoE, if you are on Fibre you will use either

PPPoE or DHCP connection.

Quick Setup

Auto detecting. This may take a while, please wait patiently ...



step2 -> step3 -> step4 -> step5 -> step6 -> step7 -> step8 step1 ->

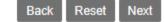
If PPPoE or DHCP is successful, please click the next button to continue to next step.

If both DHCP and PPPoE test fails,

For DSL and Fibre: please verify that your ADSL/fibre is active and the cable from the Telkom wall socket or ONT device is plugged into the blue port (Fibre) at the back of the DSL-G2562DG

Auto detect success, PPP account test passed! Suggest you choose PPPoE, Please click 'Next'.







step1 -> step2 -> step3 -> step4 -> step5 -> step6 -> step7 -> step8

Auto detect complete. Both DHCP and PPP account test fail! Please click the Reset button to reset to factory defaults, and then restart this wizard after the reset.

Select Mode: PPPoE V





Step 3

IF PPPoE Passed then user will need to enter the Username and Password as provided by the Internet Service Provider (ISP). IF DHCP passed device will automatically skip to step 5.

Username: Enter your Username here. (usually looks like an email

address like Yourname@telkomsa.net)

Password: Enter your Password here.

<u>Confirm Password:</u> Enter the same password again here.

step1 -> step2 -> step3 -> step4 -> step5 -> step6 -> step7 -> step8

Please enter your Username and Password as provided by your ISP (Internet Service

Provider). Click 'Next' to continue.

User Name:	
Password:	
Confirm Password:	

DOCK NEAL	Back	Next
-----------	------	------

Note: Using admin for the username & password will not work on this step as this is the account details for your Fibre line, which is unique to each client's account.

Step 4.

If connection is on PPPoE device will now test if the configured account is valid. If the test fails, please click on the back button and double check that the details on step 3 are correct. If the details have been entered correctly and step 4 still fails, please contact your Internet Service Provider and request for them to send your new PPPoE details. step1 -> step2 -> step3 -> step4 -> step5 -> step6 -> step7 -> step8
This may take a while,please wait patiently...
Back



Step 5

On Step 5 the user will be able to modify the Wi-Fi SSID and Preshare Key to their requirements.

<u>SSID 2.4GHz</u>: The name of the Wi-Fi network operating on 2.4GHz.
<u>Preshare key</u>: The password for the Wi-Fi network operating on 2.4GHz.
<u>SSID 5GHz</u>: The name of the Wi-Fi network operating on 5GHz.
<u>5G WPA Preshare key</u>: The password for the Wi-Fi network operating on 5GHz.
Click **Back** to go back to the pervious page, click **Skip** to skip this configuration or click **Next** to continue to **Step 6**.

step1 -> step2 ->	step3 -> step4 -> st	ep5 ·	-> step6	->	step7	->	step8
SSID 2.4GHz:	dlink-956M-2.4G-9d42						
2.4G WPA Preshare key:	•••••						
SSID 5GHz:	dlink-956M-5.8G-9d42						
5G WPA Preshare key:	•••••						

Step 6

In this step you can enter the change the web UI credentials. (The details used to log into the settings page of your router on 10.0.0.2)

AdminName: The username to log in to the web UI.

AdminPassword: Enter the password here for logging into the web UI.

AdminPassword: Enter the password for logging in to the web UI again to confirm.

Note: Password cannot contain a space.

Click **Back** to go back to the pervious page, click **Skip** to skip this configuration (not recommended for security purposes) or click **Next** to continue to **Step 8.**

step1 -> step2 -> step3 -> step4 -> step5 -> step6 -> step7 -> step8

Use the fields below to enter up to 15 characters and click "Apply" to change or create passwords.

Note: Password cannot contain a space.

AdminName:	admin
AdminPassword:	
Confirm AdminPassword:	



Next



Step 7

In this step you can enter the Site Username, Site Password, Confirm Site Password and Site LAN IP/Netmask to connect to Telkom VPN lite

Site Username: The site username.

Site Password: Enter the site password here.

<u>Confirm Site Password:</u> Enter the site password again to confirm. <u>Site LAN IP/ Netmask:</u> Enter the LAN IP or Netmask for the site here. **Note:** Password cannot contain a space.

Click Back to go back to the pervious page or click Next to continue to Step 9.

step1 -> step2 -> step3 -> step4 -> step5 -> step6 -> step7 -> step8

If you are a Telkom VPN Lite Customer, you can configure it here. Your PC's IP address needs to renew after the wizard is done - please disconnect your PC and then reconnect it.

If you're not a Telkom VPN Lite customer you can click "Skip" to continue.

Site Username:]
Site Password:]
Confirm Site Password:]
Site LAN IP/Netmask:	1	(Format: A.A.A.A/B(A:0-255,B:1-32))

Setup complete. Click "Back" to review or modify settings. Click "Apply" to apply the current settings.

Next

Skip

Back

If your Internet connection does not work after you pressed apply, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

Site Username:	
Site Password:	
Site LAN IP/Netmask:	/
Web Login Name:	admin
Web Login Password:	admin1
SSID 2.4GHz:	dlink-956M-2.4G-9d42
2.4G WPA Preshare key:	neifq89695
SSID 5GHz:	dlink-956M-5.8G-9d42
5G WPA Preshare key:	neifq89695

Step 8

In this step you can you can review everything for accuracy. Click **Back** to go back to the pervious page or click Apply to apply all of the configuration settings.

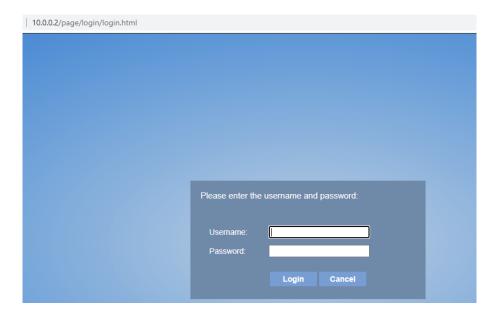
Back Apply



Configuration

Log in

To access the web interface, open a web browser and enter the IP address of the router (by default this is **10.0.0.2**) into the address bar. When the login page of the DSL-G2562DG is displayed, enter the username and password you set on step 6 of the setup wizard. By default, the login details are **admin** for the username and **admin** for the password if you chose to not change the details on the wizard. Click **Log in** to proceed or **Cancel** to clear your input.



Note: If you cannot remember your password or cannot log in, follow the factory reset procedure to restore the router to its default settings. The web interface is used to set up and change settings on the DSL-G2562DG. Follow the steps below to access the web interface and start setting up the DSL-G2562DG.



Status

Device Information

The Status menu is used to display statistics from different functions from the router. This displays basic system information and the uptime of the router.

Device Information

Product Type: The model number of the router.

<u>Device ID:</u> The device ID of the router.

Hardware Version: The hardware version of the router.

Software Version: The software version of the router.

MAC Address: The MAC address of the router.

<u>System Up Time:</u> The amount of time that the router has been on for.

 Status
Device Information
WAN
► LAN
 Statistics
ARP
Route
VolP
Quick Setup
 Basic Setup
 Advanced Setup
 Applications
Management

Device Info	
Product Type:	DWR-956M
Device ID:	f0b4d2059

Product Type:	DWR-956M
Device ID:	f0b4d2059d42
Hardware Version:	DWR-956M
Software Version:	TK_1.00TK_V1.2.12ah_20200330
MAC Address:	F0:B4:D2:05:9D:42
System Up Time:	265 hours, 8 mins, 36 secs





WAN

Network

This displays Network status information.

IPv4 / IPv6 WAN Connection Status

Connection Name: The name of the WAN connection. Type: The WAN connection type. IP Address/Mask: The IP address and subnet mask of the WAN connection. Default Gateway: The default gateway of the WAN connection. Primary DNS: The primary DNS of the WAN connection. Secondary DNS: The secondary DNS of the WAN connection. Status: The status of the WAN connection.

IPv4 WAN Connection Status

Connection Name	Туре	IP Address/Mask	Default Gateway	Primary DNS	Secondary DNS	Status
DHCP_WAN_ETH	DHCP	1				Connecting
PPPoE_WAN_ETH	PPP	105.186.219.43/255.255.255.255	105.184.43.1	196.43.42.190	196.43.50.190	Connected
LTE	DHCP	1				Disconnected

IPv6 WAN Connection Status

Connection Name	Туре	IP Address	Default Gateway	Primary DNS	Secondary DNS	Prefix	Status
No Rule Found!							



DS-Lite Status

<u>Connection Name</u>: The name of the DS-Lite connection.

<u>Type</u>: The DS-Lite connection type.

<u>Mode:</u> The DS-Lite mode of the DS-Lite connection.

<u>AFTR Address:</u> The AFTP address of the DS-Lite connection.

Status: The status of the DS-Lite connection.

L2TP LAC Status

<u>Connection Name:</u> The name of the DS-Lite connection.

<u>Type:</u> The WAN connection type.

IP Address/Mask: The IP address and subnet mask of the WAN connection.

<u>Default Gateway:</u> The default gateway of the WAN connection.

<u>Primary DNS</u>: The primary DNS of the WAN connection.

Secondary DNS: The secondary DNS of the WAN connection.

Status: The status of the DS-Lite connection.

Click **Refresh** to refresh the page.

L2TP LNS Status

Connection Name: The name of the WAN connection. Type the WAN connection type.

IP Address/Mask: The IP address and subnet mask of the WAN connection.

<u>Default Gateway:</u> The default gateway of the WAN connection.

<u>Primary DNS</u>: The primary DNS of the WAN connection.

Secondary DNS: The secondary DNS of the WAN connection.

Status: The status of the WAN connection.

Click **Refresh** to refresh the page.

DS-Lite Status

Connection Name	Туре	Mode	AFTR Address	Status
DHCP_WAN_ETH	DHCP	Auto		Disconnected
PPPoE_WAN_ETH	PPP	Auto		Disconnected

	_2TP	LAC	Status	
--	------	-----	--------	--

Connection Name	Туре	IP Address/Mask	Default Gateway	Client WAN IP	Server WAN IP	Status
No Rule Found!						

L2TP LNS Status

Connection Name	Туре	IP Address/Mask	Status	Authentication Mode	User Name
	PPP	1	Disconnected		



Ethernet

This displays Ethernet status information.

Statistics -- WAN

Status: The status of the Ethernet connection.

<u>Speed:</u> The speed of the Ethernet connection.

<u>Duplex</u>: The duplex of the Ethernet connection.

<u>Received</u>: The number of bytes and packets received on the Ethernet connection.

<u>Transmitted:</u> The number of bytes and packets sent on the Ethernet connection.

Click **Refresh** to refresh the page.

Dongle

This displays the 3G/4G failover status.

<u>Status:</u> The status of the 3G/4G connection. <u>Signal:</u> The signal strength for the connection <u>Cell id:</u> IMEI number for the DSL-G2562DG Click **Refresh** to refresh the page.

Statistics -- WAN

Refresh

Status	Speed	Duplex	Received		Transmitted	
Status 3	speeu	Duplex	Bytes	Packets	Bytes	Packets
Up	1000Mb/s	Full Duplex	590465912	463648	1736711	8492

Statistics -- WAN

Status	Provider	Network type	Signal	Cell id
Registered	Telkom-StayHomeSA	LTE	17	354586100737774

Refresh



xDSL

This will show you the status of your xDSL connection.

Status: Show the status of the DSL line up or no link

WAN - xDSL Status

Status:	Up
Refresh	



LAN

Network

This displays Network status information.

LAN Host IP Address: The IP address of the LAN connection.

IPv6 LAN Host IP Address: The IPv6 address of the LAN connection.

The LAN menu is used to display status information for the LAN interfaces on the router.

Ethernet

This displays Ethernet status information.

Interface: The name of the LAN interface. Status: The status of the LAN interface. Speed: The speed of the LAN interface. Duplex: The duplex of the LAN interface.

LAN Host

IP Address:	10.0.0.2
IPV6 LAN Host	
IPv6 Address:	fe80::1

LAN - Ethernet

Interface	Status	Speed	Duplex
LAN1	Down	-	-
LAN2	Up	1000Mb/s	Full Duplex
LAN3	Down	-	-
LAN4	Down	-	-



WLAN

This displays WLAN status information.

SSID Index: The index number of the Service Set Identifier (SSID).

SSID: The name of the SSID.

BSSID: The name of the Basic Service Set Identifier (BSSID).

Status: The status of the SSID.

<u>Authentication Mode</u>: The authentication modes supported by the SSID. <u>Encryption Mode</u>: The encryption modes supported by the SSID.

Attached Devices Info

<u>IP Address:</u> The IP address of the device connected to the SSID. <u>MAC Address:</u> The MAC address of the device connected to the SSID.

Click **Refresh** to refresh the page.

DHCP Client

This displays DHCP client status information.

<u>Host Name:</u> The host name of the DHCP client. <u>MAC Address:</u> The MAC address of the DHCP client. <u>IP Address:</u> The IP address of the DHCP client. <u>Lease Time:</u> The lease time of the IP address.

LAN - WLAN

SSID Index	SSID	BSSID	Status	Authentication Mode	Encryption Mode
SSID-1	dlink-956M-2.4G-95e3	EC:AD:E0:50:95:E4	Enable	WPA-PSK/WPA2-PSK	AESEncryption
SSID-2	dlink-956M-2.4G-2	EE:AD:E0:50:95:E4	Disable	WPA-PSK/WPA2-PSK	AESEncryption
SSID-3	dlink-956M-2.4G-3	EE:AD:E0:60:95:E4	Disable	WPA-PSK/WPA2-PSK	AESEncryption
SSID-4	dlink-956M-2.4G-4	EE:AD:E0:70:95:E4	Disable	WPA-PSK/WPA2-PSK	AESEncryption
SSID-5	dlink-956M-5.8G-95e3	EC:AD:E0:50:95:E5	Enable	WPA-PSK/WPA2-PSK	AESEncryption
SSID-6	dlink-956M-5G-2	EE:AD:E0:50:95:E5	Disable	WPA-PSK/WPA2-PSK	AESEncryption
SSID-7	dlink-956M-5G-3	EE:AD:E0:51:95:E5	Disable	WPA-PSK/WPA2-PSK	AESEncryption
SSID-8	dlink-956M-5G-4	EE:AD:E0:52:95:E5	Disable	WPA-PSK/WPA2-PSK	AESEncryption

Attached Devices Info

IP Address MAC Address
No Rule Found!

Refresh

LAN - DHCP Client

Host Name	MAC Address	IP Address	Lease Time
DESKTOP-OQGT5Q5	68:f7:28:5c:23:39	10.0.0.3	23:53:07



Statistics

The Statistics menu is used to display statistics for the different interfaces on the router.

WAN

This displays the WAN statistics.

Interface: The name of the WAN interface.

<u>Received:</u> The number of bytes and packets received, and the number of errors and discarded packets on the WAN connection.

<u>Transmitted</u>: The number of bytes and packets sent, and the number of errors and discarded packets on the WAN connection.

Click **Refresh** to refresh the page.

LAN

This displays the LAN statistics.

Port: The name of the LAN port.

<u>Transmitted</u>: The number of bytes and packets sent, and the number of errors and discarded packets on the LAN port.

<u>Received:</u> The number of bytes and packets received, and the number of errors and discarded packets on the LAN port.

Interface	
interface	

Refresh

Statistics -- WAN

Interface	Neceiveu				Transmitteu			
interface	Bytes	Packets	Error	Discard	Bytes	Packets	Error	Discard
DHCP_WAN_ETH	0	0	0	0	0	0	0	0
PPPoE_WAN_ETH	0	0	0	0	0	0	0	0
LTE	0	0	0	0	0	0	0	0

Descional

Statistics -- LAN

Refresh

Port		Transm	itted		Received				
Pon	Bytes	Packets	Error	Discard	Bytes	Packets	Error	Discard	
LAN1	0	0	0	0	0	0	0	0	
LAN2	338243	635	0	0	212803	1220	0	4	
LAN3	0	0	0	0	0	0	0	0	
LAN4	0	0	0	0	0	0	0	0	

Click **Refresh** to refresh the page.



WLAN

This displays WLAN statistics.

Port: The name of the WLAN port.

<u>Received</u>: The number of bytes and packets received, and the number of errors and discarded packets on the WLAN port.

<u>Transmitted</u>: The number of bytes and packets sent, and the number of errors and discarded packets on the WLAN port.

Click **Refresh** to refresh the page.

хТМ

Show the statistics of the DSL line.

<u>Port Number:</u> Shows the port number.

In Octets: Shows the amount of data in Octets.

Out Octets: Shows the amount of data out in Octets.

In Packets: Shows the amount of Packets received.

Out Packets: Shows the amount of packets transmitted.

In OAM Cells: Shows the amount of cells received in OAM Value (Operation, Administration, Maintenance

Out OAM Cells: Shows the amount of cells transmitted in OAM Value (Operation, Administration, Maintenance

In ASM Cells: Shows the ASM (Autonomous Status Message) value received.

Out ASM Cells: Shows the ASM (Autonomous Status Message) value transmitted.

Statistics -- WLAN

Refresh

Port		Rece	eived		Transmitted			
PUIL	Bytes	Packets	Error	Discard	Bytes	Packets	Error	Discard
SSID-1	0	0	0	0	0	0	0	0
SSID-2	0	0	0	0	0	0	0	0
SSID-3	0	0	0	0	0	0	0	0
SSID-4	0	0	0	0	0	0	0	0
SSID-5	0	0	0	0	0	0	0	0
SSID-6	0	0	0	0	0	0	0	0
SSID-7	0	0	0	0	0	0	0	0
SSID-8	0	0	0	0	0	0	0	0

Statistics -- xTM

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packets Errors	In Cell Errors
0	2207447	2768806	6805	7084	0	0	0	0	0	0
U	2207447	2700000	0005	7004	U	U	U	U	U	U



In Packet Errors: Shows the amount of errors received on the DSL line.

In Cell Errors: Shows the amount of errors transmitted on the DSL line.

Click **Refresh** to refresh the page.

xDSL

Shows you statistic and of your xDSL line.

Status: Shows whether the DSL line is connected or not.

Line Standard: Shows the DSL standard that is connected.

Current Rate (Up/Down): Shows the current speed at which the router is sync.

<u>Max Rate (Up/Down)</u>: Shows the maximum rate the DSL/Router can connect to depending on the Line standard.

Noise Margin (Up/Down): Shows the Noise Margin for the line in decibels.

InterleaveDepth (Up/Down): Shows the depth of the block of data being transmitted (ADSL up to 64bytes and VDSL 3072).

<u>Line Attenuation (Up/Down)</u>: Shows the degraded count of your line between the DSLAM and Router in decibels.

Output Power (Up/Down): Shows the power levels between DSLAM and Router in decibels.

FEC (Up/Down): Shows you the amount of FEC (Forward error correction) errors.

HEC (Up/Down): Shows the amount of HEC (Header Error Check/Correction) errors.

CRC (Up/Down): Shows the amount of CRC (Cyclic Redundancy Check) errors.

Statistics -- xDSL

Status:	Up
Line Standard:	G.992.1_Annex_A
Current Rate(Up/Down):	832/8064 kbps
Max Rate(Up/Down):	864/10992 kbps
Noise Margin(Up/Down):	6.0/17.2 dB
InterleaveDepth(Up/Down):	1/1
Line Attenuation(Up/Down):	1.0/13.0 dB
Output Power(Up/Down):	12.4/5.5 dBm
FEC(Up/Down):	0/0
HEC(Up/Down):	0/0
CRC(Up/Down):	0/2
ESTI.DISTANCE:	250m

Refresh



ESTI.DISTANCE: Shows the estimated distance between your router and the DSLAM

Click **Refresh** to refresh the page.

ARP

This displays Address Resolution Protocol (ARP) statistics.

<u>IP Address</u>: The IP address used in the ARP lookup. <u>Flags</u>: The flags returned by the ARP lookup. <u>HW Address</u>: The MAC address used in the ARP lookup. <u>Device</u>: The interface used in the ARP lookup. ARP

IP Address	Flags	HW Address	Device
10.0.0.3	Complete	68:f7:28:5c:23:39	br0
Clear Refresh			

Click **Clear** to clear the ARP statistics and click **Refresh** to refresh the page.



Route

This page will show you the current router for the router.

Destination: The Destination route address Gateway: Gateway to the Destination route Subnet Mask: Subnet for the Destination router Flag: Flag for the rule. Metric: Metric for the route Name: Wan Connection used for the Route Interface: Interface type for the route

ROUTE INFO

Refresh

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate ,D - dynamic (redirect), M - modified (redirect).									
Destination	Gateway	Subnet Mask	Flag	Metric	Name	Interface			
0.0.0.0	10.150.20.42	0.0.0.0	UG	1	LTE	ip_3_1_1			
10.0.0.0	0.0.0.0	255.255.255.0	U	0		br0			
10.150.20.40	0.0.0.0	255.255.255.252	U	0	LTE	ip_3_1_1			
192.168.253.0	0.0.0.0	255.255.255.0	U	0		br1			

VoIP

Voice Status

The VoIP menu is used to display voice status information from the router.

Line: The name of the VoIP line.

<u>Voice Register Status:</u> The status of the VoIP line.

<u>Coding Type:</u> The coding types supported by the VoIP line.

<u>Tel:</u> The telephone number associated with the VoIP line.

<u>Call State:</u> The call state of the VoIP line.

<u>Call Waiting Status:</u> The call waiting status of the VoIP line.

Conference Calling Status: The conference calling status of the VoIP line.

Click **Refresh** to refresh the page.

Voice Status

I	Line	Voice Register Status	Coding Type	Tel	Call State	Call Waiting Status	Conference Calling Status
I	Line1	Disabled	G729 G711A		Idle	Idle	Idle



Basic Setup WAN Interface

ATM

Here you can create, edit or Delete an ATM profile for ADSL connection.

Interface: Interface name for the ATM profile.

DSL Link Type: The DSL link type. This can be EoA, PPPoA or IPoA. Default is EoA.

<u>VPI/VCI</u>: This is the Values required by your ISP. Default is 8/35.

<u>QoS:</u> The QoS (Quality of Service) via the ISP DSL line. This can be **UBR, CBR, VBR-nrt, VBR-rt** or **UBR+**. Default is **UBR**.

<u>Encapsulation</u>: The type of encapsulation between DSL and DSLAM. This can be **LLC/SNAP** or **VcMux**. Default is **LLC/SNAP**.

Edit: Click edit to modify Settings

<u>Delete:</u> Delete the whole ATM profile.

Click Create to create a new ATM profile.

Click **Refresh** to refresh the page.

Interface	DSL Link Type	VPI/VCI	Qo S	Encapsulation	Edit/Delete				
ATM_8_35	EoA	8/35	UBR	LLC/SNAP	Edit Delete				
Create Refresh									



PTM

Enable or disable PTM (VDSL) connection.

Click Apply to save your settings.

Click **Refresh** to refresh the page.

Ethernet

Enable or Disable Ethernet WAN connection

Click **Apply** to save your settings.

Click **Refresh** to refresh the page.

Dongle Enable to disable 3G/4G failover. Click **Apply** to save your settings.

Click **Refresh** to refresh the page.

PTM Enable 🗸

Ethernet Enable 🗹







WAN Service

This page displays WAN Service information.

WAN Name: The name of the WAN connection profile. This can be DHCP_WAN_ETH, or PPPoE_WAN_ETH, LTE. Interface: The mode of the connection type. This can be, ETH or USB. Mode: This is the mode that the DSL-G2562DG will operate in. This can be DHCP, Static, PPPoE, Bridge or Con-Bridge. IP Protocol Type: The IP protocol version used by the WAN connection. This can be IPv4, IPv6 or IPv4&6. Service Type: The service type for the WAN connection. This can be INTERNET, TR069,

TR069_INTERNET, VOIP, INTERNET_VOIP, TR069_VOIP, TR069_INTERNET_VOIP, or Other.

Edit/Delete: Click Edit to edit the current service profile. Press Delete to delete.

Set New WAN

Interface: The interface of the connection type. This can be, **ATM_8_35**, **PTM**, **ETH** or **USB**. ADSL/VDSL (**ATM_8_35/PTM**) is used to connect to the internet via a RJ-11 copper connection. Ethernet (**ETH**) is used for direct WAN connections to a fibre ONT. Select **USB** for use with a compatible 3G/4G usb dongle connected to the DSL-G2562DG, contact your ISP to find out which connection type you should use. Choosing one of these options displays other options on the page, and each of these is documented below.

Mode: This can be DHCP, Static, PPPoE, Bridge, or Con-bridge.

Click Create to set new WAN. Click Refresh to update the list.

WAN ServiceInfo

WAN Name	Interface	Mode	IP Protocol Type	Service Type	Edit/[Delete
ATM_8_35_ADSL	ATM_8_35	PPP₀E	IPv4	TR069_INTERNET_VOIP	Edit	Delete
PTM_835_VDSL	PTM	PPP₀E	IPv4	TR069_INTERNET_VOIP	Edit	Delete
DHCP_WAN_ETH	ETH	DHCP	IPv4	TR069_INTERNET_VOIP	Edit	Delete
PPPoE_WAN_ETH	ETH	PPP₀E	IPv4	TR069_INTERNET_VOIP	Edit	Delete
Dongle	USB	PPP₀E	IPv4	TR069_INTERNET_VOIP	Edit	Delete



Interface:	ATM_8_35 ~
Mode:	DHCP 🗸





Interface: ATM_8_35		
Mode: PPPoE	WAN Service	
Connection Name: Assign a name for the connection here.	Organization Norma	
Enable: Tick this to enable this connection.	Connection Name:	ATM_8_35_ADSL
MTU: The Maximum Transmission Unit (MTU) of the WAN connection.	Enable:	
This is set to 1492 bytes by default.	MTU:	1492
<u>IP Protocol Type</u> : The IP protocol version used by the WAN connection.	IP Protocol Type:	IPv4 ►
This can be IPv4, IPv6 or IPv4&6. Choosing one of these options displays other options on the page, and	NAT:	
each of these is documented below.	Firewall:	
<u>NAT:</u> Enable or disable Network Address Translation (NAT) on the WAN connection. Tick this to enable	IPv4 Static DNS:	
NAT.	PPPoE Type:	Normal PPPoE 🗸
Firewall: Whether to enable or disable packet filtering. Tick this to enable packet filtering. This feature is	Servicename:	
ticket by default.		
IPv4 Static DNS: Whether to enable or disable static DNS entries. Tick this to enter static DNS entries,	User Name:	guest@telkomsa.net
or un-tick it assigns the DNS servers using DHCP.	Password:	•••••
Ticking the box displays other options on the page, and these are documented below.	Authentication Type:	AUTO 🗸
<u>PPPoE Type:</u> Select between Normal PPPoE or if you use a Proxy Server to connect with PPPoE then	Dial Mode:	Automatically V
select PPPoE Proxy.	Keep Alive Time:	30 (10-30)s
Service Name: Enter the Service name for your PPPoE Connection. Default is blank.	-	
Username: Enter your PPP Username provided by the ISP	Keep Alive Max Fail:	5 (1-100)
Password: Enter the password for the PPP username also provided by your ISP.	MAC Address Override:	
Authentication Type: Select you Authentication type for the ADSL connection. Default is Auto.	Enable VLAN:	
Dial Mode: Choose whether this connection needs to dial automatically or Manual.		
Keep Alive: Se the time for the connections to keep alive (Used for Manual Dial Mode).	Service Type:	TR069_INTERNET_VOIP ~
Keep Alive Max Fail: Set the about of maximum failures to dial before router will stop to dial.		
MAC Address Override:		
Whether to enable or disable MAC address override on the WAN connection.		
Choosing this option displays other options on the page, and each of these is documented below.		
Enable VLAN: Whether to enable or disable VLAN settings on the WAN connection.		



Choosing this option displays other options on the page, and each of these is documented below.

<u>Service Type:</u> The service type for the WAN connection. This can be **INTERNET**, **TR069**, **TR069_INTERNET**, **VOIP**, **INTERNET_VOIP**, or **Other**. Choosing the **INTERNET**, **TR069_INTERNET**, **INTERNET_VOIP**, or **TR069_INTERNET_VOIP** option displays other options on the page, and each of these is documented below.

Click Advanced Settings to reveal more settings.

		(Limit Retry Time of PPP)
	Limit Retry Time:	password on authentication
		error)
<u>Limit Retry Time</u> : Enable this feature to allow authentication retry.	Retry Time:	3
PPPoE Pass-through: Enable or disable to allow the router to pass-through PPPoE connections.		(0-100)
Enable dual lan: Enable or disable dual lan for ADSL connection.	PPPoEPassThrough:	
	Enable Dual Lan:	
Bound Ports: These are the ports that are bound and that can share the same service type. Tick the LAN	PPPoE address mode:	static 🗸
or SSID ports to bind these ports.	Unnumbered PPPoE IP:	
	Unnumbered LAN IP:	
	Unnumbered LAN mask:	
Note: A greyed-out port means it has been bound.	DHCP LAN Start IP:	
	DHCP LAN End IP:	
Click Apply to save your settings. Click Back to cancel and return to the previous screen.	DHCP Primary DNS:	
	DHCP Secondary DNS: Unnum Port:	
Click Refresh to update the current screen.	onnum Port.	
		Clients behind checked ports will join unnumbered LAN
	Bound Ports:	LAN1 LAN2 LAN3 LAN4
		A grey out port means it has been bound.
	Apply Back Refres	sh



Interface: PTM (VDSL)		
Mode: PPPoE		
Connection Name: Assign a name for the connection here.		
Enable: Tick this to enable this connection.	WAN Service	
MTU: The Maximum Transmission Unit (MTU) of the WAN		
connection. This is set to 1492 bytes by default.	Connection Name:	PPPoE_WAN_ETH
<u>IP Protocol Type</u> : The IP protocol version used by the WAN connection.	Enable:	
This can be IPv4, IPv6 or IPv4&6. Choosing one of these options displays	MTU:	1492
other options on the page, and each of these is documented below.	MTU.	1492
NAT: Enable or disable Network Address Translation (NAT) on the WAN connection.	IP Protocol Type:	IPv4 ►
Tick this to enable NAT.	NAT:	
Firewall: Whether to enable or disable packet filtering. Tick this to enable packet filtering.	NAL.	
This feature is ticket by default	Firewall:	
IPv4 Static DNS: Whether to enable or disable static DNS entries. Tick this to enter static DNS	IPv4 Static DNS:	
entries, or un-tick it assigns the DNS servers using DHCP.	II VY OLULE DIVO.	
Ticking the box displays other options on the page, and these are documented below.	PPPoE Type:	Normal PPPoE 🗸
<u>PPPoE Type:</u> The PPPoE type for the WAN connection.	Servicename:	
This can be Normal PPPoE or PPPoE Proxy .	Servicename.	
Choosing the PPPoE Proxy option displays other options on the page,	User Name:	guest@telkomsa.net
and each of these is documented below.	Password:	••••••
Service name: The name of the PPPoE service on the router. This is used for reference only.		
User Name: The username used to connect to the PPPoE session.		
This should be supplied to you by your ISP.		
Password: The password used to connect to the PPPoE session.		

This should be supplied to you by your ISP.



Authentication Type: The authentication type for the WAN connection. Au This can be **AUTO**, **PAP** or **CHAP**. This should be supplied to you by your ISP. Di Dial Mode: This is the method that is used to connect to the PPPoE session. This can be Ke Automatically, Dial on Demand and Manual connect. Choosing the Automatically and Dial on **Demand** options display other options on the page, and each of these is documented below. Ke Keep Alive Time: This is the interval at which to send keep alive on the PPPoE connection. This can M/ be from 10 to 30 seconds. The default is 10. Er Keep Alive Max Fail: The number of keep alive that can be missed before the connection is deemed VI to be inactive. This can be from **1** to **100**. The default is 5. MAC Address Override: Whether to enable or disable MAC address override on the WAN 8 connection. Choosing this option displays other options on the page, and each of these is V documented below. Enable VLAN: Whether to enable or disable VLAN settings on the WAN connection. Choosing this option displays other options on the page, and each of these is documented below.

This is by default enabled with 835

uthentication Type:	AUTO 🗸	
ial Mode:	Automatically	
eep Alive Time:	30 (10-30)s	
eep Alive Max Fail:	5 (1-100)	
IAC Address Override:		
nable VLAN:		
LAN ID:	835	
02.1P:	Disable 🗸	
LAN Tagging:	LAN1 LAN2 LAN3 LAN4	

<u>Service Type:</u> The service type for the WAN connection. This can be **INTERNET**, **TR069**, **TR069_INTERNET**,

VOIP, INTERNET_

VOIP, TR069_VOIP, TR069_INTERNET_VOIP, or Other.

Choosing the INTERNET, TR069_INTERNET, INTERNET_VOIP,

or TR069_INTERNET_VOIP option displays other options

on the page, and each of these is documented below.

Service Type:

TR069_INTERNET_VOIP ✓



Click Advanced Settings to reveal more settings.

Mode: PPPoE (Advanced Settings)

Limit Retry Time: Whether or not to limit the retry time on a failed PPPoE connection.

Ticking the box displays other options on the page, and these are documented below. <u>PPPoE PassThrough</u>: Whether to enable or disable PPPoE passthrough. This allows a PPPoE enabled device connected to the DSL-G2562DG to connect to the PPPoE session supplied by the ISP. Tick this to enable PPPoE passthrough.

<u>Enable Dual Lan:</u> Whether to enable or disable the dual LAN feature. Tick this to enable dual LAN.

Ticking the box displays other options on the page, and these are documented below. <u>Bound Ports</u>: These are the ports that are bound and that can share the same service type.

Note: A greyed-out port means it has been bound.

Click **Apply** to save your settings. Click **Back** to cancel and return to the previous screen.

Click **Refresh** to update the current screen.

Advanced Settings

Limit Retry Time:	$\hfill \square$ (Limit Retry Time of PPP password on authentication error)
PPPoEPassThrough:	
Enable Dual Lan:	
Bound Ports:	□LAN1 □LAN2 □LAN3 □LAN4
	A grey out port means it has been bound.
Apply Back Refrest	



Interface: ETH	WAN Service	
Mode: DHCP		
Connection Name: Assign a name for the connection here.	Connection Name:	DHCP_WAN_ETH
Enable: Tick this to enable this connection.	o onno o contra no.	
MTU: The Maximum Transmission Unit (MTU) of the WAN connection.	Enable:	
This is set to 1492 bytes by default.	MTU:	1500
IP Protocol Type: The IP protocol version used by the WAN connection.		
This can be IPv4, IPv6 or IPv4&6. Choosing one of these options displays other options	IP Protocol Type:	IPv4 ►
on the page, and each of these is documented below.	NAT:	
NAT: Enable or disable Network Address Translation (NAT) on the WAN connection.		
Tick this to enable NAT.	Firewall:	 ✓
Firewall: Whether to enable or disable packet filtering. Tick this to enable packet	IPv4 Static DNS:	
filtering. This feature is ticket by default.		_
IPv4 Static DNS: Whether to enable or disable static DNS entries. Tick this to enter	MAC Address Override:	
static DNS entries, or un-tick it assigns the DNS servers using DHCP.	Enable VLAN:	
Ticking the box displays other options on the page, and these are documented below.		
	Service Type:	TR069_INTERNET_VOIP ¥
MAC Address Override:		
Whether to enable or disable MAC address override on the WAN connection.		

Choosing this option displays other options on the page, and each of these is documented below.

Enable VLAN: Whether to enable or disable VLAN settings on the WAN connection.

Choosing this option displays other options on the page, and each of these is documented below.

<u>Service Type:</u> The service type for the WAN connection. This can be **INTERNET**, **TR069**, **TR069_INTERNET**, **VOIP**, **INTERNET_VOIP**, or **Other**. Choosing the **INTERNET**, **TR069_INTERNET**, **INTERNET_VOIP**, or **TR069_INTERNET_VOIP** option displays other options on the page, and each of these is documented below.



Click Advanced Settings to reveal more settings.

Mode: DHCP (Advanced Settings)

<u>DHCP Option 60 Setting:</u> Whether to enable or disable DHCP Option 60 when receiving DHCP information on the WAN connection. Choosing this option displays other options on the page, and each of these is documented below.
<u>DHCP Option 66:</u> Whether to enable or disable DHCP Option 66 when receiving DHCP information on the WAN connection. Tick this to enable the DHCP Option 66.
<u>DHCP Option 120:</u> Whether to enable or disable DHCP Option 120 when receiving DHCP information on the WAN connection.
Tick this to enable the DHCP Option 120.
<u>Bound Ports:</u> These are the ports that are bound and that can share the same service type. Tick the LAN or SSID ports to bind these ports.

Note: A greyed-out port means it has been bound.

Click **Apply** to save your settings. Click **Back** to cancel and return to the previous screen. Click **Refresh** to update the current screen.

Advanced Settings

DHCP Option 60 Setting:	
DHCP Option 66:	
DHCP Option 120:	
Bound Ports:	□LAN1 □LAN2 □LAN3 □LAN4
	A grey out port means it has been bound.
Apply Back Refres	h



Interface: ETH		
<u>Mode:</u> Static	WAN Service	
Connection Name: Assign a name for the connection here.		
Enable: Tick this to enable this connection.	Connection Name:	STATIC_WAN_ETH
MTU: The Maximum Transmission Unit (MTU) of the WAN connection.	Enable:	
This is set to 1492 bytes by default.	Endoro.	_
<u>IP Protocol Type:</u> The IP protocol version used by the WAN connection.	MTU:	1492
This can be IPv4, IPv6 or IPv4&6.	IP Protocol Type:	IPv4 V
Choosing one of these options displays other options on the page, and each of these is	in Thorocortype.	
documented below.	NAT:	
NAT: Enable or disable Network Address Translation (NAT) on the WAN connection.	Firewall:	~
Tick this to enable NAT.		
Firewall: Whether to enable or disable packet filtering. Tick this to enable packet	IP Address:	192.168.0.2
filtering. This feature is ticket by default.	Subnet Mask:	255.255.225.0
IPv4 Static DNS: Whether to enable or disable static DNS entries. Tick this to enter	Default Onterview	102.102.0.1
static DNS entries, or un-tick it assigns the DNS servers using DHCP.	Default Gateway:	192.168.0.1
Ticking the box displays other options on the page, these are documented below.	IPv4 Static DNS:	
MAC Address Override: Whether to enable or disable MAC address override on the	Brimery DNS Conver	192.168.0.1
WAN connection. Choosing this option displays other options on the page, and each of	Primary DNS Server:	
these is documented below.	Secondary DNS Server:	192.168.0.1
Enable VLAN: Whether to enable or disable VLAN settings on the WAN connection.	MAC Address Override:	
Choosing this option displays other options on the page, and each of these is	MAC Address Overlide.	
documented below.	Enable VLAN:	



<u>Service Type:</u> The service type for the WAN connection. This can be INTERNET, TR069, TR069_INTERNET, VOIP, INTERNET_ VOIP, TR069_VOIP, TR069_INTERNET_VOIP, or Other. Choosing the INTERNET, TR069_INTERNET, INTERNET_VOIP, or TR069_INTERNET_VOIP option displays other options on the page, and each of these is documented below.

Click Advanced Settings to reveal more settings

<u>Mode:</u> Static (Advanced Settings) <u>Bound Ports</u>: These are the ports that are bound and that can share the same service type. Tick the LAN or SSID ports to bind these ports.

Note: A greyed-out port means it has been bound.

Click **Apply** to save your settings. Click **Back** to cancel and return to the previous screen. Click **Refresh** to update the current screen.

Service Type:	TR069_INTERNET_VOIP V
Advanced Settings	
Bound Ports:	□LAN1 □LAN2 □LAN3 □LAN4
	SSID1 SSID2 SSID3 SSID4
	A grey out port means it has been bound.
Apply Back Refresh	



Interface: ETH		
Mode: PPPoE		
Connection Name: Assign a name for the connection here.		
Enable: Tick this to enable this connection.	WAN Service	
MTU: The Maximum Transmission Unit (MTU) of the WAN		
connection. This is set to 1492 bytes by default.	Connection Name:	PPPoE_WAN_ETH
IP Protocol Type: The IP protocol version used by the WAN connection.	Enable:	
This can be IPv4, IPv6 or IPv4&6. Choosing one of these options displays	MTU:	1492
other options on the page, and each of these is documented below.	WITU.	1452
NAT: Enable or disable Network Address Translation (NAT) on the WAN connection.	IP Protocol Type:	IPv4 🗸
Tick this to enable NAT.	NAT:	
Firewall: Whether to enable or disable packet filtering. Tick this to enable packet filtering.	NAL.	
This feature is ticket by default	Firewall:	
IPv4 Static DNS: Whether to enable or disable static DNS entries. Tick this to enter static DNS	IPv4 Static DNS:	
entries, or un-tick it assigns the DNS servers using DHCP.	in the state birts.	
Ticking the box displays other options on the page, and these are documented below.	PPPoE Type:	Normal PPPoE 🗸
<u>PPPoE Type:</u> The PPPoE type for the WAN connection.	Servicename:	
This can be Normal PPPoE or PPPoE Proxy .	Servicentanie.	
Choosing the PPPoE Proxy option displays other options on the page,	User Name:	guest@telkomsa.net
and each of these is documented below.	Password:	•••••
Service name: The name of the PPPoE service on the router. This is used for reference only.		
User Name: The username used to connect to the PPPoE session.		
This should be supplied to you by your ISP.		

<u>Password</u>: The password used to connect to the PPPoE session.

This should be supplied to you by your ISP.



Authentication Type: The authentication type for the WAN connection. This can be **AUTO**, **PAP** or **CHAP**. This should be supplied to you by your ISP. Dial Mode: This is the method that is used to connect to the PPPoE session. This can be Authe Automatically, Dial on Demand and Manual connect. Choosing the Automatically and **Dial on Demand** options display other options on the page, and each of these is Dial documented below. Keep Keep Alive Time: This is the interval at which to send keep alive on the PPPoE connection. This can be from 10 to 30 seconds. The default is 10. Keep Keep Alive Max Fail: The number of keep alive that can be missed before the connection is MAC deemed to be inactive. This can be from 1 to 100. The default is 5. MAC Address Override: Whether to enable or disable MAC address override on the WAN Enab connection. Choosing this option displays other options on the page, and each of these is documented below. Enable VLAN: Whether to enable or disable VLAN settings on the WAN connection.

Choosing this option displays other options on the page, and each of these is documented below.

Service Type: The service type for the WAN connection. This can be INTERNET, TR069, TR069_INTERNET, VOIP, INTERNET_ VOIP, TR069_VOIP, TR069_INTERNET_VOIP, or Other. Choosing the INTERNET, TR069_INTERNET, INTERNET_VOIP, or TR069_INTERNET_VOIP option displays other options on the page, and each of these is documented below.

entication Type:	AUTO 🗸	
Mode:	Automatically V	
Alive Time:	30) (10-30)s
Alive Max Fail:	5	(1-100)
Address Override:		
ole VLAN:		

Service Type:





Click Advanced Settings to reveal more settings.

Mode: PPPoE (Advanced Settings)

Limit Retry Time: Whether or not to limit the retry time on a failed PPPoE connection.

Ticking the box displays other options on the page, and these are documented below. <u>PPPoE Pass-through:</u> Whether to enable or disable PPPoE pass-through. This allows a PPPoE enabled device connected to the DSL-G2562DG to connect to the PPPoE session supplied by the ISP. Tick this to enable PPPoE pass-through.

<u>Enable Dual Lan:</u> Whether to enable or disable the dual LAN feature. Tick this to enable dual LAN.

Ticking the box displays other options on the page, and these are documented below. <u>Bound Ports</u>: These are the ports that are bound and that can share the same service type.

Note: A greyed-out port means it has been bound.

Click **Apply** to save your settings. Click **Back** to cancel and return to the previous screen. Click **Refresh** to update the current screen.

Interface: ETH

Mode: Bridge

<u>Connection Name</u>: Assign a name for the connection here.

Enable: Tick this to enable this connection, and un-tick it to disable it.

<u>IP Protocol Type</u>: The IP protocol version used by the WAN connection. This can be **IPv4**, **IPv6** or **IPv4&6**. Choosing one of these options displays other options on the page, and each of these is documented below.

Enable VLAN: Whether to enable or disable VLAN settings on the WAN connection.

Choosing this option displays other options on the page, and each of these is documented below.

Service Type: The service type for the WAN connection. This can be

Advanced Settings

Limit Retry Time:	$\hfill\square$ (Limit Retry Time of PPP password on authentication error)
PPPoEPassThrough:	
Enable Dual Lan:	
Bound Ports:	LAN1 LAN2 LAN3 LAN4
	A grey out port means it has been bound.
Apply Back Refresh	



Connection Name:	BRIDGE_WAN_ETH	
Enable:		
IP Protocol Type:	IPv4 V	
Enable VLAN:		
Service Type:	INTERNET 🗸	



INTERNET, TR069, TR069_INTERNET, VOIP, INTERNET_ VOIP, TR069_VOIP, TR069_INTERNET_VOIP, or Other. Choosing the INTERNET, TR069_INTERNET, INTERNET_VOIP, or TR069_INTERNET_VOIP option displays other options on the page, and each of these is documented below. Click Advanced Settings to reveal more settings.

Mode: Bridge (Advanced Settings)

<u>VLAN Pass-through</u>: Whether to enable or disable passing VLANs through from the WAN connection.
 Tick this to enable VLAN pass through. This is un-ticked by default.
 <u>DHCP Transparent</u>: Whether to enable or disable passing DHCP information through from the WAN connection. Tick this to enable DHCP transparent. This is un-ticked by default.
 <u>Bound Ports</u>: These are the ports that are bound and that can share the same service type.

Tick the LAN or SSID ports to bind these ports.

Note: A greyed-out port means it has been bound.

Click **Apply** to save your settings. Click Back to **cancel** and return to the previous screen. Click **Refresh** to update the current screen.

Advanced Settings

VLAN PassThrough:	
DHCP Transparent:	
Bound Ports:	□LAN1 □LAN2 □LAN3 □LAN4
	SSID1 SSID2 SSID3 SSID4
	A grey out port means it has been bound

Apply Back Refresh



Interface: ETH Mode: Con-bridge

Connection Name: Assign a name for the connection here.

Enable: Tick this to enable this connection.

<u>Enable VLAN</u>: Whether to enable or disable VLAN settings on the WAN connection. Choosing this option displays other options on the page, and each of these is documented below.

<u>Service Type:</u> The service type for the WAN connection. This can be **TR069 or VOIP**.

Click Advanced Settings to reveal more settings.

<u>Mode:</u> Con-bridge (Advanced Settings)

VLAN Pass-through:

Whether to enable or disable passing VLANs through from the WAN connection.
Tick this to enable VLAN pass through. This is un-ticked by default.
<u>Bound Ports:</u> These are the ports that are bound and that can share
the same service type. Tick the LAN or SSID ports to bind these ports.

Note: A greyed-out port means it has been bound.

Click **Apply**_to save your settings. Click **Back**_to cancel and return to the previous screen. Click **Refresh** to update the current screen.

WAN Service	
Connection Name:	
Enable:	
Enable VLAN:	
Service Type:	VOIP V
Advanced Settings	
VLAN PassThrough:	
Bound Ports:	□LAN1 □LAN2 □LAN3 □LAN4
	A grey out port means it has been bound

Back

Appl

Refresh



Interface: Dongle Mode: PPPoE

Connection Name: Assign a name for the connection here.

Enable: Tick this to enable this connection.

MTU: The Maximum Transmission Unit (MTU) of the WAN connection. WAN Service This is set to 1500 bytes by default. Connection Name: Dongle IP Protocol Type: The IP protocol version used by the WAN connection. Enable: ~ This can be IPv4, IPv6 or IPv4&6. 1492 MTU: Choosing one of these options displays other options on the page, and each of these is documented below. NAT: Enable or disable Network Address Translation (NAT) on the WAN connection. IPv4 🗸 IP Protocol Type: Tick this to enable NAT. NAT: ~ Firewall: Whether to enable or disable packet filtering. Tick this to enable packet filtering. The default is Firewall: ~ ticked. IPv4 Static DNS: IPv4 Static DNS: Whether to enable or disable static DNS entries. Tick this to enter PIN: static DNS entries. Ticking the box displays other options on the page, and these are documented below. APN: TelkomInternet Pin: Enter the pin code for the sim card if enabled DialNumber: *99# APN: Select APN for your mobile provider PPPoE Type Dial Number: default is set to *99# Servicename:

PPPoE Type: The PPPoE type for the WAN connection.

This can be Normal PPPoE or PPPoE Proxy.

Choosing the **PPPoE Proxy** option displays other options on the page,

and each of these is documented below.

Service name: The name of the PPPoE service on the router. This is used for reference only.

User Name: The username used to connect to the PPPoE session.

This should be supplied to you by your ISP.

Password: The password used to connect to the PPPoE session.

This should be supplied to you by your ISP.

User Name:

Password:

Normal PPPoE V



Authentication Type: The authentication type for the WAN connection. This can be **AUTO**, **PAP** or **CHAP**. This should be supplied to you by your ISP. Dial Mode: This is the method that is used to connect to the PPPoE session. This can be Automatically, Dial on Demand and Manual connect. Choosing the Automatically and Dial on **Demand** options display other options on the page, and each of these is documented below. Keep Alive Time: This is the interval at which to send keep alive on the PPPoE connection. This can be from 10 to 30 seconds. The default is 10. Keep Alive Max Fail: The number of keep Alive that can be missed before the connection is deemed to be inactive. This can be from 1 to 100. The default MAC Address Override: Whether to enable or disable MAC ad connection. Choosing this option displays other options on the documented below. Enable VLAN: Whether to enable or disable VLAN settings on the WAN connection.

MAC Address Override:	
Enable VLAN:	
	_

Authentication Type:

Keep Alive Time:

Keep Alive Max Fail:

Dial Mode:

AUTO 🗸

30

5

Automatically

~

(10-30)s

(1-100)

Choosing this option displays other options on the page, and each of these is documented below.

Service Type: The service type for the WAN connection. This can be **INTERNET**, **TR069**, **TR069**, **INTERNET**, **VOIP**, **INTERNET**, **VOIP**, TR069 VOIP, TR069 INTERNET VOIP, or Other. Choosing the INTERNET, TR069 INTERNET, INTERNET VOIP, or TR069 INTERNET VOIP option displays other options on the page, and each of these is documented below.



Click Advanced Settings to reveal more settings.

Mode: PPPoE (Advanced Settings)

Limit Retry Time: Whether or not to limit the retry time on a failed PPPoE connection.

Ticking the box displays other options on the page, and these are documented below. <u>PPPoE Pass-through:</u> Whether to enable or disable PPPoE pass-through. This allows a PPPoE enabled device connected to the DSL-G2562DG to connect to the PPPoE session supplied by the ISP. Tick this to enable PPPoE pass-through.

<u>Enable Dual Lan:</u> Whether to enable or disable the dual LAN feature. Tick this to enable dual LAN.

Ticking the box displays other options on the page, and these are documented below. <u>Bound Ports</u>: These are the ports that are bound and that can share the same service type.

Note: A greyed-out port means it has been bound.

Click **Apply** to save your settings. Click **Back** to cancel and return to the previous screen.

Click **Refresh** to update the current screen.

Advanced Settings

Limit Retry Time:	$\hfill \square$ (Limit Retry Time of PPP password on authentication error)	
PPPoEPassThrough:		
Enable Dual Lan:		
Bound Ports:	□LAN1 □LAN2 □LAN3 □LAN4	
	A grey out port means it has been bound.	
Apply Back Refrest		



LAN

IPv4 Configuration

The LAN menu is used to set IPv4/v6 Local Area Network settings on the DSL-G2562DG. This allows you to set the IP address settings and DHCP options for IPv4.

IPv4 Configuration

<u>IP Address:</u> The IP address of the router. <u>Subnet Mask:</u> The subnet mask of the router IP address. <u>Primary DNS Server:</u> The primary DNS server for the router and for the DHCP clients. <u>Secondary DNS Server:</u> The secondary DNS server for the router and for the DHCP clients. <u>Domain Name:</u> The domain name for the router.

Disable DHCP: If Disable DHCP is selected, then the internal DHCP server will not be active on the local LAN.

Enable DHCP Relay: Selected

Enable DHCP Server: Selected

<u>Relay IP:</u> The DHCP relay IP address to forward DHCP requests to from the local LAN. <u>Start (PC):</u> The start IP address of the DHCP pool. This will be the first address that can be assigned to a PC.

End (PC): The end IP address of the DHCP pool. This will be the last address that can be assigned to a PC.

<u>Lease Time</u>: The amount of time that a DHCP client will retain their IP address, before having to request a new one. The default is 86400 seconds (1 day).

IPv4 Configuration

IP Address:	10.0.0.2
Subnet Mask:	255.255.255.0
Primary DNS Server:	10.0.0.2
Secondary DNS Server:	
Domain Name:	localhost

\bigcirc Disable DHCP	○ Enable DHCP Relay	
Relay IP:	192.168.0.200	
Start(PC):	10.0.0.3	
End(PC):	10.0.254	
Lease Time:	1440 (minutes)	
	Edit Reserved IP Address	
Lan Port Map: 🗹 LAN1 🗹 LAN2 🗹 LAN3 🗹 LAN4		
	🗹 SSID1 🗹 SSID2 🗹 SSID3 🗹 SSID4	
	🗹 SSID5 🗹 SSID6 🗹 SSID7 🗹 SSID8	



Reserved IP Address Settings

This allows you to reserve IP addresses in the DHCP scope for IPv4.

Reserved IP Address Settings

<u>MAC Address</u>: The mac address of the machine you want to reserve the IP for. <u>IP Address</u>: The IP address to reserve with the mac address. <u>Description</u>: Enter a description for the rule.

Click **Back** to go back to the previous page, click **Add** to add the reserved IP address to the Reserved IP Addresses List, and click **Refresh** to refresh the page.

Reserved IP Address Settings

MAC Address:	
IP Address:	
Description:	



Reserved IP Addresses List

	Number	MAC Address	IP Address	Description	Action
No Rule Found!					



IPv6 Configuration

This allows you to set the IP address settings and DHCP options for IPv6. **RA Period Settings** <u>Max Period:</u> The maximum period between Router Advertisement (RA) messages. The default is 15 seconds. Min Period: The minimum period between Router Advertisement (RA) messages.

The default is 10 seconds.

M/O Flag Settings

<u>M/O Flag Mode</u>: The mode for the Managed Address Configuration Flag (M Flag) and the Other Stateful Configuration Flag (O Flag). This can be **Auto** or **Manual**. The default is **Auto**. <u>M Flag</u>: Whether to enable or disable the Managed Address Configuration Flag (M Flag). This is only available when M/O Flag Mode is set to Manual. Set this to **1** to enable the M Flag, and set it to **0** to disable it.

O Flag: Whether to enable or disable the Other Stateful Configuration Flag (O Flag).

This is only available when M/O Flag Mode is set to Manual. Set this to **1** to enable the O Flag, and set it to **0** to disable it.

<u>DHCPv6 Server</u>: Whether to enable or disable the DHCPv6 server. Tick this to enable the DHCPv6 server, or un-tick it to disable it. This default is ticked.

<u>Unique Local Prefix</u>: Whether to use a Unique Local Prefix for the private network.

Tick this to enable the Unique Local Prefix. This default is ticked.

<u>Unique Local Global ID:</u> The Unique Local Global ID to use on the private network.

This is 40-bit number and is globally unique. The default is: 11:22:33: 44:55.

Prefix: The method through which to assign a network prefix to clients on the LAN. This can be Prefix Delegation or Static.

If Static is chosen, then a prefix and prefix mask can be entered.

LAN Address Mode: The method through which to assign IP addresses to clients on the LAN. This can be SLAAC or DHCPv6.

LAN DNS Mode: The method through which to assign DNS information to clients on the LAN. This can be Obtain from WAN, DNS Proxy or Static.

DNS: The static DNS server to assign to IPv6 clients.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

IPv6 Configuration

RA Period Settings		
Max Period:	15	(Seconds)
Min Period:	10	(Seconds
M/O Flag Settings		
M/O Flag Mode:	Auto 🗸	
M Flag:	0 🗸	
O Flag:	0 🗸	
DHCPv6 Server:	Enable	
Unique Local Prefix	Enable	
Unique Local GlobalID:	11:22:33:44:55	
	Prefix Delegation O Stati	C
Prefix:	56	/ 64
LAN Address Mode:	OSLAAC	
	OHCPv6	
LAN DNS Mode:	Obtain From WAN	
	O DNS Proxy	
	○ Static	
DNS:		
Apply Refresh		



Wireless

Wireless Basic Configuration 2.4GHz

The Wireless menu is used to set 2.4 Ghz, 5 Ghz, and wireless security settings on the DSL-G2562DG. This allows you to set the wireless network settings for the 2.4 GHz band.

Wireless Basic Configuration 2.4GHz

<u>Enable Wireless</u>: Whether to use enable or disable the 2.4GHz Wi-Fi. Tick this to enable. This default is ticked.

<u>Choose SSID:</u> The SSID that you wish to modify. This can be from SSID1 to SSID4.

<u>Enable SSID</u>: Whether to use enable or disable the SSID. Tick this to enable the SSID. This default is ticked.

<u>Enable Isolation</u>: Whether to enable or disable station isolation. This prevents wireless clients on the same SSID from communicating with each other. Tick this to enable isolation. This default is un-ticked.

<u>Hide SSID</u>: Whether to hide or broadcast the SSID. Tick this to hide the SSID. This default is un-ticked.

<u>SSID</u>: The SSID name. Enter the name of the SSID as you want to be displayed in the router web interface and to clients.

<u>BSSID</u>: The Basic Service Set Identifier (BSSID) of the router. This is the MAC address of the wireless interface.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Wireless Basic Configuration 2.4GHz

Enable Wireless:	
Choose SSID:	SSID1 ¥
Enable SSID:	
Enable Isolation:	
Hide SSID:	
SSID:	dlink-956M-2.4G-95e3
Maximum Clients:	32
BSSID:	EC:AD:E0:50:95:E4

Apply

Refresh



Wireless Basic Configuration 5GHz

This allows you to set the wireless network settings for the 5 GHz band.

Wireless Basic Configuration 5GHz

<u>Enable Wireless</u>: Whether to use enable or disable the 2.4GHz Wi-Fi. Tick this to enable wireless. This default is ticked.

<u>Choose SSID:</u> The SSID that you wish to modify. This can be from SSID5 to SSID8.

<u>Enable SSID</u>: Whether to use enable or disable the SSID. Tick this to enable the SSID. This default is ticked.

<u>Enable Isolation</u>: Whether to use enable or disable station isolation. This prevents wireless clients on the same SSID from communicating with each other.

Tick this to enable. This default is un-ticked.

<u>Hide SSID</u>: Whether to hide or broadcast the SSID. Tick this to hide the SSID. This default is un-ticked.

<u>SSID</u>: The SSID name. Enter the name of the SSID as you want it to be displayed in the router web interface and to clients.

<u>Maximum Clients</u>: The maximum clients that can join the wireless network. The default is 32.

<u>BSSID</u>: The Basic Service Set Identifier (BSSID) of the router. This is the MAC address of the wireless interface.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Wireless Basic Configuration 5GHz

Apply

Refresh

Enable Wireless:	~
Choose SSID:	SSID5 V
Enable SSID:	~
Enable Isolation:	
Hide SSID:	
SSID:	dlink-956M-5.8G-95e3
Maximum Clients:	32
BSSID:	EC:AD:E0:50:95:E5



Wireless Security Setting Choose SSID: SSID1 V Authentication: WPA-PSK/WPA2-PSK MIXED This allows you to set the security settings for the wireless network. WPA Preshare key: Wireless Security Setting Encryption Mode: AES × Choose SSID: The SSID that you wish to modify. This can be from SSID1 to SSID8. SSID 1-4 is for 2.4GHz and SSID 5-8 is for 5GHz. Authentication: The authentication type to use with the SSID. WEP This can be None, WEP, WPA-PSK, WPA2-PSK, WPA2-PSK MIXED, or 802.1X. Authentication: ¥ Choosing the WEP, WPA-PSK, WPA2-PSK, WPA-PSK/ WPA2-PSK MIXED, or 802.1X option Encryption Mode: Open 🗸 displays other options on the page, and these are documented below. Encryption Length: 64 bits(10 hex digits) V WPA Preshare key: This is the pre-shared key that clients authenticating with WPA will need 1 🗸 Key Index: to supply in order to connect to the SSID. Key1: Encryption Mode: The encryption mode for the SSID. This can be **AES**, **TKIP** or **TKIP+AES**. Key2: Authentication: WEP Encryption Mode: The encryption mode for the SSID. This can be **Open**, Key3: Share, or Both. Key4: Encryption Length: The length of the encryption key for the SSID. This can be 4 bits (10 hex digits) or 128 bits (26 hex digits). SSID1 ¥ Choose SSID: Key Index: The default key to use for authentication. The keys are numbered 1 to 4 Authentication: 8021X and are listed below. Radius Server Address Key1: Authentication key 1. The SSID simultaneously supports up to 4 keys. Key2: Authentication key 2. The SSID simultaneously supports up to 4 keys. Radius Server Port Key3: Authentication key 3. The SSID simultaneously supports up to 4 keys. Radius Server Key Key4: Authentication key 4. The SSID simultaneously supports up to 4 keys. Authentication: 802.1X Refresh Apply Radius Server Address: The RADIUS server IP address to use for authentication.

<u>Radius Server Address</u>: The RADIUS server IP address to use for authentication. <u>Radius Server Port</u>: The RADIUS server port to use for authentication. <u>Radius Server Key</u>: The RADIUS server key to use for authentication. Click **Apply** to apply the settings and click **Refresh** to refresh the page.



Advanced Setup

WAN

xDSL Configuration

Here you can configure the different types of DSL connection.

Note: Any changes here can have an effect on your DSL connection. Please consult with your Internet Service Provider before making any changes.

WAN - Ethernet Mode Configuration

This allows you to set Ethernet settings for the WAN connection.

Port: The port name. This will usually be set to ETH (Ethernet).

<u>Status:</u> The status of the port. This will be **Up** if the link is up, or **Down** if the link is down or disconnected.

Speed: The speed of the port. This can be Auto, 10Mbp/s, 100Mbp/s, or 1000Mbp/s.

Duplex: The duplex of the port. This can be Auto, Half Duplex or Full Duplex. The duplex depends on the speed chosen.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

WAN - xDSL Configuration

G.DMT	
G.992.1_Annex_A:	
G.992.1_Annex_B:	
G.lite	
G.992.2:	
T.413	
T1.413:	
ADSL2	

WAN - Ethernet Mode Configuration

Port	Status	Speed	Duplex	
ETH	Up	Auto 🗸	Auto 🗸	
Apply Re	efresh			



LAN

The WAN menu is used to set advanced LAN settings on the DSL-G2562DG.

LAN - Ethernet Mode Configuration

This allows you to set Ethernet settings for the LAN connections.

Port: The port name. This will usually be set to LAN1 to LAN4.

<u>Status:</u> The status of the port. This will be **Up** if the link is up, or **Down** if the link is down or disconnected.

<u>Speed:</u> The speed of the port. This can be **Auto**, **10Mbp/s**, **100Mbp/s**, Or **1000Mbp/s**.

<u>Duplex</u>: The duplex of the port. This can be Auto, Half Duplex or Full Duplex. The duplex depends on the speed chosen.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

LAN - Ethernet Mode Configuration

Port	Status	Speed	Duplex
LAN1	Down	Auto 🗸	Auto 🗸
LAN2	Down	Auto 🗸	Auto 🗸
LAN3	Up	Auto 🗸	Auto 🗸
LAN4	Down	Auto 🗸	Auto 🗸

pply Refresh



Wireless

The WAN menu is used to set advanced wireless settings on the DSL-G2562DG.

Wireless Advanced Configuration 2.4GHz

This allows you to set wireless settings for the 2.4 GHz wireless band.

Wireless Advanced Configuration 2.4GHz

<u>Mode:</u> The wireless mode. This can be **802.11b**, **802.11g**, **802.11b/g**, **802.11n**, **802.11n/g**, or **802.11b/g/n**.

Choosing the **802.11n**, **802.11n/g**, **802.11b/g/n** option displays other options on the page, and these are documented below.

Rate: The rate at which to transmit and receive on. This can be Auto, 1 Mbps, 2 Mbps, 5.5

Mbps, 11 Mbps, 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54

Mbps, MCS0, MCS1, MCS2, MCS3, MCS4, MCS5, MCS6, MCS7, MCS8, MCS9, MCS10,

MCS11, MCS12, MCS13, MCS14, or MCS15. The default is Auto.

<u>Rx Chain Power Save</u>: The RX Chain Power Save feature turns one of the receive chains off to save power.

TX Power: The transmit power of the wireless radio.

This can be 100%, 80%, 50%, 30%, or 10%. The default is 100%.

Choose Country: Default is set to ZA

<u>Channel:</u> The channel to operate on. This can be Auto, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12,

or 13. The default is Auto.

<u>Current Channel</u>: This displays the current channel that the wireless radio is operating on.

Auto Channel Timer: Specifies the time interval (in hours) of auto channelling.

Wireless Advanced Configuration 2.4GHz

Mode:	802.11b/g/n 🗙	
Bandwidth:	20/40 🗸 MHz	
OBSS Coexistence:	Enable 🗸	
Rate:	Auto 🗸	
Rx Chain Power Save:	Disable V	
TX Power:	100% 🗸	
Choose Country:	ZA 🗸	
Channel:	Auto 🗸	
Current Channel:	12	
Auto Channel Timer:	1	Hour



<u>Beacon Interval</u>: The interval between SSID beacon broadcasts. The default is 100.

<u>RTS Threshold:</u> The Request to Send (RTS) packet size threshold. The default is 2347. <u>Fragment Threshold:</u> The maximum packet size a client can send. The default is 2346. <u>DTIM Interval:</u> The interval between Delivery Traffic Indication Messages (DTIM). The default is 1.

<u>Short GI (Guard Interval)</u>: Whether to enable or disable the short Guard Interval (GI). Tick this to enable the short GI. The default is ticked.

<u>WMM</u>: Whether to enable or disable Wi-Fi Multimedia (WMM). Tick this to enable WMM. The default is un-ticked.

<u>WMM APSD</u>: Whether to enable or disable WMM Automatic Power Save Delivery (APSD). Tick this to enable WMM. The default is un-ticked.

Mode: 802.11n, 802.11n/g, 802.11b/g/n

<u>Bandwidth:</u> The size of the frequency ranges to transmit and receive on.

This can be 20 MHz, 40 MHz, or 20/40 MHz The default is 20/40 MHz

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Beacon Interval:	100
RTS Threshold:	2347
Fragment Threshold:	2346
DTIM Interval:	1
Short GI(Guard Interval):	
WMM:	
WMM APSD:	

Apply Refresh



Wireless Advanced Configuration 5GHz

This allows you to set wireless settings for the 5 GHz wireless band.

Wireless Advanced Configuration 5GHz
<u>Mode:</u> The wireless mode. This can be 802.11a/n/ac , 802.11ac, 802.11n , or 802.11a .
Choosing the 802.11a/n/ac, 802.11ac , or 802.11n option displays other options on the
page, and these are documented below.
Rate: The rate at which to transmit and receive on. This can be Auto, MCS0, MCS1, MCS2,
MCS3, MCS4, MCS5, MCS6, MCS7, MCS8, MCS9, MCS10, MCS11, MCS12, MCS13, MCS14,
MCS15, or MCS32. The default is Auto.
Rx Chain Power Save: The RX Chain Power Save feature turns one of the receive chains off
to save power.
<u>TX Power:</u> The transmit power of the wireless radio. This can be 100%, 80%, 50%, 30%, or
10% . The default is 100% .
Choose Country: Default is ZA
Channel: The channel to operate on. This can be Auto, 52, 56, 60, 64, 149, 153,
157, 161, or 165. The default is Auto.
<u>Current Channel:</u> This displays the current channel that the wireless radio is operating on.

Wireless Advanced Configuration 5GHz

Mode:	802.11a/n/ac 🗸
Bandwidth:	80 🗸 MHz
Rate:	Auto 🗸
Rx Chain Power Save:	Disable 🗸
TX Power:	100% 🗸
Choose Country:	ZA 🗸
Channel:	Auto 🗸
Current Channel:	52
Auto Channel Timer:	1 Hour



Beacon Interval: The interval between SSID beacon broadcasts. The default is 100.

RTS Threshold: The Request to Send (RTS) packet size threshold. The default is 2347.

<u>Fragment Threshold:</u> The maximum size of packet a client can send. The default is 2346. DTIM Interval: The interval between Delivery Traffic Indication Messages (DTIM).

The default is 1.

<u>Short GI (Guard Interval)</u>: Whether to enable or disable the short Guard Interval (GI). Tick this to enable the short GI. The default is ticked.

<u>WMM</u>: Whether to enable or disable Wi-Fi Multimedia (WMM). Tick this to enable WMM. The default is un-ticked.

<u>WMM APSD</u>: Whether to enable or disable WMM Automatic Power Save Delivery (APSD). Tick this to enable WMM. The default is un-ticked.

<u>Mode:</u> 802.11a/n/ac, 802.11ac

Bandwidth: The size of the frequency ranges to transmit and receive on.

This can be 20 MHz, 20/40 MHz, or 80 MHz The default is 80 MHz

<u>Mode:</u> 802.11n

<u>Bandwidth:</u> The size of the frequency ranges to transmit and receive on. This can be **20 MHz** or **20/40 MHz** The default is **20/40 MHz**

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Beacon Interval:	100
RTS Threshold:	2347
Fragment Threshold:	2346
DTIM Interval:	1
Short GI(Guard Interval):	
WMM:	
WMM APSD:	



Wireless MAC Filter

Wireless MAC filter will allow you to block or allow certain devices on your Wi-Fi.	Wireless MAC	Filter
	Select SSID:	dlink-956M-2.4G-95e3 ✔
Select SSID: Select the SSID you for the rule	MAC Restrict Mode:	Oisabled \bigcirc Allow \bigcirc Deny
MAC Restrict Mode: Allow or Deny. Disabled is selected by default.		
	Wireless MA	C Filter
To add a Mac Address, click the Add button.	Wireless MA	dlink-956M-2.4G-95e3 ❤

Note: Before selecting Allow or Deny, you will need to add the Mac address first otherwise you will lock yourself out of the Selected SSID.



WPS Settings 2.4GHz

This allows you to set Wi-Fi Protected Setup (WPS) settings for the 2.4 GHz wireless band.

WPS Settings 2.4GHz

<u>Enable WPS</u>: Whether to enable or disable WPS for the 2.4 GHz wireless band. Tick this to enable WPS. The default is ticked. Choosing this option displays other options on the page, and these are documented below.

<u>Choose AP Role</u>: The WPS AP role. This can be **Registrar** or **Enrolee**. Choose Registrar for the router to act as the WPS server, and choose Enrolee for the router to act as the WPS client. Choosing these options displays other options on the page, and these are documented below. <u>Press WPS Button</u>: Press the physical WPS button on the router or the PBC button to initiate the WPS procedure.

Input PIN Number: The PIN required to join the wireless network.

Negotiation Status: The status of the WPS process.

Choose AP Role: Enrolee

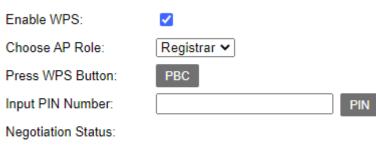
<u>Current PIN</u>: The PIN required to join the wireless network. Click **Generate New PIN** to generate a new PIN. <u>Session Status</u>: The status of the WPS process.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

WPS Settings 2.4GHz

Refresh

Apply





VAP (Virtual Access Point) Information

<u>WPS Status:</u> A status of **Configured** indicates WPS is enabled.

SSID: The name of the SSID.

<u>Authentication Mode:</u> The authentication type to use with the SSID. This can be **None**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-PSK/WPA2-PSK MIXED**, or **802.1X**. Choosing the **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-PSK/WPA2-PSK MIXED**, or **802.1X** option displays other options on the page, and these are documented below. <u>Encryption Mode:</u> The encryption mode for the SSID. This can be **AES**, **TKIP** or **TKIP+AES**.

Click Reset OOB to reset the Out of Band (OOB) access method for the router.

WPS Settings 5GHz

This allows you to set Wi-Fi Protected Setup (WPS) settings for the 5 GHz wireless band.

WPS Settings 5GHz

<u>Enable WPS:</u> Whether to enable or disable WPS for the 5 GHz wireless band. Tick this to enable WPS. The default is ticked. Choosing this option displays other options on the page, and these are documented below.

<u>Choose AP Role</u>: The WPS AP role. This can be **Registrar** or **Enrolee**. Choose Registrar for the router to act as the WPS server, and choose Enrolee for the router to act as the WPS client. Choosing these options displays other options on the page, and these are documented below.

Choose AP Role: Registrar

<u>Press WPS Button</u>: Press the physical WPS button on the router or the PBC button to initiate the WPS procedure.

<u>Input PIN Number</u>: The PIN required to join the wireless network. Negotiation Status: The status of the WPS process.

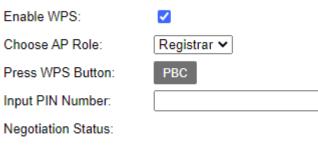
<u>Choose AP Role</u>: Enrolee <u>Current PIN</u>: The PIN required to join the wireless network. Click **Generate New PIN** to generate a new PIN. <u>Session Status</u>: The status of the WPS process. Click **Apply** to apply the settings and click **Refresh** to refresh the page.

VAP Information

WPS Status:	Configured
SSID:	dlink-956M-2.4G-95e3
Authentication Mode:	WPA-PSK/WPA2-PSK
Encryption Mode:	AES
WPA Key:	abvsp92359

Reset OOB

WPS Settings 5GHz





PIN



VAP (Virtual Access Point) Information

WPS Status: A status of **Configured** indicates WPS is enabled.

SSID: The name of the SSID.

Authentication Mode: The authentication type to use with the SSID. This can be **None**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-PSK/WPA2-PSK MIXED**, or **802.1X**. Choosing the **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-PSK/ WPA2-PSK MIXED**, or **802.1X** option displays other options on the page, and these are documented below. Encryption Mode: The encryption mode for the SSID. This can be **AES**, **TKIP** or **TKIP+AES**.

Click Reset OOB to reset the Out of Band (OOB) access method for the router.

WDS Settings

This allows you to set Wireless Distribution System (WDS) settings for the 2.4GHz and 5 GHz wireless bands.

WDS Settings

<u>Wireless Mode:</u> The wireless mode to enable WDS for. This can be **2.4G** or **5G**. <u>WDS Mode:</u> The WDS mode. This can be **Disabled**, **Lazy Mode**, **Repeater Mode**, **Bridge Mode**. The default is **Disabled**.

Choosing the Lazy Mode, Repeater Mode, or Bridge Mode option displays other options on the page, and these are documented below.

WDS Mode: Lazy Mode

<u>WDS Security:</u> The WDS security type. This can be **None**, **WEP**, **TKIP** or **AES**. Choosing the **WEP**, **TKIP** or **AES** option displays other options on the page, and these are documented below.

<u>WDS Mode</u>: Repeater Mode or Bridge Mode <u>AP1 MAC Address</u>: The MAC address of AP 1 in the WDS. <u>AP2 MAC Address</u>: The MAC address of AP 2 in the WDS. <u>AP3 MAC Address</u>: The MAC address of AP 3 in the WDS.

WDS Settings Wireless Mode: 2.4G 🗸 WDS Mode: Disabled ~ Refresh Apply Scan SSID BSSID Channel Signal(%) Security Wireless Mode Action Scan

VAP Information

WPS Status:	Configured
SSID:	dlink-956M-5.8G-95e3
Authentication Mode:	WPA-PSK/WPA2-PSK
Encryption Mode:	AES
WPA Key:	abvsp92359

Reset OOB



<u>AP4 MAC Address</u>: The MAC address of AP 4 in the WDS. <u>WDS Security</u>: The WDS security type. This can be **None**, **WEP**, **TKIP** or **AES**. Choosing the **WEP**, **TKIP** or **AES** option displays other options on the page, and these are documented below. <u>WDS Key</u>: The wireless key to use with WDS. For WEP, this can be 5 or 13 characters, or for TKIP and AES, it is 8 to 63 characters.

Click **Apply** to apply the settings and click **Refresh** to refresh the page. Click **Scan** to scan for wireless APs in the area to join to the WDS.

Channel Information

This allows you to scan the local area for wireless networks. Click **Scan** to scan for wireless APs in the area.

Scan	

SSID	BSSID	Channel	Signal(%)	Security	Wireless Mode

Scan



NAT

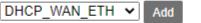
The Network Address Translation (NAT) menu is used to set advanced NAT settings on the DSL-G2562DG.

Virtual Server

This allows you to set up NAT rules on the DSL-G2562DG. Virtual Server WAN Connection: The WAN connection to apply the NAT rules to.

Virtual Server

WAN Connection:



Number	Enable	Description	Remote IP Address	Protocol	External Port	Internal Port	Internal IP Address	NAT Loopback	Action
No Rule F	ound!								

Click Add to add a NAT rule to the WAN connection.

Virtual Server Settings

This allows you to enable and disable NAT rules on the DSL-G2562DG.

Enable: Whether to enable or disable the NAT rule. Tick this to enable the

NAT rule. The default is un-ticked.

<u>Description</u>: The description for the NAT rule.

<u>Remote IP Address</u>: The source address for the NAT rule. Leave this blank to accept any addresses.

<u>Network Mask:</u> The network mask for the NAT rule. Leave this blank to accept any network mask.

<u>Protocol</u>: The protocol for the NAT rule. This can be **TCP**, **UDP** or **TCP/UDP**. <u>External Port</u>: The external port to NAT to/from. This can be a range or a single port.

Virtual Server Settings

Enable:			
Description:			
Remote IP Address:	0.0.0.0		
Network Mask:	0.0.0.0		
Protocol:	TCP 🗸		
External Port:		-[
Internal Port:		-[
Internal IP Address:			
NAT Loopback:			
Back Apply Refree	sh		



Internal Port: The internal port to NAT to/from.

Internal IP Address: The internal IP address for the NAT rule.

<u>NAT Loopback</u>: Permits the access of a service via the public IP address from inside the local network.

Tick to enable.

Click **Back** to go back to the previous page, click **Apply** to apply the settings and click **Refresh** to refresh the page.



Port Triggering

This allows you to set up port triggering rules on the DSL-G2562DG.

Port Triggering WAN Connection: The WAN connection to apply the port triggering rules to.

Port Triggering

WAN Connection: DHCP_WAN_ETH V Add

 Number
 Name
 Interface
 Protocol
 Start Port
 End Port
 Open Start Port
 Open End Port
 Enable
 Action

 No Rule Found!

 <

Click **Add** to add a port triggering rule to the WAN connection.

Port Triggering Setting

This allows you to set up automatic port triggering rules on the DSL-G2562DG.

<u>Enable</u>: Whether to enable or disable the port triggering rule. Tick this to enable the port triggering rule. The default is un-ticked.

<u>Triggering Type:</u> The port triggering type. Choose **Customization** to enter custom ports, or choose **Application** to use pre-set ports for an application. Choose the pre-set

application from the **Choose...** drop-down menu.

<u>Protocol</u>: The protocol for the port triggering rule. This can be **TCP**, **UDP** or T**CP/UDP**.

Name: The name for the port triggering rule.

<u>Start Port:</u> The start port for the port triggering rule.

End Port: The end port for the port triggering rule.

<u>Open Start Port</u>: The start port to open for the port triggering rule.

<u>Open End Port:</u> The end port to open for the port triggering rule.

Click **Back** to go back to the previous page, click **Apply** to apply the settings and click **Refresh** to refresh the page.

Port Triggering Setting

Back

Apply

Refresh

Enable:		
Triggering Type:	Customization O Application Choose	\sim
Protocol:	TCP 🗸	
Name:		
Start Port:		
End Port:		
Open Start Port:		
Open End Port:		



Multi-NAT

This allows you to set up one-to-one and many-to-one NAT rules on the DSL-G2562DG.

Multi-NAT

Number	Interface	Туре	Local Start IP	Local End IP	Public IP	Enable	Action
No Rule Found	ļ!						

Click **Add** to add a multi-NAT rule to the WAN connection.

Multi-NAT Edit

This allows you to set up one-to-one and many-to-one NAT rules on the DSL-G2562DG.

Multi-NAT Edit

Enable: Whether to enable or disable the multi-NAT rule. Tick this to enable the multi-NAT rule. The default is ticked. WAN Connection: The WAN connection to apply the multi-NAT rules to. Type: The multi-NAT rule type. This can be **One-to-One** or **Many-to-One**, and allows either one private IP to be mapped to one public IP, or multiple private IPs to be mapped to a single public IP. Choosing the **many-to-one** option displays other options on the page, and these are documented below. Local Start IP: The start IP address for the multi-NAT rule. Public IP: The public IP address for the multi-NAT rule.

Type: Many-to-One

Local End IP: The end IP address for the multi-NAT rule.

Click **Back** to go back to the previous page, click **Apply** to apply the settings and click **Refresh** to refresh the page.

Multi-NAT Edit

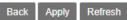
Type:

Type:

Local Start IP:

Local End IP: Public IP

Enable: ~ DHCP WAN ETH 🗸 WAN Connection: One-to-One V Local Start IP: Public IP:



G	lar	nv-te	 	v

ų	interity to one
ſ	
L	
Y	
ċ	
L	
ι	
ſ	
L	



DMZ Settings

This allows you to set up a De-Militarized Zone (DMZ) on the DSL-G2562DG.

DMZ Settings <u>Enable DMZ</u>: Whether to enable or disable the DMZ. Tick this to enable the DMZ. <u>WAN Connection</u>: The WAN connection to apply the multi-NAT rules to. <u>DMZ Host IP Address</u>: The host IP address on the local network to put into the DMZ.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

ALG Settings

This allows you to set the Application Level Gateway (ALG) options on the DSL-G2562DG.

ALG Settings

TFTP Pass-through: Whether to enable or disable TFTP pass-through. FTP Pass-through: Whether to enable or disable FTP pass-through. PPTP Pass-through: Whether to enable or disable PPTP pass-through. RTSP Pass-through: Whether to enable or disable RTSP pass-through. L2TP Pass-through: Whether to enable or disable L2TP pass-through. H323 Pass-through: Whether to enable or disable H323 pass-through. SIP Pass-through: Whether to enable or disable SIP pass-through. IPSEC Pass-through: Whether to enable or disable IPsec pass-through.

All the above settings can be ticked to enable, and un-ticked to disable. By default, all options are enabled

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

DMZ Settings	
Enable DMZ:	
WAN Connection:	DHCP_WAN_ETH V
DMZ Host IP Address:	
Apply Refresh	

ALG Settings

Enable

TFTP Passthrough:	✓
FTP Passthrough:	✓
PPTP Passthrough:	✓
RTSP Passthrough:	✓
L2TP Passthrough:	✓
H323 Passthrough:	✓
SIP Passthrough:	✓
IPSEC Passthrough:	~





Security

The security menu is used to set advanced security settings on the DSL-G2562DG.

IP Filtering

This allows you to set up packet-filtering rules.

IP Filtering

<u>Firewall Enable</u>: Whether to enable or disable packet filtering. Tick this to enable packet filtering. The default is ticked. <u>WAN > LAN</u>: Whether to add a whitelist or blacklist rule. Choose **Whitelist** or **Blacklist** and click Add to add a new rule. This is in the inbound direction.

<u>LAN > WAN:</u> Whether to add a whitelist or blacklist rule. Choose **Whitelist** or **Blacklist** and click Add to add a new rule. This is in the outbound direction.

Click Apply to apply the settings and click Refresh to refresh the page.

IP Filtering

Refresh

Note: when the firewall is enabled on a WAN interface, all incoming IP traffic is BLOCKED. However some IP traffic can be ACCEPTED by setting up filters. WAN→LAN Add Number Enable IP Range/Port Range(Source) IP Range/Port Range(Destination) Protocol Description Device Name Action No Rule Found! Note: by default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters. LAN→WAN Add Number Enable IP Range/Port Range(Source) IP Range/Port Range(Destination) Protocol Description Device Name Action No Rule Found!



Port Filter Rule Settings

This allows you to add packet-filtering rules on the DSL-G2562DG.

Port Filter Rule Settings

IP Version: The IP version to match with the rule. This can be IPv4 or IPv6. Connection: The WAN connection to use with the packet filtering rule. Description: The description to use for the packet filtering rule. Enable: Whether to enable or disable the packet filtering rule. Tick this to enable the packet filtering rule. The default is un-ticked. Protocol: The protocol to use for the packet filtering rule. This can be ALL, TCP, UDP, ICMP or TCP/UDP. Source IP: The source IP to use for the packet filtering rule. Source Port: The source port to use for the packet filtering rule. Destination IP: The destination IP to use for the packet filtering rule. Destination Port: The destination port to use for the packet filtering rule.

Click **Back** to go back to the previous page, click **Apply** to apply the settings and click **Refresh** to refresh the page.

MAC Filter

This allows you to set up MAC-filtering rules on the DSL-G2562DG. **MAC** Filter

Enable: Whether to enable or disable MAC filtering. Tick this to enable MAC filtering. The default is un-ticked.

Filter Mode: Whether to permit (whitelist) or deny (blacklist) MAC addresses as part of the MAC filter rule. This can be Whitelist or Blacklist.

MAC List

MAC Address: The MAC address to add to the MAC filtering rule. Click Add to add the rule.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Port Filter Rule Settings ID-4 at IP Version

IP version.	1PV4 V
Connection:	- v (only firewall enabled WAN connections and
connection.	available.)
Description:	
Enable:	
Protocol:	ALL 🗸
Source IP:	-
Source Port:	-
Destination IP:	-
Destination Port:	-
Back Apply F	Refresh

MAC Filter		
Enable:		
Filter Mode:	● Blacklist ○ Whitelist	
Apply Refresh		
MAC List		
MAC Address:	Add	
Input MAC address to a Whitelist means that onl Blacklist means that the	elect whitelist or blacklist,click "apply" to dd a rule in MAC list box, click "add" to s y the current MAC address can be permi current MAC address can not be permit cxxxxxxxxxxx(x=0~f,hex).	ubmit. it to login CPE and access interne
Number	MAC Address	Action
No Rule Found		



DDoS Protection

This allows you to set up Denial of Service (DoS) prevention rules on the DSL-G2562DG.

Attack Protection Settings

<u>Enable</u>: Whether to enable or disable attack protection. Tick this to enable attack protection. The default is ticked. <u>Attack Logs</u>: Whether to enable or disable attack logs. Tick this to enable attack logs. The default is un-ticked.

Individual Protection Settings

<u>Prevent SYN Flood:</u> Whether to enable or disable Prevent SYN Flood protection. <u>Peak SYN Number:</u> The peak number of TCP SYN packets that can be received per second. The default is **30**.

Drop Broadcast ICMP Echo Request: Whether to enable or disable Drop Broadcast ICMP Echo Request protection.

Fraggle Attack Protection: Whether to enable or disable Fraggle Attack protection.

Echo Chargen Attack Protection: Whether to enable or disable Echo Chargen Attack protection.

IP Land Attack Protection: Whether to enable or disable IP Land Attack protection.

Port Scan Attack Protection: Whether to enable or disable attack protection

All the above settings can be ticked to enable, and un-ticked to disable. By default, all options are enabled

Attack Protection Settings

Enable:	~
Attack Logs:	

Individual Protection Settings

Prevent SYN Flood:	
Peak SYN Number:	30 (number/second)
Drop Broadcast ICMP Echo Request:	
Fraggle Attack Protection:	
Echo Chargen Attack Protection:	
IP Land Attack Protection:	
Port Scan Attack Protection:	



Prevent Illegal Packets

<u>TCP Flags</u>: Set "SYN FIN": Whether to enable or disable preventing illegal packets by setting SYN FIN.

<u>TCP Flags:</u> Set "SYN RST": Whether to enable or disable preventing illegal packets by setting SYN RST.

<u>TCP Flags:</u> Set "FIN RST": Whether to enable or disable preventing illegal packets by setting FIN RST.

<u>TCP Flags</u>: Unset "ACK", Set "FIN": Whether to enable or disable preventing illegal packets by unsetting ACK and setting FIN

<u>TCP Flags:</u> Unset "ACK", Set "PSH": Whether to enable or disable preventing illegal packets by unsetting ACK and setting PSH.

<u>TCP Flags:</u> Unset "ACK", Set "URG": Whether to enable or disable preventing illegal packets by unsetting ACK and setting URG.

<u>TCP Flags</u>: Unset "SYN ACK FIN RST URG PSH": Whether to enable or disable preventing illegal packets by unsetting SYN ACK FIN RST URG PSH.

<u>TCP Flags:</u> Set "SYN ACK FIN RST URG PSH": Whether to enable or disable preventing illegal packets by setting SYN ACK FIN RST URG PSH.

<u>TCP Flags:</u> Unset "PSH", Set "SYN ACK FIN RST URG": Whether to enable or disable preventing illegal packets by unsetting PSH and setting SYN ACK FIN RST URG.

<u>TCP Flags:</u> Unset "SYN ACK RST URG PSH", Set "FIN": Whether to enable or disable preventing illegal packets by unsetting SYN ACK RST URG PSH and setting FIN.

<u>TCP Flags:</u> Unset "SYN ACK RST", Set "FIN URG PSH": Whether to enable or disable preventing illegal packets by unsetting SYN ACK RST and setting FIN URG PSH.

All the above settings can be ticked to enable, and un-ticked to disable. By default, all options are enabled

Prevent Illegal Packets

TCP Flags: Set "SYN FIN":
TCP Flags: Set "SYN RST":
TCP Flags: Set "FIN RST":
TCP Flags: Unset "ACK", Set "FIN":
TCP Flags: Unset "ACK", Set "PSH":
TCP Flags: Unset "ACK", Set "URG":
TCP Flags: Unset "SYN ACK FIN RST URG PSH":
TCP Flags: Set "SYN ACK FIN RST URG PSH":
TCP Flags: Unset "PSH", Set "SYN ACK FIN RST URG":
TCP Flags: Unset "SYN ACK RST URG PSH", Set "FIN":
TCP Flags: Unset "SYN ACK RST", Set "FIN URG PSH":

Apply Refresh

 \checkmark

 \checkmark



Parental Control

The parental control menu is used to set parental control features on the DSL-G2562DG.

Access Time Restriction

This allows you to set up access rules to block hosts from accessing the network, based on the time of day.

Access Time Restriction

<u>Enable Time Restriction:</u> Whether to enable or disable time restrictions. Tick this to enable time restrictions. The default is un-ticked.

Note: a maximum of 16 access rules can be created.

Click **Apply** to apply the settings and click **Refresh** to refresh the page. Click **Add** to add a new access time restriction rule.

Access Time Restriction Configuration

This allows you to add an access rule to block hosts from accessing the network, based on the time of day.

Access Time Restriction Configuration

User Name: Custom name of the restriction.

Mac Address: Enter the mac address which the rule will be applied to.

<u>Days of the week:</u> The days of the week to block the host for. Tick the days of the week when you want to block the host.

<u>Blocking Time:</u> The time that the host will be blocked for. This can be from **0** to **24** and from **0** to **59**. It is in the format: HH: MM.

Click **Back** to go to back to the previous page and click **Apply** to apply the settings.

Acce	ss Time Re	striction										
Enable	e Time Restrictio	n: 🗌										
Apply	Refresh											
Note:	A maximum 16	entries can be co	nfigure	ed.								
	ber User Nam		Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	Stop	Action
No R	ule Found!											
ork, bas	sed	Name: Address:]] (x	xxx	000000	cxx)	
	Days	of the week:		Sun	M	on 🗆	Tue	□w	ed [Thu	🗆 Fri	Sat
	Block	ing Time:			-			(hh:	mm)			
f the w	eek ^{Allow:} Intern	s access to the et:]								
to 24 a	nd											

Apply

Back



URL & IP Filter

This allows you to set up access rules to either block or allow access to a URL, based on the time of day.

URL & IP Filter	URL & IP Filter
<u>Enable:</u> Whether to enable or disable URL filters. Tick this to enable URL filters.	
The default is un-ticked.	Enable:
Filter Mode: The filter mode for the URL filter. This can be Blacklist or Whitelist. Choose	Blacklist to Filter Mode:
block URLs, and choose Whitelist to allow URLs.	The mode.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

URL & IP List

Note: a maximum of 16 access rules can be created.

URL & IP List

Note: A maximum 16 entries can be configured.

Number	Description:	URL Key	LAN PC IP	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	Stop	Action
No Rule F	ound!												

Click **Add** to add a new URL and IP filter rule.

Enable:	
Filter Mode:	Blacklist O Whitelist

Refresh

Apply



Access Time Restriction Configuration

This allows you to set up access rules to either block or allow access to a URL, based on the time of day.

Access Time Restriction Configuration Description: The description for the time restriction rule. Source IP: The source IP addresses for the time restriction rule. Enter a range Des of IP addresses to apply the URL filter to. LAN URL: The URL to either block or allow access to. URI Days of the week: The days of the week to block the host for. Tick the days of Day the week when you want to block the URL. Blog Blocking Time: The time that the URL will be blocked for. This can be from 0 to 24 and from 0 to 59. It is in the format: HH: MM.

Click **Back** to go to back to the previous page and click **Apply** to apply the settings.

Access Time Restriction Configuration

This page adds time of day restriction to access some URL for a special LAN device connected to the Router.

scription:	
N PC IP:	-
L Key:	(http:// and https:// in key will be ignored)
/s of the week:	□Sun □Mon □Tue □Wed □Thu □Fri □Sat
cking Time:	(hh:mm)



Routing

The routing menu is used to set routing information on the DSL-G2562DG.

Static Route

This allows you to set up static routes to define how to route traffic for remote networks.

Click **Add** to add a new static route.

	Destination Subnet	maan	Gateway	Metrics	туре	Error Message	Action
No Rule Found!							
Rule Found!							

Static Route Setting

This allows you to set up static routes to define how to route traffic for remote networks.

Static Doute



Static Route Setting

<u>Connection Name</u>: The connection name for the static route.

Choosing the LAN option displays other options on the page, and these are documented below.

<u>Enable</u>: Whether to enable or disable the static route. Tick this to enable the static route. The default is un-ticked.

Destination

Subnet: The destination network to route traffic for.

Subnet Mask: The destination subnet mask to route traffic for.

<u>Gateway:</u> The router address to route traffic to for the route.

<u>Metrics</u>: The metric to associate with the route. This is used to prefer one route over another.

Connection Name: LAN

<u>Gateway:</u> The router address to route traffic to for the route.

Click **Back** to go back to the previous page, click **Apply** to apply the settings and

click **Refresh** to refresh the page.

Static Route Setting

Connection Name:	~
Enable:	
Destination Subnet:	
Subnet Mask:	
Gateway:	
Metrics:	

Back Apply Refresh



Dynamic Route

This allows you to set up dynamic routes to define how to route traffic for remote networks.

Click Add to add a new dynamic route.

Dynamic Route Setting

This allows you to set up dynamic routes to define how to route traffic for remote networks.

Dynamic Route Setting

<u>Connection Name</u>: The connection name for the static route. <u>Enable</u>: Whether to enable or disable dynamic routing. Tick this to enable dynamic routing. <u>Protocol</u>: The dynamic routing protocol. This can be **RIPv1**, **RIPv2**, **OSPF**, or **BGP**. Choosing the **RIPv1**, **RIPv2**, or **BGP** option displays other options on the page, and these are documented below.

Click **Back** to go back to the previous page, click **Apply** to apply the settings and click **Refresh** to refresh the page.

IPv6 Static Route

This allows you to set up static IPv6 routes to define how to route traffic for remote networks.

Click Add to add a new static route.

Static Route

Add

Number	Status	Destination Address	Mask	Gateway	Metrics	Туре	Error Message	Action
No Rule F	ound!							

Dynamic Route

Number	Status	Protocol	Interface	Action
No Rule Found!				



Dynamic Route Setting

Connection Name:	LAN 🗸
Enable:	
Protocol:	RIPv1 🗸
RIP Passive:	
Back Apply Refr	esh



IPv6 Static Route Setting

This allows you to set up static IPv6 routes to define how to route traffic for remote networks.

Static Route Setting

<u>Connection Name</u>: The connection name for the static route.
<u>Enable</u>: Whether to enable or disable the static route. Tick this to enable the static route.
The default is un-ticked.
<u>Destination Address</u>: The destination network to route traffic for.
<u>Subnet Prefix Length</u>: The destination prefix length to route traffic for.
<u>Gateway</u>: The router address to route traffic to for the route.
<u>Metrics</u>: The metric to associate with the route. This is used to prefer one route over another.
Click **Back** to go back to the previous page, click **Apply** to apply the settings and click **Refresh** to refresh the page.

IPv6 Dynamic Route

This allows you to set up dynamic IPv6 routes to define how to route traffic for remote networks.

Dynamic Route

<u>Port:</u> Whether to enable or disable the dynamic routing on a port. Tick this to enable dynamic routing on the port. The default is un-ticked. Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Static Route Setting

Connection Name:	LAN 🗸
Enable:	
Destination Address:	
Subnet Prefix Length:	
Gateway:	
Metrics:	

Back Apply Refresh

Dynamic Route







Quality of Service

The Quality of Service (QoS) menu is used to set QoS information for traffic passing through the DSL-G2562DG.

QoS Queue

This allows you to set QoS information based on traffic type.

QoS Global Settings

<u>Enable QoS Profile</u>: The QoS profile to enable. Choose one of the pre-configured profiles or select **Custom Profile** to create a new profile.

Note: Changing the profile will affect all QoS settings.

Enable: Whether to enable or disable the QoS settings.

Tick this to enable the QoS settings. The default is un-ticked.

Upstream Bandwidth: The maximum upstream bandwidth from the router.

Enter **0** to not limit the upstream bandwidth.

Scheduling Policy: The scheduling policy for prioritizing traffic. This can be Strict Priority

(SP), Committed Access Rate (CAR), or Weighted Fair Queuing (WFQ).

Choosing these options displays other options on the page. These are shown below.

Enable Force Bandwidth: Whether to enable or disable Force Bandwidth.

Tick this to enable Force Bandwidth. The default is un-ticked.

<u>DSCP/TC Mark:</u> Whether to enable or disable the Differentiated Services Code Point (DSCP)/Traffic Class (TC) mark. Tick this to enable the DSCP/TC mark. The default is un-ticked.

<u>802.1P Tag:</u> Whether to enable or disable the IEEE 802.1P tag. Tick this to enable the 802.1P tag. The default is un-ticked.

QoS Global Settings

IPTV,INTERNET V (Changing profile will affect all QoS settings) Enable QoS Profile: Enable: 0 Upstream Bandwidth Kbps (0 means no rate limit) Scheduling Policy: SP 🗸 Enable Force Bandwidth: DSCP/TC Mark: \Box 802.1P Tag: TCP Connection Number Limit:

Upstream Queue Settings

Number	Enable	Priority(1 is the highest)
1		1
2		2
3		3
4		4
5		5
6		6
7		7
8		8



<u>TCP Connection Number Limit:</u> Whether to enable or disable the TCP connection number limit.
Tick this to enable the TCP connection number limit. The default is un-ticked.
Choosing this options displays other options on the page, and these are documented below.
<u>Scheduling Policy:</u> SP
<u>Number:</u> The QoS level for the Strict Priority (SP) scheduling method.
<u>Enable:</u> Whether to enable or disable the level for the SP scheduling method.
Tick this to enable the level for the SP scheduling method.
<u>Priority (1 is the highest):</u> The priority for each QoS level.
<u>Scheduling Policy:</u> CAR
<u>Number:</u> The QoS level for the Committed Access

Rate (CAR) scheduling method.

Enable: Whether to enable or disable the level for the CAR scheduling method. Tick this to enable the level for the CAR scheduling method. <u>Guaranteed Bandwidth (kbps):</u> The guaranteed bandwidth in kbps for each QoS level. <u>Scheduling Policy</u>: WFQ Number: The QoS level for the Weighted Fair Queuing

(WFQ) scheduling method.

<u>Enable</u>: Whether to enable or disable the level for the WFQ scheduling method.
Tick this to enable the level for the WFQ scheduling method.
<u>Percent (%)</u>: The percentage of the bandwidth for each QoS level.
<u>TCP Connection Number Limit</u>: Ticked
<u>Limit Mode</u>: The limit mode for the QoS profile. This can be **Percent Mode** or **Number Mode**. Enter the value for each mode in the box to the right.

Click Apply to apply the settings and click Refresh to refresh the page.



Classification List

This allows you to classify traffic based on the traffic type.

Classification List

Number	Enable	Traffic Type	Mark	Queue	Action
No Rule Found!					
Add Traffic Type					
Number	Enable	Classification Rules		Mark	Queue
No Rule Found!					

Add Flow

Click Add Traffic Type to add a traffic type and click Add Flow to add a traffic flow.



Classification Traffic Base

This allows you to classify traffic based on the traffic type.

Classification Traffic Base

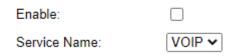
<u>Enable</u>: Whether to enable or disable the traffic base. Tick this to enable the traffic base. <u>Service Name</u>: The service name for the traffic base.

Classification Match Result

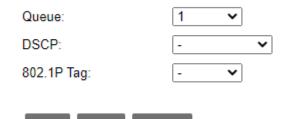
<u>Queue:</u> The queue number for the match result. <u>DSCP:</u> The DSCP value for the match result. This can be **Default**, **AF11(001010)**, **AF12(001100)**, **AF13(001110)**, **AF21(010010)**, **AF22(010100)**, **AF23(010110)**, **AF31(011010)**, **AF32(011100)**, **AF33(011110)**, **AF41(100010)**, **AF42(100100)**, **AF43(100110)**, **CS1(001000)**, **CS2(010000)**, **CS3(011000)**, **CS4(100000)**, **CS5(101000)**, **CS6(110000)**, **CS7(111000)**, or **EF (101110)**. 802.1P Tag: The 802.1P tag for the match result. This can be **0**, **1**, **2**, **3**, **4**, **5**, **6**, or **7**.

Click **Back** to go back to the previous page, click **Apply** to apply the settings and click **Refresh** to refresh the page.

Classification Traffic Base



Classification Match Result



Refresh

Back

Apply



Classification Traffic Base Settings

Here you can set the different mac address to interface for the QoS to use as well as the DSCP, IP Protocol and 802.1P.

IP Version: Select IPv4 or IPv6	Classification Traf	fic Base	
<u>LAN interface:</u> Choose LAN1 – LAN4			
WAN Connection: Choose the WAN connection to use	IP Version:	IPv4 🗸	
Source MAC: enter the Mac address connected to the LAN interface	LAN Interface:	LAN4 🗸	
Destination MAC: enter the Destination MAC address	WAN Connection:	PPPoE_	
<u>VLAN</u> : enter the VLAN for the QoS	Source MAC:		(00:22:33:aa:bb:cc)
802.1P: Select the priority from 1-7 where 7 is the highest	Destination MAC:		(00:22:33:aa:bb:cc)
Source Address: Enter the IP address connected to the LAN interface	VLAN:		
Source Mask: enter the subnet mask for the connected device	802.1P:	7 🗸	
Destination Address: Enter the destination address	Source Address:		(8.8.8.8)
Destination Mask: enter the subnet mask for the destination	Source Mask:		(255.255.255.0)
<u>DSCP:</u> The DSCP value for the match result. This can be Default ,	Destination Address:		(8.8.8.8)
AF11(001010), AF12(001100), AF13(001110), AF21(010010),	Destination Mask:		(255.255.255.0)
AF22(010100), AF23(010110), AF31(011010), AF32(011100),	DSCP:	AF42(100100) 🗸	()
AF33(011110), AF41(100010), AF42(100100), AF43(100110),			
CS1(001000), CS2(010000), CS3(011000), CS4(100000),	IP Protocol Type:		
CS5(101000), CS6(110000), CS7(111000), or EF (101110).	Source Port Range:		-
	Destination Port Range:		-

<u>IP Protocol:</u> Select the Protocol for the QoS. This can be TCP, UDP, ICMP or IGMP.

Source Port Range: Choose the port range for the rule. Works with TCP and UDP.

Destination Port Range: Enter the port range for the rule. Works with TCP and UDP Classification Match Result

<u>Queue:</u> Choose the number for the queue



<u>DSCP:</u> The DSCP value for the match result. This can be **Default**, AF11(001010), AF12(001100), AF13(001110), AF21(010010), AF22(010100), AF23(010110), AF31(011010), AF32(011100), AF33(011110), AF41(100010), AF42(100100), AF43(100110), CS1(001000), CS2(010000), CS3(011000), CS4(100000), CS5(101000), CS6(110000), CS7(111000), or EF (101110). <u>802.1P tag:</u> Select the priority from 1-7 where 7 is the highest

QoS TCP Flags

This allows you to prioritize TCP flags.

<u>Prioritize TCP Flags</u>: Whether to enable or disable prioritizing TCP flags. Tick this to enable.

Click **Apply** to apply the settings and return to the previous page.

Classification Match Result



Prioritize TCP Flags:

Apply



Bandwidth Limit

The bandwidth limit menu is used to limit the bandwidth of traffic passing through the DSL-G2562DG.

Port Bandwidth Limit Configuration

This allows you to limit bandwidth based on port.

Port Bandwidth Limit Configuration

Enable: Whether to enable or disable the port bandwidth limit. Tick this to enable the port bandwidth limit. Choose LAN Port: The LAN port to limit the bandwidth on. Ingress Rate: The maximum ingress speed, in kbps. Enter 0 to disable the limit. Egress Rate: The maximum egress speed, in kbps. Click **Apply** to apply the settings and click **Refresh** to refresh the page.

IP Bandwidth Limit Configuration

This allows you to limit bandwidth based on IP address.

IP Bandwidth Limit Configuration

<u>Enable</u>: Whether to enable or disable the IP bandwidth limit. Tick this to enable the IP bandwidth limit, and un-tick it to disable it.

IPs: The range of IP addresses to apply the IP bandwidth limit to.

<u>Ingress Rate</u>: The maximum ingress speed, in kbps. Enter 0 to disable the limit.

Egress Rate: The maximum egress speed, in kbps.

Click Apply to apply the settings and click Refresh to refresh the page.

Port Bandwidth Limit Configuration

Enable:		
Choose Lan Port:	LAN1 🗸	
Ingress Rate:	0	Kbps (0 means no rate limit)
Egress Rate:	0	Kbps

IP Bandwidth Limit Configuration

Refresh

Enable:		
IPs:		-
Ingress Rate:	0	Kbps (0 means no rate limit)
Egress Rate:	0	Kbps
Apply Refresh		
IP BW Limit Rules		

Number	Enable	IP Range	Ingress BW	Egress BW	Action
No Rule F	ound!				



IP Tunnel

The IP tunnel menu is used to create tunnels for routing various types of traffic across a particular type of network.

IPv4 In IPv6

DSL-Lite Tunnel Settings

6 in 4 Tunnel Configuration

This allows you to create an IPv4 tunnel that tunnels IPv6 traffic.

Enable: Whether to enable or disable the 6 in 4 tunnel configuration.

Tick this to enable the 6 in 4 tunnel configuration.

<u>Tunnel Name:</u> The name of the 6 in 4 tunnel.

Mechanism: The mechanism through which to establish the 6 in 4 tunnel.

Note: Currently only IPv6 Rapid Deployment (6rd) is supported.

DS-Lite Tunnel Settings

Refresh

Apply

IPv6 Connection:	- 🗸
Enable DS-Lite:	
AFTR Setup Mode:	Auto 🗸
AFTR Address:	



<u>Associated WAN Interface:</u> The WAN interface associated with the 6 in 4 tunnel. Choose **Manual** to enter the 6 in 4 tunnel information manually, and choose Automatic to input it manually.

6 in 4 tunnel information automatically.
<u>IPv4 Mask Length:</u> The IPv4 mask length for the 6 in 4 tunnel.
6rd Prefix with
<u>Prefix Length:</u> The 6rd prefix and prefix length to use with the 6 in 4 tunnel.
Border Relay IPv4

<u>Address:</u> The border relay IPv4 address for the 6 in 4 tunnel.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Generic Routing Encapsulation

This allows you to create a Generic Routing Encapsulation (GRE) tunnel that can tunnel multiple traffic types.

Generic Routing Encapsulation

Nur	nber	Tunnel Name	Interface IP Address	Remote IP Address	Local Addresses	Action
No	No Rule Found!					

Add

Click **Add** to add a new GRE tunnel.

GRE Setting

This allows you to create a Generic Routing Encapsulation (GRE) tunnel that can tunnel multiple traffic types.

6 in 4 Tunnel Configuration

Refresh

Currently, only 6rd configuration is supported.

Enable		
Tunnel Name:		
Mechanism:	6RD 🗸	
Associated WAN Interface:	DHCP_WAN_ETH V	
	\bigcirc Manual \bigcirc Automatic	
IPv4 Mask Length:		
6rd Prefix with Prefix Length	:	::/
Border Relay IPv4 Address:		



<u>Connection Name</u>: The connection name for the GRE tunnel. <u>Tunnel Name</u>: The tunnel name for the GRE tunnel.

Note: this must start with "gre-".

<u>Interface IP Address:</u> The interface IP address to use with the GRE tunnel. <u>Subnet Mask:</u> The interface IP address subnet mask to use with the GRE tunnel. <u>Tunnel Remote IP:</u> The remote tunnel IP address to use with the GRE tunnel. <u>Max TTL:</u> The maximum Time to Live (TTL) of the GRE tunnel packets.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

GRE Setting

Back Apply Refresh

Connection Name:	DHCP_WAN_ETH V	
Tunnel Name:] Tunnel name must begin with 'gre-'
Interface IP Address:]
Subnet Mask:]
Tunnel Remote IP:]
Max TTL:	255]

Applications

Storage Service

The Applications menu is used to set application settings on the DSL-G2562DG.

Storage Device Info

This displays information about any attached external USB storage devices.

Storage Service - File Sharing Service Setup

This is used to enable or disable the Samba file sharing service.

Storage Service - File Sharing Service Setup

<u>Enable Samba Service</u>: Whether to enable or disable the Samba service. Tick this to enable the Samba service. Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Storage Service - FTP Service Setup

This is used to enable or disable the FTP server service.

Storage Service - FTP Service Setup

<u>Enable FTP Service</u>: Whether to enable or disable the FTP service. Tick this to enable the FTP service.

<u>FTP Directory</u>: The directory to make available for use by the FTP service. Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Storage Device Info

Number	Provider	Product Type	Capacity(MB)
No Rule Found!			

Storage Service - File Sharing Service Setup

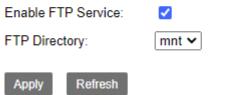
Note: To enable Samba Server, Please insert at least one storage device.

Enable Samba Service:

Apply Refresh

Storage Service - FTP Service Setup

Note: To enable FTP Server, at least one storage device would be inserted.





Storage Service - FTP Client Settings

This is used to set FTP client settings.

Storage Service - FTP Service Setup

<u>User Name</u>: The username to connect to the remote FTP server with. <u>Password</u>: The password to connect to the remote FTP server with. <u>Download URL</u>: The URL to the file on the remote FTP server that you wish to download.

Port: The port to connect to the remote FTP server on.

<u>Device</u>: The device to download the file specified in the download URL to. <u>Save Path</u>: The location on the device to download the file specified in the download URL to.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Storage Service - TFTP Service Setup

This is used to enable or disable the TFTP server service.

Storage Service - FTP Service Setup

<u>Enable TFTP Service</u>: Whether to enable or disable the TFTP service. Tick this to enable the TFTP service. <u>TFTP Directory</u>: The directory that the TFTP service uses.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Storage Service - FTP Client Settings

User Name:	
Password:	•••••
Download URL:	ftp://
Port:	21
Device:	~
Save Path:	xdown

Download

The latest 10 download records

Refresh

 User Name
 Password
 Port
 Download URL
 Save Path
 Progress
 Status
 Action

 No Rule Found!

 Action

Storage Service - TFTP Service Setup

Note: To enable the TFTP Server, a storage device may be needed.

Enable TFTP Service:

Apply Refresh



Printer Service Setup

This is used to enable or disable the printer service.

Printer Service Setup

<u>Enable Printer Service</u>: Whether to enable or disable the printer service. Tick this_to enable the printer service. <u>Queue Name</u>: The printer queue name.

Click Apply to apply the settings and click Refresh to refresh the page.

Multimedia Share Setup

This is used to enable or disable the Digital Media Server (DMS) service.

Multimedia Share Setup

Multimedia Share Setup

Enable DMS: Whether to enable or disable the DMS service.

Tick this to enable the DMS service.

<u>Share Folders:</u> The folders to share using the DMS service.

Choose Share All Folders to share all folders, and choose Custom Shared Folder to share a

custom folder. Choosing the Custom Shared Folder option displays other options on the page, and these are documented below.

Share Folders: Custom Shared Folder

<u>Custom Shared Folder:</u> The custom shared folder to share using the DMS_service.

Select a folder in the file browser and click the Add button to share it using the DMS service.

Click Apply to apply the settings and click Refresh to refresh the page.

Printer Service Setup

Enable Printer Servic	e:	
Queue Name:	myprinter	
Apply Refresh		
Multimedia Share	Setup	
Enable DMS:		
Share Folders:	○ Share All Folders	
	Custom Shared Folder	
Custom Shared Folder:		Add
		-



DNS

The DNS menu is used to set dynamic DNS settings on the DSL-G2562DG.

DDNS Settings

This is used to set dynamic DNS settings, so that the router can automatically update an external service with its current IP address.

DDNS Settings

Enable: Whether to enable or disable the DDNS settings. Tick this to enable the DDNS settings, and un-tick it to disable it. Click **Apply** to apply the settings. Click Add to add a new DDNS entry.

DDNS Server: The DDNS service to use with the router. This can be one of the predefined entries, or choose **Other** to enter a custom DDNS service. Host Name: The DNS name that you wish to update. WAN Connection: The WAN connection to use for the DDNS settings. User Name: The username for the DDNS service. Password: The password for the DDNS service.

Click **Back** to go back to the previous page and click **Apply** to apply the settings.

DDNS Settings

2	Enable: Apply	
Add		
DDNS Server:	oray.com 🗸	
Host Name:		
WAN Connection:	DHCP_WAN_ETH ¥	
User Name:		
Password:	•••••	
Back Apply		

Number	DDNS Status	Host Name	Action
No Rule Found!			



UPnP

This is used to set Universal Plug and Play (UPnP) settings, so that devices on the LAN can automatically open ports on the router firewall.

Enable UPnP IGD: Whether to enable or disable the Internet Gateway Device

(IGD) Protocol. Tick this to enable the IGD Protocol.

<u>WAN Connection</u>: The WAN connection to use with the IGD Protocol.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Blacklist

<u>Enable</u>: Whether to enable or disable the blacklist entry. Tick this to enable the blacklist entry.

<u>IP Address</u>: The IP address to blacklist from using the IGD Protocol.

Click **Add** to add a new blacklist entry.

UPnP

Enable UPnP IGD:			
WAN Connection:	DHCP_WAN_ETH V	/	
Apply Refresh			
Blacklist			
Enable:			
IP Address:			
Add			
Enable	Number	IP Address	Action
No Rule Found!			



Multicast

The multicast menu is used to set multicast settings on the DSL-G2562DG.

IGMP Settings

This is used to set Internet Group Management Protocol (IGMP) settings. <u>Default Version</u>: The default version of IGMP to use on the router. This can be **IGMPv2** or **IGMPv3**. The default is IGMPv2.

<u>Query Interval(s)</u>: The query interval for IGMP. The default is 125 seconds. <u>Query Response Interval(1/10s)</u>:

The query response interval for IGMP. The default is 100 seconds. Last Member Query Interval(1/10s):

The last member query interval for IGMP. The default is 10 seconds. Robustness Value: The Robustness Value for IGMP. The default is 2. <u>Maximum Multicast Data Source (for IGMPv3)</u>:

The maximum multicast data sources for IGMPv3. The default is 10. Fast Leave Enable: Whether to enable or disable Fast Leave. Tick this to enable Fast Leave.

Membership Join Immediate(IPTV):

Whether to enable or disable Membership Join Immediate. Tick this to enable Membership, Join Immediate.

Click Apply to apply the settings and click Refresh to refresh the page.

<u>Enable IGMP Snooping</u>: Whether to enable or disable IGMP snooping. Tick this to enable IGMP snooping.

Click Apply to apply the settings and click Refresh to refresh the page.

Enable IGMP Proxy: Whether to enable or disable IGMP proxy. Tick this to enable IGMP proxy.

WAN Connection: Whether to enable or disable IGMP for the WAN connection. Tick this to enable IGMP for the WAN connection.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

IGMP Settings

Enter IGMP protocol configuration fields if you want modify default vaules shown below. NOTE:Query Interval is advised to no longer than 125s.

Default Version:		IGMP v2 ✓	
Query Interval(s):		125	
Query Response Interval(1/10s):		100	
Last Member Query Interval(1	1/10s):	10	
Robustness Value:		2	
Maxinum Multicast Data Sour	ce(for IGMPv3):	10	
Fast Leave Enable:			
Membership Join Immediate(IPTV):		
Apply Refresh			
Enable IGMP Snooping:			
Apply Refresh			
Enable IGMP Proxy:			
WAN Connection	Enable IGMP		
DHCP_WAN_ETH			
PPPoE_WAN_ETH			
LTE			
Apply Refresh		_	



MLD Settings

This is used to set Multicast Listener Discovery (MLD) settings.

Default Version: The default version of MLD to use on the router.

This can be MLDv1 or MLDv2. The default is MLDv2.

<u>Query Interval(s)</u>: The query interval for MLD. The default is 125 seconds. <u>Query Response Interval(1/10s)</u>: The query response interval for MLD. The

default is 100 seconds.

Last Member Query Interval(1/10s): The last member query interval for MLD. The default is 10 seconds.

Robustness Value: The Robustness Value for MLD. The default is 2.

<u>Maximum Multicast Data Source (for mldv2)</u>: The maximum multicast data sources for MLDv2. The default is 10.

Fast Leave Enable: Whether to enable or disable Fast Leave.

Tick this to enable Fast Leave.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

<u>Enable MLD Snooping</u>: Whether to enable or disable MLD snooping. Tick this to enable MLD snooping, and un-tick it to disable it.

Click Apply to apply the settings and click Refresh to refresh the page.

Enable MLD Proxy: Whether to enable or disable MLD proxy.

Tick this to_enable MLD proxy.

<u>WAN Connection</u>: Whether to enable or disable MLD for the WAN connection.

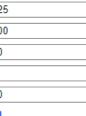
Tick this to enable MLD for the WAN connection.

Click Apply to apply the settings and click Refresh to refresh the page.

MLD Settings

Enter MLD protocol(IPv6 Multicast)configure fields if you want modify default values shown below.

Default Version: MLD v2 🗸 Query Interval(s): 125 100 Query Response Interval(1/10s): Last Member Query Interval(1/10s): 10 2 Robustness Value: Maxinum Multicast Data Source(for mldv2): 10 Fast Leave Enable: ~ Refresh Apply Enable MLD Snooping: ~ Refresh Enable MLD Proxy ~ WAN Connection Enable MLD No Rule Found! Refresh





SNMP Settings

This is used to set Simple Network Management Protocol (SNMP) settings for remote network management.

Enable SNMP: Whether to enable or disable SNMP. Tick this to enable SNMP.

The default is un-ticked.

System Contact: The SNMP system contact.

<u>System Name:</u> The SNMP system name.

System Location: The SNMP system location.

Public community: The SNMP public community string.

Private community: The SNMP private community string.

<u>Trap Enable</u>: Whether to enable or disable SNMP. Tick this to enable SNMP.

The default is un-ticked.

Trap Version: The SNMP trap version. This can be SNMPv1 or SNMPv2.

<u>Trap Address</u>: The SNMP trap server IP address.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

SNMP Settings

Enable SNMP System Contact System Name System Location Public community Private community

Trap Enable

Trap Version

Trap Address

Refresh

Apply

SNMP V1 🗸	
192.168.1.100	



VOIP

The VOIP menu is used to set VOIP settings on the DSL-G2562DG.

Link Test Interval: The number of seconds between VOIP link tests.

Retry Interval The number of seconds before retrying registration.

Enable P-Asserted-Identity: Tick to enable P-Asserted-Identity.

Allow SIP Source: IP address of the allow SIP source.

Basic Setup

Basic Setup Port: 5060 (1024 ~ 65535) Port: The port to use for VOIP service. Register Server: Address of the register server. Register Server: Proxy: Address of the proxy. Proxy: Outbound Server: Address of the outbound server. Outbound Server: Port: Port for to use for the outbound server. 5060 Port: $(1024 \sim 65535)$ **Backup Register** Backup Register Server: Backup Porxy: Server: Backup address of the register server. Backup Proxy: Backup address of the proxy. Backup Outbound Server: 5060 Backup Outbound Server: Backup address of the outbound server. Backup Port: (1024 ~ 65535) Backup Port: Port for to use for the backup outbound server. 1800 Register Life TIme: Second Enable Link Test: Register Life Time: Lifetime of the registration process. 20 Link Test Interval: Second Enable Link Test: Tick to enable testing of VOIP link. 20 Retry Interval: Second

Enable P-Asserted-Identity:

0.0.0.0

Allow SIP source



Connection 1	Connection 1	
Enable: By default, the box is ticked Username: Enter the username as provided by the VoIP/SIP provider.	Enable:	
Password: Enter the password as provided by your VoIP/SIP provider.	User Name:	
URI: Enter the URI (Uniform Resource Identifier) if applicable to your service.	Password:	•••••
Instance ID: Enable SIP instance ID to register the same account on multiple devices linked to the DSL-	URI:	
G2562DG	Instance Id:	
Click Annly to annly the settings and click Refresh to refresh the page	Apply Refresh	

Click **Apply** to apply the settings and click **Refresh** to refresh the page.



Advance VoIP Setup

DTMF Settings: Select between RFC2833 or inbound.
<u>DTMF Relay PT:</u> Enter the RTP port Relay number for the connection. Default is 97
Begin RTP Port: Enter the RTP port begin number for the connection. Default is 4000
Jitter Buffer: Select between Auto or Fixup
Min: Enter the minimum jitter time in milliseconds
Max: Enter the maximum jitter time in milliseconds
Media Negotiatory: Select between remote or local negotiation. Default is set to
Remote side.

Connection 1

<u>Echo Cancellation</u>: Echo cancellation eliminates the echo affect from sound on both parties. It is best to have this enabled to improve the voice quality. <u>VAD</u>: Select this option to enable Voice Activation Detection. Default is un-ticked <u>Send Gain</u>: Change the value of gain send via mic piece of handset. <u>Receive Gain</u>: Change the value of gain received via ear piece of handset.

Advanced Setup

DTMF Settings:	RFC2833 ¥	
DTMF Relay PT:	97	
Begin RTP Port:	4000	
Jitter Buffer:	Auto 🗸	
Min:	20	ms
Max:	200	ms
Media Negotiatory:	Remote 🗸	
Connection 1		
Echo Cancellation:	Enable 🗸	
VAD:		
Send Gain:	0	(-14~6)
Receive Gain:	0	(-14~6) (-14~6)
Apply Refresh		



Media Settings

Here you can select which codec to use for voice calls and the priority in which it should work. By default, G711A and G729 is used.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Media Settings

Connection 1

Refresh

Apply



Fax Settings

Here you can enable to disable the Fax Protocol for the Device.

Enable T38: Click to disable fax protocol. This will prevent the device to look for fax transmition if a call is received

Click Apply to apply the settings and click Refresh to refresh the page.



Voice Service

Here you can select the VoIP number configured to modify call settings.

Voice Service

<u>Tel:</u> Select the number of the register VoIP services
Call Forward Unconditional: Tick to enable Unconditional forwarding of registered VoIP
number
To: Enter the Destination number for unconditional call forwarding.
Call Forward On Busy: Tick to enable call forwarding when line is busy.
To: Enter the Destination number for call forwarding when busy.
Call Forward On No Answer: Tick to enable call forwarding when call is not answered.
To: Enter the Destination number to forward the calls when not answered.
Call Waiting: Untick to disable call waiting.
Blind Transfer: Untick to disable blind transfer.
Consecutive Transfer: Untick to disable Consecutive Transfer.
Call Hold: Untick to disable Call Hold feature.
<u>3 Way Talking</u> : untick to disable conference call feature.
Hot Line: Select between Default, Right Now and Delay.
Destination Number: Enter the new Destination number if hot line is changed to Right Now
or Delay
Delay Line Timer: Enter the Delay time in ms when hotline is not set to default.
Anti-Pole: Tick to enable Anti-Pole feature.
Enable Subscribe: Tick to enable Subscribe services.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Tel:	▼	
Call Forward Unconditional:		
To:		
Call Forward On Busy:		
To:		
Call Forward On No Answer:		
To:		
Call Waitting:		
Blind Transfer:		
Consultive Transfer:		
Call Hold:		
3 Way Talking:		
Hot Line:	Default 🗸	
Destination Number:		
Delay Line Timer:	5000	ms
Anti-Pole:		
Enable Subscribe:		

Apply Refresh

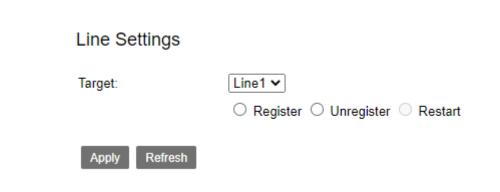


Line Settings

Here you can register, Unregister or restart the registration for the VoIP account configured.

<u>Target:</u> Select the line you want to Register, Unregister or Restart. There is only one line for the router.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.



Digital Map

This is where you can modify the dialling pattern for the router. If you wish to use a certain pattern to dial out, you can do it here.

Please Input Number Table

<u>Number Table:</u> Enter or modify the dialling pattern for the DSL-G2562DG

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Please Input Number Table

Digital Map

[2-	
	1[3458] <u>xxxxxxxxx</u> 01[3458] <u>xxxxxxxxx 0xxxxxxxxxxxx 0311xxxxxxxxx</u> 037[179] <u>xxx</u>
] <u>1xxxxxxxx</u> <u>0432xxxxxxx</u> 051[0-
	052[37] <u>xxxxxxxx</u> 053[12] <u>xxxxxxxx</u> 057[13-
79] <u>xxxxxxx</u>	x 059[15]xxxxxxxx 0731xxxxxxxx 075[457]xxxxxxxxx 076[09]xxxxxxxx 0898xxxx
xxx 9xxxx	1[0124-
]x 118xxx	100xx 20x 400xxxxxx 800xxxxxx 955xx 58426x. 58427 1630 06 99699 8*#
[*#][*#0-9][0-9*]#x.# ## **xx x[0-9*].# *xx*x.# *xx*xx*xx.# *xx# x[0-
	#xx# *xx*xx# *xx*xx.*x.# #xx*x.# *#xx*x.*x.# *xx*x.*x.# *xx*xxxx.# *xx#xx# *#xx **
	x **xx **xxx. *53*xxx.# *31*xxx. xxx.

Apply Refresh



Basic Call Control

Here you can modify the timers for the DSL-G2562DG incoming and outgoing calls.

<u>Short Timer:</u> Modify the short timer value for pre-dialing timeout. <u>Long Timer:</u> Modify the long timer value for post-dialling timeout. <u>Dial Tone Timer:</u> Modify the dial tone timer before timeout. <u>Ring Without Answer Timer:</u> Modify the time before the call is hung-up. <u>Howl Tone Timer:</u> Modify the Howl timer value. <u>Busy Tone Timer:</u> Modify the Busy Tone timer timeout while busy tone is played. Country Tone: Change the Country dial tone.

Connection 1

<u>Flash Min:</u> Change the flash timer minimum value. <u>Flash Max:</u> Change the flash timer maximum value.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

CID

Here you can select which mode to use for Caller Identity.

CID Mode: Choose between FSK or DTMF

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Basic Call Control

Short Timer:	4	Second
Long Timer:	4	Second
Dial tone Timer:	20	Second
Ring Without Answer Timer:	60	Second
Howl Tone Timer:	60	Second
Busy Tone Timer:	40	Second
Country Tone	SouthAfrica 🗸	
Connection 1		
Flash Min:	50	ms(10-1300)
Flash Max:	130	ms(10-1300)
Apply Refresh		
CID		
CID Mode:	FSK ¥	
Apply Refresh		



CDR

Show last CDR info

CDR

Show you the call history for the calls made on this router.

Info: Shows you the call history

Note: before this can work you would need to use a USB flash drive connected to the router.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

	/
	//

Clear Download Refresh



VPN

The VPN menu is used to set IPsec and L2TP tunnel settings on the DSL-G2562DG.

IPsec

This is used to set basic IPsec settings.

IPsec Tunnel Mode Connections

<u>IPsec Hardware Accelerate</u>: Whether to enable or disable IPsec hardware acceleration. Tick this to enable IPsec hardware acceleration, and untick it to disable it. The default is un-ticked.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Action
No Rule Found!				

Add

Click **Add** to add a new IPsec tunnel.

IPSec Tunnel Mode Connections

IPSec Hardware		
Accelerate)	
Apply	Refresh	



IPsec Settings

This is used to set basic IPsec tunnel settings.

IPsec Connection Name: The connection name for the IPsec tunnel.
Tunnel Mode: The tunnel mode for the IPsec tunnel. This can be Encapsulating
Security Payload (ESP) or Authentication Header (AH).
WAN Connection: The WAN connection to use with the IPsec tunnel.
Local IPsec Gateway Address: The local IPsec gateway address.
This is the source for the IPsec tunnel. The default is 0.0.0.0 (the local router).
Remote IPsec Gateway Address: This is the destination for the IPsec tunnel.

Tunnel access from local IP addresses:

The addresses that are allowed to access the IPsec_tunnel. This can be **Subnet** or **Single Address**. Choosing the Subnet option displays other options on the page, and these are documented below. <u>IP Address for VPN:</u> The IP addresses that are allowed to access the IPsec tunnel <u>IP Subnet mask:</u> The subnet mask for the IP addresses allowed to access the IPsec tunnel.

Tunnel access from remote IP addresses:

The remote addresses that are allowed to access the IPsec tunnel.

This can be **Subnet** or **Single Address**. Choosing the Subnet option displays other options on the page, and these are documented below.

<u>IP Address for VPN:</u> The remote IP addresses that are allowed to access the IPsec tunnel. <u>IP Subnet mask</u>: The subnet mask for the remote IP addresses allowed to access the IPsec tunnel.

IPSec Settings

IPSec Connection Name:	new connection
Tunnel Mode:	ESP ¥
WAN Connection:	DHCP_WAN_ETH V
Local IPsec Gateway Address:	0.0.0.0
Remote IPsec Gateway Address:	0.0.0.0
Tunnel access from local IP addresses:	Subnet 🗸
IP Address for VPN:	0.0.0
IP Subnetmask:	255.255.255.0
Tunnel access from remote IP addresses:	Subnet 🗸
IP Address for VPN:	0.0.0
IP Subnetmask:	255.255.255.0
Key Exchange Method:	Auto(IKE) 🗸
Authentication Method:	Pre-Shared Key 🗸
Pre-Shared Key:	key
Perfect Forward Secrecy:	Enable 🗸
Advanced IKE Settings:	Show Advanced Settings





Key Exchange Method:

The key exchange method for the IPsec tunnel. This can be **Auto(IKE)** or **Manual**. The default is Auto(IKE).

Choosing these options displays other options on the page, and these are documented below.

Authentication Method:

The authentication method for the IPsec tunnel.

This can be **Pre-Shared Key** or **Certificate (X.509)**. The default is Pre-Shared Key.

Choosing these options displays other options on the page, and these are documented below.

Perfect Forward Secrecy:

Whether to enable or disable perfect forward secrecy.

Tick this to enable perfect forward secrecy, and untick it to disable it. The default is un-ticked.

Advanced IKE Settings: Click Show Advanced Settings to show advanced Auto(IKE) settings.

Choosing this option displays other options on the page, and these are documented below.

Phase 1 Mode: The Auto(IKE) mode to use with the IPsec tunnel. This can be Main or Aggressive. The default is Main.

Encryption Algorithm: The encryption algorithm to use with the IPsec tunnel.

This can be **DES**, **3DES**, **AES**. The default is DES.



<u>Integrity Algorithm:</u> The authentication algorithm to use with the IPsec tunnel. This can be **MD5** or **SHA1**. The default is MD5.

<u>Diffie-Hellman Group</u>: The Diffie-Hellman Group key size to use with the IPsec tunnel.

This can be **768bit**, **1024bit**, **1536bit** or **2048bit**. The default is 1024bit.

<u>Key Life Time</u>: The key lifetime for the IPsec tunnel. The default is 3600 seconds. <u>Phase 2 Encryption Algorithm</u>: The encryption algorithm to use with the IPsec tunnel.

This can be **DES**, **3DES**, **AES**. The default is DES.

<u>Encryption Algorithm:</u> The encryption algorithm to use with the IPsec tunnel. This can be **DES**, **3DES**, **AES**. The default is DES.

<u>Integrity Algorithm:</u> The authentication algorithm to use with the IPsec tunnel. This can be **MD5** or **SHA1**. The default is MD5.

<u>Diffie-Hellman Group</u>: The Diffie-Hellman Group key size to use with the IPsec tunnel.

This can be **768bit**, **1024bit**, **1536bit** or **2048bit**. The default is 1024bit.

Key Life Time: The key lifetime for the IPsec tunnel. The default is 3600 seconds.

Phase 1
Mode:
Encryption Algorithm:
Integrity Algorithm:
Diffie-Hellman Group:
Key Life Time:
Phase 2
Encryption Algorithm:
Integrity Algorithm:
Diffie-Hellman Group:
Key Life Time:

Refresh

Back

Apply

Main 🗸
DES 🗸
MD5 🗸
1024bit 🗸
3600
DES 🗸
MD5 🗸
1024bit 🗸
3600



L2TP

This is used to set basic L2TP settings.

L2TP LAC Tunnel Setting

This is used to set basic L2TP tunnel settings.

L2TP LAC Tunnel Settings

<u>Connection Name:</u> The connection name for the L2TP tunnel.

<u>Enable</u>: Whether to enable or disable the L2TP tunnel. Tick this to enable the L2TP tunnel. The default is un-ticked.

Tunnel Name: The tunnel name for the L2TP tunnel.

<u>Tunnel Interface IP Mode</u>: This can be Static or Dynamic. The default is Dynamic.

<u>Tunnel Interface IP</u>: The IP address to listen on for the L2TP tunnel. Option only available when Tunnel Interface IP Mode is set to static.

<u>NAT</u>: Whether to enable or disable Network Address Translation. Tick this to enable NAT. The default is un-ticked.

Default Route: Allow all LAN-WAN to be directed via the VPN.

Authentication Type: Auto, PAP or CHAP. The Authentication Type of the LAC tunnel.

LNS Addr Mode: The LNS addressing mode. This can be FQDN or IP. Default is FQDN

LNS Domain Name/IP: The LNS FQDN/IP address to use with the L2TP tunnel.

<u>User Name:</u> The username for the L2TP tunnel.

<u>Password:</u> The password for the L2TP tunnel.

Max Redial: Amount to re-dial if connection is not successful. Min 1, Recommended 3-5.

Click Apply to apply the settings and click Refresh to refresh the page.

L2TP LAC Rule List View the L2TP Rule created

L2TP LAC Tunnel Settings

If enable Default Route, all traffic will pass through by the VPN; else only traffic specified by Remote Network can pass through

Connection Name:	DHCP_WAN_ETH V	
Enable:		
Tunnel Name:]
Tunnel Interface IP Mode:	Static V	
Tunnel Interface IP:]
NAT:	✓	
Default Route:	✓	
Authentication Type:	AUTO 🗸	
LNS Addr Mode:	FQDN 🗸	
LNS Domain Name:]
User Name:]
Password:	•••••]
Max redial:		(at least 1)



Number	Tunnel Name	Enable	Tunnel Interface IP Mode	NAT	Remote Network	User Name	Authentication Mode	LNS Addr Mode	Action
No Rule F	ound!								



L2TP LNS Tunnel Settings

Connection Name: The connection name for the L2TP tunnel. Enable: Whether to enable or disable the L2TP tunnel. Tick this to enable the L2TP tunnel. The default is un-ticked. <u>Tunnel Name:</u> The tunnel name for the L2TP tunnel. <u>Tunnel Interface IP</u>: The IP address to listen on for the L2TP tunnel. <u>Tunnel LAC IP</u>: The starting IP address for the DHCP table range. <u>Authentication Type:</u> The Authentication type for the LNS tunnel. <u>Access Lac</u>: Whether to enable or disable access to the LAC. Tick this to enable access. The default is un-ticked.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

L2TP LNS User List

<u>Number:</u> The LNS user number. <u>User Name:</u> The username of the LNS user. <u>Password:</u> The LNS user's password. <u>Action:</u> Press to remove/edit the LNS user. <u>User Name:</u> Enter the User Name of a new LNS user. Password: Enter the Password of a new LNS user.

Click Add to add a new LNS user.

L2TP LNS Tunnel Settings

Connection Name:	DHCP_WAN_ETH V
Enable:	
Tunnel Name:	
Tunnel Interface IP:	
Tunnel Lac IP:	
Authentication Type:	AUTO 🗸
Access Lac:	
Apply Refresh	

L2TP LNS User List

Number	User Name	Password	Action		
No Rule Found!					
User Name	e:				
Password: ••••••					

Add



VPN Lite

VPN Lite Configuration

<u>Connection Name:</u> The connection name for the L2TP tunnel. <u>Enable:</u> Whether to enable or disable VPN Lite. Tick this to enable the VPN Lite. The default is un-ticked. <u>User Name:</u> The user name for the VPN Lite Configuration. <u>Password:</u> The password for the VPN Lite Configuration. <u>Site LAN IP/ Netmask:</u> The IP address of the LAN or netmask. <u>NAT:</u> Whether to enable or disable Network Address Translation. Tick this to enable NAT. The default is un-ticked. <u>Firewall:</u> Whether to enable or disable a firewall. Tick this to enable a firewall. The default is un-ticked.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Static Route List

<u>Number</u>: The number of the static route in the list (ascending order). Destination Subnet: The IP address for the destination subnet.

Mask: The IP address for the mask.

Action: Press the icon to delete a static route from the list.

VPN Lite Configuration

Connection Name:	DHCP_WAN_ETH ¥	
Enable:		
User Name:]
Password:	•••••]
Site LAN IP/Netmask:	1	(Format: A.A.A.A/B(A:0-255,B:1-32))
NAT:		
Firewall:		
Apply Refresh		

Static Route List

Number	Destination Subnet	Mask	Action
1	10.0.0.0	255.0.0.0	Ĩ
2	172.16.0.0	255.240.0.0	Ũ
3	192.168.0.0	255.255.0.0	Ũ

Add



Management

The Management menu is used to perform maintenance tasks on the DSL-G2562DG.

Reboot

This is used to reboot the router.

Click **Reboot** to reboot the router.

Settings

Backup This is used to back up the router settings.

Click **Backup Settings** to save the router settings to a file on your PC.

Reboot

Click below button to reboot the router!

Reboot

Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

Backup Settings



DHCP Option 66 Files

This is used to download the DHCP Option 66 files to store on a TFTP server.

Click Global to download all DHCP Option 66 files on the router to your PC.

Click **Specific MAC** to download the DHCP Option 66 file for a specific MAC address to your PC.

Settings - DHCP Option 66 Files

Backup DHCP Option 66 configuration files on your PC to manually be stored in your TFTP Server.

- Global file will be used to update settings to a few devices.
- Specific MAC file will be used to update settings to a specific device whose MAC address matches the filename.



Update Settings

This is used to restore previously saved router settings.

Click **Browse...** to select a file on your PC to upload. This must be a file previously saved using the settings backup feature.

Click Update Settings to restore the previously saved router settings.

Restore Default Settings

This is used to restore the default settings of the router.

Click Restore Default Settings to restore the router to factory defaults.

Settings - Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name: Browse...

owse... File not found

Update Settings

Settings - Restore Default Settings

Restore Broadband Router settings to the factory defaults.

Restore Default Settings



Update Software

This is used to update the router firmware.

Click Browse... to select a router firmware image file on your PC.

Click Update Software to upgrade the router firmware.

Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the 'Browse' button to locate the image file. Step 3: Click the 'Update Software' button once to upload the new image file.

Note: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Software File Name: Browse... File not found

Update Software

Account Management - Passwords

This is used to change user passwords.

<u>Username</u>: The user to reset the password for. <u>Old Password</u>: The user's old password. <u>New Password</u>: The user's new password. <u>Confirm Password</u>: Confirm the user's new password.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Logs

Log Level This is used to set logging settings.

Account Management - Passwords

Note: Password cannot contain a space.

Username:	admin	~
Old Password:		
New Password:		
Confirm Password:		

Apply Refresh



Account Management – Log Level

Refresh to refresh the page.

Enable Log: Whether to enable or disable logging.

Tick this to enable logging. The default is un-ticked.

Log Level: The logging level to report logs for. This can be Emergency, Alert, Critical, Error,

Warning, Notice, Informational, or Debug. The default is Critical.

TFTP Server: The address of a TFTP server to upload the log files to.

Press Upload Log File once the address has been entered to upload the log file.

Enable Log Server: Whether to enable or disable logging to an external logging server.

Tick this to enable logging to an external logging server. The default is un-ticked.

<u>Remote Log Server:</u> The address of the remote logging server.

<u>Port:</u> The port to use with the remote logging server.

Account Management - Log Level

Attention: Enabling logging may affect the gateway performance.

Enable Log:		
Log Level:	Warning 🗸	
TFTP Server:		Upload Log File
Enable Log Server:		
Remote Log Server:		
Port:	514	

Account Management - Logs

Download Log File

Refresh

	Show Log Level:	Critical 🗸	
Logs		Manufacturer:D-Link;	
This is used to view the router logs.		ProductClass:DWR-956M; SerialNumber:ecade05095e3; IPInterfaceIPAddress:10.0.0.2; HardwareVersion:DWR-956M; SoftwareVersion:TK_1.00TK;	
Account Management – Logs		1970-01-01 02:00:13 [Critical] dnsmasq[1889]: bad command line options: tryhelp	
Show Log Level: The logging level to show the logs for.		1970-01-01 02:00:13 [Critical] dnsmasq[1889]: FAILED to start up 1970-01-01 02:00:13 [Critical] dnsmasq[1954]: bad command line options: tryhelp	
This can be Emergency, Alert, Critical, Error, Warning, Notice ,		1970-01-01 02:00:13 [Critical] dnsmasq[1954]: FAILED to start up 1970-01-01 02:00:12 [Critical] dnsmasq[1829]: bad command line options: tryhelp	
Informational, or Debug. The default is Critical.		1970-01-01 02:00:13 [Critical] dnsmasq[1829]: FAILED to start up 1970-01-01 02:00:13 [Critical] dnsmasq[1884]: bad command line options: tryhelp 1970-01-01 02:00:13 [Critical] dnsmasq[1884]: FAILED to start up	
Click Clear Log File to clear the router log file, click		1970-01-01 02:00:13 [Critical] dnsmasq[1914]: bad command line options: tryhelp 1970-01-01 02:00:13 [Critical] dnsmasq[1914]: FAILED to start up 1970-01-01 02:00:13 [Critical] dnsmasq[1935]: bad command line options: tryhelp 1970-01-01 02:00:13 [Critical] dnsmasq[1935]: FAILED to start up	-
Download Log File to download the router log file, and click		1970-01-01 02:00:13 [Critical] dnsmasq[1921]: bad command line options: tryhelp	11

Clear Log File



Service Control

This is used to add, remove and edit firewall rules.

Access Control -- IP Address Configuration

<u>ACL Enable</u>: Whether to enable or disable the firewall rules. Tick this to enable the firewall rules. The default is un-ticked.

Click **Apply** to apply the settings. Click **Add** to add a new firewall rule.

Access Control -- IP Address Configuration

This is used to add a firewall rule.

Protocol: The protocol for the firewall rule. This can be HTTP, TELNET,
FTP, SAMBA, ICMP, TFTP, SNMP, SSH, TCP or UDP.
Choosing the HTTP, TELNET, FTP, TFTP, SSH, TCP or UDP options displays other options on the page, and these are documented below.
Access Control: The access control interface for the firewall rule.
IP Protocol Type: The protocol type for the firewall rule.
This can be IPv4, IPv6 or IPv4&6.
Enable: Whether to enable or disable the firewall rule. Tick this to enable the firewall rule. The default is un-ticked.
Source IP: The source IP address(es) for the firewall rule.
Enter a single IP address for the source address, or enter a range of addresses in the beginning and end boxes.
Action: The action for the firewall rule. This can be ACCEPT or DROP.
Protocol: HTTP, TELNET, FTP, SSH, TCP or UDP
Port: The port number for the firewall rule.

Access Control -- IP Address Configuration

ACL Enable	Арр
Add	

Access Control -- IP Address Configuration

Protocol:	HTTP 🗸
Port	80
Access Control	WAN 🗸
IP Protocol Type:	IPv4 🗸
Enable:	
Source IP:	-
Action	ACCEPT V
	_

Back Apply Refresh



Click **Back** to go back to the previous page, click **Apply** to apply the settings and click **Refresh** to refresh the page.

Internet Time

This is used to set Internet time settings, for synchronizing the router with an Internet time source.

Time Settings



Current Time: The current router date and time, including the time zone.

Time Service Enable:

Whether to enable or disable the time service. Tick this to enable the time service.

The default is un-ticked.

Synchronization Status:

- The status of the synchronization process.
- Time Server 1: An Internet time source to synchronize with.
- Time Server 2: An Internet time source to synchronize with.
- Time Server 3: An Internet time source to synchronize with.
- Time Server 4: An Internet time source to synchronize with.
- Time Server 5: An Internet time source to synchronize with.
- <u>Update Interval</u>: The interval at which to synchronize the local router clock with an Internet time source.
- <u>Retry Interval</u>: The interval at which to re-try router clock synchronization, in the event of a failure.
- <u>Time Zone:</u> The router time zone.
- <u>Daylight-Saving:</u> Whether to enable or disable daylight saving time.
- Tick this to enable daylight saving time. The default is un-ticked.
- Start Time: The start date and time for daylight saving time.
- End Time: The start date and time for daylight saving time.

Click **Apply** to apply the settings and click **Refresh** to refresh the page.

Time Settings

Current Time:	2020-06-26T15:52:22 GMT +02:00
Time Service Enable:	
Synchronization Status:	Synchronized
Time Server 1:	ntp.saix.net
Time Server 2:	za.pool.ntp.org
Time Server 3:	induna.saix.net
Time Server 4:	ntp1.dlink.com
Time Server 5:	ntp1.dlink.com.tw
Update Interval:	86400 (Seconds)
Retry Interval:	60 (Seconds)
Time Zone:	GMT+02:00) Athens, Istanbul, Cairo, Harare, Jerusalem 🗸
Daylight-Saving:	
Start Time:	2000 04 01 02 00 00
End Time:	2000 09 01 02 00 00

Apply Refresh



xDSL Diag

In this menu, you can enable or disable the xDSL diag. This is used for diagnosing DSL connection issues. (Used by vendors)

Click the **Apply** Button to save the settings.

Click **Refresh** to reload the page.

xDSL Diag

Enable xDSL Diag Debug Tools:

Apply Refresh



Tools

Ping

The Tools menu is used to perform connectivity tests on the DSL-G2562DG. This is used to perform ping tests. The results are displayed below the ping test options.

Host: The host to send the ICMP message to.

Repeat Number: The number of times to repeat the ping test.

Timeout (milliseconds):

The amount of time to wait before deciding that the ping test has failed.

Packet Size: This size of the ICMP packet.

Protocol Type: The protocol type to perform the ping test using.

This can be **IPv4** or **IPv6**.

WAN Connection: The WAN connection to use for the ping test.

Click **Ping** to perform the ping test and click **Refresh** to refresh the page.

Trace

This is used to perform traceroute tests. The results of the test are displayed below the traceroute test options.

Host: The host to send the ICMP messages to.

Max TTL: The maximum Time to Live (TTL) for the ICMP messages.

The is the maximum number of hops that an ICMP packet

can pass through before the target host being declared unreachable.

This can be from 1 to 128. The default is 30.

Waiting Time: The amount of time to wait before deciding that

the host is not replying to ICMP messages.

WAN Connection: The WAN connection to use for the traceroute.

Click Trace to perform the traceroute and click Refresh to refresh the page.

Tools - Ping

Host:	
Repeat Nmuber:	5
Timeout(milliseconds):	5000
Packet Size:	56
Protocol Type:	IPv4 ₩
WAN Connection:	DHCP_WAN_ETH ¥



Refresh

Tools - Trace		
Host:		
Max TTL:	30	(1-128)
waitting Time:	5000	(2000-60000ms)
WAN Connection:	DHCP_WAN_ETH V	





Connect a Wireless Client to your Router

WPS Button

The easiest way to connect your wireless devices to the router is with WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the DSL-G2562DG router. Please refer to your user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

Step 1 - Press the WPS button on the DSL-G2562DG for about 1 second. The WPS LED on the front will start to blink.



Step 2 - Within 2 minutes, press the WPS button on your wireless device (or launch the software utility and start the WPS process).

Step 3 - Allow up to 1 minute for your connection to be configured. Once the WPS LED stops blinking, you will be connected and your wireless connection will be encrypted with WPA2.



Windows[®] 10

When connecting to the DSL-G2562DG wirelessly for the first time, you will need to input the wireless network name (SSID) and Wi-Fi password (security key) of the device you are connecting to. If your product has a Wi-Fi configuration card, you can find the default network name and Wi-Fi password here. Otherwise refer to the product label for the default Wi-Fi network SSID and password, or enter the Wi-Fi credentials set during the product configuration.

- 1. To join an existing network, locate the wireless network icon in the taskbar, next to the time display and click on it.
- 2. Clicking on this icon will display a list of wireless networks which are within range of your computer. Select the desired network by clicking on the SSID.
- 3. To connect to the SSID, click Connect.
- 4. To automatically connect with the router when your device next detects the SSID, click the **Connect Automatically** check box.
- 5. You will then be prompted to enter the Wi-Fi password (network security key) for the wireless network. Enter the password into the box and click **Next** to connect to the network. Your computer will now automatically connect to this wireless network when it is detected.
- You can also use Wi-Fi Protected Setup (WPS) to connect to the router.
 Press the WPS button on your D-Link device and you will be automatically connected.



Windows[®] 8

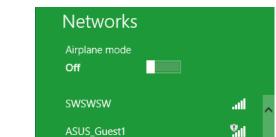
It is recommended that you enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key (Wi-Fi password) being used.

Wi-Fi

d-link-07725

Connected

- 1. To join an existing network, locate the wireless network icon in the taskbar next to the time display.
- 2. Clicking on this icon will display a list of wireless networks that are within connecting proximity of your computer. Select the desired network by clicking on the network name.
- 3. You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.
- 4. If you wish to use Wi-Fi Protected Setup (WPS) to connect to the router, you can also press the WPS button on your router during this step to enable the WPS function.
- 5. When you have established a successful connection to a wireless network, the word **Connected** will appear next to the name of the network to which you are connected to.



TP-PLC Router

Wireless Icon

11:35 AM 1/21/2013

9



Windows[®] 7

It is recommended that you enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Click on the wireless icon in your system tray (lower-right corner).



Wireless Icon

2. The utility will display any available wireless networks in your area.

3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

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

4. The following window appears while your computer tries to connect to the router.





WPS

Command Prompt

Pictures

Music

Computer

Control Panel

Devices and Printers

Default Programs

Help and Support

Shut down 🕨

0

1

Q

TeamViewer 14

Notepad

QXDM

Snipping Tool

Getting Started

Connect to a Projecto

Calculator

Sticky Notes

All Programs

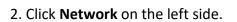
Search programs and files

Launch Virtual Serial Port Driver

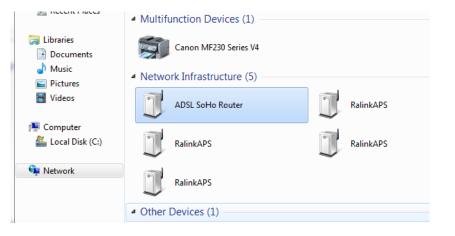
The WPS feature of the DSL-G2562DG can be configured using WindowsR 7. Carry out the following steps to use WindowsR 7 to configure the WPS feature:

1. Click the **Start** button and select **Computer** from the Start menu.





3. Double-click the DSL-G2562DG (Will be displayed as RAlinkAPS).





4. Input the WPS PIN number (on the router label) in the **Setup** > **Wireless Setup** menu in the Router's Web UI) and click **Next**.

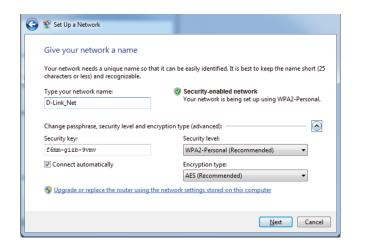
5. Type a name to identify the network.

😰 Set Up a Network	
Give your network a name	
Your network needs a unique name so t characters or less) and recognizable.	hat it can be easily identified. It is best to keep the name short (2
Type your network name:	🖉 Security-enabled network
D-Link_Net	Your network is being set up using WPA2-Personal.
Upgrade or replace the router using	the network settings stored on this computer

Set Up a Network	
To set up a network, type the 8-digit PIN from the router label	
You can find the numeric PIN on a label attached to the router or in the printed information that came from the manufacture. PIN:	
Next	Cancel

6. To configure advanced settings, click the Arrow icon.

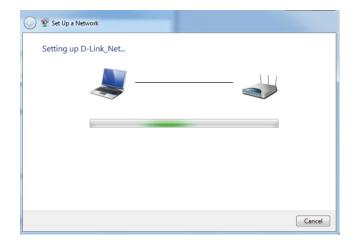
Click Next to continue.





7. The following window appears while the DSL-G2562DG is being configured.

Wait for the configuration to complete.



8. The following window informs you that WPS on the DSL-G2562DG has been set up successfully.

Make a note of the security key as you may need to provide this security key if adding an older wireless device to the network in the future.

9. Click **Close** to complete WPS setup.

	d an older wireless device to this network, you might need to provide this security key
	894g-eyd5-g5wb
For a	ming consoles or computers running Windows XP, convite network public to a USB drive
	sming consoles or computers running Windows XP, <u>copy the network profile to a USB drive</u> set up.



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DSL-G2562DG. Read the following descriptions if you are having problems. The examples below are illustrated in WindowsR XP. If you have a different operating system, the screenshots on your computer will look similar to these examples.

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

When entering the IP address of the D-Link router (**10.0.0.2** for example), make sure you are not connected to a website, you don't have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
 - Microsoft Internet ExplorerR 10 or higher
 - Microsoft EDGE Browser 20 or higher
 - Mozilla Firefox 11 or higher
 - Google™ Chrome 17 or higher
 - Apple Safari 5 or higher
- Verify physical connectivity by checking for solid LAN lights on the device. If you do not get a solid LAN light, try using a different cable, or connect to a different port on the device. If the computer is turned off, the link light may not be on.
- Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black ICE, Sygate, Norton Personal Firewall, and WindowsR XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.
- Configure your Internet settings:
 - Go to Start > Settings > Control Panel. Double-click the Internet Options Icon. From the Security tab, click the button to restore the settings to their defaults.
 - Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.
 - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
 - Close your web browser (if open) and open it.



- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

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

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

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, press and hold the rest button down for 20-25 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is **10.0.0.2**. When logging in, the default username is admin and the default password it admin.

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

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

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

- Click on **Start** and then click **Run**.
- Windows[®] 95, 98, and Me users type in command (WindowsR NT, 2000, XP, Vista, 7, 8.x, and 10 users type in cmd) and press Enter (or click OK).
 - Once the window opens, you'll need to do a special ping.
 Use the following syntax: ping [url] [-f] [-l] [MTU value]
 Example: ping yahoo.com -f -l 1472

	C:\>ping yahoo.com -f -1 1482
	Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:
).	Packet needs to be fragmented but DF set. Packet needs to be fragmented but DF set. Packet needs to be fragmented but DF set. Packet needs to be fragmented but DF set.
	Ping statistics for 66.94.234.13: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
b	C:∖>ping yahoo.com -f -l 1472
	Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:
	Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52 Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52 Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52 Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52
	Ping statistics for 66.94.234.13: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 93ms, Maximum = 203ms, Average = 132ms
	C+\ >



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

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

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

- Open your browser, enter the IP address of your router (192.168.1.1) and click **OK**.
- Enter your username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on Setup and then click Manual Configure.
- To change the MTU, enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.



Wireless Basics

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

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

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards. Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A wireless router is a device used to provide this link.

What is Wireless?

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

Why D-Link Wireless?

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



How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

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

Who uses wireless?

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

Home Uses/Benefits

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



Small Office and Home Office Uses/Benefits

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

Where is wireless used?

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

Using a D-Link USB adapter with your laptop, you can access the hotspot to connect to the Internet from remote locations like: airports, hotels, coffee shops, libraries, restaurants, and convention centres.

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

Tips

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

Centralize your router or access point

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



Eliminate Interference

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

Security

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

Wireless Modes

There are basically two modes of networking:

- Infrastructure All wireless clients will connect to an access point or wireless router.
- Ad-hoc Directly connecting to another computer for peer-to-peer communication using wireless network adapters on each computer, such as two or more DSL-G2562DG wireless network USB adapters.

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

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

Networking Basics

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

Click on Start > Run. In the run box type cmd and click OK. (WindowsR 7/Vista users type cmd in the Start Search box.)

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

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

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

C:\WINDOWS\system32\cmd.exe
Connection-specific DNS Suffix . : localhost
Vireless LAN adapter Local Area Connection* 11:
Media State Media disconnected Connection-specific DNS Suffix . :
Vireless LAN adapter Local Area Connection* 14:
Media State Media disconnected Connection-specific DNS Suffix . :
Vireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix .: Link-local IPv6 Address : fe80::14d5:9f08:b952:b322%17 IPv4 Address : 192.168.100.160 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.100.1
C:\Users\Dawie>



Statically Assign an IP address

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

Step 1

Windows[®] 7- Click on Start > Control Panel > Network and Internet > Network and Sharing Centre > Change Adaptor Options Windows[®] 8,10 - Click on Start > Search for Control Panel > Network and Internet > Network and Sharing Centre > Change adaptor settings.

Step 2

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

Step 3

Highlight Internet Protocol version 4 (TCP/IP) and click Properties.

Step 4

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

Example: If the router's LAN IP address is 10.0.0.2, make your IP address 10.0.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set the Default Gateway the same as the LAN IP address of your router (I.E. 10.0.0.2).

Set Primary DNS the same as the LAN IP address of your router (10.0.0.2). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5

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

Internet Protocol Version 4 (TCP/IPv4)	Properties	×
General		
You can get IP settings assigned auton this capability. Otherwise, you need to for the appropriate IP settings.		
Obtain an IP address automatical	у	
Use the following IP address:		_
IP address:	10 . 0 . 0 . 5	
Subnet mask:	255.0.0.0	
Default gateway:	10 . 0 . 0 . 2	
Obtain DNS server address autom	natically	
Use the following DNS server add	resses:	- 1
Preferred DNS server:	10 . 0 . 0 . 2	
Alternate DNS server:		
Validate settings upon exit	Advanced	
	OK Cane	cel



Wireless Security

This section will show you the different levels of encryption you can use to help protect your data from intruders. The DSL-G2562DG offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA2-PSK (Pre-Shared Key)
- WPA (Wi-Fi Protected Access)
- WPA-PSK (Pre-Shared Key)

What is WPA?

WPA (Wi-Fi Protected Access), is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more robust public-key encryption system to ensure that only authorized network users can access the network.

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

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more robust public key encryption system to ensure that only authorized network users can access the network.



Technical Specifications

Device Interfaces

- 4 x RJ-45 Gigabit Ethernet LAN ports
- 1 x FXS RJ-11 ports
- 1 x RJ-45 Gigabit Ethernet WAN port
- 2.4 GHz and 5 GHz wireless for 802.11 a/b/g/n/ac
- 1 x USB 3.0 port

Antenna Types

• 2 external dual band detachable antennas

Standards

- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n
- IEEE 802.11ac
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3az
- IEEE 802.3x
- IEEE 802.11e
- IEEE 802.1p

Wi-Fi Encryption

- WPA[™] Personal/Enterprise
- WPA2[™] Personal/Enterprise
- Wi-Fi Protected Setup (WPS) PIN/PBC

Power

- Input: 100 to 240 V AC, 50/60 Hz
- Output: 12 V DC, 1.5 A

Operating Temperature

• 0 to 40 °C (32 to 104 °F)

Storage Temperature

• -20 to 80 °C (-4 to 176 °F)

Operating Humidity

• 5% to 85% maximum (non-condensing)

Certifications

• CE

Dimensions

• 210 x 150 x 37 mm (8.26 x 5.91 x 1.46 in)

Weight

• 475.7 g (1.05 lbs)



Regulatory Information

CE EMI Class A Warning

This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

CE

	Frequency Band(s)	Max. Output Power (EIRP)
	Frequenzband	Max. Output Power
	Fréquence bande(s)	Consommation d'énergie max.
	Bandas de Frecuencia	Potencia máxima de Salida
	Frequenza/e	Potenza max. Output
	Frequentie(s)	Max. Output Power
5 GHz	5.15 – 5.25 GHz	200mW
	5.25 – 5.35 GHz	200Mw
	5.47 – 5.725 GHz	1W
2.4 GHz	2.4 – 2.4835 GHz	100 mW