



DG-HR1420

150Mbps WI-FI BROADBAND 3G HOME ROUTER

WITH USB PORT

User Manual

V1.0

2014-09-23

As our products undergo continuous development the specifications are subject to change without prior notice

COPYRIGHT

Copyright 2014 by Smartlink Network Systems Ltd. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company.

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents thereof without obligation to notify any person of such revision or changes.

Trademarks:

DIGISOL™ is a trademark of Smartlink Network Systems Ltd. All other trademarks are the property of the respective manufacturers.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

INDEX

1. Product Introduction.....	4
1-1 Introduction.....	4
1-2 Safety Information.....	5
1-3 System Requirements.....	6
1-4 Package Contents.....	6
2 Get Familiar with your new wireless broadband router.....	7
2-1 Front Panel.....	7
2-2 Back Panel.....	9
2-3 Hardware Installation.....	10
3. Quick Install Guide.....	12
3-1 Connecting to wireless broadband router by web browser.....	12
3-2 Getting Started.....	15
3-3 Using Wizard.....	17
3-4 Using Setup.....	24
3-5 Advanced.....	48
3-6 Service.....	62
3-7 Maintenance.....	73
4. Appendix.....	79
5. Glossary.....	81

1. Product Introduction

1-1 Introduction

Thank you for purchasing DG-HR1420 150Mbps 802.11n Wireless Broadband Home Router! DG-HR1420 is the best choice for Small office / Home office users, all computers and network devices can share a single xDSL / cable modem internet connection at high speed. Easy install procedures allow computer users to setup a network environment in very short time - within minutes, even inexperienced users. When the number of your computers and network-enabled devices grow, you can also expand the number of network slots by simply connecting a hub or switch, to extend the scope of your network.

All computers and IEEE 802.11b/g/n wireless-enabled network devices (including PDA, cellular phone, game console and more) can connect to this wireless router without additional cabling. With a compatible wireless card installed in your PC, you can transfer files up to 150Mbps (transfer data rate).

Other features of this router include:

- High Internet Access throughput.
- Wireless speed up to 150Mbps.
- Allows multiple users to share a single Internet line.
- Shares a single Cable or xDSL internet connection.
- Access private LAN servers from the internet.
- Four wired LAN ports (10/100M) and one WAN port (10/100M).
- Works with IEEE 802.11b/g/n wireless LAN devices.
- Supports DHCP (Server/Client) for easy IP-address setup.
- Supports multiple wireless modes like: AP, Client, Wireless Bridge and Universal Repeater.
- Advanced network and security features like: Special Applications, QoS, DMZ, Virtual Servers, Access Control, Firewall.
- Allows you to monitor the router's status like: DHCP Client Log, System Log, Security Log and Device/Connection Status.
- Easy to use Web-based GUI for network configuration and management purposes.
- Remote management function allows configuration and upgrades from a remote computer (over the Internet).
- Provides Auto MDI / MDI-X function for all wired Ethernet ports.

1-2 Safety Information

In order to keep the safety of users and your properties, please follow the safety instructions as mentioned below:

1. This router is designed for indoor use only; **DO NOT** place this router outdoor.
2. **DO NOT** place this router close to a hot or humid area, like kitchen or bathroom. Also, do not leave this router in the car during summer.
3. **DO NOT** pull any connected cable with force; disconnect it from the router first.
4. If you want to place this Router at a height or mount on the wall, please make sure it is firmly secured. Falling from a height would damage the router and its accessories and warranty will be void.
5. Accessories of this router, like antenna and power supply, are dangerous to small children. **KEEP THIS ROUTER OUT OF REACH OF CHILDREN.**
6. The Router will get heated up when used for long time (This is normal and is not a malfunction). **DO NOT** put this Access Point on paper, cloth, or other flammable materials.
7. There's no user-serviceable part inside the router. If you find that the router is not working properly, please contact your dealer of purchase and ask for help. **DO NOT** disassemble the router, warranty will be void.
8. If the router falls into water when it's powered, **DO NOT** use your hands to pick it up. Switch the electrical power off before you do anything, or contact an experienced electrical technician for help.
9. If you smell something strange, or even see some smoke coming out from the router or power supply, remove the power supply or switch the electrical power off immediately, and call the dealer of purchase for help.

1-3 System Requirements

- Notebook or desktop computer with network adapter. (wired/wireless)
- Internet connection, provided by xDSL or cable modem with a RJ-45 Ethernet port.
- Windows 98/ME/2000/XP/Vista
- Web browser (Microsoft Internet Explorer 4.0 or above, Netscape Navigator 4.7 or above, Opera web browser, or Safari web browser).
- An available AC power socket (100 – 240V, 50/60Hz).

1-4 Package Contents

Before you start using this router, please check if there's anything missing in the package, and contact your dealer of purchase to claim for missing items:

- DG-HR1420 Wireless Broadband Home Router
- Power adapter (5V DC, 1.5 A)
- Rubber feet (4 Nos.)
- Quick Installation Guide
- Installation Guide CD (includes User Manual & QIG)
- Patch Cord (1 No.)
- USB extension cable (1 No.)

2 Get Familiar with your new wireless broadband router

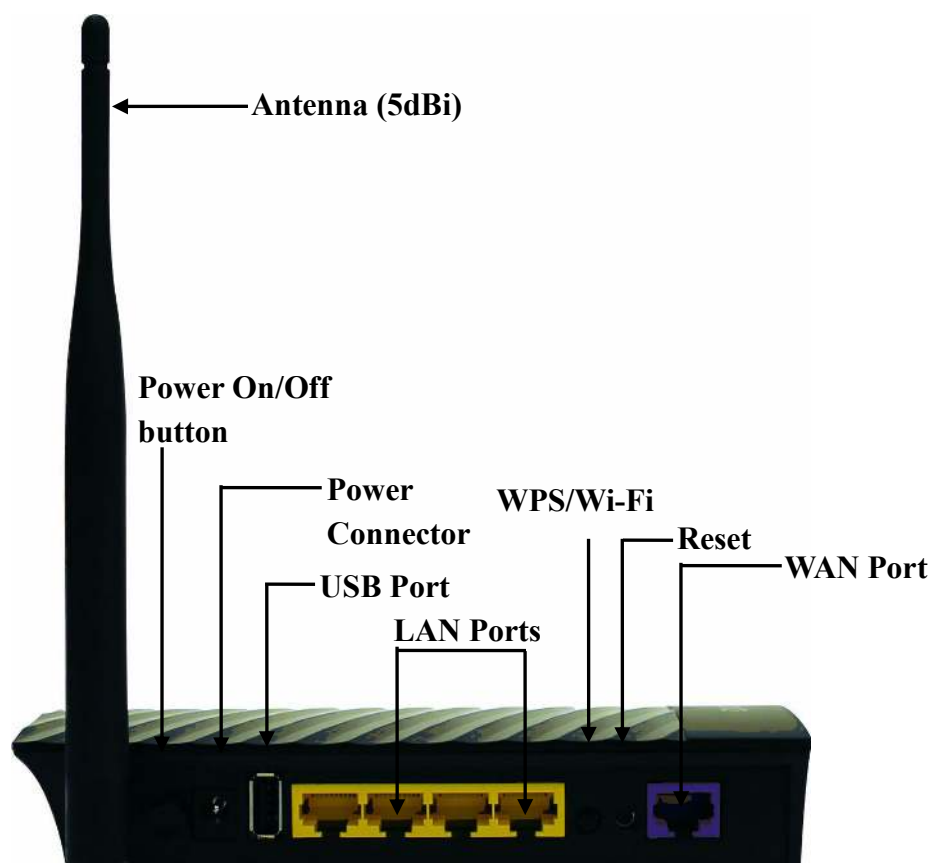
2-1 Front Panel



LED Name	LED Status	Indication
Power (PWR)	On	Router is switched on and correctly powered.
WAN	On	WAN port is connected.
	Off	WAN port is not connected.
	Blinking	WAN activity (transferring or receiving data).
LAN(1-4)	On	LAN port is connected.
	Off	LAN port is not connected.

	Blinking	LAN activity (transferring or receiving data).
WLAN	On	Wireless network is switched on.
	Off	Wireless network is switched off.
	Blinking	Wireless LAN activity (transferring or receiving data).
WPS	On	A wireless device has been successfully added to the network by WPS function.
	Off	WPS process is not initiated.
	Blinking	A wireless device is connecting to the network by WPS function.
USB	On	USB device is connected.
	Off	USB device is not connected.

2-2 Back Panel

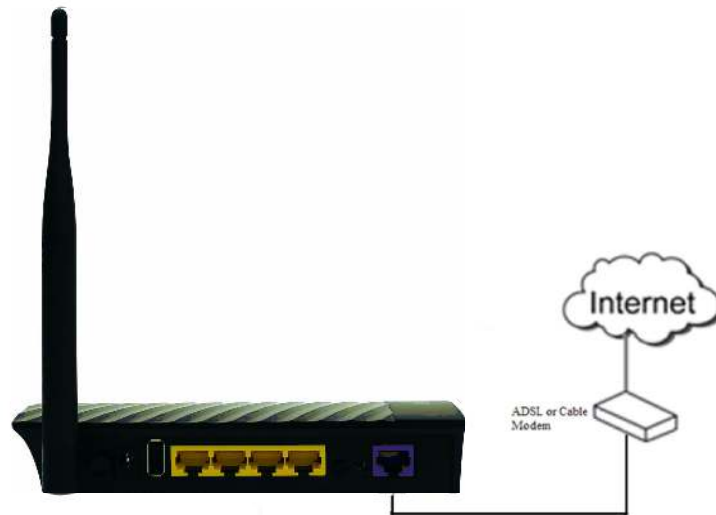


Interfaces	Description
Antenna	This antenna is a 5dBi dipole antenna.
Power on/off button	Press this button to power on/off the router.
Power Connector	The Power socket is where you will connect the power adapter. Please use the power adapter provided with this Wireless Router.
USB Port	To connect compatible USB Devices. (3G Dongle, USB Mass Storage)
LAN (1 – 4)	Local Area Network (LAN) ports 1 to 4.
WPS/WIFI	The WPS/WIFI button has two functions. WPS: Press this button for more than 5 seconds to initiate WPS. WIFI: Press this button for less than 5 seconds to enable WLAN.
Reset	Reset the router to factory default settings (clear all settings). Press this button and hold for 5 seconds to restore all settings to factory defaults.
WAN	Wide Area Network (WAN / Internet) port.

2-3 Hardware Installation

Please follow the below mentioned instructions to build the network connection between your new WIRELESS router and your computers network devices:

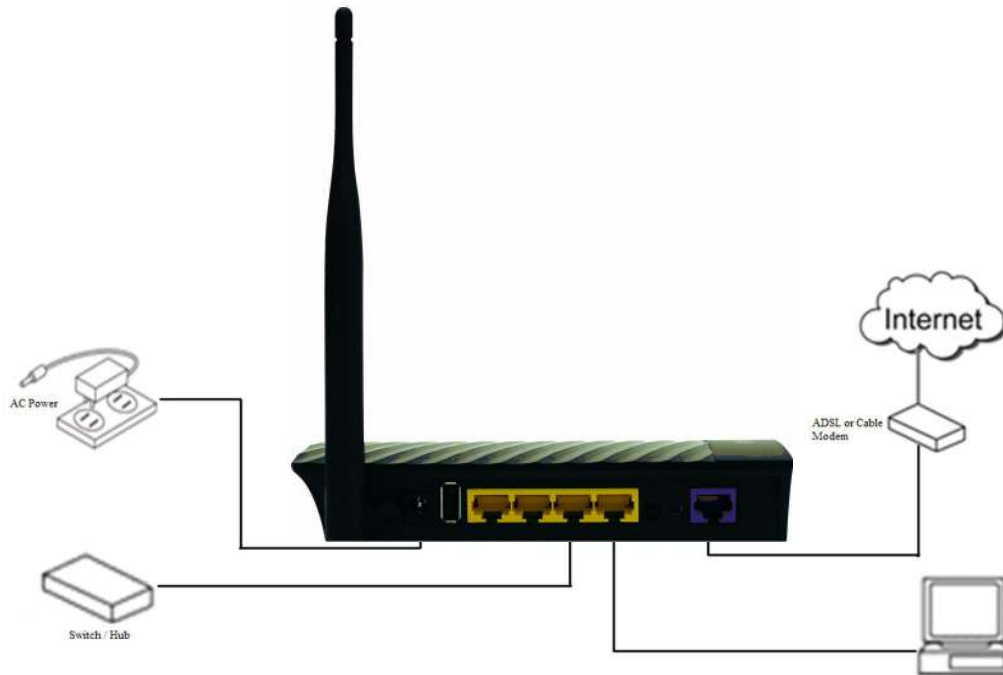
1. Connect your xDSL / cable modem to the WAN port of the router by an Ethernet cable.



2. Connect all your computers, network devices (switch / hub) to the LAN port of the router.



3. Connect the power adapter (5V DC / 1.5A) to the wall socket, and then connect it to the '**P**ower' socket of the router.



4. Please check all LEDs on the front panel. Power LED '**PWR**' should be steadily ON, WAN and LAN LEDs should be ON. Check if the computer/network device connected to the respective port of the router is powered ON and correctly connected. If power LED '**PWR**' is not ON, or any LED you expected is not ON, please recheck the cabling.

3. Quick Install Guide

3-1 Connecting to wireless broadband router by web browser

After the network connection is setup, next step is to setup the router with proper network parameters, so it can work properly in your network environment.

Please use the web browser to configure the router. A computer with wired Ethernet connection to the router is required for this first-time configuration.

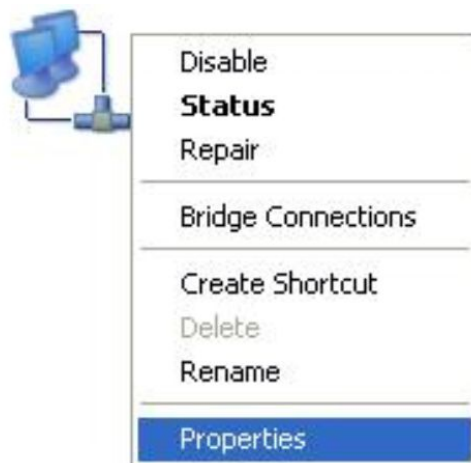
Before you start to configure the router (**default IP 192.168.1.1**), please configure the IP address of the computer in the same network class as that of the router.

Set the Network Configurations:

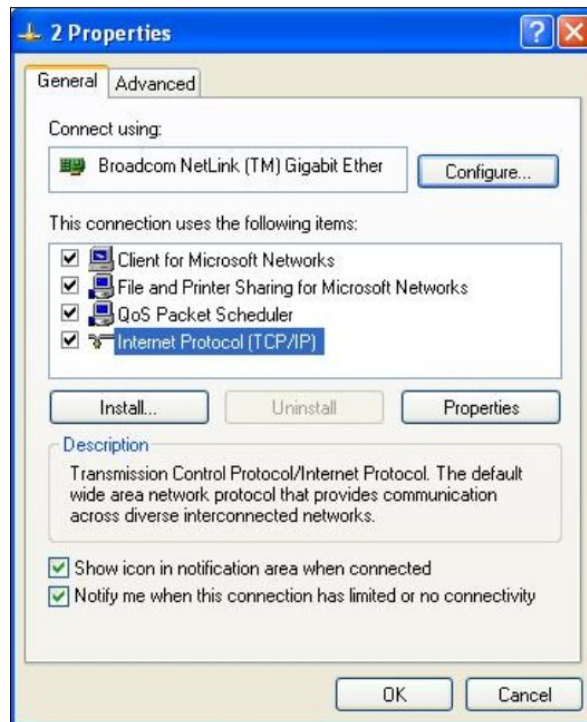
1. On your computer desktop right click "**My Network Places**" and select "**Properties**".



2. Right click "**local Area Network Connection**" and select "**Properties**".



3. Select "**Internet Protocol (TCP/IP)**" and click "**Properties**".



4. Select "**Obtain an IP address automatically**" or select "**Use the following IP address**".

- A. Select "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**". Click "**OK**".



B. "Use the following IP address"

IP Address: 192.168.1.XXX (XXX is a number from 2~254)

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

DNS Server: You need to input the DNS server address provided by your ISP.

Otherwise, you can use the Router's default gateway as the DNS proxy server.

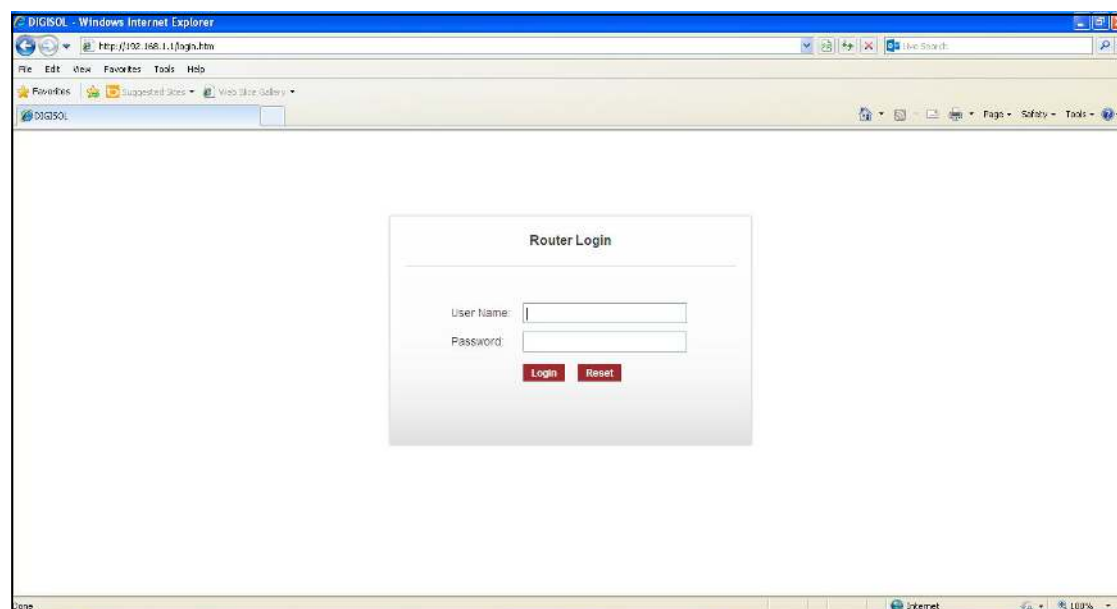
Click "**OK**" to save the configurations.

3-2 Getting Started

Connecting the router's management interface by web browser:

After you assign an IP address to the computer, open the web browser, and type the IP address of the router in the address bar as '**http://192.168.1.1**'.

The following message should be shown:



Please input the user name and password in the field respectively, default user name is '**admin**', and default password is '**1234**', then press '**Login**' button, and you can see the web management interface of this router:

DG-HR1420
150Mbps Wireless
3G Broadband Router

Status
Wizard
Setup
Advanced
Service
Firewall
Maintenance

Device_info

> Device_info

Statistics

Wireless Router Status

This page shows the current status and some basic settings of the device.

System

Alias Name	DG-HR1420
Uptime	0 0:14:57
Date/Time	Sun Jan 1 2012 5:44:57
Firmware Version	V1.0.0
Built Date	Sep 3 2014 10:06:30

LAN Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
IPv6 Address	fe80::205:1dff:fe03:405
DHCP Server	Enable
MAC Address	00:17:7C:31:27:65

DNS Status

DNS Mode	Manual
DNS Servers	4.2.2.2 4.2.2.3 8.8.8.8
IPv6 DNS Mode	Auto
IPv6 DNS Servers	

Ethernet WAN Interfaces

Interface	Droute	Protocol	IP Address	Gateway	Status
WAND	On	STATIC IP	121.242.57.56	121.242.57.33	down

Ethernet WAN IPv6 Configuration

Interface	Protocol	IPv6 Address	Prefix	Gateway	Droute	Status
WAND	STATIC IP					down

WAN 3G Connections

Interface	Droute	Protocol	IP Address	Gateway	Status

Refresh

Technical Support - 1800 209 3444

NOTE: If you can't see the web management interface, and you're being prompted to input user name and password again, it means you did not input username and password correctly. Please retype user name and password again.

TIP: This page shows the current status and some basic settings of the device.

3-3 Using Wizard

This router provides a ‘**Quick Setup Wizard**’ procedure, which will help you to complete all required settings you need to access the Internet in very short time. Please follow the instructions mentioned below to complete the ‘**Quick Setup**’:

Please go to Quick Setup menu by clicking on ‘**Wizard**’ button.

DIGISOL™ DG-HR1420 150Mbps Wireless 3G Broadband Router

Status **Wizard** Setup Advanced Service Firewall Maintenance

Quick Setup Wizard

Quick Setup Wizard

Quick Setup
The wizard will help you do some basic configurations step by step.
Step 1: WAN Connection Setting
Step 2: WLAN Connection Setting
Step 3: Save Setting

Step 1: WAN Connection Setting: Please select the wan connection mode

Connection Mode:
 DHCP Client
 Static IP
 PPP over Ethernet(PPPoE)
 3G Mode

PPP Settings: Username: Password:

WAN IP Settings: Attain IP Automatically

Default Route: Enable Disable

DNS Settings: Attain DNS Automatically
 Set DNS Manually :

DNS Server 1:

DNS Server 2:

Next

Technical Support - 1800 209 3444

Please follow the steps and complete the router configuration.

Step 1 WAN Connection Setting:

1) If “DHCP Client” option is selected the following screen will appear.

Step 1: WAN Connection Setting:
Please select the wan connection mode

Connection Mode:

DHCP Client

Static IP

PPP over Ethernet(PPPoE)

3G Mode

WAN IP Settings:

Attain IP Automatically

DNS Settings:

Attain DNS Automatically

Set DNS Manually :

DNS Server 1:

DNS Server 2:

Next

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
Connection Mode	Mode of WAN connection.
WAN IP Settings	Under DHCP Mode, the Router will obtain the IP address on WAN port.
DNS Settings	You can attain DNS automatically.

After the settings are done click on “Next”.

2) If “Static IP” is selected, the following screen will appear.

Step 1: WAN Connection Setting:
Please select the wan connection mode

Connection Mode:

DHCP Client

Static IP

PPP over Ethernet(PPPoE)

3G Mode

WAN IP Settings:

Attain IP Automatically

IP Manually:

IP Address:

Netmask:

Gateway:

Default Route: Enable Disable

DNS Settings:

Attain DNS Automatically

Set DNS Manually :

DNS Server 1:

DNS Server 2:

Next

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
Connection Mode	Select the mode of WAN connection.
IP address	Enter the IP address.
Net mask	Enter the net mask.
Gateway	Enter the gateway.
Default Route	Enable or Disable the default route.
DNS Settings	You can either attain DNS automatically or Set DNS manually.
DNS Server1/2	User can define the DNS server address.

After the settings are done click on “Next”.

3) If “PPPoE” is selected, the following screen will appear.

Step 1: WAN Connection Setting:
Please select the wan connection mode

Connection Mode:

DHCP Client

Static IP

PPP over Ethernet(PPPoE)

3G Mode

PPP Settings:

Username: Password:

WAN IP Settings:

Attain IP Automatically

Default Route:

Enable Disable

DNS Settings:

Attain DNS Automatically

Set DNS Manually :

DNS Server 1:

DNS Server 2:

Next

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
Connection Mode	Select the mode of WAN connection.
PPP Settings	Enter the user name and password assigned by your Internet service provider here.
WAN IP Settings	The Router will obtain the IP address from the ISP.
Default Route	Enable or Disable the default route.
DNS Settings	You can either attain DNS automatically or Set DNS manually.
DNS Server1/2	User can define the DNS server address.

After the settings are done click on “Next”.

4) 3G

Router will support only compatible USB 3G Dongles and the support list can be downloaded from www.digisol.com or call 1800 209 3444 or email to helpdesk@smartlink.co.in

Quick Setup
 The wizard will help you do some basic configurations step by step.
 Step 1: WAN Connection Setting
 Step 2: WLAN Connection Setting
 Step 3: Save Setting

Step 1: WAN Connection Setting: Please select the wan connection mode

Connection Mode:

DHCP Client

Static IP

PPP over Ethernet(PPPoE)

3G Mode

3G Connection Settings Please config the settings if 3G USB card is plugged

PIN:

APN:

Dial Number:

Authentication: ▼

User Name:

Password:

Next

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
PIN	Enter the Pin – Check with 3G Service provider.
APN	Enter the APN - Check with 3G Service provider.
Dial Number	Enter the dial number e.g. *99#, #777 etc. as per ISP.

User Name	Enter username – Check with 3G service provider.
Password	Enter password – Check with 3G service provider.

After the settings are done click on “**Next**”.

Step 2: Wireless Settings

Step 2: Wireless Settings: Please config basic settings about wireless.

Wireless: Enable Disable

Band: 2.4 GHz (B+G+N) ▼

SSID: DIGISOL

Wireless Security: None ▼

Back **Next**

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
Wireless	You can enable or disable wireless.
Band	You can select the appropriate band setting form the list.
SSID	This is the name of wireless network. Input the SSID name.
Wireless Security	If wireless security is enabled on the access point, you have to follow the same settings in order to access it.

After the settings are done click on “**Next**”.

Step 3: Save Settings

Step 3: Save Settings	Please click "Apply Changes" if you want to save the settings to router.
Settings as follow:	
WAN Mode:	DHCP
IP Setting:	Ip Automatically
DNS Setting:	DNS Automatically
Wireless :	Enable
Back	Apply Changes Cancel
Technical Support - 1800 209 3444	

Here is the description of every setup item:

Parameter	Description
WAN Mode	The selected WAN mode will appear here.
IP Setting	IP setting as configured will be displayed here.
DNS Setting	DNS Setting as configured will appear here.
Wireless	Enable or Disable will appear for wireless.

To apply the changes, click on “**Apply Changes**”. To cancel the changes, click on “**Cancel**”. To go back to the previous screen click on “**Back**”.

3-4 Using Setup

Step 1 Setup WAN Connection Type:

WAN Configuration

This page is used to configure the parameters for the WAN interface of your Ethernet Modem/Router. Note : When connect type of PPPoE and PPPoA only is "Manual", the "Connect" and "Disconnect" button will be enabled.

WAN Mode:

Host Name: MTU:

IP Protocol:

DNS Settings:

Attain DNS Automatically Set DNS Manually

MAC Clone: (ex. 00E086710502)

Default MAC MAC from PC MAC Manual

WAN Port Speed:

IPv6 WAN Setting:

WAN Interfaces Table:

Select	Inf	Mode	IP Addr	Remote IP	NetMask	Status
<input type="radio"/>	WAN0	Static IP	121.242.57.56	121.242.57.33	255.255.255.0	Down

Technical Support - 1800 209 3444

Below given 'WAN Connection Type' screen will appear.

Please choose the broadband (Internet connection) type you're using in this page. There are three types of Internet connection DHCP, Static IP and PPPoE.

If you're not sure, please contact your Internet service provider. A wrong Internet connection type will cause connection problem, and you will not be able to connect to the internet.

If you want to go back to previous step, please press 'Back' button.

NOTE: Some service providers use ‘DHCP’ (Dynamic Host Configuration Protocol) to assign IP address to your router. In this case, you can choose ‘Dynamic IP’ as Internet connection type.

A) Setup procedure for ‘DHCP’:

Select DHCP to obtain IP Address information automatically from your ISP.

Usually Cable Modem and the router will automatically obtain an IP address from the DHCP server.

WAN Configuration

This page is used to configure the parameters for the WAN interface of your Ethernet Modem/Router. Note : When connect type of PPPoE and PPPoA only is "Manual", the "Connect" and "Disconnect" button will be enabled.

WAN Mode:	<input type="text" value="DHCP"/>		
Host Name:	<input type="text"/>	MTU:	<input type="text" value="1500"/>

IP Protocol:	<input type="text" value="Ipv4/Ipv6"/>
--------------	--

DNS Settings:

Attain DNS Automatically
 Set DNS Manually

MAC Clone:	<input type="text" value="d027885ebcf2"/> (ex. 00E086710502)
<input checked="" type="radio"/> Default MAC <input type="radio"/> MAC from PC <input type="radio"/> MAC Manual	

WAN Port Speed:	<input type="text" value="Auto Negotiation"/>
-----------------	---

IPv6 WAN Setting:

Apply Changes
Refresh

WAN Interfaces Table:

Select	Inf	Mode	IP Addr	Remote IP	NetMask	Status
<input type="radio"/>	WAN0	Static IP	121.242.57.56	121.242.57.33	255.255.255.0	Down

Technical Support - 1800 209 3444

B) Setup procedure for 'Static IP':

Select Static IP Address if IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address and DNS address provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format. Below given screen will be displayed.

WAN Configuration

This page is used to configure the parameters for the WAN interface of your Ethernet Modem/Router. Note : When connect type of PPPoE and PPPoA only is "Manual", the "Connect" and "Disconnect" button will be enabled.

WAN Mode:	<input type="text" value="Static IP"/>		
		MTU:	<input type="text" value="1500"/>

IP Protocol:	<input type="text" value="Ipv4/Ipv6"/>
---------------------	--

WAN IP Settings:			
Local IP Address:	<input type="text"/>	Remote IP Address:	<input type="text"/>
NetMask:	<input type="text"/>		

DNS Settings:	
<input checked="" type="radio"/> Attain DNS Automatically	<input type="radio"/> Set DNS Manually

Mac Clone:	<input type="text" value="d027885ebcf2"/> (ex. 00E086710502)	
<input checked="" type="radio"/> Default Mac	<input type="radio"/> Mac from pc	<input type="radio"/> Mac Manual

WAN Port Speed:	<input type="text" value="auto"/>
------------------------	-----------------------------------

IPv6 WAN Setting:	<input type="text" value="v"/>
--------------------------	--------------------------------

Apply Changes
Refresh

WAN Interfaces Table:

Select	Inf	Mode	IP Addr	Remote IP	NetMask	Status
<input type="radio"/>	WAN0	Static IP	121.242.57.56	121.242.57.33	255.255.255.0	Down

Technical Support - 1800 209 3444

C) Setup procedure for 'PPPoE':

Choose PPPoE. (Point to Point Protocol over Ethernet) If your ISP uses a PPPoE connection it will provide you with a username and password. This option is typically used for DSL services. Below given screen will be displayed.

WAN Configuration

This page is used to configure the parameters for the WAN interface of your Ethernet Modem/Router. Note : When connect type of PPPoE and PPPoA only is "Manual", the "Connect" and "Disconnect" button will be enabled.

WAN Mode:	PPPoE <input type="button" value="v"/>		
Service Name:	<input type="text"/>	MTU:	<input type="text" value="1492"/>

IP Protocol:	Ipv4/Ipv6 <input type="button" value="v"/>
---------------------	--

PPP Settings:			
User Name:	<input type="text"/>	Password:	<input type="text"/>
Type:	Continuous <input type="button" value="v"/>	Idle Time (min):	<input type="text"/>

DNS Settings:	
<input checked="" type="radio"/> Attain DNS Automatically	<input type="radio"/> Set DNS Manually

Mac Clone:	<input type="text" value="d027885ebcf2"/>	<small>(ex. 00E086710502)</small>
<input checked="" type="radio"/> Default Mac	<input type="radio"/> Mac from pc	<input type="radio"/> Mac Manual

WAN Port Speed:	auto <input type="button" value="v"/>
------------------------	---------------------------------------

IPv6 WAN Setting:	<input type="button" value="v"/>
--------------------------	----------------------------------

WAN Interfaces Table:						
Select	Inf	Mode	IP Addr	Remote IP	NetMask	Status
<input type="radio"/>	WAN0	Static IP	121.242.57.56	121.242.57.33	255.255.255.0	Down

Technical Support - 1800 209 3444

Step 2 Setup 3G Connection Type:

This page is used to configure the parameters for your 3G network access.

3G Settings

This page is used to configure the parameters for your 3G network access.

3G Signal & Card Status:	Disconnected	Refresh
3G WAN:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	
PIN Code:	<input type="text"/>	
APN:	<input type="text"/>	
Dial Number:	<input type="text" value="*99#"/>	
Authentication:	auto <input type="button" value="v"/>	
User Name:	<input type="text"/>	
Password:	<input type="text"/>	
Connection Type:	persistent <input type="button" value="v"/>	
Idle Time(min):	<input type="text" value="0"/>	
NAPT:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	
Default Route:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	
MTU:	<input type="text" value="1500"/>	
IP Type:	IPv4 <input type="button" value="v"/>	
3G to Wired switch time(s):	<input type="text" value="10"/>	

Apply Changes **Reset**

WAN 3G Connections

Interface	Route	Protocol	IP Address	Gateway	Status
-----------	-------	----------	------------	---------	--------

Refresh

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
PIN Code	Enter the Pin code – Check with 3G Service provider.
APN	Enter the APN - Check with 3G Service provider.
Dial Number	Enter the dial number e.g: *99#, #777 etc. as per ISP.
User Name	Enter username – Check with 3G service provider.
Password	Enter password – Check with 3G service provider.
Connection type	Persistent means Automatic dial & Manual means manual dial.
Idle time	Please set the time in minutes if connection type is manual mode.
NAPT	Enable/Disable Network Address Port Translation.
Default Route	Enable/ Disable default route.
MTU	Set Maximum Transfer Unit.Default value is 1500.
IP Type	Select IPv4 or IPv6 or Both.
3G to wired switch time(s)	Set the time in seconds.

Note: WAN Fail over to 3G mode functions only when the RJ-45 WAN port is physically down or the cable is unplugged.

To apply the changes, click on “**Apply Changes**”. To cancel the changes, click on “**Reset**”.

Step 3 Setup LAN:

A) Below given 'LAN' screen will appear.

Here is the description of every setup item:

Parameter	Description
IP address	Enter the LAN IP address.
Subnet Mask	Enter the subnet mask.
Secondary IP	Secondary IP address of any subnet can be added to manage the router.
IGMP Snooping	If enabled, the router will listen to the IGMP traffic or conversations between the hosts and routers on the network.
MAC Address Control	Using this feature the LAN clients are allowed and disallowed access to internet on the selected LAN/WLAN port.
MAC Address Table	The MAC address listed will be allowed to access the internet.

When you finish with all settings, press 'Next'; if you want to go back to previous menu, click 'Back'.

B) DHCP MODE

This page can be used to configure the DHCP mode i.e. DHCP relay or DHCP server.

- 1) Enable the DHCP server if you are using this device as DHCP server. This page lists the IP address pools available to host on your LAN. The device distributes numbers in the pool to host on your network as they request internet access.
- 2) Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your host on the LAN. You can set the DHCP server IP address.
- 3) If you choose “None”, then the router will do nothing when the host requests an IP address.

WAN

LAN

- > LAN
- > DHCP
- > DHCP Static
- > LAN IPv6

Wireless

DHCP Mode

This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.
 (1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to host on your LAN. The device distributes numbers in the pool to host on your network as they request Internet access.
 (2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your host on the LAN. You can set the DHCP server IP address.
 (3)If you choose "None", then the modem will do nothing when the host request a IP address.

LAN IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0

DHCP Mode: None

Apply Changes
Undo

Set Vendor Class IP Range

Technical Support - 1800 209 3444

C) DHCP Static

This page lists the fixed IP/MAC address on your LAN. The device distributes the number configured to hosts on your network as they request internet access.

DHCP Static IP Configuration

This page lists the fixed IP/MAC address on your LAN. The device distributes the number configured to hosts on your network as they request Internet access.

IP Address:

Mac Address: (ex. 00E086710502)

Add
Delete Selected
Undo

DHCP Static IP Table:		
Select	IP Address	MAC Address

Technical Support - 1800 209 3444

D) LAN IPv6

This page is used to configure IPv6 LAN settings. User can set RA server work mode and LAN DHCPv6 server work mode.

LAN IPv6 Setting
This page is used to configurate ipv6 lan setting. User can set lan RA server work mode and lan DHCPv6 server work mode.

Lan Global Address Setting

Global Address: /

Apply Changes

RA Setting

Enable:

M Flag:

O Flag:

Max Interval: Secs

Min Interval: Secs

Prefix Mode: ▾

ULA Enable:

RA DNS Enable:

Apply Changes

DHCPv6 Setting

DHCPv6 Mode: ▾

IPv6 Address Suffix Pool: - (ex: :1:1:1:1 or ::1)

IPv6 DNS Mode: ▾

Apply Changes

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
Global Address	Specify the LAN global ipv6 address, which may be assigned by ISP.
RA Setting	
Enable	Enable or disable the Router Advertisement feature.
M Flag	Enable or disable the “Managed address configuration” flag in RA packet.
O Flag	Enable or disable the “Other configuration” flag in RA packet.
Max interval	The maximum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. Note: The Max Interval must not be less than 4 seconds and not greater than 1800 seconds.

Min Interval	The minimum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. Note: The Min Interval must not be less than 3 seconds and not greater than 0.75 * Max Interval.
Prefix Mode	Specify the RA feature prefix mode: “Auto”: The RA prefix will use WAN dhcp-pd prefix. “Manual”: User will specify the prefix Address, Length, Preferred time and Valid time.
DHCPv6 Setting	
DHCPv6 Mode	Specify the dhcpv6 server mode: “None”: Close dhcpv6 server. “Manual”: dhcpv6 server is opened and user specifies the dhcpv6 server address pool and other parameters. “Auto”: dhcpv6 server is opened and it can use Wan dhcp-pd prefix to generate address pool.

Step 4 Wireless Setup:

This page is used to configure the parameters for your wireless network.

- WAN
- LAN
- WLAN
- > Basic
- > Security
- > MBSSID
- > Access Control List
- > Advanced
- > WPS
- > Repeater

Wireless Basic Settings

This page is used to configure the parameters for your wireless network.

Disable Wireless LAN Interface

Band:

2.4 GHz (B+G+N)

Mode:

AP

SSID:

DIGISOL555

Channel Width:

40MHZ

Control Sideband:

Upper

Channel Number:

Auto

Current Channel: 2

Radio Power (Percent):

100%

Associated Clients:

Show Active Clients

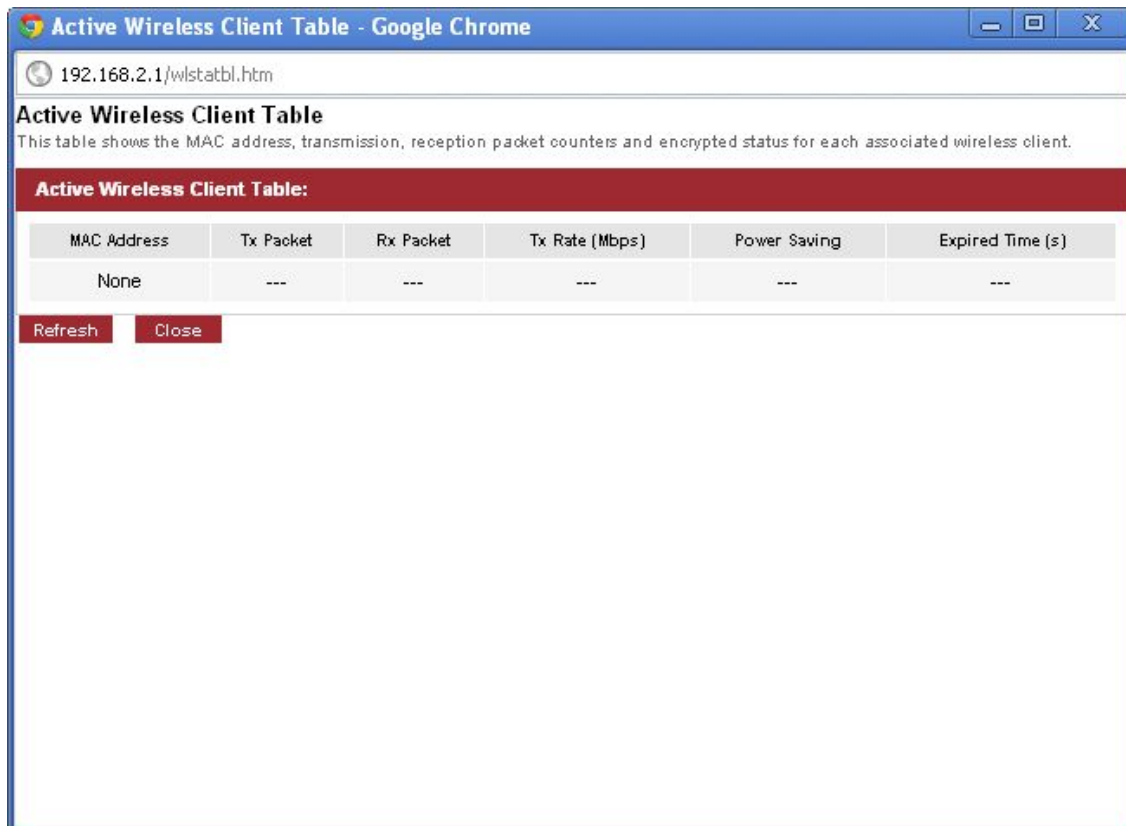
Apply Changes

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
Band	Select the appropriate radio band. The default setting is 2.4GHz (B+G+N).
Mode	Select the desired mode.
SSID	This is the name of wireless network. Input the SSID name.

Channel width	Select any channel width from the pull-down list.
Control sideband	There are two bands upper and lower. The upper band comprises of channel numbers from 5 to 11. The lower band comprises of channel numbers from 1 to 7.
Channel number	Select the channel number from the list. You can choose any channel number you want to use, and almost all wireless clients can locate the channel you are using automatically without any problem. However, it is still useful to remember the channel number you use, some wireless client supports manual channel number select, and this would help in certain scenario when there is some radio communication problem.
Radio Power (Percent)	You can choose the transmission power of the radio signal. The default one is 100%. It is recommended to choose the default value 100%.
Associated clients	Click ' Show Active Clients ' button, then an " Active Wireless Client Table " will pop up. You can see the status of all active wireless stations that are connected to the access point.



Active Wireless Client Table - Google Chrome

192.168.2.1/wlstatbl.htm

Active Wireless Client Table

This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.

Active Wireless Client Table:					
MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
None	---	---	---	---	---

Refresh Close

When you finish with all settings, press ‘**Apply changes**’.

Security Setup: This page allows you to set up the wireless security. Turning ON WEP or WPA by using encryption keys could prevent any unauthorized access to your wireless network.

WAN	Wireless Security Setup This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.
LAN	
Wireless	
> Basic	
> Security	
> MBSSID	
> Access Control List	
> Advanced	
> WPS	
> WDS	
> Repeater	
<div style="border: 1px solid black; padding: 5px;"> <div style="display: flex; justify-content: space-between;"> SSID TYPE: <input checked="" type="radio"/> Root <input type="radio"/> VAP0 <input type="radio"/> VAP1 <input type="radio"/> VAP2 <input type="radio"/> VAP3 </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> Encryption: None ▼ </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <input type="checkbox"/> Use 802.1x Authentication <input type="radio"/> WEP 64bits <input type="radio"/> WEP 128bits </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> WPA Authentication Mode: <input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key) </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> Pre-Shared Key Format: Passphrase ▼ </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> Pre-Shared Key: ***** </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> Authentication RADIUS Server: Port <input type="text" value="1812"/> IP address <input type="text" value="0.0.0.0"/> Password <input type="text"/> </div> <div style="font-size: x-small; margin-top: 5px;"> <i>Note: When encryption WEP is selected, you must set WEP key value.</i> </div> <div style="text-align: center; margin-top: 10px;"> Apply Changes </div> </div>	
Technical Support - 1800 209 3444	

Here is the description of every setup item:

Parameter	Description
SSID Type	Select the SSID type.
Encryption	Select the encryption type from the list.
Use 802.1x Authentication	Select the check box to enable 802.1x authentication.
WPA-Authentication Mode	Select Personal (Pre-Shared Key), enter the pre-shared key in the Pre-Shared Key field. Select Enterprise (RADIUS), enter the port, IP address and password of the Radius server. You need to enter the username and password provided by the Radius server when the wireless client connects the router. If the encryption is set to WEP, the router uses 802.1x authentication, which is Radius authentication.
Pre-shared key format	Select HEX or Pass phrase key type.
Pre-shared key	Enter an encryption key.
Authentication Radius Server	Enter the port, IP address and password of the Radius server.

When you finish with all settings, press ‘**Apply changes**’.

Encryption options available:

WEP

Wireless Security Setup
 This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID TYPE: Root VAP0 VAP1 VAP2 VAP3

Encryption: WEP ▼

Key Length: 64-bit ▼

Key Format: ASCII (5 character) ▼

Default Tx Key: Key 1 ▼

Encryption Key 1:

Encryption Key 2:

Encryption Key 3:

Encryption Key 4:

Use 802.1x Authentication WEP 64bits WEP 128bits

WPA Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

Pre-Shared Key Format: Passphrase ▼

Pre-Shared Key:

Authentication RADIUS Server: Port 1812 IP address 0.0.0.0 Password

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
Key length	There are two types of WEP key lengths: 64-bit and 128-bit. Using '128-bit' is safer than '64-bit', but will reduce some data transfer performance.
Key format	There are two types of key formats: ASCII and Hex. When you select a key format, the number of characters of key will be displayed. For example, if you select '64-bit' as key

	length, and 'Hex' as key format, you'll see the message at the right of 'Key Format' is Hex (10 characters), which means the length of WEP key is 10 characters.
Default Tx key	You can set the WEP key here.
Encryption keys 1-4	Input WEP key characters here, the number of characters must be the same as the number displayed at 'Key Format' field. You can use any alphanumerical characters (0-9, a-z and A-Z) if you select 'ASCII' key format, and if you select 'Hex' as key format, you can use characters 0-9, a-f and A-F.
Use 802.1x authentication	IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this wireless router before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encrypt the data during communication. If there is a RADIUS server in your environment, please enable this function. Check this box and another sub-menu will appear:
Pre-Shared key format	Select the type of pre-shared key, you can select pass phrase (8 or more alphanumerical characters, up to 63), or Hex (64 characters of 0-9 and a-f).
Pre-Shared key	Please input the WPA pass phrase here. It is not recommended to use a word that can be found in a dictionary due to security reason.

When you finish with all settings, press '**Apply changes**'.

WPA (TKIP) / WPA2 (TKIP)

Wireless Security Setup
 This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID TYPE: Root VAP0 VAP1 VAP2 VAPS

Encryption: WPA (TKIP)

Use 802.1x Authentication WEP 64bits WEP 128bits

WPA Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Authentication RADIUS Server: Port IP address Password

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
Use 802.1x Authentication	IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this wireless router before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encrypt the data during communication. If there is a RADIUS server in your environment, please enable this function. Check this box and another sub-menu will appear:
Pre-shared Key Format	Select the type of pre-shared key, you can select Pass phrase (8 or more alphanumerical characters, up to 63), or Hex (64 characters of 0-9 and a-f).
Pre-shared Key	Please input the WPA pass phrase here. It is not recommended to use a word that can be found in a dictionary due to security reason.
Authentication RADIUS server	If you have a RADIUS server, this router can work with it and provide safer wireless authentication.

When you finish with all settings, press '**Apply changes**'.

WPA (AES) / WPA2 (AES)

Wireless Security Setup
 This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID TYPE: Root VAP0 VAP1 VAP2 VAP3

Encryption: WPA (AES)

Use 802.1x Authentication WEP 64bits WEP 128bits

WPA Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Authentication RADIUS Server: Port 1912 IP address 0.0.0.0 Password

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
Use 802.1x Authentication	IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this wireless router before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encrypt the data during communication. If there is a RADIUS server in your environment, please enable this function. Check this box and another sub-menu will appear:
Pre-shared Key Format	Select the type of pre-shared key, you can select Pass phrase (8 or more alphanumerical characters, up to 63), or Hex (64 characters of 0-9 and a-f).
Pre-shared Key	Please input the WPA pass phrase here. It is not recommended to use a word that can be found in a dictionary due to security reason.
Authentication Radius server	If you have a RADIUS server, this router can work with it and provide safer wireless authentication.

When you finish with all settings, press '**Apply changes**'.

WPA2 Mixed

Wireless Security Setup
 This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID TYPE: Root VAP0 VAP1 VAP2 VAP3

Encryption: WPA2 Mixed

Use 802.1x Authentication WEP 64bits WEP 128bits

WPA Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Authentication RADIUS Server: Port: IP address: Password:

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
Use 802.1x Authentication	IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this wireless router before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encrypt the data during communication. If there is a RADIUS server in your environment, please enable this function. Check this box and another sub-menu will appear:
Pre-shared Key Format	Select the type of pre-shared key, you can select Pass phrase (8 or more alphanumerical characters, up to 63), or Hex (64 characters of 0-9 and a-f).
Pre-shared Key	Please input the WPA pass phrase here. It is not recommended to use a word that can be found in a dictionary due to security reason.
Authentication Radius server	If you have a RADIUS server, this router can work with it and provide safer wireless authentication.

When you finish with all settings, press '**Apply changes**'.

MBSSID: Here we provide several guest networks for your guests to use your router to surf the Internet temporary. You can configure your SSID, security options and so on. Guests can only access your router if you enable your guest network.

Choose menu “**Wireless→MBSSID**”, below given screen will be displayed.

Wireless Multiple BSSID Setup

This page allows you to set virtual access points(VAP). Here you can enable/disable virtual AP, and set its SSID and authentication type. click "Apply Changes" to take it effect.

<input type="checkbox"/> Enable VAP0	
SSID:	DIGISOL_1
Broadcast SSID:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Relay Blocking:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Authentication Type:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto

<input type="checkbox"/> Enable VAP1	
SSID:	DIGISOL_2
Broadcast SSID:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Relay Blocking:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Authentication Type:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto

<input type="checkbox"/> Enable VAP2	
SSID:	DIGISOL_3
Broadcast SSID:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Relay Blocking:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Authentication Type:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto

<input type="checkbox"/> Enable VAP3	
SSID:	DIGISOL_4
Broadcast SSID:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Relay Blocking:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Authentication Type:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto

Technical Support - 1800 209 3444

Access Control List:

You can specify what kind of service should be enabled in WAN on this page. Packets available in the ACL list or from IP specified can enter the AP Router.

Choose menu “**Wireless→Access Control List**”, below given screen will be displayed.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Disable

MAC Address: Allow Listed

Current Access Control List:

MAC Address	Select
-------------	--------

Technical Support - 1800 209 3444

There are three wireless access control modes: Disable, Allow Listed and Deny Listed. If you choose ‘**Allow Listed**’, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your access point. When ‘**Deny Listed**’ is selected, these wireless clients on the list will not be able to connect the access point.

Advanced:

Wireless Advanced Settings
 These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
Fragment Threshold:	<input type="text" value="2346"/> (256-2346)
RTS Threshold:	<input type="text" value="2347"/> (0-2347)
Beacon Interval:	<input type="text" value="100"/> (20-1024 ms)
DTIM Interval:	<input type="text" value="1"/> (1-255)
Data Rate:	<input type="text" value="Auto"/>
Preamble Type:	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble
Broadcast SSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Relay Blocking:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Ethernet to Wireless Blocking:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Wifi Multicast to Unicast:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Aggregation:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Short GI:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
Fragment Threshold	Used to fragment packets which help improve performance in the presence of radio frequency (RF) interference.
RTS Threshold	Determines the packet size of a transmission through the use of the router to help control traffic flow.
Beacon Interval	Set the beacon interval of wireless radio. Do not modify default value if you don't know what it is, default value is 100.
DTIM Interval	Set the DTIM period of wireless radio. Do not modify default value if you don't know what it is, default value is 1.
Data Rate	Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically, it's not necessary to change this value unless you know what will happen after modification.
Preamble Type	This is the length of the CRC (Cyclic Redundancy Check) block for communication between the router and wireless clients. High network traffic areas should select Short preamble

	type.
Broadcast SSID	Decide if the wireless router will broadcast its own ESSID or not. You can hide the ESSID of your wireless router (set the option to 'Disable'), so only people those who know the ESSID of your wireless router can get connected.
Relay Blocking	Wireless isolation. Once this field is Enabled, the wireless clients that are connected to the router cannot intercommunicate.
Ethernet to Wireless Blocking	When enabled, the wireless network can communicate with the Ethernet network or not.
WiFi Multicast to Unicast	Enable it to use unicast to transmit multicast packets.
Aggregation	It is applied when the destination end of all MPDU are for one STA.
Short GI	It is not recommended to enable GI in obvious environment of Multi-path effect.

When you finish with all settings, press '**Apply changes**'.

WPS

Through this process, you can easily add wireless clients to the network without the need for any specific configuration, such as SSID, security mode or password.

Choose menu “**Wireless**→**WPS**”, below given screen will be displayed.

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

<input type="checkbox"/> Disable WPS	
WPS Status:	<input type="radio"/> Configured <input checked="" type="radio"/> UnConfigured
Self-PIN Number:	<input type="text" value="17132213"/> <input type="button" value="Regenerate PIN"/>
Push Button Configuration:	<input type="button" value="Start PBC"/>

<input type="text"/>	<input type="button" value="Start PIN"/>
----------------------	--

Technical Support - 1800 209 3444

WPS (Wi-Fi Protected Setup) is an easy way to connect to a wireless router.

To use the wizard to add a wireless client to WPS-enabled wireless router, the client must support WPS.

Check the user manual or the box of the wireless client to confirm whether it supports the WPS.

If the wireless client does not support WPS, you must configure it manually.

You can add wireless client by PIN mode. If you use PIN mode, you should input client PIN code. Meanwhile you should start client WPS process. You can find client PIN code on client manager.

WDS

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate within the table and then enable the WDS. This page also allows you to setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

Choose menu “**Wireless**→**WDS**”, below given screen will be displayed.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

Enable WDS

Add WDS AP

MAC Address:

Comment:

Apply Changes **Reset**

Current WDS AP List:

MAC Address	Comment	Select

Delete Selected **Delete All**

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
MAC Address	Input the MAC address of other wireless routers.
Comment	You can add some comment for this item.

Repeater

This feature is used to configure the parameters for wireless repeater.

Click “**Site survey**”. Wireless networks will be displayed in the list below. Select one network and click “**Next**”.

Wireless Repeater Settings
 This page is used to configure the parameters for wireless repeater.
 Step 1: click "Site Survey". Sites surveyed will be displayed in the list below. Select one item, and click "Next".

Repeater Enabled(DHCP mode will be set to "none" if the repeater is enabled.)

SSID of AP:

#	SSID	MAC Address	Channel	Signal	Security	Select
1	IT Infra	00:17:7c:16:43:f8	11	100%	WPA2-PSK(AES)	<input type="radio"/>
2	smartlinkgoa	00:17:7c:37:1c:54	1	100%	WPA2-PSK(AES)	<input type="radio"/>
3	DIGISOL	00:17:7c:2e:10:48	11	100%	None	<input type="radio"/>
4	DigilinkAirstation1	00:17:7c:16:44:40	11	97%	WPA2-PSK(AES)	<input type="radio"/>
5	DIGISOLQA	00:17:7c:24:dc:5e	1	2%	WPA2-PSK(AES)	<input type="radio"/>

Click "Next" to Continue repeater settings

Technical Support - 1800 209 3444

Click on “**Next**”. The following screen will appear. Setup the wireless security. Turning on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Wireless Repeater Security Settings
 Step 2: Setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Wireless Security Settings

Encryption:

Attention: if you select WEP, you must set key.

Technical Support - 1800 209 3444

Click on “**Apply**”. It is strongly recommend that you modify IP address of the local gateway to avoid IP address conflicts with the center of the AP. (ex. if IP address of AP is 192.168.1.1, you can modify IP address of the local gateway to 192.168.1.2).

Finish Repeater Configuration

Step 3: click "Finish" to save the configuration.

We strongly recommend that you modify IP address of the local gateway to avoid IP address conflicts with the center of the AP. (ex. if IP address of AP is 192.168.1.1, you can modify IP address of the local gateway to 192.168.1.2).

IP Address:

Subnet Mask:

Finish

Technical Support - 1800 209 3444

3-5 Advanced

Click ‘**Advanced**’ menu on the top of web management interface, and the following message will be displayed on your web browser:

Static Route

Route

- > Static Route
- > IPv6 Static Route
- > RIP

NAT

QoS

Port Mapping

Others

Routing Configuration

This page is used to configure the routing information. Here you can add/delete IP routes.

Enable:

Destination:

Subnet Mask:

Next Hop:

Metric:

Interface:

Add Route
Update
Delete Selected
Show Routes

Static Route Table:

Select	State	Destination	Subnet Mask	NextHop	Metric	Itf

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
Enable	Select the check box to enable routing.
Destination	Enter the IP address of the destination device.
Subnet Mask	Enter the subnet mask of the destination device.
Next Hop	Enter the IP address of the next hop in the IP route to the destination device.
Metric	The metric cost for the destination.
Interface	The interface for the specified route.
Static Route Table	Lists the routing information here.

IPv6 Static Route



Here is the description of every setup item:

Parameter	Description
Destination	Enter the IP address of the destination device.
Prefix Length	Enter the prefix length of the IPv6 address.
Next Hop	Enter the IP address of the next hop in the IP route to the destination device.
Interface	The interface for the specified route.
IPv6 Static Route Table	Lists the routing information here.

RIP

Enable the RIP if you are using this device as a RIP-enabled router to communicate with others using the Routing Information Protocol.

Route	<p>RIP Configuration</p> <p>Enable the RIP if you are using this device as a RIP-enabled router to communicate with others using the Routing Information Protocol.</p> <p>RIP: <input checked="" type="radio"/> Off <input type="radio"/> On <input type="button" value="Apply"/></p> <p>interface: LAN</p> <p>Recv Version: RIP1</p> <p>Send Version: RIP1</p> <p><input type="button" value="Add"/> <input type="button" value="Delete"/></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #800000; color: white;"> <th colspan="4">Rip Config List:</th> </tr> <tr style="background-color: #f0f0f0;"> <th>Select</th> <th>interface</th> <th>Recv Version</th> <th>Send Version</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table> <p style="text-align: center; color: #800000; font-weight: bold;">Technical Support - 1800 209 3444</p>	Rip Config List:				Select	interface	Recv Version	Send Version				
Rip Config List:													
Select	interface	Recv Version	Send Version										
NAT													
QoS													
Port Mapping													
Others													

Here is the description of every setup item:

Field	Description
RIP	Select On. The router communicates with other RIP-enabled devices.
Apply	Click it to save the settings of this page.
Interface	Choose the router interface that uses RIP.
Receive Version	Choose the interface version that receives RIP messages. You can choose RIP1, RIP2, or Both. Choose RIP1 indicates that the router receives RIP v1 messages. Choose RIP2 indicates that the router receives RIP v2 messages. Choose Both indicates that the router receives RIP v1 and RIP v2 messages.
Send Version	The working mode for sending RIP messages. You can choose RIP1 or RIP2. Choose RIP1 indicates the router broadcasts RIP1 messages only. Choose RIP2 indicates the router multicasts RIP2 messages only.
Add	Click it to add the RIP interface to the Rip Config List.
Delete	Select a row in the Rip Config List and click it to delete the row.

NAT

DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Choose menu “**Advanced**→**DMZ**”, below given screen will be displayed.

Here is the description of every setup item:

Parameter	Description
WAN Interface	Select the WAN interface from the drop down list.
DMZ Host IP Address	Enter DMZ host IP Address. Specify the LAN IP address of the PC on which you want to have unrestricted Internet communication.

Virtual Server

The page allows you to configure virtual server, so others can access the server through the Gateway.

Choose menu “**Advanced**→**Virtual Server**”, below given screen will be displayed.

Here is the description of every setup item:

Parameter	Description
Usual Service Name	You can choose the type for the Usual Application Name on the pull-down list.
User-defined Service Name	Enter a name for the rule.
Protocol	The protocol used for this application, either TCP, UDP.
WAN Port	Enter the port that you want to open next to WAN port.
LAN Open Port	Enter the port that you want to open next to LAN port.
LAN IP Address	Enter the IP address of the computer on your local network that you want to allow the incoming service to.

ALG

This feature sets up NAT ALG and Pass-Through configuration. Application Layer Gateway (ALG) is a special function of this router. It includes many preset routing rules for numerous applications which require special support. With these supports, those applications which required special support will be able to work with NAT architecture.

Route	NAT	NAT ALG and Pass-Through	
NAT		Setup NAT ALG and Pass-Through configuration:	
QoS	Port Mapping	IPsec Pass-Through: <input checked="" type="checkbox"/> Enable L2TP Pass-Through: <input checked="" type="checkbox"/> Enable PPTP Pass-Through: <input checked="" type="checkbox"/> Enable FTP: <input checked="" type="checkbox"/> Enable H.323: <input checked="" type="checkbox"/> Enable SIP: <input checked="" type="checkbox"/> Enable RTSP: <input checked="" type="checkbox"/> Enable ICQ: <input checked="" type="checkbox"/> Enable MSN: <input checked="" type="checkbox"/> Enable	
Others	Others	Apply Changes Reset	
Technical Support - 1800 209 3444			

NAT EXCLUDE IP

This page is used to configure some source IP address which use the purge route mode when you access internet through the specified interface.

Route	NAT	NAT EXCLUDE IP									
NAT		This page is used to config some source ip address which use the purge route mode when access internet through the specified interface.									
QoS	Port Mapping	interface: <input type="text" value="v"/>									
Others	Others	IP Range: <input type="text" value=""/> ... <input type="text" value=""/>									
Apply Changes Reset											
Current NAT Exclude IP Table:											
<table border="1"> <thead> <tr> <th>WAN Interface</th> <th>Low IP</th> <th>High IP</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>				WAN Interface	Low IP	High IP	Action				
WAN Interface	Low IP	High IP	Action								
Technical Support - 1800 209 3444											

NAT PORT TRIGGER

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Route

NAT

- > DMZ
- > Virtual Server
- > ALG
- > NAT Exclude IP
- > Port Trigger
- > FTP ALG Port
- > Nat IP Mapping

QoS

Port Mapping

Others

Nat Port Trigger

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Nat Port Trigger: Enable Disable

Apply Changes

Application Type:

Usual Application Name: ▼

User-defined Application Name:

Start Match Port	End Match Port	Trigger Protocol	Start Relate Port	End Relate Port	Open Protocol	Nat Type
<input type="text"/>	<input type="text"/>	UDP ▼	<input type="text"/>	<input type="text"/>	UDP ▼	outgoing ▼
<input type="text"/>	<input type="text"/>	UDP ▼	<input type="text"/>	<input type="text"/>	UDP ▼	outgoing ▼
<input type="text"/>	<input type="text"/>	UDP ▼	<input type="text"/>	<input type="text"/>	UDP ▼	outgoing ▼
<input type="text"/>	<input type="text"/>	UDP ▼	<input type="text"/>	<input type="text"/>	UDP ▼	outgoing ▼
<input type="text"/>	<input type="text"/>	UDP ▼	<input type="text"/>	<input type="text"/>	UDP ▼	outgoing ▼
<input type="text"/>	<input type="text"/>	UDP ▼	<input type="text"/>	<input type="text"/>	UDP ▼	outgoing ▼
<input type="text"/>	<input type="text"/>	UDP ▼	<input type="text"/>	<input type="text"/>	UDP ▼	outgoing ▼
<input type="text"/>	<input type="text"/>	UDP ▼	<input type="text"/>	<input type="text"/>	UDP ▼	outgoing ▼
<input type="text"/>	<input type="text"/>	UDP ▼	<input type="text"/>	<input type="text"/>	UDP ▼	outgoing ▼

Apply Changes

Current Port Trigger Table:

ServerName	Trigger Protocol	Direction	Match Port	Open Protocol	Relate Port	Action

Technical Support - 1800 209 3444

FTP ALG PORT

This page is used to configure FTP Server ALG and FTP Client ALG ports.

Route

NAT

- > DMZ
- > Virtual Server
- > ALG
- > NAT Exclude IP
- > Port Trigger
- > FTP ALG Port
- > Nat IP Mapping

QoS

Port Mapping

Others

FTP ALG Configuration

This page is used to configure FTP Server ALG and FTP Client ALG ports .

FTP ALG port:

FTP ALG ports Table:

Select	Ports
<input type="radio"/>	21

Technical Support - 1800 209 3444

NAT IP MAPPING

Entries in this table allow you to configure one IP pool for specified source IP address from LAN, so one packet whose source IP is in range of the specified address will select one IP address from pool for NAT.

Route

NAT

- > DMZ
- > Virtual Server
- > ALG
- > NAT Exclude IP
- > Port Trigger
- > FTP ALG Port
- > Nat IP Mapping

QoS

Port Mapping

Others

NAT IP MAPPING

Entries in this table allow you to config one IP pool for specified source ip address from lan,so one packet which's source ip is in range of the specified address will select one IP address from pool for NAT.

Type: One-to-One

Local Start IP:

Local End IP:

Global Start IP:

Global End IP:

Current NAT IP MAPPING Table:

Local Start IP	Local End IP	Global Start IP	Global End IP	Action

Technical Support - 1800 209 3444

QoS

You can enable or disable IP QoS. Click enable and click “**Add Rule**”, the following screen will appear.

IP QoS

IP QoS: disable enable

Schedule Mode:

Apply

QoS Rule List

src MAC	dest MAC	src IP	sPort	dest IP	dPort	proto	phy port				
QoS Rule List(Continue)											
IPP	TOS	DSCP	TC	802.1p	Prior	IPP Mark	TOS Mark	DSCP Mark	TC Mark	802.1p Mark	sel

Delete
Add Rule

Add Or Modify QoS Rule

Source MAC:	<input type="text"/>
Destination MAC:	<input type="text"/>
Source IP:	<input type="text"/>
Source Mask:	<input type="text"/>
Destination IP:	<input type="text"/>
Destination Mask:	<input type="text"/>
Source Port:	<input type="text"/>
Destination Port:	<input type="text"/>
Protocol:	<input type="text" value=""/> <input type="button" value="v"/>
Phy Port:	<input type="text" value=""/> <input type="button" value="v"/>
IPP/DS Field:	<input type="radio"/> IPP/TOS <input checked="" type="radio"/> DSCP
IP Precedence Range:	<input type="text" value=""/> <input type="button" value="v"/> ~ <input type="text" value=""/> <input type="button" value="v"/>
Type of Service:	<input type="text" value=""/> <input type="button" value="v"/>
DSCP Range:	<input type="text" value=""/> ~ <input type="text" value=""/> (Value Range:0~63)
Traffic Class Range:	<input type="text" value=""/> ~ <input type="text" value=""/> (Value Range:0~255)
802.1p:	<input type="text" value=""/> <input type="button" value="v"/> ~ <input type="text" value=""/> <input type="button" value="v"/>
Priority:	<input type="text" value="p3(Lowest)"/> <input type="button" value="v"/>
<input type="checkbox"/> insert or modify QoS mark	

Apply

The following table describes the parameters and buttons of this page:

Field	Description
IP QoS	Select to enable or disable IP QoS function. You need to enable IP QoS if you want to configure the parameters of this page.
Schedule Mode	You can choose strict prior or WFQ (4:3:2:1).
Source MAC	The MAC address of the source data packet.
Destination MAC	The MAC address of the Destination data packet.
Source IP	The IP address of the source data packet.
Source Mask	The subnet mask of the source IP address.
Destination IP	The IP address of the destination data packet.
Destination Mask	The subnet mask of the destination IP address.
Source Port	The port of the source data packet.
Destination Port	The port of the destination data packet.
Protocol	The protocol responds to the IP QoS rules. You can choose TCP, UDP or ICMP.
Phy Port	The LAN interface responds to the IP QoS rules.
802.1p	You can choose from 0 to 7.
Set priority	The priority of the IP QoS rules. P0 is the highest priority and P3 is the lowest.

Port Mapping

To manipulate a mapping group:

1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.
3. Click "**Apply Changes**" button to save the changes.

Note that the selected interfaces will be removed from their existing groups and added to the new group.

Route

NAT

QoS

Port Mapping

Port Mapping

Others

Port Mapping Configuration

To manipulate a mapping group:

1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.
3. Click "Apply Changes" button to save the changes.

Note that the selected interfaces will be removed from their existing groups and added to the new group.

Disable Enable

WAN

LAN

-Add>

<Del-

Select	Interfaces
Default	LAN1, LAN2, LAN3, LAN4, wlan, wlan-vap0, wlan-vap1, wlan-vap2, wlan-vap3
Group1 <input type="radio"/>	
Group2 <input type="radio"/>	
Group3 <input type="radio"/>	
Group4 <input type="radio"/>	

Apply

Technical Support - 1800 209 3444

Others

Bridge Setting

This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.

Bridge Setting
This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.

Ageing Time: (seconds)

802.1d Spanning Tree: Disabled Enabled

[Apply Changes](#) [Undo](#) [Show MACs](#)

Technical Support - 1800 209 3444

Client Limit

This page is used to configure how many devices can access to Internet which limits the internet users connectivity to the router.

Client Limit Configuration
This page is used to configure the capability of force how many device can access to Internet!

Client Limit Capability: Disable Enable

[Apply Changes](#)

Technical Support - 1800 209 3444

Tunnel

This page is used to configure v6inv4 tunnel or v4inv6 tunnel.

Tunnel Configuration
This page is used to configure v6inv4 tunnel or v4inv6 tunnel.

V6inV4 Tunnel:

Enable:

Interface: (Only support IPv4 Wan Interface)

Mode:

Relay Router:

Apply Changes

DS-Lite Tunnel:

Enable:

Interface: (Only support IPv6 Wan Interface)

Mode:

Apply Changes

Technical Support - 1800 209 3444

The following table describes the parameters and buttons of this page:

Parameters	Description
Enable	Enable or disable the DS-Lite tunnel.
Interface	Select current wan interface used as tunnel interface.
Mode: 6to4 Tunnel	Select 6to4 Tunnel or 6th Tunnel.

Others

Here you can set other miscellaneous advanced settings.

Half Bridge when enabled, the PPPoE (PPPoA)'s connection type will set to Continuous.

Route	Other Advanced Configuration
NAT	Here you can set other miscellaneous advanced settings.
QoS	Half Bridge: When enable Half Bridge, that PPPoE(PPPoA)'s connection type will set to Continuous.
Port Mapping	Half Bridge: <input checked="" type="radio"/> Disable <input type="radio"/> Enable
Others	Interface: <input type="text"/>
> Bridge Setting	<input type="button" value="Apply Changes"/> <input type="button" value="Undo"/>
> Client Limit	
> Tunnel	
> Others	
	Technical Support - 1800 209 3444

3-6 Service

IGMP

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by doing the following:

IGMP

- > IGMP Proxy
- > MLD

IGMP Proxy Configuration

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by doing the follows:

- Enable IGMP proxy on WAN interface (upstream), which connects to a router running IGMP.
- Enable IGMP on LAN interface (downstream), which connects to its hosts.

IGMP Proxy:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Multicast Allowed:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Robust Count:	<input type="text" value="2"/>
Last Member Query Count:	<input type="text" value="2"/>
Query Interval:	<input type="text" value="60"/> (seconds)
Query Response Interval:	<input type="text" value="100"/> (*100ms)
Group Leave Delay:	<input type="text" value="2000"/> (ms)

Apply Changes
Undo

Technical Support - 1800 209 3444

Here is the description of every setup item:

Parameter	Description
IGMP Proxy	The Router will act as an IGMP proxy for hosts if enabled.
Multicast Allowed	Enable or Disable the multicast packets.
Robust Count	The Robust Count allows tuning for expected packet loss on a network. By default, the value is set to 2.
Last member query count	This parameter indicates last member query interval. It is the maximum response time in seconds for an IGMP host in reply to group-specific queries.
Query Interval	This parameter indicates the query interval. It is the interval in seconds (s) between general queries sent by the querier.
Query Response Interval	This parameter indicates the query response interval. It is the maximum response time in seconds for an IGMP host in reply to general queries.
Group Leave Delay	The message is sent when a host leaves a group.

MLD

MLD Proxy and Snooping can be configured here.

Here is the description of every setup item:

Parameter	Description
MLD Snooping	With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports.
Robust Counter	The Robust Count allows tuning for expected packet loss on a network.
Query Interval	This parameter indicates the query interval. It is the interval in seconds between general queries sent by the querier.
Query Response Interval	This parameter indicates the query response interval. It is the maximum response time in seconds for an MLD host in reply to general queries.
Response interval of last group member	Default value is 1 second.

UPnP

This page is used to configure UPnP. The system acts as a daemon when you enable UPnP.

The screenshot shows the 'UPnP Configuration' page. On the left is a navigation menu with items: IGMP, UPnP (selected), DNS, DDNS, FTP Server, and USB Storage. The main content area is titled 'UPnP Configuration' and includes a sub-header: 'This page is used to configure UPnP. The system acts as a daemon when you enable UPnP.' Below this, there are two rows of configuration options: 'UPnP:' with radio buttons for 'Disable' and 'Enable' (the 'Enable' option is selected), and 'WAN Interface:' with a dropdown menu. At the bottom of the configuration area is an 'Apply Changes' button. At the very bottom of the page, there is a 'Technical Support - 1800 209 3444' link.

DNS

This page is used to configure the DNS server IP addresses for DNS Relay.

The screenshot shows the 'DNS Configuration' page. On the left is a navigation menu with items: IGMP, UPnP, DNS (selected), DDNS, FTP Server, and USB Storage. The main content area is titled 'DNS Configuration' and includes a sub-header: 'This page is used to configure the DNS server ip addresses for DNS Relay.' Below this, there are two radio button options: 'Attain DNS Automatically' (selected) and 'Set DNS Manually'. Underneath, there are three rows for DNS server IP addresses: 'DNS 1:' with a text box containing '0.0.0.0', 'DNS 2:', and 'DNS 3:'. At the bottom of the configuration area are 'Apply Changes' and 'Reset Selected' buttons. At the very bottom of the page, there is a 'Technical Support - 1800 209 3444' link.

IPv6 DNS

This page is used to configure the DNS server ipv6 addresses.

IGMP

UPnP

DNS

» DNS

» IPv6 DNS

DDNS

FTP Server

USB Storage

IPv6 DNS Configuration

This page is used to configure the DNS server ipv6 addresses.

Attain DNS Automatically
 Set DNS Manually

DNS 1:	<input type="text"/>	Interface:	<input type="text"/>
DNS 2:	<input type="text"/>	Interface:	<input type="text"/>
DNS 3:	<input type="text"/>	Interface:	<input type="text"/>

Technical Support - 1800 209 3444

DDNS

This page is used to configure the Dynamic DNS address from DynDNS.org, TZO, PHDNS or NO-IP. Here you can Add/Remove to configure Dynamic DNS.

IGMP

UPnP

DNS

DDNS

» DDNS

FTP Server

USB Storage

Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS:

DDNS provider:

Hostname:

Interface:

Enable:

DynDns Settings:

Username:
 Password:

TZO Settings:

Email:
 Key:

NO-IP Settings:

Email:
 Password:

Dynamic DDNS Table:					
Select	State	Service	Hostname	Username	Interface
<input type="checkbox"/>					

Technical Support - 1800 209 3444

FTP Server

Check start to start the FTP server.

IGMP

UPnP

DNS

DDNS

FTP Server

▶ FTP Server

USB Storage

FTP Server

start

Technical Support - 1800 209 3444

USB Storage

This page is used to configure USB storage Enable or Disable. When enable USB storage and plug hard disk or USB disk in USB port, you can browse/upload/download disk files by FTP (eg:"ftp://192.168.1.1").

IGMP

UPnP

DNS

DDNS

FTP Server

USB Storage

▶ USB Storage

USB Storage

This page is used to configure USB storage Enable or Disable. When enable USB storage and plug hard disk or U disk in usb port, you can browse/upload/download disk files by FTP(eg:"ftp://192.168.1.1").

USB Storage: Disable Enable

Technical Support - 1800 209 3444

Firewall

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

MAC Filter
 > MAC Filter

IP/Port Filter

URL Filter

ACL

DoS

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Policy: Deny Allow

Incoming Default Policy: Deny Allow

Direction:

Action: Deny Allow

Source MAC: (ex. 00E086710502)

Destination MAC: (ex. 00E086710502)

Current MAC Filter Table:

Select	Direction	Source MAC	Destination MAC	Action

Technical Support - 1800 209 3444

IP/Port Filter

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

- MAC Filter
- IP/Port Filter
- > IP/Port Filter
- > IPv6/Port Filter
- URL Filter
- ACL
- DoS

IP/Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Policy: Permit Deny

Incoming Default Policy: Permit Deny

Rule Action: Permit Deny

WAN Interface:

Protocol:

Direction:

Source IP Address: Mask Address:

Dest IP Address: Mask Address:

SPort: - DPort: -

Enable:

Current Filter Table:

Rule	WanIf	Protocol	Source IP/Mask	SPort	Dest IP/Mask	DPort	State	Direction	Action

Technical Support - 1800 209 3444

IPv6/Port Filter

Entries in this table are used to restrict certain types of ipv6 data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

MAC Filter

IP/Port Filter

- > IP/Port Filter
- > IPv6/Port Filter

URL Filter

ACL

DoS

IPv6/Port Filtering

Entries in this table are used to restrict certain types of ipv6 data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Policy: Permit Deny

Incoming Default Policy: Permit Deny

Rule Action: Permit Deny

Protocol: ICMP6Type:

Direction:

Source IPv6 Address: Prefix Length:

Dest IPv6 Address: Prefix Length:

SPort: - DPort: -

Enable:

Current Filter Table:

Rule	Protocol	Source IPv6/Prefix	SPort	Dest IPv6/Prefix	DPort	ICMP6Type	State	Direction	Action
Technical Support - 1800 209 3444									

URL Filter

This page is used to configure the filtered keyword. Here you can add/delete filtered keyword.

MAC Filter

IP/Port Filter

URL Filter

- > URL Filter

ACL

DoS

URL Blocking Configuration

This page is used to configure the filtered keyword. Here you can add/delete filtered keyword.

URL Blocking Capability: Disable Enable

Keyword:

URL Blocking Table:

Select	Filtered Keyword
Technical Support - 1800 209 3444	

ACL

You can specify which services are accessible form LAN or WAN side. Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.

Using of such access control can be helpful in securing or restricting the Gateway management.

MAC Filter

IP/Port Filter

URL Filter

ACL

→ ACL

→ IPv6 ACL

DoS

ACL Configuration

You can specify which services are accessible form LAN or WAN side.
 Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.
 Using of such access control can be helpful in securing or restricting the Gateway management.

LAN ACL Mode: White List Black List

WAN ACL Mode: White List Black List

Direction Select: LAN WAN

LAN ACL Switch: Enable Disable

IP Address: - (The IP 0.0.0.0 represent any IP)

Services Allowed:

any

Current ACL Table:

Select	Direction	IP Address/Interface	Service	Port	Action

Technical Support - 1800 209 3444

IPv6 ACL

You can specify which services are accessible from LAN or WAN side.

Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.

Using of such access control can be helpful in securing or restricting the Gateway management.

MAC Filter

IP/Port Filter

URL Filter

ACL

- > ACL
- > IPv6 ACL

DoS

ACL Configuration

You can specify which services are accessible from LAN or WAN side.
 Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.
 Using of such access control can be helpful in securing or restricting the Gateway management.

Direction Select: LAN WAN

LAN ACL Switch: Enable Disable

IP Address: /

Services Allowed:

Any

Current IPv6 ACL Table:

Direction	IPv6 Address/Interface	Service	Port	Action
WAN	any	ping6	--	Delete

Technical Support - 1800 209 3444

DoS

A "**denial-of-service**" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

Denial of Service (DoS) is a common attack measure, by transmitting a great amount of data or request to your Internet IP address and server, the Internet connection will become very slow, and server may stop responding because it is not capable to handle too much traffic.

MAC Filter	DoS Setting A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.																																																						
IP/Port Filter																																																							
URL Filter																																																							
ACL																																																							
DoS																																																							
> DoS																																																							
<div style="border: 1px solid #ccc; padding: 10px;"> <input type="checkbox"/> Enable DoS Prevention </div> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <tr> <td><input type="checkbox"/> Whole System Flood: SYN</td> <td style="text-align: center;">100</td> <td>Packets/Second</td> </tr> <tr> <td><input type="checkbox"/> Whole System Flood: FIN</td> <td style="text-align: center;">100</td> <td>Packets/Second</td> </tr> <tr> <td><input type="checkbox"/> Whole System Flood: UDP</td> <td style="text-align: center;">100</td> <td>Packets/Second</td> </tr> <tr> <td><input type="checkbox"/> Whole System Flood: ICMP</td> <td style="text-align: center;">100</td> <td>Packets/Second</td> </tr> <tr> <td><input type="checkbox"/> Per-Source IP Flood: SYN</td> <td style="text-align: center;">100</td> <td>Packets/Second</td> </tr> <tr> <td><input type="checkbox"/> Per-Source IP Flood: FIN</td> <td style="text-align: center;">100</td> <td>Packets/Second</td> </tr> <tr> <td><input type="checkbox"/> Per-Source IP Flood: UDP</td> <td style="text-align: center;">100</td> <td>Packets/Second</td> </tr> <tr> <td><input type="checkbox"/> Per-Source IP Flood: ICMP</td> <td style="text-align: center;">100</td> <td>Packets/Second</td> </tr> <tr> <td><input type="checkbox"/> TCP/UDP PortScan</td> <td style="text-align: center;">Low</td> <td>Sensitivity</td> </tr> <tr> <td><input type="checkbox"/> ICMP Smurf</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> IP Land</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> IP Spoof</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> IP TearDrop</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> PingOfDeath</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> TCP Scan</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> TCP SynWithData</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> UDP Bomb</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> UDP EchoChargen</td> <td></td> <td></td> </tr> </table> <div style="margin-top: 10px;"> <input type="button" value="Select ALL"/> <input type="button" value="Clear ALL"/> </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <input type="checkbox"/> Enable Source IP Blocking 300 Block time (sec) </div> <div style="margin-top: 10px;"> <input type="button" value="Apply Changes"/> </div>		<input type="checkbox"/> Whole System Flood: SYN	100	Packets/Second	<input type="checkbox"/> Whole System Flood: FIN	100	Packets/Second	<input type="checkbox"/> Whole System Flood: UDP	100	Packets/Second	<input type="checkbox"/> Whole System Flood: ICMP	100	Packets/Second	<input type="checkbox"/> Per-Source IP Flood: SYN	100	Packets/Second	<input type="checkbox"/> Per-Source IP Flood: FIN	100	Packets/Second	<input type="checkbox"/> Per-Source IP Flood: UDP	100	Packets/Second	<input type="checkbox"/> Per-Source IP Flood: ICMP	100	Packets/Second	<input type="checkbox"/> TCP/UDP PortScan	Low	Sensitivity	<input type="checkbox"/> ICMP Smurf			<input type="checkbox"/> IP Land			<input type="checkbox"/> IP Spoof			<input type="checkbox"/> IP TearDrop			<input type="checkbox"/> PingOfDeath			<input type="checkbox"/> TCP Scan			<input type="checkbox"/> TCP SynWithData			<input type="checkbox"/> UDP Bomb			<input type="checkbox"/> UDP EchoChargen		
<input type="checkbox"/> Whole System Flood: SYN	100	Packets/Second																																																					
<input type="checkbox"/> Whole System Flood: FIN	100	Packets/Second																																																					
<input type="checkbox"/> Whole System Flood: UDP	100	Packets/Second																																																					
<input type="checkbox"/> Whole System Flood: ICMP	100	Packets/Second																																																					
<input type="checkbox"/> Per-Source IP Flood: SYN	100	Packets/Second																																																					
<input type="checkbox"/> Per-Source IP Flood: FIN	100	Packets/Second																																																					
<input type="checkbox"/> Per-Source IP Flood: UDP	100	Packets/Second																																																					
<input type="checkbox"/> Per-Source IP Flood: ICMP	100	Packets/Second																																																					
<input type="checkbox"/> TCP/UDP PortScan	Low	Sensitivity																																																					
<input type="checkbox"/> ICMP Smurf																																																							
<input type="checkbox"/> IP Land																																																							
<input type="checkbox"/> IP Spoof																																																							
<input type="checkbox"/> IP TearDrop																																																							
<input type="checkbox"/> PingOfDeath																																																							
<input type="checkbox"/> TCP Scan																																																							
<input type="checkbox"/> TCP SynWithData																																																							
<input type="checkbox"/> UDP Bomb																																																							
<input type="checkbox"/> UDP EchoChargen																																																							
Technical Support - 1800 209 3444																																																							

3-7 Maintenance

Firmware Update

This page allows you to upgrade the Router firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

The screenshot shows the 'Upgrade Firmware' page. On the left is a navigation menu with 'Update' selected, containing 'Firmware Update' and 'Backup/Restore'. Below it are other menu items: 'Password', 'Reboot', 'Time', 'Log', and 'Diagnostics'. The main content area is titled 'Upgrade Firmware' and includes a warning: 'This page allows you upgrade the Router firmware to new version. Please note, do not power off the device during the upload because it may crash the system.' Below this is a note: 'Note: System will reboot after file is uploaded.' A file selection area contains 'Select File:', a 'Choose File' button, and the text 'No file chosen'. At the bottom of this area are 'Upload' and 'Reset' buttons. A footer at the bottom right reads 'Technical Support - 1800 209 3444'.

Backup/Restore

Once the router is configured you can save the configuration settings to a configuration file on your hard drive. You also have the option to load configuration settings.

The screenshot shows the 'Backup/Restore Settings' page. The left navigation menu is the same as in the previous screenshot, but 'Backup/Restore' is now selected. The main content area is titled 'Backup/Restore Settings' and includes the text: 'Once the router is configured you can save the configuration settings to a configuration file on your hard drive. You also have the option to load configuration settings.' Below this are two sections: 'Save Settings to File:' with a 'Save...' button, and 'Load Settings from File:' with a 'Choose File' button, the text 'No file chosen', and an 'Upload' button. A footer at the bottom right reads 'Technical Support - 1800 209 3444'.

Password

This page is used to add user account to access the web server of Router. Empty user name or password is not allowed.

- Update
- Password
- > Password
- Reboot
- Time
- Log
- Diagnostics

User Account Configuration

This page is used to add user account to access the web server of ADSL Router. Empty user name or password is not allowed.

User Name:

Privilege:

Old Password:

New Password:

Confirm Password:

Add
Modify
Delete
Reset

User Account Table:		
Select	User Name	Privilege
<input type="radio"/>	admin	root
<input type="radio"/>	user	user

Technical Support - 1800 209 3444

Reboot

This page is used to reboot your system or restore to default setting.

- Update
- Password
- Reboot
- > Reboot
- Time
- Log
- Diagnostics

Reboot

This page is used to reboot your system or restore to default setting.

Reboot
Restore to Default Setting

Technical Support - 1800 209 3444

Time

This page is used to configure the system time and Network Time Protocol (NTP) server. Here you can change the settings or view some information on the system time and NTP parameters.

[Update](#)
[Password](#)
[Reboot](#)
[Time](#)
[Log](#)
[Diagnostics](#)

System Time Configuration

This page is used to configure the system time and Network Time Protocol(NTP) server. Here you can change the settings or view some information on the system time and NTP parameters.

System Time: Year Month Day Hour min sec
 DayLight:

Apply Changes
Reset

NTP Configuration:

State: Disable Enable

Server:

Server2:

Interval: Every hours

Time Zone:

GMT time: Sun Jan 1 2:24:4 2012

Apply Changes
Reset

NTP Start:

Technical Support - 1800 209 3444

Log

This page is used to display the system event log table. By checking Error or Notice (or both) will set the log flag. By clicking the ">>|", it will display the newest log information below.

[Update](#)
[Password](#)
[Reboot](#)
[Time](#)
[Log](#)
[Diagnostics](#)

Log Setting

This page is used to display the system event log table. By checking Error or Notice (or both)will set the log flag. By clicking the ">>|", it will display the newest log information below.

Error: Notice:

Apply Changes
Reset

Event log Table:

Old

 New

Time	Index	Type	Log Information
Page: 1/1			

Technical Support - 1800 209 3444

Diagnostics

A) Ping

Update	Ping Diagnostic Host : <input type="text"/> PING Technical Support - 1800 209 3444
Password	
Reboot	
Time	
Log	
Diagnostics	
> Ping	
> Ping6	
> Traceroute	
> Traceroute6	
> Diag-Test	

The following table describes the parameters and buttons of this page:

Field	Description
Host	Enter the valid IP address or domain name.
Ping	Click it to start to Ping.

B) Ping6

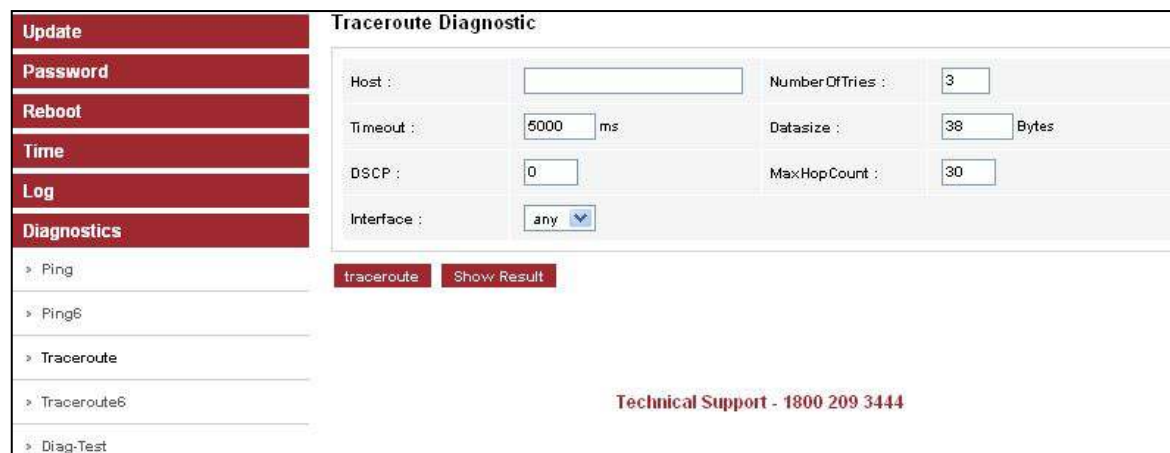
Update	Ping6 Diagnostic Target Address: <input type="text"/> Interface: <input type="text"/> PING Technical Support - 1800 209 3444
Password	
Reboot	
Time	
Log	
Diagnostics	
> Ping	
> Ping6	
> Traceroute	
> Traceroute6	
> Diag-Test	

The following table describes the parameters and button of this page:

Field	Description
Target Address	Enter an IP address for Ping6 diagnostic.
Interface name	Enter an interface through which the Ping6 diagnostic is performed.

C) Traceroute Diagnostic

Click **Traceroute** in the left pane, and the following page appears. By Traceroute Diagnostic, you can track the route path of information flow from your computer to the other side host.



Here is the description of every setup item:

Parameters	Description
Host	Enter the destination host address for diagnosis.
NumberOfTries	Number of repetitions.
Timeout	Put in the timeout value.
Data size	Packet size.
DSCP	Differentiated Services Code Point, you should set a value between 0-63.
MaxHopCount	Maximum number of routes.
Interface	Select the interface.
Traceroute	Click start traceroute.

D) Traceroute6

Update	Traceroute6 Diagnostic Host : <input type="text"/> NumberOfTries : <input type="text" value="3"/> Timeout : <input type="text" value="5000"/> ms Datasize : <input type="text" value="38"/> Bytes MaxHopCount : <input type="text" value="30"/> Interface : <input type="text" value="any"/> <input type="button" value="traceroute"/> <input type="button" value="Show Result"/> <p style="text-align: center;">Technical Support - 1800 209 3444</p>
Password	
Reboot	
Time	
Log	
Diagnostics	
> Ping	
> Ping6	
> Traceroute	
> Traceroute6	
> Diag-Test	

E) Diag-Test

The Router is capable of testing your WAN connection. The individual tests are listed below. If a test displays a fail status, click "**Run Diagnostic Test**" button again to make sure the fail status is consistent.

Update	Diagnostic Test <small>The Router is capable of testing your WAN connection. The individual tests are listed below. If a test displays a fail status, click "Run Diagnostic Test" button again to make sure the fail status is consistent.</small> Select the Internet Connection: <input type="text" value="v"/> <input type="button" value="Run Diagnostic Test"/> <p style="text-align: center;">Technical Support - 1800 209 3444</p>
Password	
Reboot	
Time	
Log	
Diagnostics	
> Ping	
> Ping6	
> Traceroute	
> Traceroute6	
> Diag-Test	

Click "**Run Diagnostic Test**" to start testing.

4. Appendix

- **Hardware Specifications**
 - Flash: 2MB
 - SDRAM: 16MB
 - 1 USB 2.0 port
 - Antenna: One fixed 5 dBi antenna
 - WPS/WLAN Push Button
 - Factory reset button

- **Network Ports**
 - 1 * 10/100Mbps UTP WAN Port
 - 4 * 10/100Mbps UTP LAN Ports

- **Status LED**
 - Power, WAN, USB, LAN (1-4), WLAN, WPS

- **Standards Compliance**
 - IEEE802.3 10 Base-T Ethernet
 - IEEE802.3u 100 Base-TX Ethernet
 - IEEE802.11b, IEEE802.11g, IEEE802.11n

- **Frequency Band**
 - 2.4000 ~ 2.4835 GHz

- **WLAN Data Transfer Rates**
 - IEEE802.11b up to 11Mbps
 - IEEE802.11g up to 54Mbps
 - IEEE802.11n up to 150Mbps

- **Wireless Output Power**
 - IEEE802.11b: 23 +/- 1 dBm
 - IEEE802.11g: 19 +/- 1 dBm
 - IEEE802.11n: 18 +/- 1 dBm

- **Environmental Specifications**

- Operating temperature: 0 to 40°C
- Storage Temperature: -40 to 70°C
- Operating Humidity: 10 % to 90 %
- Storage Humidity: 5% to 95%

- **Power Supply**

- 5V DC, 1.5 A Switching Power Adapter

5. Glossary

Default Gateway (Router): Every non-router IP device needs to configure a default gateway IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it to the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.Broadbandrouter.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "Broadbandrouter.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

Idle Timeout: Idle Timeout is designed so that after there is no traffic on the Internet for a pre-configured amount of time, the connection will automatically get disconnected.

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, which identifies a single, unique Internet computer host in an IP network. Example: 192.168.2.1. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": `aaa.aaa.aaa.aaa`, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".": `bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb`, where each "b" can be either 0 or 1.

A network mask is also a 32-bit binary pattern, and consists of consecutive leading 1's followed by consecutive trailing 0's, such as 11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as "x" number of leading 1's.

When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is, 11111111.11111111.11110000.00000000

It means the device's network address is

11011001.10110000.10010000.00000000, and its host ID is, 00000000.00000000.00000000.00000111. This is a convenient and efficient method for routers to route IP packets to their destination.

ISP Gateway Address: (see ISP for definition). The ISP Gateway Address is an IP address for the Internet router located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as home or office). Your home network is considered a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that correspond to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

NAT: Network Address Translation. This process allows all the computers on your home network to use one IP address. Using the broadband router's NAT capability, you can access Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port: Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UDP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

PPPoE: (Point-to-Point Protocol over Ethernet.) Point-to-Point Protocol is a secure data transmission method originally created for dial-up connections; PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communication protocol for transmitting information over Ethernet between different manufacturers.

Protocol: A protocol is a set of rules for interaction agreed upon between multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

Router: A router is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by Inter NIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocols. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

Web-based management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.

This product comes with lifetime warranty.
For further details about warranty policy and
product registration, please visit support
section of www.digisol.com



"PRODUCTS SOLD OUTSIDE INDIA CARRY 1 YEAR WARRANTY ONLY"