DG-HR1020S

150MBPS WIRELESS 3.75G MODEM BROADBAND ROUTER

User Manual

V1.0

2014-09-05

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

COPYRIGHT

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

1-1 Introduction and Safety Information

Thank you for purchasing DG-HR1020S 150Mbps wireless 3.75G modem broadband router! The Mobile Router gives you high-speed access to the Internet wherever you are and lets you share it on the go. The built-in 3G antenna provides a reliable connection to your 3G service provider, and a separate Wi-Fi antenna gives extended coverage to the computers and mobile devices connected to DG-HR1020S.

DG-HR1020S is truly plug and play, with drivers built into the router so you can connect without the need to install anything. Open a browser, connect the router, and you can set up your network right from a web interface. This means that notebooks and net books without a CD ROM drive can connect and start running in no time. Once the device is set up, you can simply power it on to start up your portable mobile network, meaning that you can share your mobile Internet connection without the need of a computer.

Other features of this router include:

- Supports up to 21.6Mbps 3G speed.
- Wireless speed up to 150Mbps.
- High-Speed Mobile Internet with 3G Connectivity.
- Mobile Internet for All of Your Devices.
- Built-in Software for Instant Access Anywhere.
- Designed for True Portability.
- Connects up to 8 wireless clients.
- Creates instant 3G Wi-Fi Hot spots.
- Router with firewall and parental control.
- Supports 2G/3G SIM.

1-2 Safety Information

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

1. Always unplug and turn off the router before installing or removing the SIM card. **DO NOT** insert or remove the SIM card while the router is in use.

2. Protect the device from liquids, dust and excessive temperatures.

3. **DO NOT** apply adhesive labels to the device; they might cause the device to potentially overheat or alter the performance of the antenna.

4. **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.

5. 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.

1-3 System Requirements

- A compatible SIM card with mobile data services.
- A computer with Windows®, Macintosh®, or Linux-based operating systems.
- Internet Explorer 8, Firefox 12.0, Chrome 20.0, or Safari 4.0.

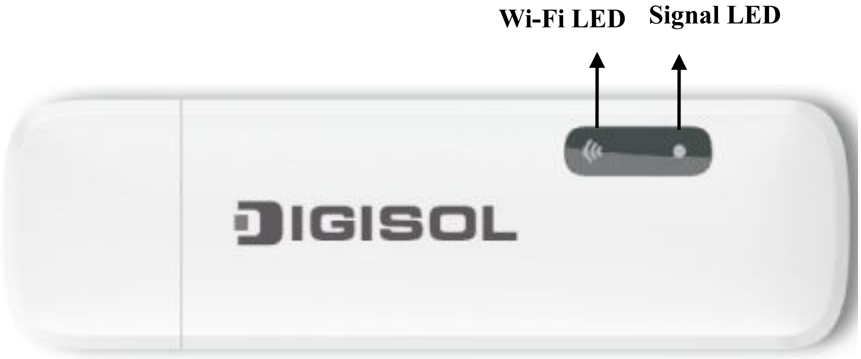
1-4 Package Contents

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-HR1020S 150Mbps Wireless 3.75G Modem Broadband Router
- Quick Installation Guide

2. Hardware Installation

2-1 Get Familiar with your new wireless broadband router



Interface	Status	Description
Wi-Fi LED	Solid Green	WI-Fi activated
	Blinking Green	Data is transmitting
Signal LED	Red	SIM error or No Service
	Blinking Green	Data is transmitting

2-2 Connect to your network

Hardware Installation:

1. Slide your SIM card into the slot provided, ensuring that the alignment is the same as indicated by the logo next to the slot. The gold contacts on the card should be facing downwards.

Caution: Always unplug the router before installing or removing the SIM card. Never insert or remove the SIM card while the router is in use.

2. After a few moments, the LED display will show the current status of the router.

Insert a microSD Card

1. Ensure that your modem broadband Router is plugged in properly.

2. Open the cover of the microSD slot on the side of the router.

3. Insert the microSD card into the slot and push it in until it locks into place.

2-3 Driver Installation

When you plug the device into your computer, any necessary drivers will immediately install.

Note: These drivers are Windows-only. Mac and Linux users will still be able to configure the device using the web configuration utility described in Configuration Utility.

Wireless Installation Considerations

DG-HR1020S can be accessed using a wireless connection from anywhere within the operating range of its wireless network. Keep in mind that the quantity, thickness, and location of walls, ceilings, or other objects that the wireless signals must pass through may adversely affect wireless signals. Ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or office. The key to maximizing the wireless range is to follow these basic guidelines:

1. Minimize the number of walls and ceilings between the router and other network devices. Each wall or ceiling can reduce your adapter's range from1 to 90 feet (1 to 30 meters).

2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters) appears to be almost 3 feet (1 meter) thick at a 45-degree angle. At a 2-degree angle it appears over 42 feet (14 meters) thick. Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

3. Try to position access points, wireless routers and computers so that the signal passes through open doorways and drywall. Materials such as glass, metal, brick, insulation, concrete and water can affect wireless performance. Large objects such as fish tanks, mirrors, file cabinets, metal doors and aluminum studs may also have a negative effect on range.

4. If you are using a 2.4 GHz cordless phone, make sure that the 2.4 GHz phone base is as far away from your wireless device as possible. The base transmits a signal even if the phone is not in use. In some cases, cordless phones, X-10 wireless devices and electronic equipments such as ceiling fans, fluorescent lights and home security systems may dramatically degrade wireless connectivity.

Configuration

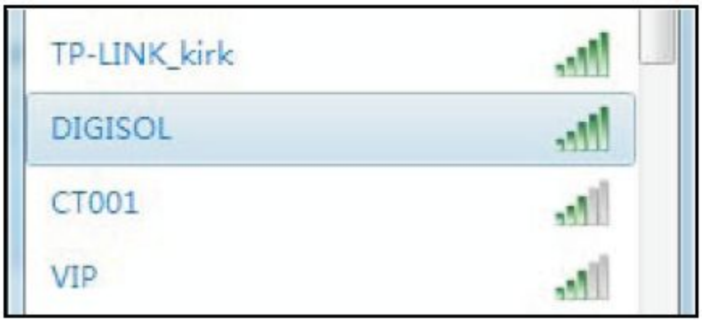
This section will show you how to configure your new modem broadband router using the web-based user interface.

When configuring the router for the first time, you will need to establish a direct connection with the router in order to access the web-based user interface. This can be done by connecting wirelessly to DG-HR1020S. Once you have configured your router, you will be able to connect using the Wi-Fi settings that you have specified in the configuration process.

Connect via Wi-Fi

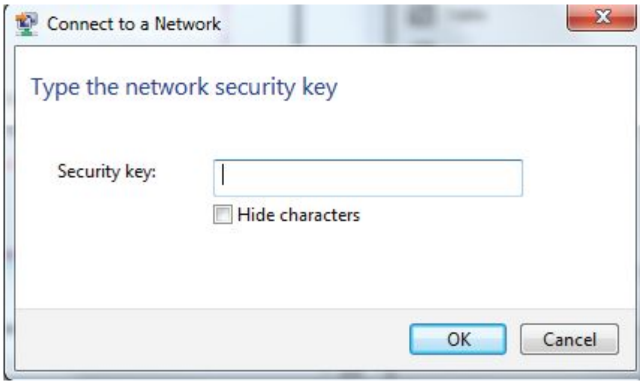
Note: The following example uses Windows 7's built-in wireless connection utility. If you are using a different operating system, or a third party connection utility, the process may be different. Please refer to the documentation that came with your operating system or wireless client for further information on how to connect to a wireless network.

To connect to the router using Wi-Fi, open your operating system's wireless networking utility and scan for available networks to connect to. By default, the network name (SSID) of DG-HR1020S will be in the format "DIGISOL",the default password is 12345678.



Once you have located this network with your wireless utility, connect to the network using your wireless networking utility.

You will then be prompted to enter the network security key for your router. The unique security key for your router will be displayed on the router. Enter the security key in the box provided and click OK. Your wireless connection utility should confirm that the connection is successful, and you can move to the next step to continue to configuration process.

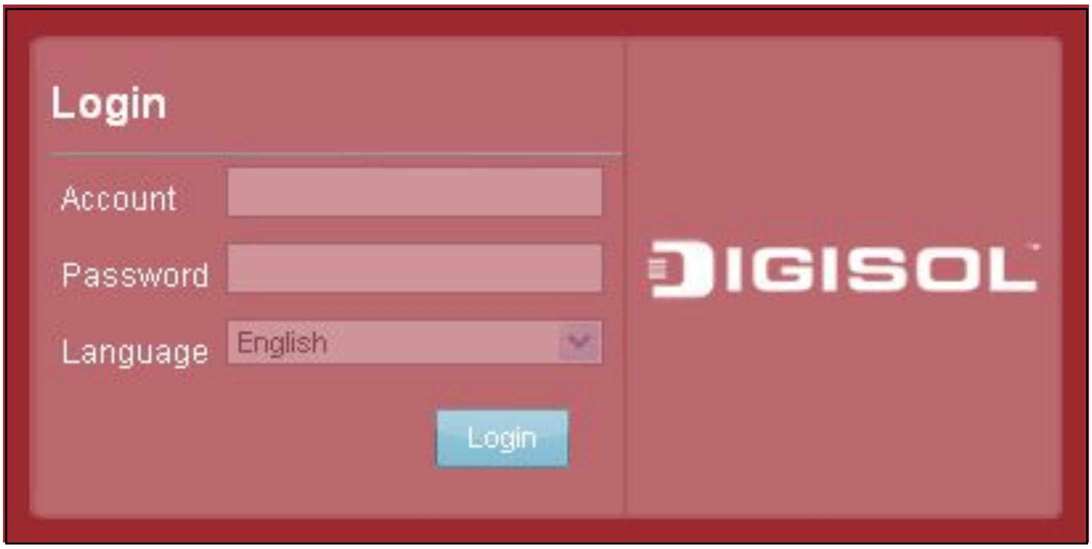


3. Quick Install Guide

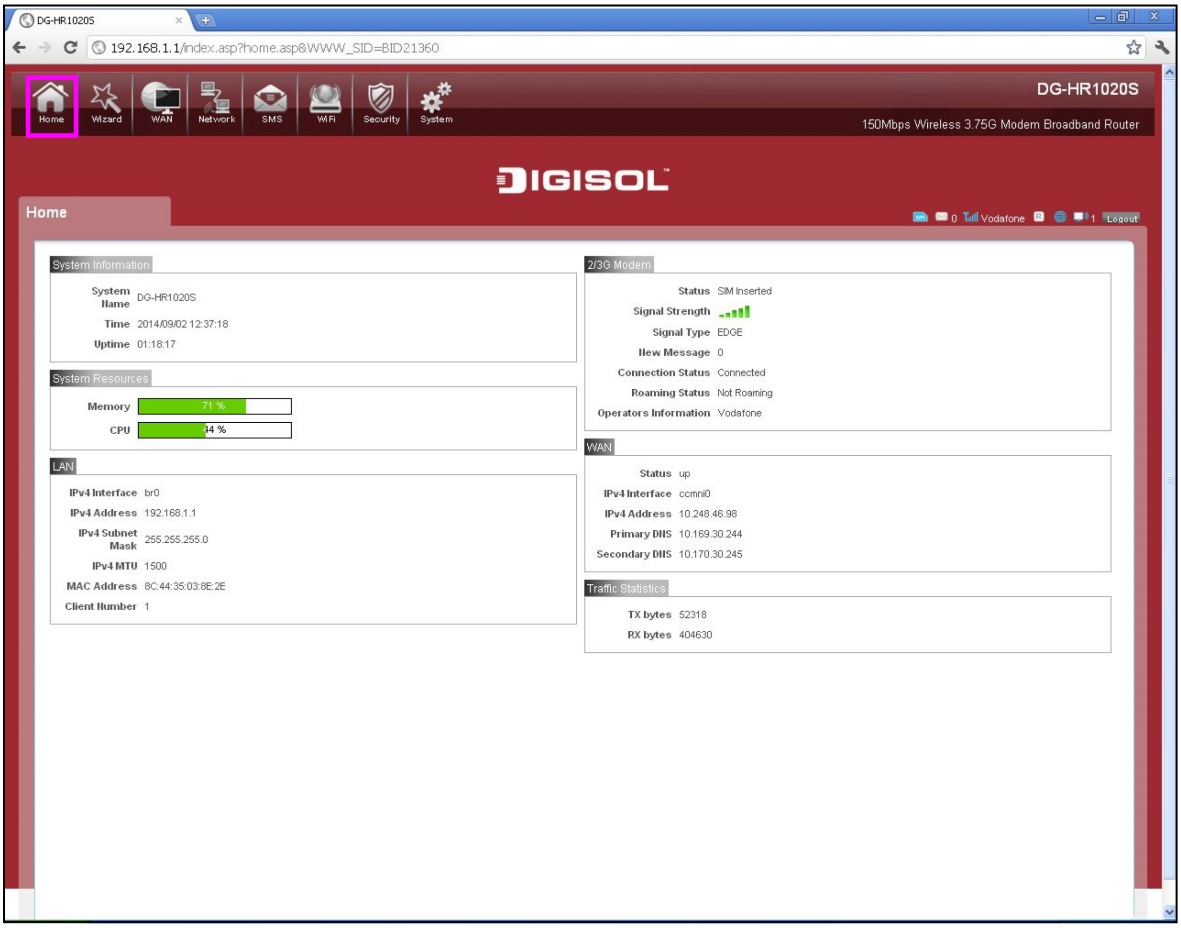
3-1 Getting Started

Connecting the router's management interface by web browser:
Type the IP address of the router in the address bar as '**http://192.168.1.1**'.

The following screen should be shown:



Please input 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-HR1020S
192.168.1.1/index.asp?home.asp&WWW_SID=BID21360
Home
Wizard
WAN
Network
SMS
WiFi
Security
System
DG-HR1020S
150Mbps Wireless 3.75G Modem Broadband Router
DIGISOL™
0
Vodafone
1
Logout

Home

System Information

System Name	DG-HR1020S
Time	2014/09/02 12:37:18
Uptime	01:18:17

System Resources

Memory	71 %
CPU	44 %

LAN

IPv4 Interface	br0
IPv4 Address	192.168.1.1
IPv4 Subnet Mask	255.255.255.0
IPv4 MTU	1500
MAC Address	8C:44:35:03:8E:2E
Client Number	1

2/3G Modem

Status	SIM Inserted
Signal Strength	
Signal Type	EDGE
New Message	0
Connection Status	Connected
Roaming Status	Not Roaming
Operators Information	Vodafone

WAN

Status	up
IPv4 Interface	ccmni0
IPv4 Address	10.248.46.98
Primary DNS	10.169.30.244
Secondary DNS	10.170.30.245

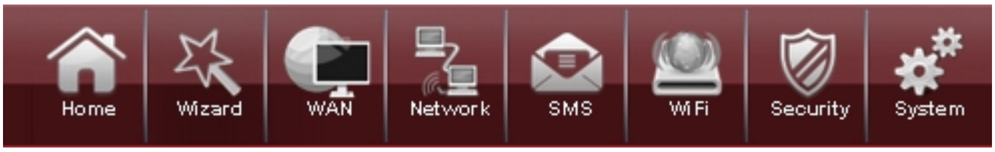
Traffic Statistics

TX bytes	52318
RX bytes	404630

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.

Throughout the interface you will find a menu bar at the top of the page which includes tabs for easy navigation, and a summary bar in the upper right corner with a quick view of essential information.



Home: The Home tab will bring you back to the home page, where a summary of the system information is shown.

Wizard: Click on this tab to start the setup wizard, which will guide you through the basic setup process.

WAN: This tab gives you Internet setup and settings options.

Network: The Network tab allows you to configure the network settings for your Local Area Network (LAN).

SMS: From the SMS you can view and send SMS messages via your mobile network.

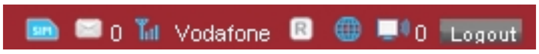
Wi-Fi: The Wi-Fi allows you to configure your Wi-Fi network, as well as add new devices using WPS.

Security: The Security allows you to configure firewall and security settings to protect your network from WAN-side intrusions.

System: From this tab, you can manage the administrative configuration of your router, such as time and date, firmware upgrade, language and system logs.

Device Status

A summary of the device’s current status will be displayed on the information panel at the top of the right-hand side of the navigation bar. The following is a description of the indications, from left to right.



SIM: This icon shows whether or not a compatible SIM card has been inserted into the device.

SMS: The number to the right of this icon indicates the number of unread messages in the SMS inbox.

Signal Strength: Indicates the current strength of the mobile network signal being received.

Operator Name: The name of the mobile network operator to which the device is currently connected.

Internet: Indicates that there is an Internet connection present.

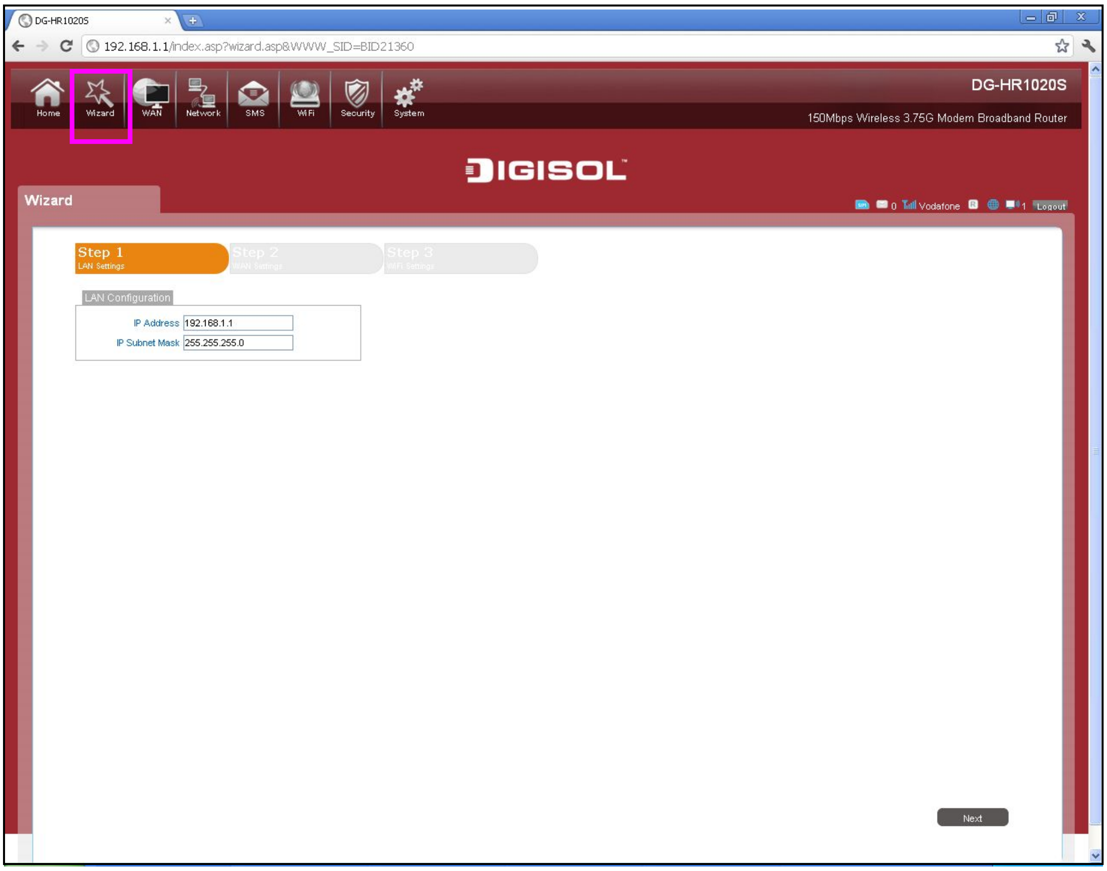
Wi-Fi Network: Indicates that the router’s Wi-Fi network is currently active. The number to the right of this icon indicates the number of wireless clients currently connected to the router’s Wi-Fi network.

Logout: Click this button to log out of the configuration interface.

3-2 Wizard

The Wizard page will guide you through the steps required to configure the basic settings of your router such as the IP address, network name (SSID) and password. Click on the Wizard button on the navigation bar to commence the wizard.

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



192.168.1.1/index.asp?wizard.asp&WWW_SID=BID21360

DG-HR1020S

150Mbps Wireless 3.75G Modem Broadband Router

Wizard

Step 1 LAN Settings

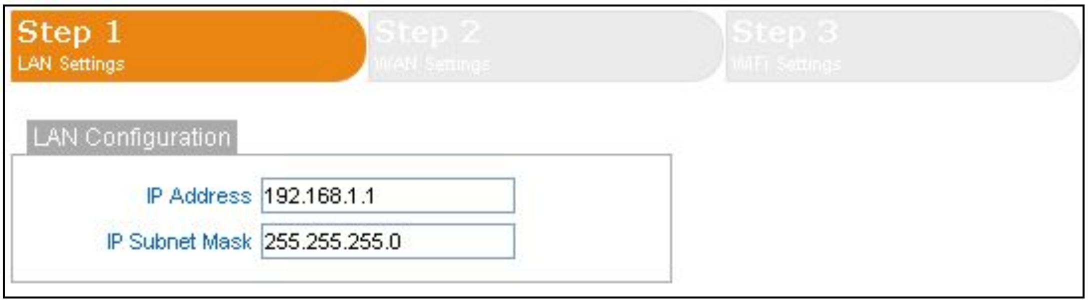
LAN Configuration

IP Address 192.168.1.1

IP Subnet Mask 255.255.255.0

Please follow the steps and complete the router configuration.

Step 1 LAN Connection Setting:



LAN Configuration

IP Address 192.168.1.1

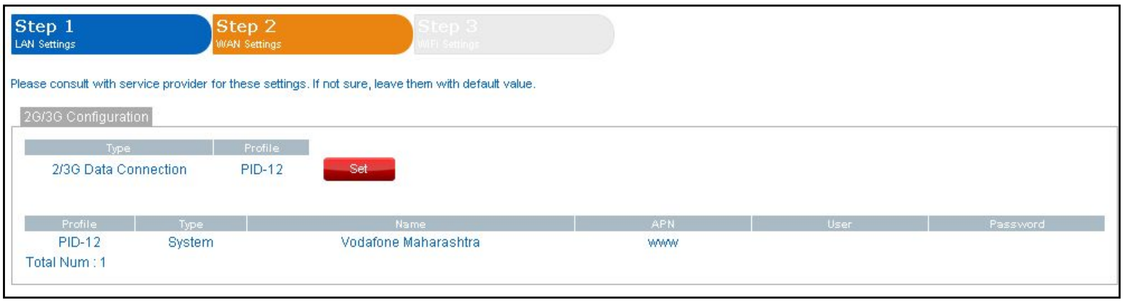
IP Subnet Mask 255.255.255.0

Here is the description of every setup item:

Parameter	Description
IP Address	If you wish to change the router's IP address, enter the new address here. If you change the IP address from the default, you will need to enter the new address in your Internet browser's address bar in order to access the web-based configuration utility.
IP Subnet Mask	If you wish to change the router's subnet mask, enter it here.

After the settings are done click on "**Next**".

Step 2 2G/3G Configuration:



Please consult with service provider for these settings. If not sure, leave them with default value.

2G/3G Configuration

Type	Profile
2/3G Data Connection	PID-12

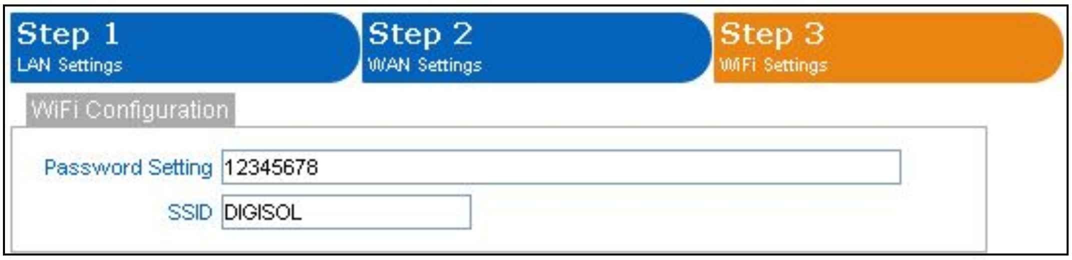
Profile	Type	Name	APN	User	Password
PID-12	System	Vodafone Maharashtra	www		

Total Num : 1

If you wish to change the 2G or 3G service provider or connection type, click on a profile in the list to highlight it, and click "**Set**" to set that profile as the default.

Click "**Next**" to continue, or "**Back"** to return to the previous step.

Step 3 Wi-Fi Configuration



WiFi Configuration

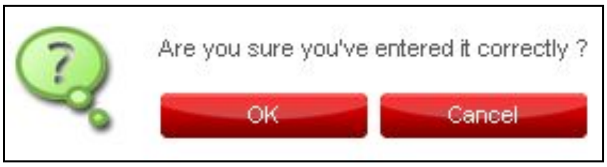
Password Setting 12345678

SSID DIGISOL

Here is the description of every setup item:

Parameter	Description
Password Setting	Choose a password for your wireless security. Clients will need this password in order to access your network wirelessly. If you are currently connected to the router using Wi-Fi, you will need to reconnect to the router using your new password once the wizard has been completed.
SSID	If you wish to change your wireless network name (SSID), enter a new name in the field provided. If you change the SSID, you may need to re-connect to the router using the new SSID before you can access your network or the configuration utility.

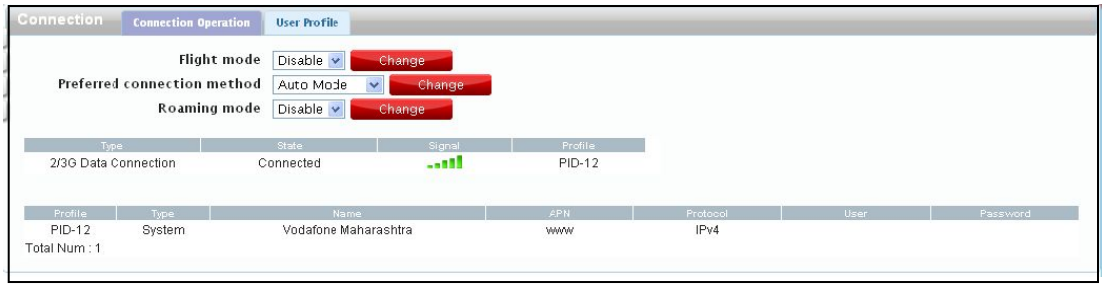
Click “**Done**” to complete the wizard, or click Back to return to the previous page. After you have clicked Done, a confirmation window will appear. Click “**OK**” to save the configuration.


Are you sure you've entered it correctly ?

3-3 WAN

This page allows you to configure the Internet settings for your mobile network connection. Use the tabs in the left-hand column to navigate through the different settings categories.

1) Connection Operation



Flight mode: Disable

Preferred connection method: Auto Mode

Roaming mode: Disable

Type	State	Signal	Profile
2/3G Data Connection	Connected		PID-12

Profile	Type	Name	APN	Protocol	User	Password
PID-12	System	Vodafone Maharashtra	www	IPv4		

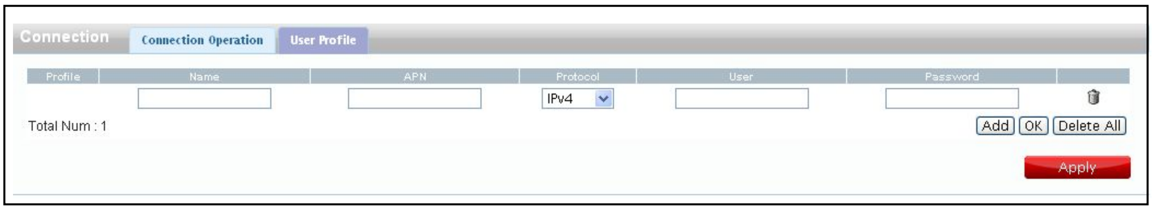
Total Num : 1

Here is the description of every setup item:

Parameter	Description
Flight mode	Flight mode turns off all communications. Select whether you want to Enable or Disable flight mode from the drop down menu, and click Change to effect the change.
Preferred connection method	Select your preferred cellular network connection mode: Auto Mode - The router will automatically connect to your preferred mobile network and remain connected while the device is powered on. Manual Mode - You must manually connect to the preferred mobile network. On Demand - The router will connect to the preferred mobile network when Internet access is required.
Roaming Mode	Select whether you would like to Enable or Disable mobile network roaming from the drop-down menu. **Caution: Roaming on networks other than your own may incur additional usage charges.**
Connection	Shows the type and status of the current mobile connection.

User Profile

Profiles: The profiles table shows the details of currently configured user profiles. To add a new user profile, navigate to the User Profile tab at the top of this section.



Profile	Name	APN	Protocol	User	Password	
			IPv4			

Total Num : 1

Click “**Add”** to add a new user profile.

Here is the description of every setup item:

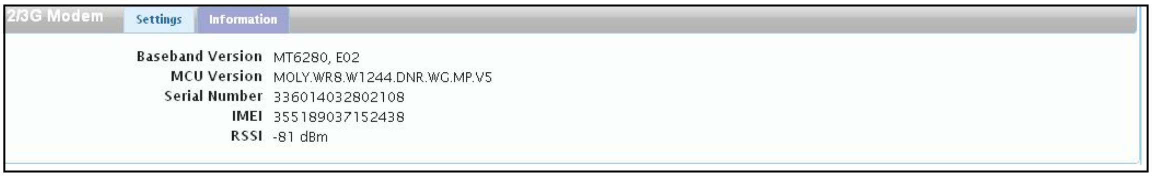
Parameter	**Description**
Name	Enter a name to identify the new user profile.
APN	Enter the Access Point Name (APN) for the connection. If you do not know this information, please contact your service provider.
Protocol	Select the protocol to be used for the connection from the drop-down menu.
User	Enter the username to be used for this connection.
Password	Enter the password to be used for this connection.
Delete	Click the delete icon to delete this profile from the list. Click OK to save the profile. To edit the rule click on the rule itself.

Click “**Apply**” to apply the profile settings and return to the Internet menu.

2) 2G/3G Modem

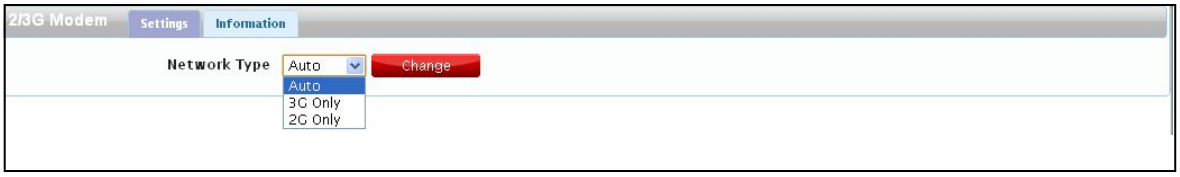
This section displays information about your 2G or 3G modem connection.

Information: Displays information about your 2G or 3G modem.



Baseband Version MT6280, E02
MCU Version MOLY.WR8.W1244.DNR.WG.MP.V5
Serial Number 336014032802108
IMEI 355189037152438
RSSI -81 dBm

Settings: Select your preferred modem type from the drop-down menu:

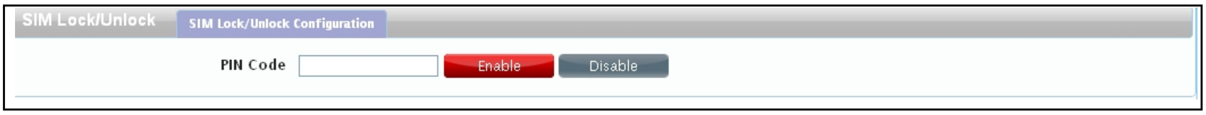


Network Type Auto

Here is the description of every setup item:

Parameter	**Description**
Network Type	Auto - The modem will automatically select the modem type depending on the network it is connected to. 3G Only - The modem will only connect to 3G networks. 2G Only - The modem will only connect to 2G networks.

3) SIM

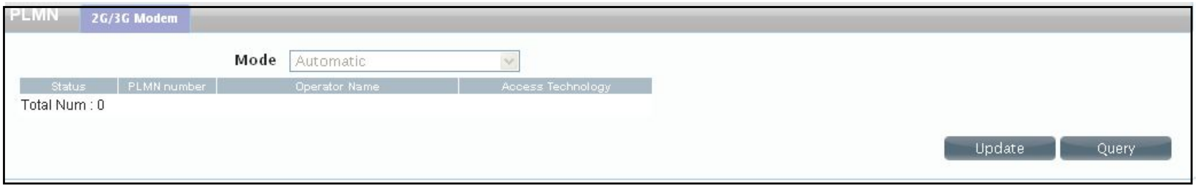


PIN Code

This section allows you to turn SIM lock on or off for the SIM card which is currently inserted into the router.

PIN Code: Enter the PIN code for the SIM card. Click Enable to turn on SIM lock, or click Disable to turn off SIM lock.

4) PLMN



Mode: Automatic

Status	PLMN number	Operator Name	Access Technology

Total Num : 0

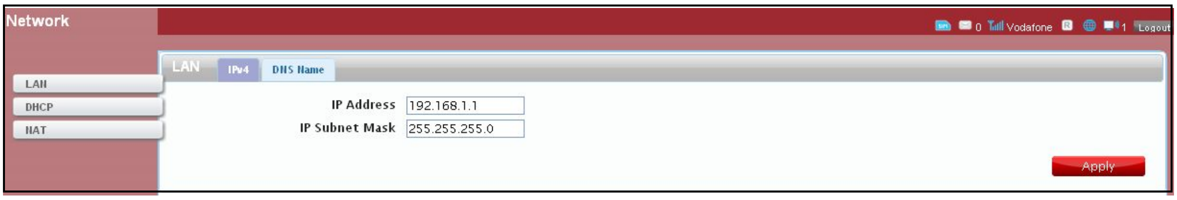
This page allows you to view available Public Land Mobile Networks (PLMN). This page can also be used to select a preferred network when you are roaming outside your home network.

Mode: Select Automatic to allow the router to automatically connect to the first available network when roaming. Select Manual to choose your preferred roaming network from the list below.

If you have selected Manual mode, click on the preferred network to select it, and then click the Update button to select that network as the preferred network. Click Query to refresh the list of available networks.

Note: You will need to manually disconnect the current mobile data service before selecting a network using PLMN.

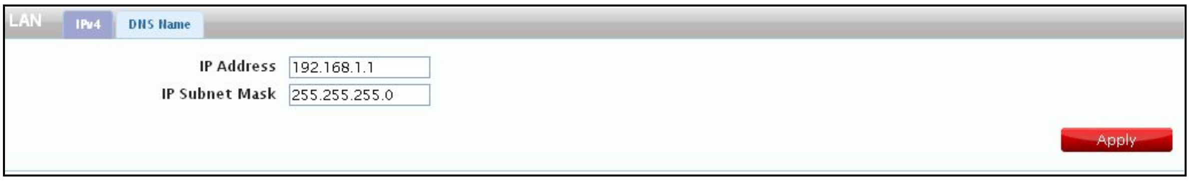
3-4 Network



IP Address 192.168.1.1
IP Subnet Mask 255.255.255.0

The Network pages allow you to check the current status of your Local Area Network (LAN) and make changes to LAN Settings.

1) LAN



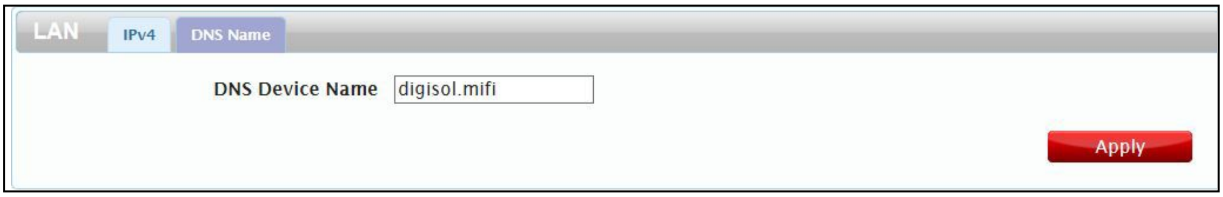
IP Address 192.168.1.1
IP Subnet Mask 255.255.255.0

IP Address: Enter the IPv4 address for your Wi-Fi network. If you change this address, you will need to enter the new address in your web browser's address bar in order to access the web-based configuration utility.

IP Subnet Mask: Enter the IPv4 subnet mask for your Wi-Fi network.

2) DNS Name

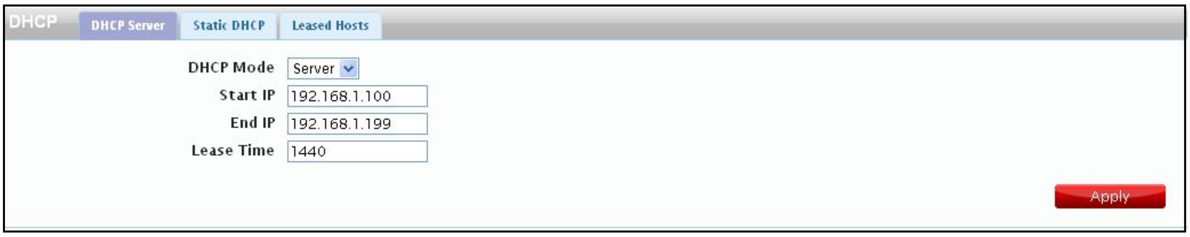
DNS Device Name: Enter your router's DNS device name in the field provided.



DNS Device Name digisol.mifi

3) DHCP

DHCP Server

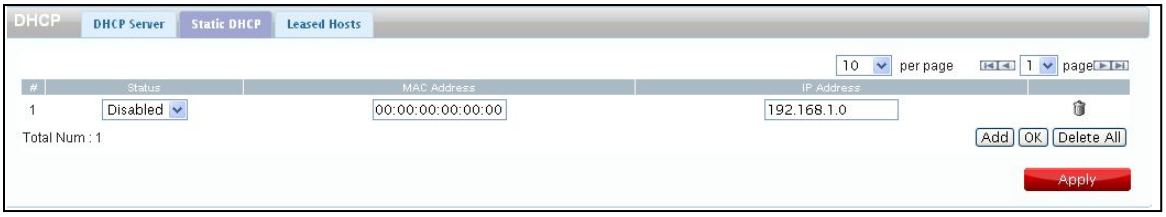


DHCP Mode: Server
Start IP: 192.168.1.100
End IP: 192.168.1.199
Lease Time: 1440

Here is the description of every setup item:

Parameter	**Description**
DHCP Mode	Select the desired DHCP mode from the drop down menu: None - Turns off DHCP functionality. Server - The router will act as a DHCP server and assign IP addresses to connected devices.
Start IP	Enter the starting address for the DHCP pool.
End IP	Enter the ending address for the DHCP pool.
Lease Time	Enter the lease time (in minutes) for assigned IP addresses.

Static DHCP



#	Status	MAC Address	IP Address
1	Disabled	00:00:00:00:00:00	192.168.1.0

Total Num : 1

Use this option to specify a DHCP address reservation to a particular device or machine based on MAC address. To add a new reservation, click "**Add**".

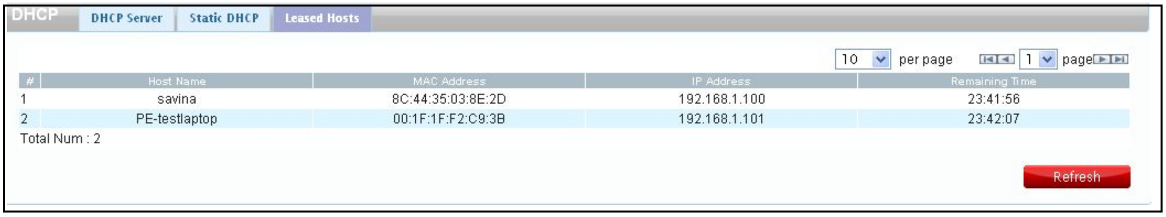
Here is the description of every setup item:

Parameter	**Description**
MAC Address	Enter the MAC address of the device or machine for which you

	wish to make the DHCP reservation.
IP Address	Enter the IP address that you wish to reserve. This address must be within the DHCP address pool.

Click “**OK**” to save the reservation.

Leased hosts



#	Host Name	MAC Address	IP Address	Remaining Time
1	savina	8C:44:35:03:8E:2D	192.168.1.100	23:41:56
2	PE-testlaptop	00:1F:1F:F2:C9:3B	192.168.1.101	23:42:07

Total Num : 2

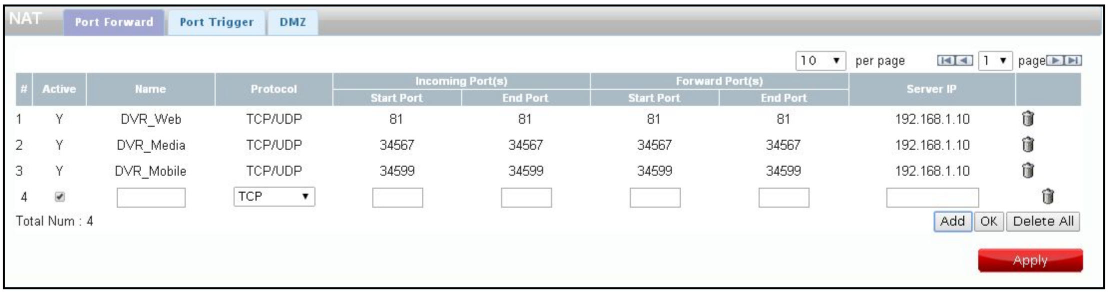
This table shows the details of clients currently receiving a DHCP address from the DHCP server. Click “**Refresh**” to update the table.

4) NAT

This section allows you to configure functions related to Network Address Translation (NAT) such as port forwarding, port triggering and the Demilitarized Zone (DMZ)

Port Forwarding

Use this option to have inbound traffic directly forwarded to a static address on the LAN when triggered by outbound traffic. By default port forwarding has three rules. To add a new port forwarding rule, click “**Add**”.



#	Active	Name	Protocol	Incoming Port(s)		Forward Port(s)		Server IP	
				Start Port	End Port	Start Port	End Port		
1	Y	DVR_Web	TCP/UDP	81	81	81	81	192.168.1.10	🗑
2	Y	DVR_Media	TCP/UDP	34567	34567	34567	34567	192.168.1.10	🗑
3	Y	DVR_Mobile	TCP/UDP	34599	34599	34599	34599	192.168.1.10	🗑
4	☑		TCP						🗑

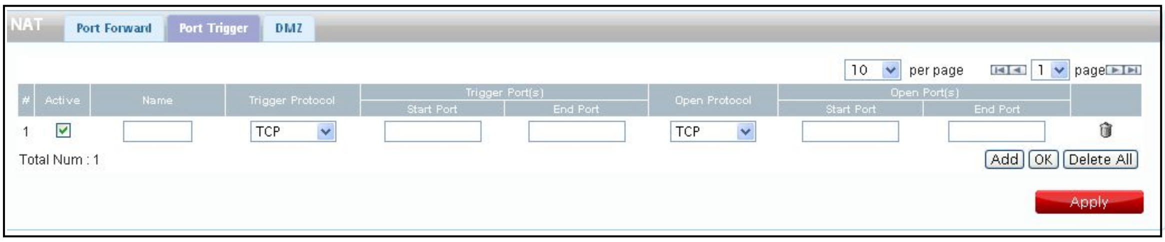
Total Num : 4

Here is the description of every setup item:

Parameter	Description
Active	Check the box to activate this rule.
Name	Specify a name to identify the rule.
Protocol	Select TCP,UDP or TCP/UDP as the protocol for the forwarded ports from the drop-down menu.
Incoming Port(s)	Enter the starting and ending port to be opened for the rule.
Forward Port(s)	Enter the starting and ending ports to be forwarded.
Server IP	Enter the IP address of the server or PC for which the port has been forwarded.
Delete	Click the Delete icon to delete the rule.
Delete All	Click delete all to delete all the rules.

Click “**OK**” to save the rule. Click “**Apply**” to apply the current rules and return to the Network page.

Port Trigger



#	Active	Name	Trigger Protocol	Trigger Port(s)		Open Protocol	Open Port(s)		
				Start Port	End Port		Start Port	End Port	
1	☑		TCP			TCP			🗑

Total Num : 1

Use this option to have inbound traffic automatically forwarded to a dynamic address on the LAN when triggered by outbound traffic. To add a new port triggering rule, click “**Add**”.

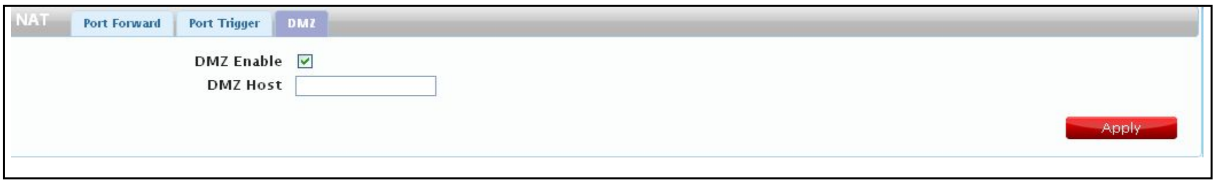
Here is the description of every setup item:

Parameter	Description
Active	Check the box to activate this rule.
Name	Specify a name to identify the rule.
Trigger Protocol	Select TCP, UDP or TCP/UDP as the protocol for the trigger ports from the drop-down menu.
Trigger Port	Enter the starting and ending trigger port for the rule.

Open Protocol	Select TCP, UDP or TCP/UDP as the protocol for the ports to be opened from the drop-down menu.
Open Port(s)	Enter the starting and ending ports to be opened when the trigger occurs.
Delete	Click the Delete icon to delete the rule. To edit the rule click on the rule itself.

Click "**OK**" to save the rule. Click "**Apply**" to apply the current rules and return to the Network page.

DMZ



DMZ Enable ☑
DMZ Host

If a machine on your network is having trouble running an application from behind the router's firewall, you can choose to enable the DMZ, which will expose the selected machine completely to the Internet. It is recommended that this is only used as a last resort, and that you understand the security implications before enabling the DMZ.

Here is the description of every setup item:

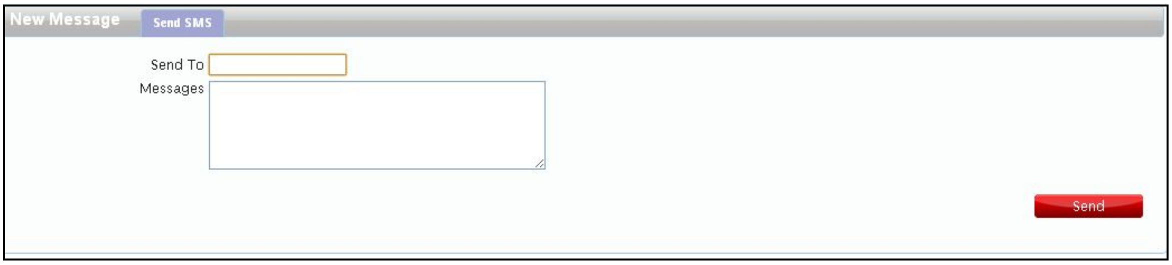
Parameter	Description
DMZ Enable	Check the box to enable the DMZ function.
DMZ Host	Enter the IP address of the machine that you wish to place in the DMZ. If this machine receives an IP address from the DHCP server, you should make a DHCP reservation to ensure that the machine always receives the same IP address.

Click "**Apply**" to save the settings and return to the Network page.

3-5 SMS

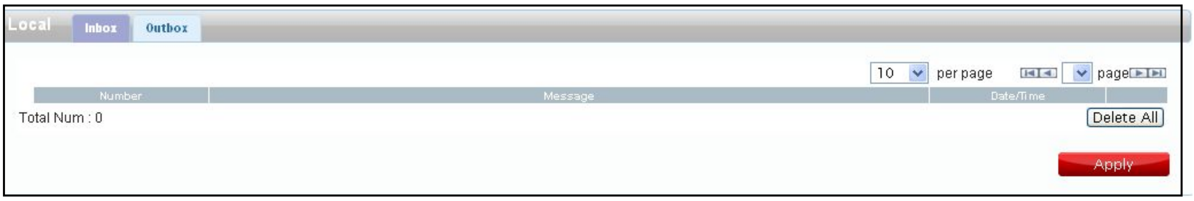
DG-HR1020S can send or receive SMS text messages through the mobile network's SMS function. In this section you can check the SIM card's inbox and outbox, as well as send new messages.

New Message



Send To: Enter the phone number that you wish to send the message to.
Messages: Enter the body of the message to be sent.

Local



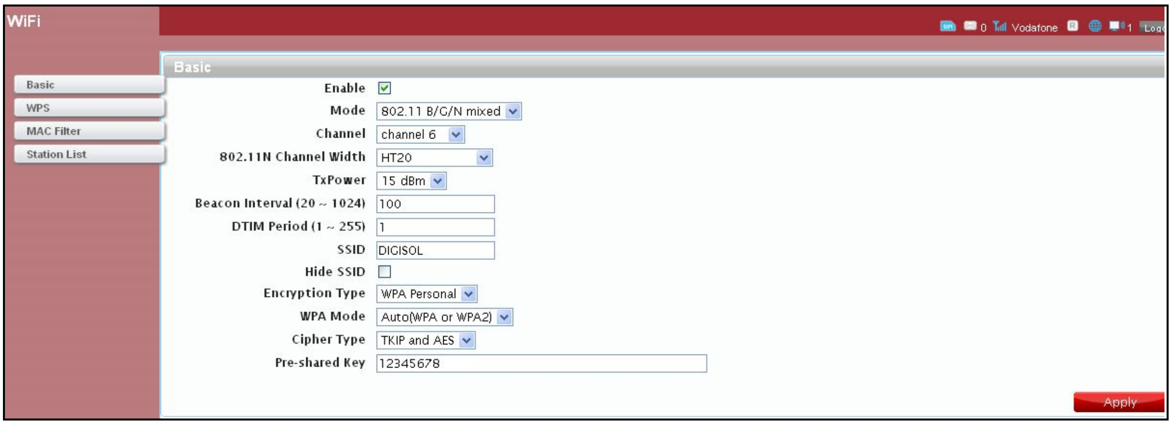
Total Num : 0

Inbox: This tab shows a summary of SMS messages in the inbox.
Outbox: This tab shows a summary of messages in the outbox which are yet to be sent.

3-6 Wi-Fi

The Wi-Fi pages allow you to check the current status of your Wi-Fi network, and make changes to Wi-Fi settings.

1) Basic



Basic

Enable	☑
Mode	802.11 B/G/N mixed
Channel	channel 6
802.11N Channel Width	HT20
TxPower	15 dBm
Beacon Interval (20 ~ 1024)	100
DTIM Period (1 ~ 255)	1
SSID	DIGISOL
Hide SSID	□
Encryption Type	WPA Personal
WPA Mode	Auto(WPA or WPA2)
Cipher Type	TKIP and AES
Pre-shared Key	12345678

This section allows you to configure your Wi-Fi network and specify the wireless security method to be used to secure your network.

Here is the description of every setup item:

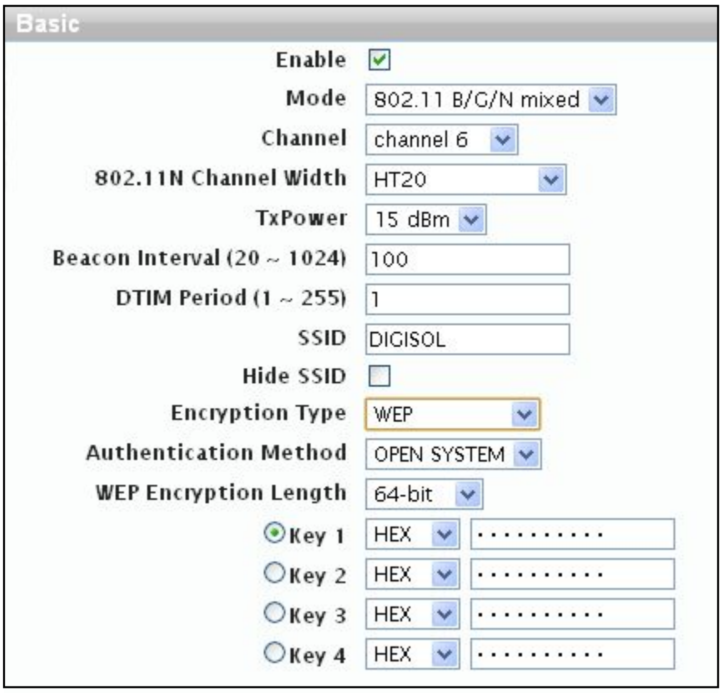
Parameter	Description
Enable	Check the box to enable Wi-Fi function.
Mode	Select the desired 802.11 wireless mode from the drop down menu. You should make your selection based on the standards supported by the wireless clients which will be connecting to your network.
Channel	To have the router automatically select the optimal wireless channel, select Auto from the drop-down menu. If you wish to select a particular channel, select if from the drop-down menu.
802.11N Channel Width	If you are using the 802.11n standard, you can manually select the channel width which best suits your network environment.
Tx Power	Specifies the strength of the wireless transmission signal.
Beacon Interval	The beacon interval determines how often information about the wireless network is broadcast. It is recommended that you

	do not adjust this setting unless instructed to do so.
DTIM Period	The Delivery Traffic Indication Message broadcasts information about buffered data to clients that are currently in low-power mode. Enter the desired DTIM period as a number of beacon intervals.
SSID	Enter the SSID (network name) to identify your wireless network.
Hide SSID	Check the box to hide the SSID of your network. If the SSID is hidden, wireless clients must manually enter it in order to connect to your network.
Encryption Type	Select the wireless encryption method that you wish to use from the drop-down menu. If you do not wish to enable wireless security, select None from the drop-down menu. Click Apply to save the current settings.

Wireless security

It is recommended that you enable wireless security on your router in order to protect your wireless network from unauthorized access. You should select a wireless security protocol that is compatible with the wireless clients which will be accessing your network.

WEP



Basic

Enable ☑

Mode 802.11 B/G/N mixed

Channel channel 6

802.11N Channel Width HT20

TxPower 15 dBm

Beacon Interval (20 ~ 1024) 100

DTIM Period (1 ~ 255) 1

SSID DIGISOL

Hide SSID □

Encryption Type WEP

Authentication Method OPEN SYSTEM

WEP Encryption Length 64-bit

● Key 1 HEX ··········

○ Key 2 HEX ··········

○ Key 3 HEX ··········

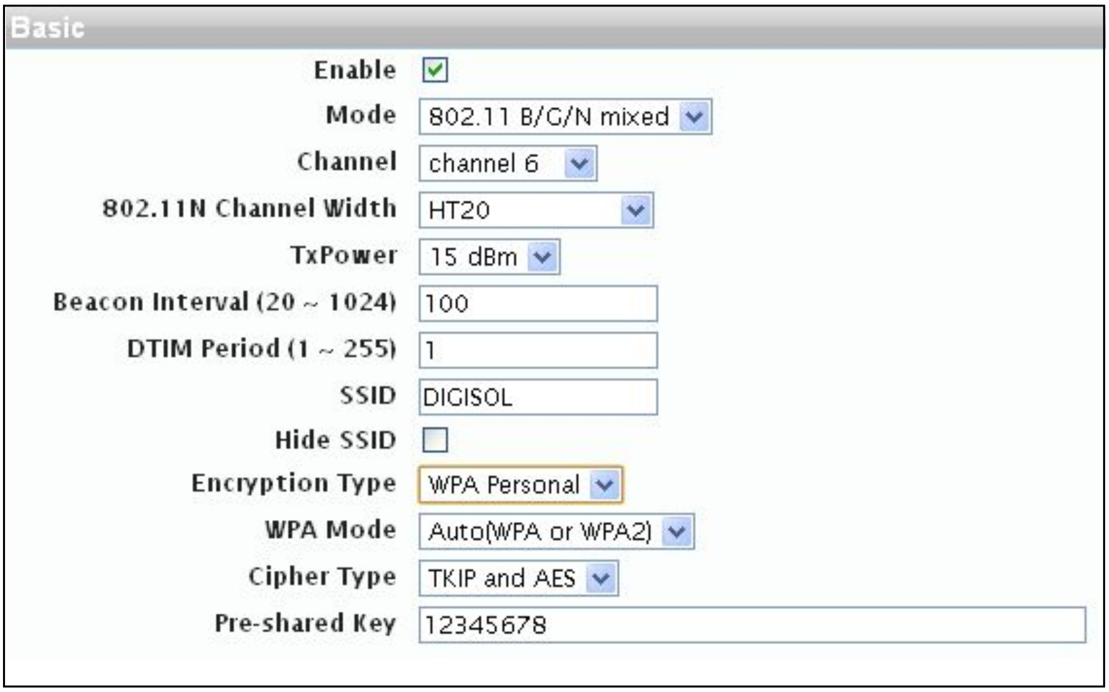
○ Key 4 HEX ··········

Wired Equivalent Privacy (WEP) is an older wireless security standard, which although providing more protection than no security at all, has some weaknesses which could make it vulnerable to intrusion. It is recommended that you only use WEP if your wireless clients do not support Wi-Fi Protected Access (WPA). WEP is not supported by the 802.11n standard, and therefore you will not be able to achieve 802.11n speeds if you are using WEP.

Here is the description of every setup item:

Parameter	**Description**
Encryption Type	Select WEP from the drop-down menu.
Authentication Method	Select the desired authentication method from the drop down menu: Auto - The router will automatically determine the authentication method based on the client that is connecting to it. Open System - Clients do not require authentication in order to associate with the router. The encryption key will be used to encrypt data packets sent over the network. Shared - The encryption key is used for authentication as well as to encrypt data packets.
WEP Encryption Length	Select the length of the encryption key to be used. 64-bit - A 64-bit key comprises a string of 10 hexadecimal characters, or 5 ASCII characters. 128-bit - A 128-bit key comprises a string of 26 hexadecimal characters, or 13 ASCII characters.
Key 1-4	You can predetermine up to 4 WEP keys. Select the WEP key you wish to use by clicking on the radio buttons next to the keys. Select whether you wish to use HEX or ASCII characters in your key using the drop-down menu. Enter the desired key in the field provided. Click Apply to save the current settings.

Wi-Fi Protected Access (WPA)



Enable	☑
Mode	802.11 B/G/N mixed
Channel	channel 6
802.11N Channel Width	HT20
TxPower	15 dBm
Beacon Interval (20 ~ 1024)	100
DTIM Period (1 ~ 255)	1
SSID	DIGISOL
Hide SSID	□
Encryption Type	WPA Personal
WPA Mode	Auto(WPA or WPA2)
Cipher Type	TKIP and AES
Pre-shared Key	12345678

Wi-Fi Protected Access (WPA) is a newer and more secure encryption protocol which makes significant improvements over WEP. There are two versions of WPA; the original WPA, and the newer WPA2.

Here is the description of every setup item:

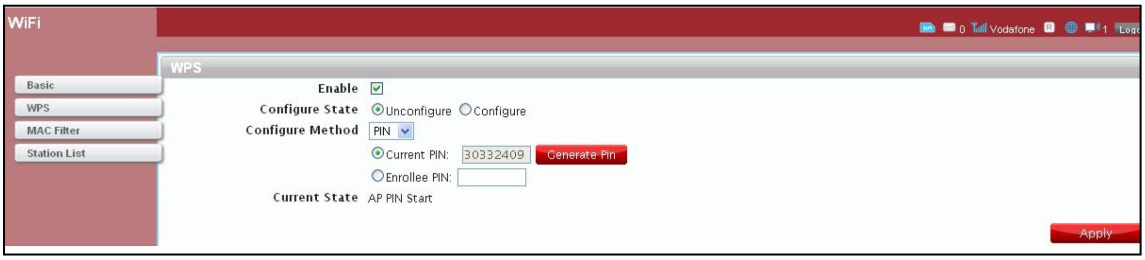
Parameter	Description
Encryption Type	Select WPA Personal from the drop-down menu. WPA Mode: Select the desired authentication method from the drop-down menu: Auto (WPA or WPA2) - The router will automatically determine the version of WPA to be used based on the client that is connecting to it. WPA - Clients will only be able to associate with the router using the WPA standard. WPA2 - Clients will only be able to associate with the router using the WPA2 standard. Clients that do not support WPA2 will not be able to associate with the router.

Cipher Type	Select the desired cipher type from the drop-down menu: TKIP - This cipher is used by the WPA standard. AES - A newer cipher used by the WPA2 standard. Use of this cipher type is required in order to achieve 802.11 speeds.
Pre-Shared Key	The pre-shared key is the password which clients will require in order to connect to your network. Enter a password between 8 and 63 characters in length.

Click “**Apply**” to save the current settings

2) WPS

Wi-Fi Protected Setup (WPS) enables you to quickly and securely add compatible devices to your wireless network.



WPS

Enable ☑

Configure State ● Unconfigure ○ Configure

Configure Method PIN

● Current PIN: 30332409

○ Enrollee PIN:

Current State AP PIN Start

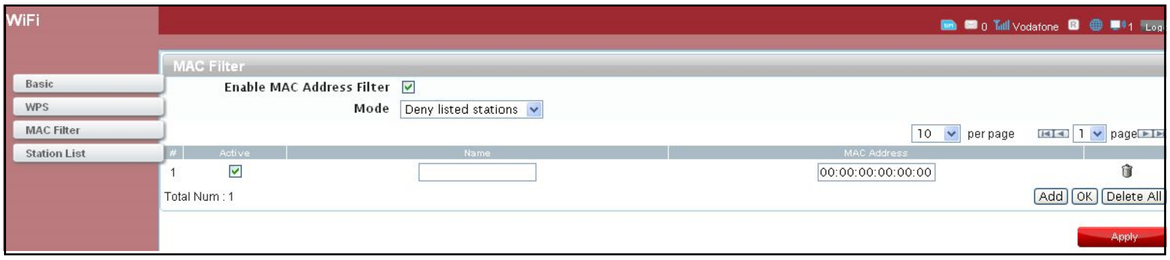
Here is the description of every setup item:

Parameter	**Description**
Enable	Check the box to enable the Wi-Fi Protected Setup feature.
Configure State	Shows the current status of the WPS function.
Configure Method	Select the WPS method that you wish to use. If your device supports Push Button Connection (PBC), simply select this option and click Apply to start the connection process. You will then have 120 seconds to press the WPS button on your wireless device in order to initiate the connection. If your device does not support PBC, you can select the PIN method and continue to the next step.
Current PIN	A PIN is a unique number that can be used to add the router to an existing network or to create a new network.
Generate PIN	For extra security, a new PIN can be generated. Click

	“Generate Pin” to create a new PIN. The current PIN will be shown in the field next to Current PIN. This PIN can be used by wireless clients to join your network using the PIN method
Enrollee PIN	If the device you are trying to add to the network was provided with a PIN number, select this option and enter the device’s PIN in the field.

Click “**Apply**” to commence the connection process.

3) MAC Filter



MAC Filter

Enable MAC Address Filter ☑

Mode: Deny listed stations

10 per page 1 page

#	Active	Name	MAC Address	
1	☑		00:00:00:00:00:00	🗑

Total Num : 1

The MAC filtering option allows you to allow or deny access to wireless clients based on their MAC address.

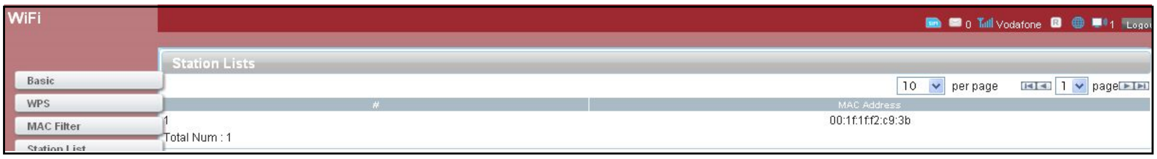
Here is the description of every setup item:

Parameter	**Description**
Enable MAC Address Filter	Check the box to enable the MAC filtering feature.
Mode	Select the filtering mode from the drop-down menu. You can choose to Deny Listed Stations access to your network, or Allow Listed Stations access. To add a new filtering rule, click Add.
Active	Check the box to activate the rule.
Name	Enter a name to identify the machine or station which will be filtered.
MAC Address	Enter the MAC address of the machine or station which you wish to filter.
Delete	Click the Delete icon to delete the rule from the table. To edit the rule click on the rule itself.

Click “**OK**” to save the current rule and add it to the table. Click “**Apply**” to save all changes and return to the Wi-Fi page.

4) Station List

The Station List tab shows a list of all wireless clients currently connected to your wireless network.



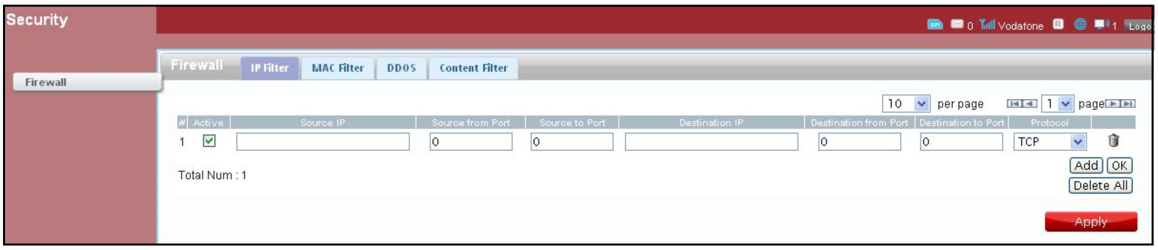
#	MAC Address
1	00:1f:1f:f2:c9:3b

Total Num : 1

3-7 Security

The Security tab allows you to configure your router’s firewall settings and enable features to protect your network from outside intrusions and malicious attacks.

1) IP Filter



#	Active	Source IP	Source from Port	Source to Port	Destination IP	Destination from Port	Destination to Port	Protocol
1	☑		0	0		0	0	TCP

Total Num : 1

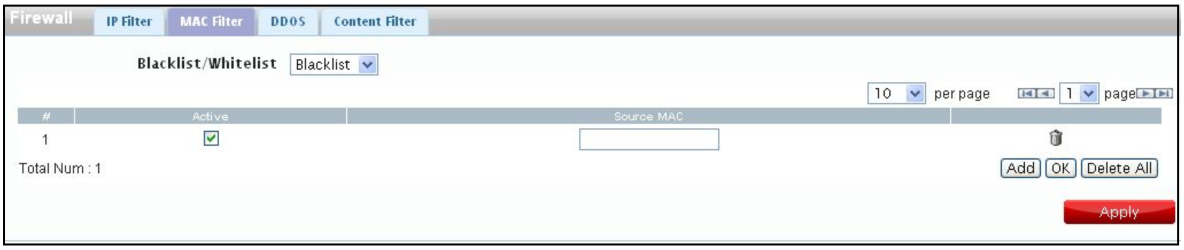
Here is the description of every setup item:

Parameter	Description
Active	Check the box to activate the IP filter rule.
Source IP	Enter the source IP address to be filtered.
Source From Port	Enter the starting port on the source IP.
Source To Port	Enter the ending port on the source IP.
Destination IP	Enter the destination IP address to be filtered.
Destination From Port	Enter the starting port of the destination IP.
Destination To Port	Enter the ending port of the destination IP.
Protocol	Select the protocol for the IP filter rule.
Delete	Click the icon to delete the IP filtering rule. To edit the rule click on the rule itself.

2) MAC Filter

The MAC filter allows you to allow or deny access to your wireless network based on a client’s MAC address.

Click “**Add**” to add the current rule to the rules list.



Blacklist/Whitelist: Blacklist

10 per page 1 page

#	Active	Source MAC	
1	☑		🗑

Total Num : 1

Here is the description of every setup item:

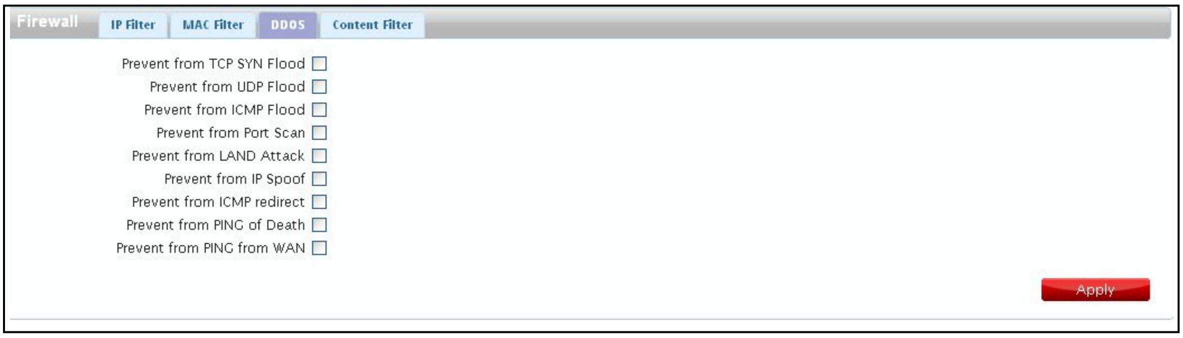
Parameter	Description
Blacklist/White list	Select Blacklist to deny access to only the MAC addresses listed below. Select White list to allow access to only the MAC addresses listed below.
Active	Check the box to activate the MAC filter rule.
Source MAC	Enter the MAC address of the machine or device which you wish to filter packets coming from.
Delete	Click the icon to delete this MAC filtering rule. To edit the rule click on the rule itself.

3) DDOS

This section allows you to enable various security features to protect against Denial of Service (DoS) attacks.

DoS Prevention Filters: Check the box next to the rule to enable prevention against that specific kind of DoS attack.

Click “**Apply**” to save the current configuration

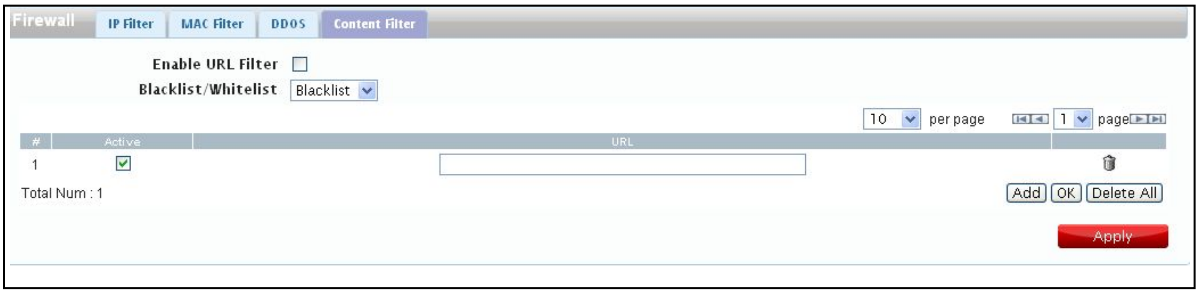


Prevent from TCP SYN Flood ☐
Prevent from UDP Flood ☐
Prevent from ICMP Flood ☐
Prevent from Port Scan ☐
Prevent from LAND Attack ☐
Prevent from IP Spoof ☐
Prevent from ICMP redirect ☐
Prevent from PING of Death ☐
Prevent from PING from WAN ☐

4) Content Filter

The content filter allows you to allow or deny access to specific URLs.

Click “**Add**” to save the rule and add it to the rule table.



Enable URL Filter ☐
Blacklist/Whitelist: Blacklist

#	Active	URL
1	☑	

Total Num : 1

Here is the description of every setup item:

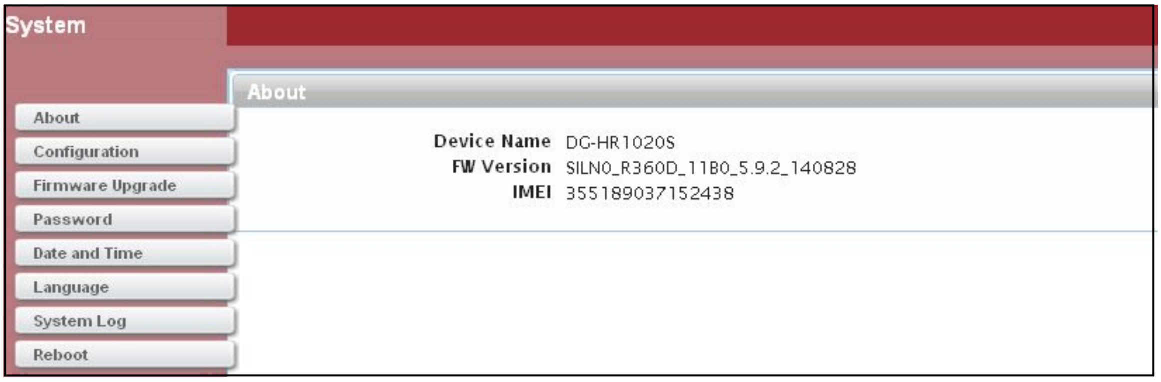
Parameter	Description
Enable URL Filter	Check the box to enable URL filtering.
Blacklist/Whitelist	Select Blacklist to deny access to only URLs listed in the rule table. Select Whitelist to allow access to only URLs listed in the rule list.
Active	Check the box to activate the URL filtering rule.
URL	Enter the URL that you wish to allow or deny access to. If you enter a domain name, all URLs under this domain will be allowed or denied access.
Delete	Click the icon to delete the rule. To edit the rule click on the rule itself.

3-8 System

This tab allows you to configure the router's administrative functions, such as time & date, remote access, firmware upgrade, and access the system log.

1) About

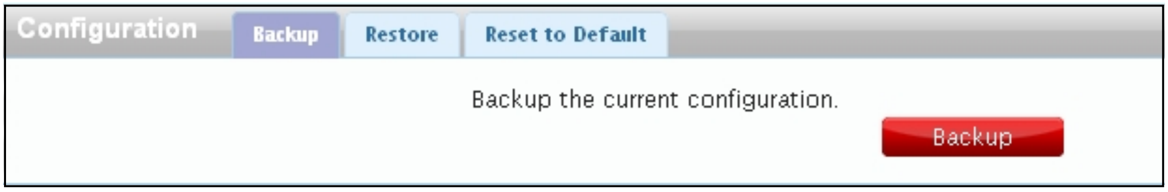
This tab shows the router's basic information.



Device Name DG-HR1020S
FW Version SILNO_R360D_11B0_5.9.2_140828
IMEI 355189037152438

2) Configuration

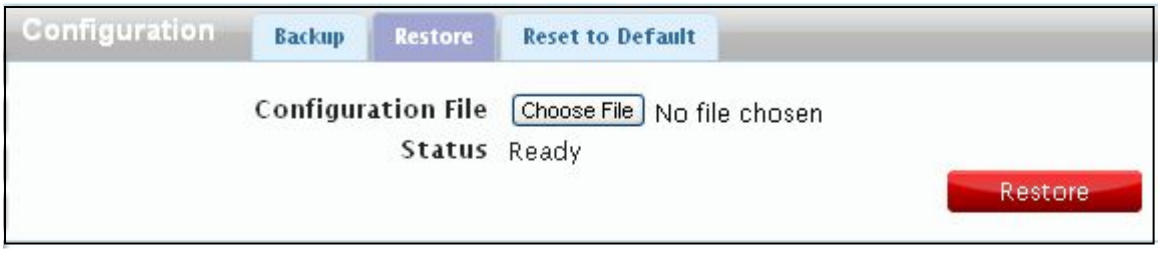
Back up



Backup the current configuration.

Click "**Backup**" to save the router's current configuration to a file on your computer. You will then be prompted with a"**save file**"pop up, where you can choose where to save the configuration file.

Restore

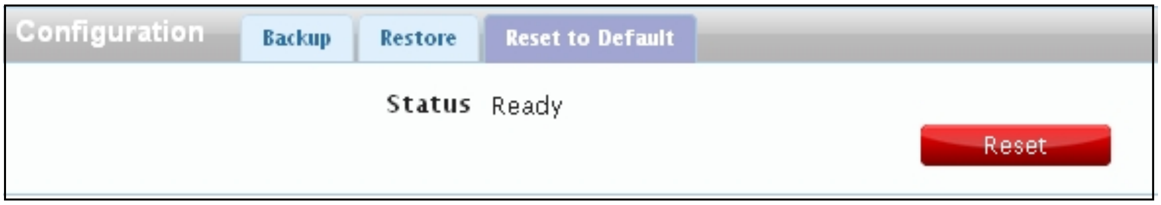


Configuration File No file chosen
Status Ready

Click "**Choose file**" to locate a previously saved configuration file on your computer.

Once you have located the file, click Restore to configure the router according to the selected configuration file.

Reset to Default

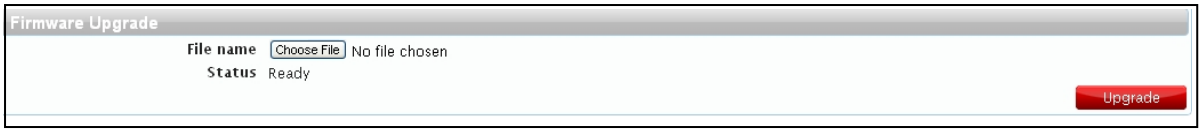


Status Ready

Click "**Reset to default**" to restore the router's settings to the factory defaults.

Warning: All settings stored on the router will be lost following a factory reset.

3) Firmware Upgrade

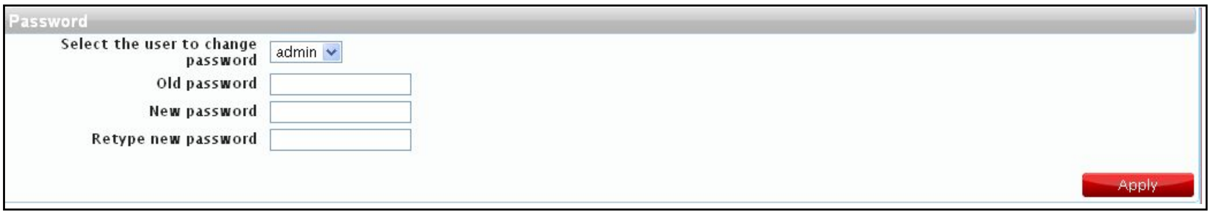


File name No file chosen
Status Ready

You can upgrade the firmware of the router here. Make sure the firmware file you want to use is on the local hard drive of the computer.
Click "**Choose file**" to locate a previously downloaded firmware file on your computer. Once the file has been located, click Upgrade to carry out the firmware upgrade process.

Warning: All current settings will be restored to their factory defaults following a firmware upgrade.

4) Password



Select the user to change password: admin
Old password
New password
Retype new password

This page lets you change the configuration interface passwords for the Administrator (Admin) and User accounts.

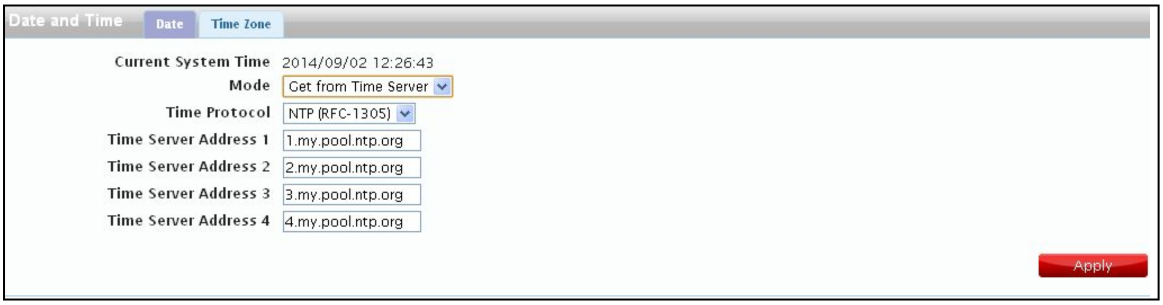
Here is the description of every setup item:

Parameter	Description
Select the user to change password	Select whether you wish to change the password for the admin or user account from the drop down menu.
Old Password	Enter the existing password for this account.
New Password	Enter the new password for this account.
Retype New Password	Type the new password again to confirm.

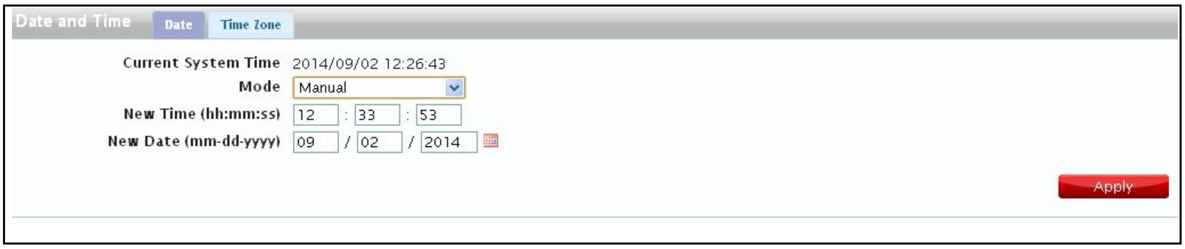
5) Date and Time

This page lets you set the time and date for your router, and also configure automatic time synchronization and daylight savings time.

Date



Current System Time 2014/09/02 12:26:43
Mode Get from Time Server
Time Protocol NTP (RFC-1305)
Time Server Address 1 1.my.pool.ntp.org
Time Server Address 2 2.my.pool.ntp.org
Time Server Address 3 3.my.pool.ntp.org
Time Server Address 4 4.my.pool.ntp.org



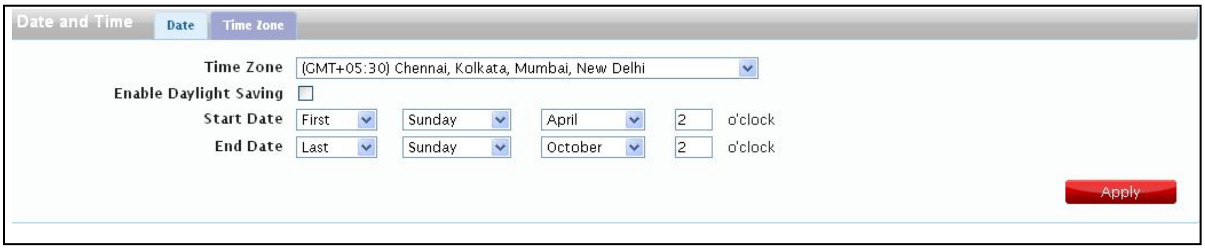
Current System Time 2014/09/02 12:26:43
Mode Manual
New Time (hh:mm:ss) 12 : 33 : 53
New Date (mm-dd-yyyy) 09 / 02 / 2014

Here is the description of every setup item:

Parameter	Description
Current System Time	Displays the current time and date according to the router's system clock.
Mode	Select Manual to manually set the time and date, or select Get from Time Server to have the router automatically synchronize the time with a Network Time Protocol (NTP) server.
New Time	If you selected Manual mode, enter the current time.
New Date	If you selected Manual mode, enter the current date.
Time Protocol	If you selected Get time From Server, select the desired time protocol from the drop-down menu.
Time Server Address 1-4	Enter up to four NTP server addresses which will be used to synchronize the router's system time and date.

Click "**Apply**" to save the current settings.

Time Zone



Time Zone: (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi

Enable Daylight Saving: □

Start Date: First | Sunday | April | 2 o'clock

End Date: Last | Sunday | October | 2 o'clock

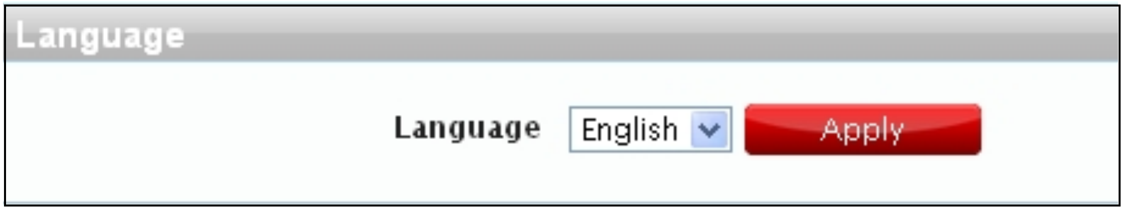
Here is the description of every setup item:

Parameter	Description
Time Zone	Select your time zone from the drop-down menu.
Enable Daylight Saving	Check the box to enable automatic adjustment for daylight saving.
Start Date	Enter the details of the starting date and time for daylight saving time in your region.
End Date	Enter the details of the ending date and time for daylight saving time in your region.

Click “**Apply**” to save the current settings

6) Language

Language: Select your preferred language from the drop-down menu.



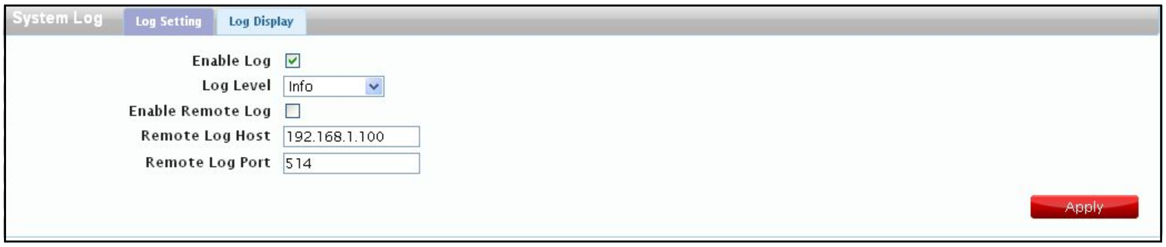
Language: English

Click “**Apply**” to save the current configuration.

7) System Log

The system log displays a record of all events which occur while the router is running.

Log Setting

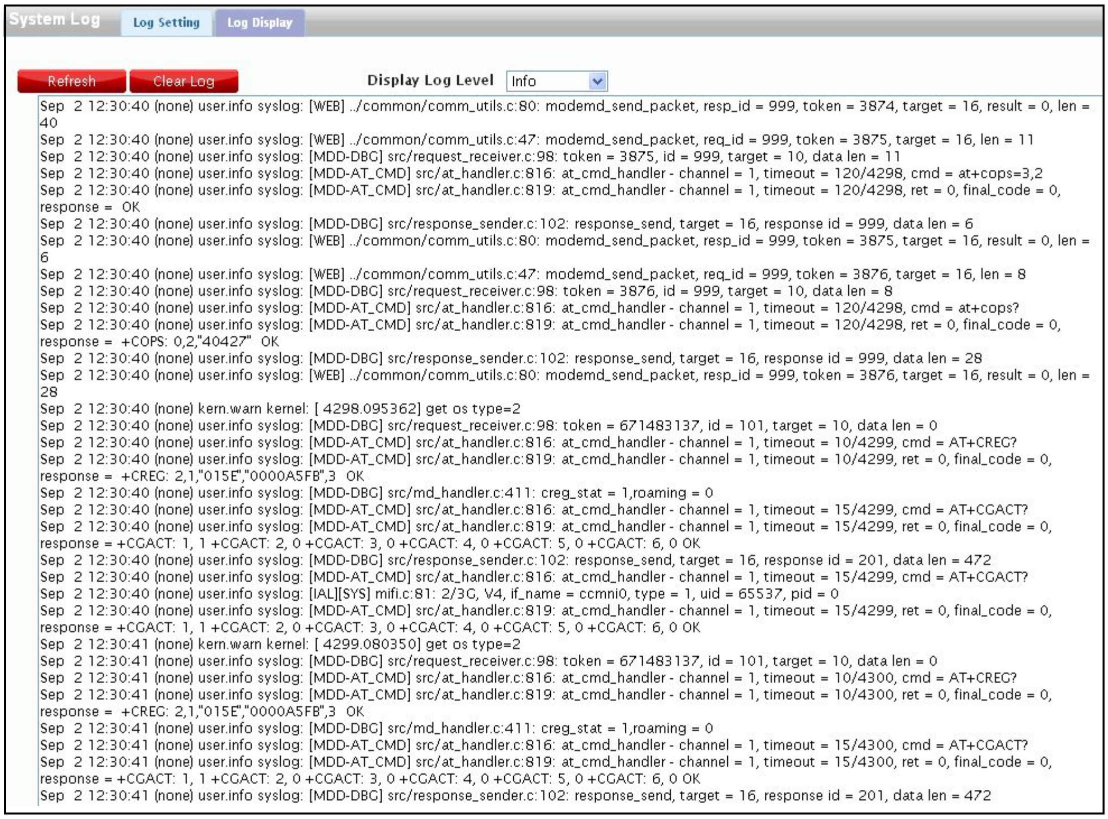


Enable Log ☑
Log Level: Info
Enable Remote Log ☐
Remote Log Host: 192.168.1.100
Remote Log Port: 514

Enable Log: Check the box to enable the router’s log-keeping function.

Click “**Apply**” to save the current configuration.

Log Display



Display Log Level: Info

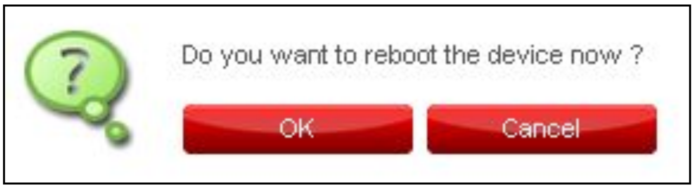
```
Sep  2 12:30:40 (none) user.info syslog: [WEB] ../common/comm_utils.c:80: modemd_send_packet, resp_id = 999, token = 3874, target = 16, result = 0, len =
40
Sep  2 12:30:40 (none) user.info syslog: [WEB] ../common/comm_utils.c:47: modemd_send_packet, req_id = 999, token = 3875, target = 16, len = 11
Sep  2 12:30:40 (none) user.info syslog: [MDD-DBG] src/request_receiver.c:98: token = 3875, id = 999, target = 10, data len = 11
Sep  2 12:30:40 (none) user.info syslog: [MDD-AT_CMD] src/at_handler.c:816: at_cmd_handler - channel = 1, timeout = 120/4298, cmd = at+cops=3,2
Sep  2 12:30:40 (none) user.info syslog: [MDD-AT_CMD] src/at_handler.c:819: at_cmd_handler - channel = 1, timeout = 120/4298, ret = 0, final_code = 0,
response =  OK
Sep  2 12:30:40 (none) user.info syslog: [MDD-DBG] src/response_sender.c:102: response_send, target = 16, response id = 999, data len = 6
Sep  2 12:30:40 (none) user.info syslog: [WEB] ../common/comm_utils.c:80: modemd_send_packet, resp_id = 999, token = 3875, target = 16, result = 0, len =
6
Sep  2 12:30:40 (none) user.info syslog: [WEB] ../common/comm_utils.c:47: modemd_send_packet, req_id = 999, token = 3876, target = 16, len = 8
Sep  2 12:30:40 (none) user.info syslog: [MDD-DBG] src/request_receiver.c:98: token = 3876, id = 999, target = 10, data len = 8
Sep  2 12:30:40 (none) user.info syslog: [MDD-AT_CMD] src/at_handler.c:816: at_cmd_handler - channel = 1, timeout = 120/4298, cmd = at+cops?
Sep  2 12:30:40 (none) user.info syslog: [MDD-AT_CMD] src/at_handler.c:819: at_cmd_handler - channel = 1, timeout = 120/4298, ret = 0, final_code = 0,
response =  +COPS: 0,2,"40427"  OK
Sep  2 12:30:40 (none) user.info syslog: [MDD-DBG] src/response_sender.c:102: response_send, target = 16, response id = 999, data len = 28
Sep  2 12:30:40 (none) user.info syslog: [WEB] ../common/comm_utils.c:80: modemd_send_packet, resp_id = 999, token = 3876, target = 16, result = 0, len =
28
Sep  2 12:30:40 (none) kern.warn kernel: [ 4298.095362] get os type=2
Sep  2 12:30:40 (none) user.info syslog: [MDD-DBG] src/request_receiver.c:98: token = 671483137, id = 101, target = 10, data len = 0
Sep  2 12:30:40 (none) user.info syslog: [MDD-AT_CMD] src/at_handler.c:816: at_cmd_handler - channel = 1, timeout = 10/4299, cmd = AT+CREG?
Sep  2 12:30:40 (none) user.info syslog: [MDD-AT_CMD] src/at_handler.c:819: at_cmd_handler - channel = 1, timeout = 10/4299, ret = 0, final_code = 0,
response =  +CREG: 2,1,"015E","0000A5FB",3  OK
Sep  2 12:30:40 (none) user.info syslog: [MDD-DBG] src/md_handler.c:411: creg_stat = 1,roaming = 0
Sep  2 12:30:40 (none) user.info syslog: [MDD-AT_CMD] src/at_handler.c:816: at_cmd_handler - channel = 1, timeout = 15/4299, cmd = AT+CGACT?
Sep  2 12:30:40 (none) user.info syslog: [MDD-AT_CMD] src/at_handler.c:819: at_cmd_handler - channel = 1, timeout = 15/4299, ret = 0, final_code = 0,
response = +CGACT: 1, 1 +CGACT: 2, 0 +CGACT: 3, 0 +CGACT: 4, 0 +CGACT: 5, 0 +CGACT: 6, 0 OK
Sep  2 12:30:40 (none) user.info syslog: [MDD-DBG] src/response_sender.c:102: response_send, target = 16, response id = 201, data len = 472
Sep  2 12:30:40 (none) user.info syslog: [MDD-AT_CMD] src/at_handler.c:816: at_cmd_handler - channel = 1, timeout = 15/4299, cmd = AT+CGACT?
Sep  2 12:30:40 (none) user.info syslog: [IAL][SYS] mifi.c:81: 2/3G, V4, if_name = ccmni0, type = 1, uid = 65537, pid = 0
Sep  2 12:30:40 (none) user.info syslog: [MDD-AT_CMD] src/at_handler.c:819: at_cmd_handler - channel = 1, timeout = 15/4299, ret = 0, final_code = 0,
response = +CGACT: 1, 1 +CGACT: 2, 0 +CGACT: 3, 0 +CGACT: 4, 0 +CGACT: 5, 0 +CGACT: 6, 0 OK
Sep  2 12:30:41 (none) kern.warn kernel: [ 4299.080350] get os type=2
Sep  2 12:30:41 (none) user.info syslog: [MDD-DBG] src/request_receiver.c:98: token = 671483137, id = 101, target = 10, data len = 0
Sep  2 12:30:41 (none) user.info syslog: [MDD-AT_CMD] src/at_handler.c:816: at_cmd_handler - channel = 1, timeout = 10/4300, cmd = AT+CREG?
Sep  2 12:30:41 (none) user.info syslog: [MDD-AT_CMD] src/at_handler.c:819: at_cmd_handler - channel = 1, timeout = 10/4300, ret = 0, final_code = 0,
response =  +CREG: 2,1,"015E","0000A5FB",3  OK
Sep  2 12:30:41 (none) user.info syslog: [MDD-DBG] src/md_handler.c:411: creg_stat = 1,roaming = 0
Sep  2 12:30:41 (none) user.info syslog: [MDD-AT_CMD] src/at_handler.c:816: at_cmd_handler - channel = 1, timeout = 15/4300, cmd = AT+CGACT?
Sep  2 12:30:41 (none) user.info syslog: [MDD-AT_CMD] src/at_handler.c:819: at_cmd_handler - channel = 1, timeout = 15/4300, ret = 0, final_code = 0,
response = +CGACT: 1, 1 +CGACT: 2, 0 +CGACT: 3, 0 +CGACT: 4, 0 +CGACT: 5, 0 +CGACT: 6, 0 OK
Sep  2 12:30:41 (none) user.info syslog: [MDD-DBG] src/response_sender.c:102: response_send, target = 16, response id = 201, data len = 472
```

Refresh: Click to update the log display.

Clear Log: Click to clear all log entries.

Display Log Level: Select the level of log event which you wish to view from the drop-down menu.

8) Reboot



Do you want to reboot the device now ?

Press “**OK**” to reboot the device

4. Appendix

- **Hardware Specifications**
  - 1 X USB interface
  - Antenna 1x1 2.4GHz internal embedded antenna
  - LED: 2G/3G status and Wi-Fi status
  - Micro SD card slot, up to 32 GB
  - SIM card slot

- **Weight**
  - Net: 24 gms
  - Gross: 87 gms

5. Glossary

- 3G — Third Generation. 3G refers to the third generation of mobile telephony technology.

- 4G LTE — Fourth Generation. 4G LTE refers to the fourth generation of mobile Telephony technology.

- 802.11 (b, g, n) — A set of WLAN communication standards in the 2.4 frequency Bands.

- bps — Bits per second. The rate of data flow.

- Broadband — High-capacity high-speed transmission channel with a wider bandwidth than conventional modem lines. Broadband channels can carry video, voice and data simultaneously.

- CDMA — Code Division Multiple Access. It is the underlying channel access method used by some mobile phone standards.

- DHCP — Dynamic Host Configuration Protocol. Software found in servers and routers that automatically assigns temporary IP addresses to clients logging into an IP network.

- DHCP Server — A server or service with a server that assigns IP addresses.

- DNS — Domain Name System. A system for converting host names and domain names into IP addresses on the Internet or on local networks that use the TCP/IP Protocol.

- Firmware — A computer program embedded in an electronic device. Firmware usually contains operating code for the device.

- Hotspot — A Wi-Fi (802.11) access point or the area covered by an access point. Used for connecting to the Internet.

- HTTP — Hypertext Transfer Protocol. An application-level protocol for accessing the World Wide Web over the Internet.

- IEEE — Institute of Electrical and Electronics Engineers.

- IMEI — International Mobile Equipment Identity. Used in LTE networks to identify the device. It is usually printed on the device and can often be retrieved using a USSD code.

- IP — Internet Protocol. The mechanism by which packets are routed between computers on a network.

- IP Type — The type of service provided over a network.

- IP address — Internet Protocol address. The address of a device attached to an IP network (TCP/IP network).

- ISP — Internet Service Provider. Also referred to as the service carrier, an ISP provides Internet connection service.

- Kbps — Kilobits per second. The rate of data flow.

- LAN — Local Area Network. A type of network that lets a group of computers, all in close proximity (such as inside an office building), communicate with one another. It does not use common carrier circuits though it can have gateways or bridges to other public or private networks.

- LTE — Long Term Evolution. A wireless broadband technology designed to support roaming Internet access via cell phones and handheld devices. Because LTE offers significant improvements over older cellular communication standards, some refer to it as a 4G (fourth generation) technology along with WiMax.

- MAC Address — Media Access Control. A number that uniquely identifies each network hardware device. MAC addresses are 12-digit hexadecimal numbers. This is also known as the physical or hardware address.

- Mbps — Megabits per second.

- MSID — Mobile Station Identifier. A number for a mobile phone that identifies that phone to the network. These numbers are carrier specific.

- Network Operator — The vendor who provides you wireless access. Known by different names in different regions, some examples are: wireless provider, network provider and service provider.

- Network Technology — The technology on which a particular network provider's system is built; such as CDMA or EVDO.

- Port — A virtual data connection used by programs to exchange data. It is the endpoint in a logical connection. The port is specified by the port number.

- Port Forwarding — A process that allows remote devices to connect to a specific computer within a private LAN.

- Port Number — A 16-bit number used by the TCP and UDP protocols to direct traffic on a TCP/IP host. Certain port numbers are standard for common Applications.

- PRL — Preferred Roaming List. A list that your wireless phone or device uses to determine which networks to connect when you are roaming. (Network operator specific).

- Protocol — A standard that enables connection, communication and data transfer between computing endpoints.

- Proxy — A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it.

- Rev A — CDMA EV-DO Rev. A is a leading-edge wireless technology with higher data rates and higher system capacity. It is a fully backward compatible standard and remains interoperable with deployed EV-DO networks and devices around the world.

- Router — A device that directs traffic from one network to another.

- SIM — Subscriber Identification Module. Found in GSM network technology, the SIM is a card containing identification information for the subscriber and their account. The SIM card can be moved to different devices.
- SSID — Service Set Identifier. The name assigned to a Wi-Fi network.

- TCP/IP — Transmission Control Protocol/Internet Protocol. The set of Communication protocols used for the Internet and other similar networks.

- USB — Universal Serial Bus. A connection type for computing device peripherals such as a printer, mobile modem, etc. USB connectors may be used for data transfer or charging.

- USB Port Types — The USB ports on computers and hubs have a rectangular Type A socket, and peripheral devices have a cable with a Type A plug. Peripherals that do not have an attached cable have a square Type B socket on the device and a separate cable with a Type A and Type B plug. Ports and connectors are available in different sizes (for example, standard, mini and micro).

- VPN — Virtual Private Network. A secure private network that runs over the public Internet. Commonly used to connect to an office network from elsewhere.

- WWAN — Wireless Wide Area Network. A public network that extends beyond architectural, geographical, or political boundaries (unlike a LAN, which is usually a private network located within a room, building, or other limited area).

- WEP — Wired Equivalent Privacy. An IEEE standard security protocol for 802.11 networks. Superseded by WPA and WPA2.

- Wi-Fi — Wireless Fidelity. Any system that uses the 802.11 standard developed and released in 1997 by the IEEE.

- Wi-Fi Client — A wireless device that connects to the Internet via Wi-Fi.

- WPA/WPA2 — Wi-Fi Protected Access. A security protocol for wireless 802.11 networks from the Wi-Fi Alliance