

Overview

The NetComm 3G25W-R integrates a Wireless LAN and 3G WAN into one unit. Connection to the Internet is achieved through either a 3G service or via a fixed line xDSL/Cable/Satellite connection to the 3G25W-R's WAN port, providing you with the flexibility to choose how you access the Internet. The 3G25W-R's automatic failover ensures you are always connected by activating the 3G connection should the xDSL/Cable/Satellite connection drop out.

Users are able to share a single 3G connection via both a wired and wireless connection to the 3G25W-R. With a built in 802.11n wireless access point, this router provides wireless speeds of up to 150Mbps, 150% faster than 11g technology¹. On top of this, the 3G25W-R has four LAN ports for wired connections to multiple devices. Rather than being restricted to certain USB modems, the 3G25W-R allows the user to simply insert an active SIM and utilise 3G Mobile Broadband for internet connectivity.

The 3G25W-R includes advanced security features such as VPN pass-through, a full complement of wireless security options and a built in firewall.

1 Maximum wireless signal rate and coverage values are derived from IEEE Standard 802.11g and 802.11n Draft 2.0 specifications. Actual wireless speed and coverage are dependent on network and environmental conditions included but not limited to volume of network traffic, building materials and construction/layout.

3G25W-R Features:

- Powerful wireless router with support for 3G Mobile Broadband
- Creates instant Wireless hotspots to share the Internet connection of a 3G USB modem or DSL/Cable modem
- Supports Wireless N standard with data speeds up to 150Mbps¹
- One WAN port for alternate wired Internet connection (DSL/Cable/Satellite via Ethernet)
- Four LAN ports to connect wired devices like PCs or gaming consoles
- Ensures connectivity and business continuity with auto Internet failover from WAN port to 3G Mobile Broadband
- Easy WiFi Protected Setup (WPS) by the single touch of a button to establish a secure wireless connection
- Full Wireless security - WEP, WPA, WPA2
- Browser based interface for configuration and management: OS independent and easy to use

Package Contents

Your 3G25W-R Wireless Router with voice Package contains the following items:

- 3G25W-R Wireless Router
- Quick Installation Guide
- User Guide on CD
- Power Supply Unit
- Ethernet Cable

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

Minimum System Requirements

Before continuing with the installation of your 3G25W-R Wireless Router, please confirm that you comply with the minimum system requirements.

- Active SIM card for 3G Broadband access if you want to use a 3G Broadband service.

Note: Subject to terms and conditions from your 3G Broadband Internet Service.

- Computer with Windows, Macintosh, or Linux-based operating systems with a working Ethernet adapter with TCP/IP Protocol installed.
- Internet Explorer version 6.0 or Netscape Navigator version 7.0 and above.

Wireless Computer System Requirements

- Computer with a working 802.11b, 802.11g, 802.11n wireless adapter

LED indicators:

(PICTURES)

	LED color	Description
Status	Green in flash	Device status is working.
3G Signal Strength LED	Red in flash	Disconnected. No SIM card / signal or unverified PIN code
	Amber in flash	Connecting.
	Red	Connected. Signal strength in level one (weak)
	Red in quick flash	Roaming alert, and 3G signal is weak
	Amber	Connected. Signal strength in level two or

		three (middle)
	Amber in quick flash	Roaming alert, and 3G signal is middle
	Green	Connected. Signal strength in level four or five (strong)
	Green in quick flash	Roaming alert, and 3G signal is strong
2G/2.5G LED	Green	EDGE or GPRS connection is established
	Green in flash	Data packet transferred via 2G/2.5G
3G/3.5G LED	Green	UMTS/HSDPA/HSUPA connection is established
	Green in flash	Data packet transferred via 3G/3.5G
USB / 3G LED	Green	Connected with 3G dongle via USB port
WAN LED	Green	RJ45 cable is plugged
	Green in flash	Data access
LAN LED	Green	RJ45 cable is plugged
	Green in flash	Data access
WiFi LED	Green	WLAN is on
	Green in flash	Device is in WPS PBC mode
	Green in fast flash	Device is in WPS PBC mode

Restoring Factory Defaults

This feature will reset the Router to its factory default configuration. Occasions may present themselves where you need to restore the factory default settings on your router. Typical situations are:

- You have lost your password and unable to login to the router;

- You have purchased the router from someone else and need to reconfigure the device.
- You are asked to perform a factory reset by a member of the excellent NetComm Support Staff.
- In order to restore your router to its factory default settings, please follow these steps:
- Ensure that the router is powered on (for at least 20 seconds).
- Use a paper clip or a pencil tip to depress the reset button for ten seconds and release. At this point, the reset is in progress. Do not power off the unit at this point.
- After the router reboots, the default settings are now restored. This entire process takes several minutes to complete.
- Once you have reset the router to its default settings you will be able to access the device's web configuration using <http://192.168.1.1> with password "admin".

Default Settings

LAN (Management)

Static IP Address: 192.168.1.x

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

WAN (Internet)

WAN mode: DHCP

Wireless

SSID: (refer to the wireless security card insert)

Security: WPA2-PSK

WEP Key: (refer to the wireless security card insert)

Modem Access

Password: admin

Connecting your 3G25W-R Wireless Router

Step 1: Attach the antenna.

1. Remove the antenna from its plastic wrapper.
2. Screw the antenna in a clockwise direction to the back panel of the unit.
3. Once secured, position the antenna upward at its connecting joint. This will ensure optimal reception.
4. And pull out the “USIM/SIM & PWR” labelled tag.
5. Ensure the Power Switch is off.

DO NOT connect the 3G25W-R to power before performing the installation steps below.

Step 2: Insert a SIM/USIM into the 3G25W-R.

Step 3: Insert the Ethernet cable into the LAN Port:

Insert the Ethernet cable into LAN port on the back panel of the 3G25W-R, and an available Ethernet port on the network adapter on the computer you will use to configure the 3G25W-R.

Step 4: Power on the 3G25W-R:

1. Connect the power adapter to the receptor on the back panel of your 3G25W-R.
2. Then plug the other end of the power adapter into a wall outlet or power strip.
3. Turn on the Power Switch.

Step 5: Complete the setup.

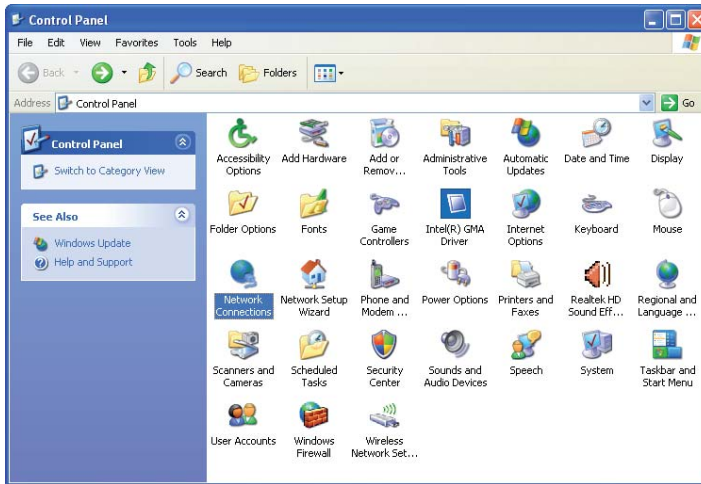
1. All LEDs will flash to indicate power has been applied.
2. The LEDs will flash ON and OFF as the 3G25W-R performs its startup initialisation and Internet connection processes. This will take a few minutes.
3. When complete, the Status LED will flash.

Setting up your PC

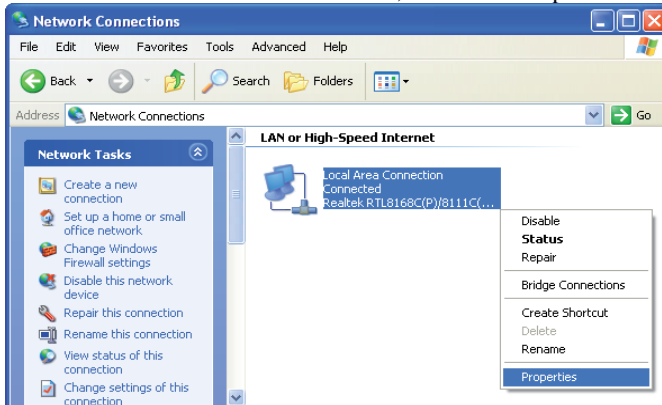
Having physically connected your 3G25W-R, the next step is to configure the router to establish a broadband connection. Depending on your computers current settings you may first need to reconfigure the TCP/IP (Network Settings) to access your Wireless Router. Follow the instructions for your operating system.

For Windows 98SE/ME/2000/XP

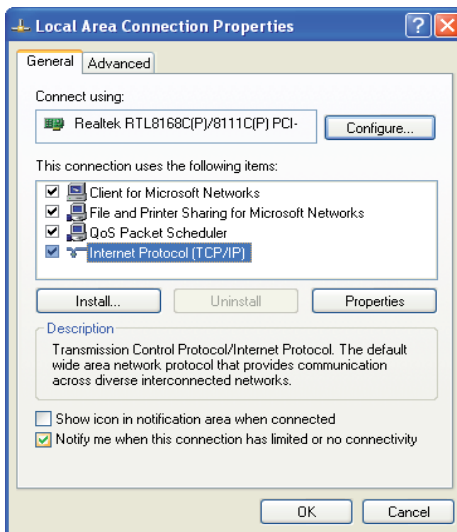
1. Click on “Start” -> “Control Panel” (in Classic View). In the Control Panel; double click on “Network Connections” to continue.



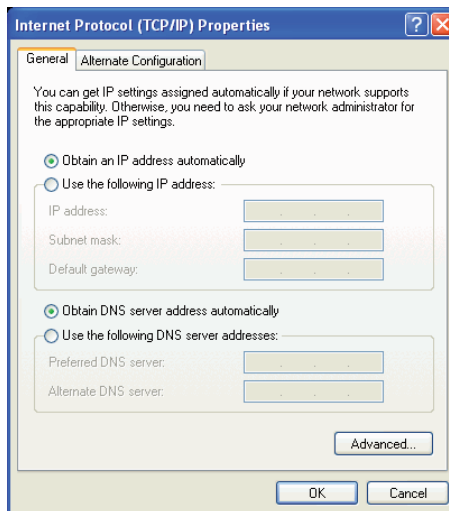
2. Single RIGHT click on “Local Area connection”, then click “Properties”.



3. Double click on “Internet Protocol (TCP/IP)”.



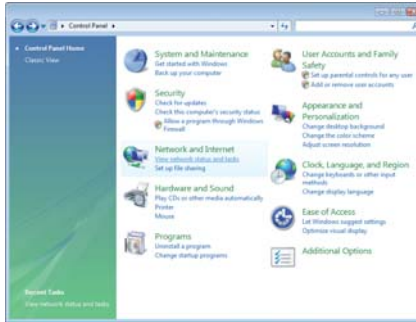
4. Check “Obtain an IP address automatically” and “Obtain DNS server address automatically” then click on “OK” to continue



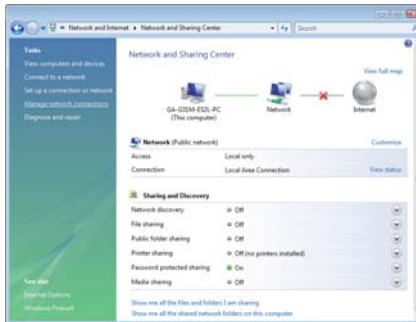
5. Click “Show icon in notification area when connected” (see screen image in 3. above) then click on “OK” to complete the setup procedures.

For Windows Vista-32/64

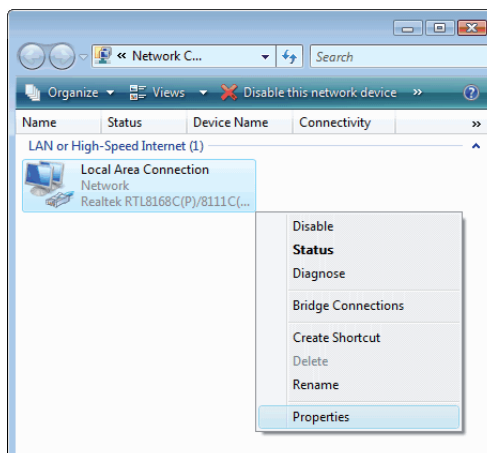
1. Click on “Start” -> “Control Panel” -> “Network and Sharing Center”.



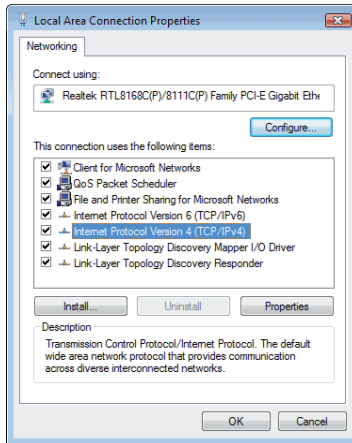
2. In the Manage network connections, click on “Manage network connections” to continue.



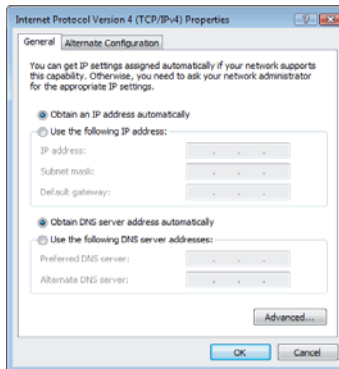
3. Single RIGHT click on “Local Area connection”, then click “Properties”.



4. The screen will display the information “User Account Control” and click “Continue” to continue.
5. Double click on “Internet Protocol Version 4 (TCP/IPv4)”.



6. Check “Obtain an IP address automatically” and “Obtain DNS server address automatically” then click on “OK” to continue.

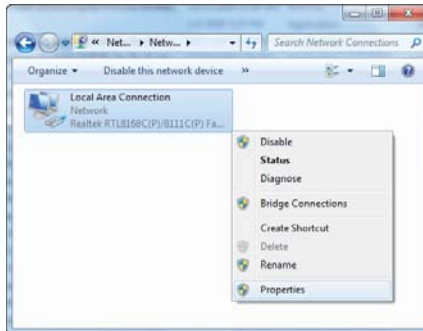


For Windows 7-32/64

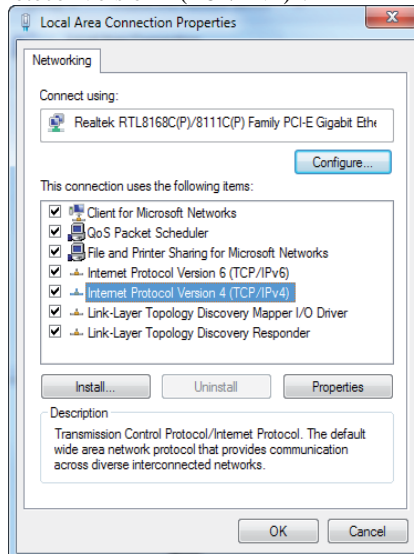
1. Click on “Start” -> “Control Panel” (in Category View) -> “View network status and tasks”.



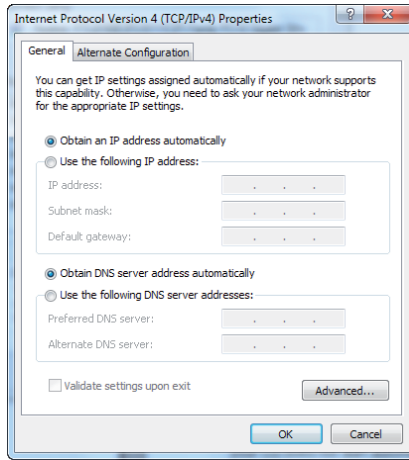
2. In the Control Panel Home, click on “Change adapter settings” to continue.
3. Single RIGHT click on “Local Area Connection”, then click “Properties”.



4. Double click on “Internet Protocol Version 4 (TCP/IPv4)”.

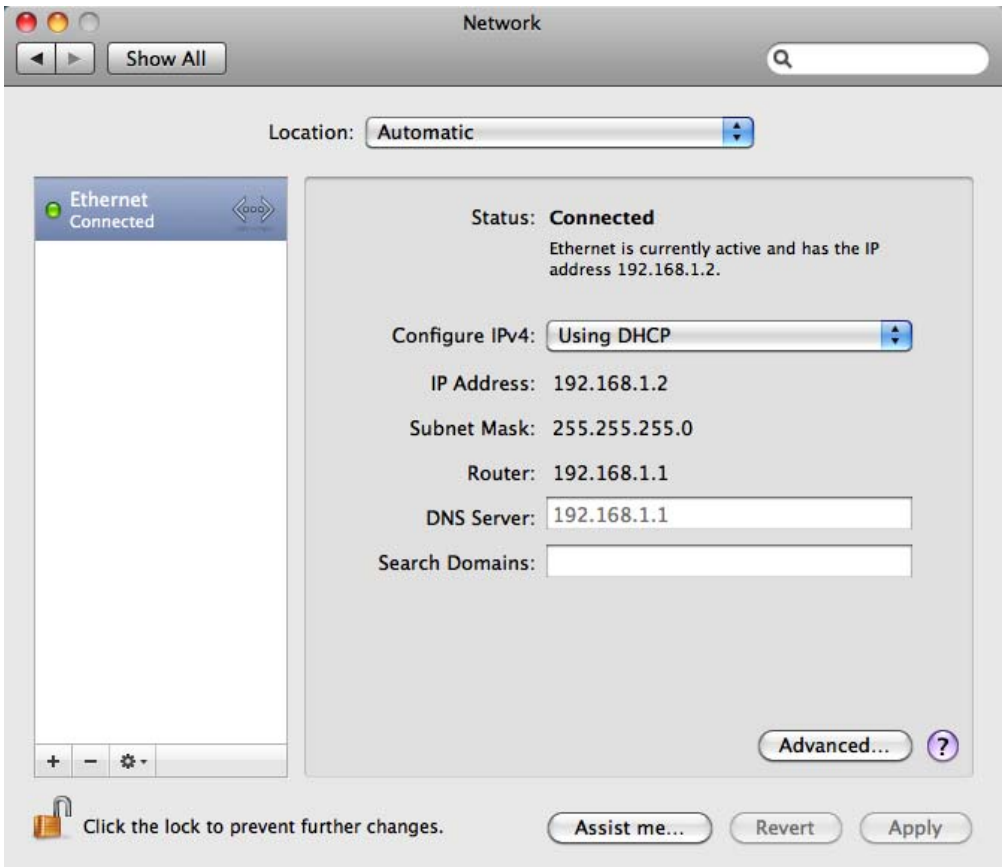


5. Check “Obtain an IP address automatically” and “Obtain DNS server address automatically” then click on “OK” to continue.



For Mac OS X 10.6

1. Click the Apple icon and choose System Preferences.
2. Click on Network icon.
3. Set Location to Automatic and Show to Built-In Ethernet.
4. In the Configure option, choose Using DHCP.
5. Click on Apply Now.



Web Configuration Wizard

Having physically connected your 3G25W-R, the next step is to establish the broadband connection to the internet. Please follow the steps below to configure your 3G25W-R Wireless router via the web configuration wizard utility.

1. Open your web browser (e.g. Internet Explorer/Firefox/Safari) and navigate to <http://192.168.1.1/>



2. At the login screen, type in "admin" (without quotes) in the System Password field. Then click on Login.



Notes: admin is the default login password for the unit.

3. Click on Wizard and then on Enter.



4. This page shows you the steps needed to configure your 3G25W-R unit. Click Next to continue.



5. After choosing 3G, you need to enter the information below, this will have been provided to you by your 3G broadband service provider. Click Apply Setting once you finished.

6. After several minutes the 3G25W-R will save all the settings and the wizard is complete. Click Finish to go back to the Status page and the unit will now use the new settings.



7. If everything is configured properly, the System Status page will show that your 3G service is online and the WAN IP address that has been assigned.

ADMINISTRATOR'S MAIN MENU **Status** **Wizard** **Advanced** **Logout**

System Status [HELP]

Item	Status	Sidenote
IP Address	122.149.127.138	
Subnet Mask	255.255.255.255	
Gateway	10.64.64.64	
Domain Name Server	202.136.43.197, 202.136.42.229	
Connection Time	00:03:26	

Wireless Modem Information

Item	Status	Sidenote
Card Info	HSPA Data Card	
Link Status	Connected	
Signal Strength	54%	
Network Name	YES OPTUS	

Wireless Status

Item	WLAN Status	Sidenote
Wireless mode	Enable	(B/G/N Mixed)
SSID	3G32WV	
Channel	11	
Security	WPA2-PSK	(AES)

Statistics Information

Statistics of WAN	Inbound	Outbound
Oclcts	760	3597
Unicast packets	20	60
Multicast packets	0	0

View Log... Clients List... NAT Status... Refresh

Device Time: Thu, 08 Jul 2010 00:43:47 +0000

Advanced Setup

To access the Advanced Setup option of your 3G25W-R, you need to access the 3G25W-R's web configuration outlined in the Web configuration section and click on the Advanced Setup menu at the top of the page.

The screenshot displays the web configuration interface for the 3G25W-R. At the top, there is a navigation bar with the following items: ADMINISTRATOR's MAIN MENU, Status, Wizard, and Advanced. Below the navigation bar, there are two expandable sections:

- System Status** (with a [HELP] link):

Item	Status	Sidenote
IP Address	122.149.127.138	
Subnet Mask	255.255.255.255	
Gateway	10.64.64.64	
Domain Name Server	202.136.43.197 , 202.136.42.229	
Connection Time	00:07:15	
- Wireless Modem Information** (with a [HELP] link):

Item	Status	Sidenote
Card Info	HSPA Data Card	
Link Status	Connected.	
Signal Strength	54%	
Network Name	YES OPTUS	

For first time installation, you will be presented with the following page. Choose Advanced to access the Advanced Setup page.

The screenshot displays the web configuration interface for the 3G25W-R. At the top, there is a navigation bar with the following items: ADMINISTRATOR's MAIN MENU, Status, Wizard, and Advanced. Below the navigation bar, there is one expandable section:

- System Status** (with a [HELP] link):

Item	Status	Sidenote
IP Address	122.149.127.138	
Subnet Mask	255.255.255.255	

After that, click on any of the top menu to access the respective setting pages.



BASIC SETTING



FORWARDING RULES



SECURITY SETTING



ADVANCED SETTING



TOOLBOX

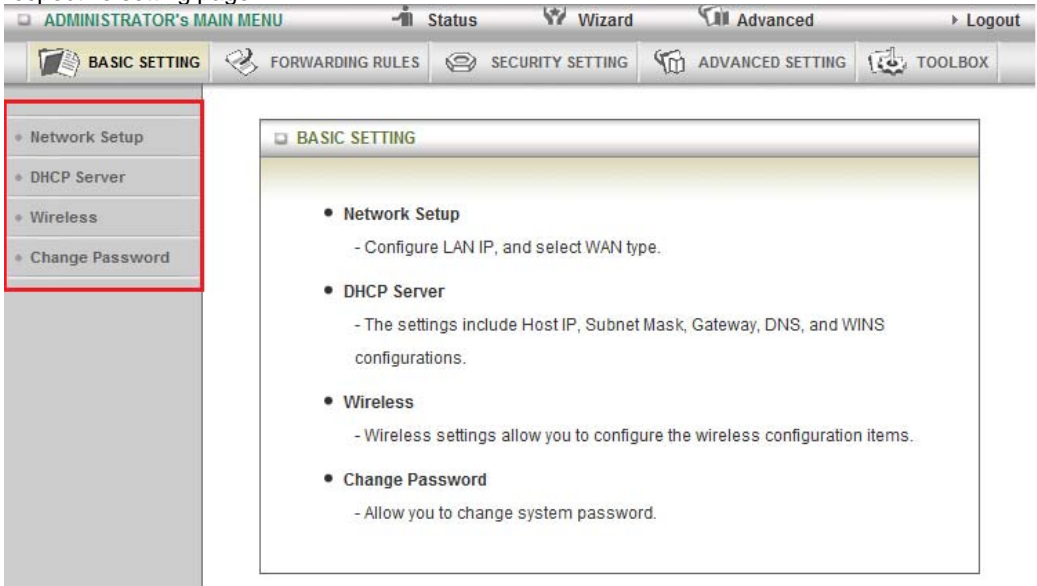
• Network Setup

• DHCP Server

▣ BASIC SETTING

Basic Setting

The Basic Setting page allows you to configure a number of basic settings on the unit. This section deals with these features. Click on any of the menu on the left to configure the respective setting page.



ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Network Setup
- DHCP Server
- Wireless
- Change Password

BASIC SETTING

- **Network Setup**
 - Configure LAN IP, and select WAN type.
- **DHCP Server**
 - The settings include Host IP, Subnet Mask, Gateway, DNS, and WINS configurations.
- **Wireless**
 - Wireless settings allow you to configure the wireless configuration items.
- **Change Password**
 - Allow you to change system password.

Basic Setting > Network Setup

This Page allows you to change the LAN (Local Area Network) settings on your 3G25W-R Wireless router and the WAN (Wide Area Network) connection.

1. **LAN IP Address:** the local IP address of the 3G25W-R. The computers on your network must use this IP address as their Default Gateway. You can change it if necessary.
2. **Subnet Mask:** Enter 255.255.255.0 in the subnet field.
3. **WAN Interface:** Select Ethernet WAN or Wireless WAN.
4. **WAN Type:** WAN connection type. Click the WAN Type pulldown menu to choose the appropriate connection type from the following options:

LAN Setup	
Item	Setting
▶ LAN IP Address	192.168.123.254
▶ Subnet Mask	255.255.255.0
Internet Setup [HELP]	
▶ WAN Interface	Ethernet WAN ▼
▶ WAN Type	Static IP Address ▼
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ WAN IP Address	<input type="text"/>
▶ WAN Subnet Mask	<input type="text"/>
▶ WAN Gateway	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ NAT disable	<input type="checkbox"/> Enable
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

- Static IP Address

- Enter the WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS as supplied by your ISP.

LAN Setup	
Item	Setting
▶ LAN IP Address	192.168.123.254
▶ Subnet Mask	255.255.255.0
Internet Setup [HELP]	
▶ WAN Interface	Ethernet WAN ▼
▶ WAN Type	Dynamic IP Address ▼
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ Host Name	<input type="text"/> (optional)
▶ ISP registered MAC Address	<input type="text"/> <input type="button" value="Clone"/>
▶ Connection Control	Connect-on-Demand ▼
▶ NAT disable	<input type="checkbox"/> Enable
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

- Dynamic IP Address

- **Activate WWAN for Auto-Failover:** The WAN type will be change to wireless-WAN automatically if the wired-WAN connection disconnects.
- **Host Name:** Set the hostname for your connection (optional - Refer to your ISP for more information).
- **ISP register MAC address:** You can change the WAN port MAC address if needed to clone your 3G modem (optional - Refer to your ISP for more information).
- **Connection Control:** There are 3 modes to select :-

Connect-on-demand: The 3G25W-R will connect to the internet when a client sends outgoing packets.

Auto Reconnect (Always-on): The 3G25W-R will automatically reconnect to the internet until the connection is manually disconnected.

Manually: The 3G25W-R will not connect to the internet until someone clicks the connect button in the Status-page.

- **NAT disable:** This option disables "Network Address Translation" for this connection type.

Internet Setup [HELP]	
▶ WAN Interface	Ethernet WAN ▼
▶ WAN Type	PPP over Ethernet ▼
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ PPPoE Account	<input type="text"/>
▶ PPPoE Password	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ Connection Control	Connect-on-Demand ▼
▶ Maximum Idle Time	600 seconds
▶ PPPoE Service Name	<input type="text"/> (optional)
▶ Assigned IP Address	<input type="text"/> (optional)
▶ MTU	0 (0 is auto)
▶ NAT disable	<input type="checkbox"/> Enable
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

- PPP over Ethernet

- **Activate WWAN for Auto-Failover:** The WAN type will be change to wireless-WAN automatically if the wired-WAN connection disconnects.
- **PPPoE Account and Password:** The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty.
- **Primary DNS/Secondary DNS:** This feature allows you to manually assign a Primary/Secondary DNS Server (Refer to your ISP for more information).
- **Connection Control:** There are 3 modes to select :-

Connect-on-demand: The 3G25W-R will connect to the internet when a client sends outgoing packets.

Auto Reconnect (Always-on): The 3G25W-R will automatically reconnect to the internet until the connection is manually disconnected.

Manually: The 3G25W-R will not connect to the internet until someone clicks the connect button in the Status-page.

- **Maximum Idle Time:** The amount of inactivity on the internet connection before it is disconnected. Set it to zero or enable "Auto-reconnect " to disable this feature.
- **PPPoE Service Name:** Enter the service name if your ISP requires it (optional).

- Assigned IP address: Enter the IP address assigned to your service. This is usually left blank.
- Maximum Transmission Unit (MTU): The default MTU value is 0(auto). It is set automatically when you connect.
- NAT disable: This option disables "Network Address Translation" for this connection type.

Internet Setup [HELP]	
▶ WAN Interface	Ethernet WAN ▾
▶ WAN Type	PPTP ▾
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ IP Mode	Dynamic IP Address ▾
▶ My IP Address	<input type="text"/>
▶ My Subnet Mask	<input type="text"/>
▶ Gateway IP	<input type="text"/>
▶ Server IP Address/Name	<input type="text"/>
▶ PPTP Account	<input type="text"/>
▶ PPTP Password	<input type="text"/>
▶ Connection ID	<input type="text"/> (optional)
▶ Maximum Idle Time	600 seconds
▶ Connection Control	Connect-on-Demand ▾
▶ MTU	0 (0 is auto)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

- PPTP

Please verify your connection type and select the appropriate IP Mode - Static IP Address or Dynamic IP Address.

If you are using a Static address enter the information provided to you by your service provider.

- Activate WWAN for Auto-Failover: The WAN type will be change to wireless-WAN automatically if the wired-WAN connection disconnects.
- My IP Address, My Subnet Mask and WAN Gateway IP: the private IP address, subnet mask and Gateway IP your service provider assigned to you.
- Server IP Address/Name: the IP address or URL of the PPTP server.
- PPTP Account and Password: The account and password your PPTP provider assigned to you. If you don't want to change the password, keep it empty.

- Connection ID: Enter your connection ID if required.
- Maximum Idle Time: The amount of inactivity on the internet connection before it is disconnected. Set it to zero or enable “Auto-reconnect” to disable this feature.
- Connection Control: There are 3 modes to select :-

Connect-on-demand: The 3G25W-R will connect to the internet when a client sends outgoing packets.

Auto Reconnect (Always-on): The 3G25W-R will automatically reconnect to the internet until the connection is manually disconnected.

Manually: The 3G25W-R will not connect to the internet until someone clicks the connect button in the Status-page.

- Maximum Transmission Unit (MTU): The default MTU value is 0(auto). It is set automatically when you connect.

Internet Setup [HELP]	
▶ WAN Interface	Ethernet WAN ▼
▶ WAN Type	L2TP ▼
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ IP Mode	Dynamic IP Address ▼
▶ IP Address	<input type="text"/>
▶ Subnet Mask	<input type="text"/>
▶ WAN Gateway IP	<input type="text"/>
▶ Server IP Address/Name	<input type="text"/>
▶ L2TP Account	<input type="text"/>
▶ L2TP Password	<input type="text"/>
▶ Maximum Idle Time	600 seconds
▶ Connection Control	Connect-on-Demand ▼
▶ MTU	0 (0 is auto)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

- L2TP

Please verify your connection type and select the appropriate IP Mode - Static IP Address or Dynamic IP Address.

If you are using a Static address enter the information provided to your by your service provider.

- **Activate WWAN for Auto-Failover:** The WAN type will be change to wireless-WAN automatically if the wired-WAN connection disconnects.
- **IP Address, Subnet Mask and WAN Gateway IP:** the private IP address, subnet mask and Gateway IP your service provider assigned to you.
- **Server IP Address/Name:** The IP address or URL of the L2TP server.
- **L2TP Account and Password:** The account and password your L2TP provider assigned to you. If you don't want to change the password, keep it empty.
- **Maximum Idle Time:** The amount of inactivity on the internet connection before it is disconnected. Set it to zero or enable "Auto-reconnect" to disable this feature.
- **Connection Control:** There are 3 modes to select :-

Connect-on-demand: The 3G25W-R will connect to the internet when a client sends outgoing packets.

Auto Reconnect (Always-on): The 3G25W-R will automatically reconnect to the internet until the connection is manually disconnected.

Manually: The 3G25W-R will not connect to the internet until someone clicks the connect button in the Status-page.

- **Maximum Transmission Unit (MTU):** The default MTU value is 0(auto). It is set automatically when you connect.

Internet Setup		[HELP]
▶ WAN Interface	Ethernet WAN ▾	
▶ WAN Type	L2TP ▾	
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>	
▶ IP Mode	Dynamic IP Address ▾	
▶ IP Address	<input type="text"/>	
▶ Subnet Mask	<input type="text"/>	
▶ WAN Gateway IP	<input type="text"/>	
▶ Server IP Address/Name	<input type="text"/>	
▶ L2TP Account	<input type="text"/>	
▶ L2TP Password	<input type="text"/>	
▶ Maximum Idle Time	600 seconds	
▶ Connection Control	Connect-on-Demand ▾	
▶ MTU	0 (0 is auto)	
<input type="button" value="Save"/> <input type="button" value="Undo"/>		

- 3G

Please note: The WAN fields may not be necessary for your 3G connection. The information on this page will only be used when required by your 3G service provider.

Please contact your 3G provider to obtain this information if needed.

- Dial-Up Profile: Select auto or manual to continue.
- Country: select your country.
- Telecom: select your 3G provider.
- 3G Network: select the 3G Network type.
- APN: Enter the APN for your 3G service.
- Pin Code: Enter the Pin Code for your SIM card.
- Dial-Number: This number required to connect to your 3G service.
- Account: The username provided by your 3G service provider to enable access to your 3G service.
- Password: The password provided by your 3G service provider to enable access to your 3G service.

- Authentication: Choose the appropriate authentication type for your 3G service.
- Primary DNS: Manually assign a Primary DNS Server.
- Secondary DNS: Manually assign a Secondary DNS Server.
- Connection Control: There are 3 modes to select :-

Connect-on-demand: The 3G25W-R will connect to the internet when a client sends outgoing packets.

Auto Reconnect (Always-on): The 3G25W-R will automatically reconnect to the internet until the connection is manually disconnected.

Manually: The 3G25W-R will not connect to the internet until someone clicks the connect button in the Status-page.

- Keep Alive: Enables the 3G25W-R to maintain your internet connection.

Basic Setting > DHCP Server

DHCP Server [HELP]	
Item	Setting
▶ DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
▶ IP Pool Starting Address	<input type="text" value="100"/>
▶ IP Pool Ending Address	<input type="text" value="200"/>
▶ Lease Time	<input type="text" value="86400"/> Seconds
▶ Domain Name	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="More..."/> <input type="button" value="Clients List..."/> <input type="button" value="Fixed Mapping..."/>	

1. DHCP Server: Enable or disable the DHCP server.
2. Lease Time: Length of the DHCP lease time
3. IP Pool Starting/Ending Address: Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool
4. Domain Name: Optional, this information will be passed to the client

Click "Save" to save these settings or Undo to cancel.

You can also check the DHCP client list by pressing the Client List button.

Fixed Mapping button allows you to map a specific IP address to a specific MAC address.

Press "More..." for more options,

DHCP Clients List

The list of DHCP clients is shown here.

DHCP Clients List					
IP Address	Host Name	MAC Address	Type	Lease Time	Select
<input type="button" value="Delete"/> <input type="button" value="Back"/> <input type="button" value="Refresh"/> <input type="button" value="Fixed Mapping"/>					

DHCP Fixed Mapping

The DHCP Server will reserve a specific IP for a specific MAC address, shown below.

Fixed Mapping				[HELP]				
DHCP clients				-- select one --	<input type="button" value="Copy to"/>	ID	--	<input type="button" value="v"/>
ID	MAC Address	IP Address	Enable					
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>					
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>					
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>					
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>					
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>					
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>					
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>					
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>					
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>					
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>					
				<input type="button" value=" << Previous"/>	<input type="button" value=" Next >>"/>	<input type="button" value=" Save"/>	<input type="button" value=" Undo"/>	<input type="button" value=" Back"/>

Basic Setting > Wireless

This page allows you to configure the wireless network features of the router.

Wireless Setting [HELP]	
Item	Setting
Wireless Module	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID(SSID)	<input type="text" value="3G32WV"/>
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	<input type="text" value="11"/>
Wireless Mode	<input type="text" value="B/G/N mixed"/>
Authentication	<input type="text" value="WPA2-PSK"/>
Encryption	<input type="text" value="AES"/>
Preshare Key	<input type="text" value="a1b2c3d4e5"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting..."/> <input type="button" value="WPS Setup..."/> <input type="button" value="Wireless Client List..."/>	

The Wireless settings page allows you to set the wireless configuration items.

1. Network ID (SSID): Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. (The factory default setting is "3G25W-R")
2. SSID Broadcast: The router will broadcast the SSID so that wireless clients can find the wireless network.
3. Channel: The wireless radio channel in use by your network.
4. Wireless Mode: Choose B/G Mixed, B only, G only, and N only, G/N Mixed or B/G/N mixed. The factory default setting is B/G/N mixed.
5. Authentication mode: You may select from seven kinds of authentication to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK.

WPA-PSK/WPA2-PSK - A newer type of security is WPA-PSK-TKIP and WPA-PSK2-ADE. This type of security gives a more secure network compare to WEP. Use TKIP Encryption Type for WPA-PSK and AES for WPA2-PSK. Please enter the key in the Passphrase field. The key needs to be more then 8 characters and less then 63 characters and it can be any combination of letters and numbers.

The factory default setting is: a1b2c3d4e5

Please note that the configuration for WPA-PSK and WPA2-PSK is identical

Notes: After configuring wireless security, you also need to configure your wireless adapter to use the same security settings before you can connect wirelessly. Not all wireless adapter supports WPA-PSK/WPA2-PSK/WPA/WPA2 security, please refer to your wireless adapter user guide for more details. It is strongly recommended to set up wireless security such as WPA-PSK (when the wireless client supports WPA) in order to secure your network.

Click "Save" to save these settings or click "Undo" to cancel.

WDS(Wireless Distribution System)

WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.

Wireless Bridging [HELP]	
Item	Setting
▶ Wireless Bridging	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Remote AP MAC 1	<input type="text"/>
Remote AP MAC 2	<input type="text"/>
Remote AP MAC 3	<input type="text"/>
Remote AP MAC 4	<input type="text"/>
▶ Encryption type	TKIP ▼
▶ Encryption key	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/>	

WPS Setup

WPS is a Wi-Fi Protection Setup which is similar to WCN-NET and offers safe and easy way to connect Wirelessly.

Wi-Fi Protected Setup	
Item	Setting
▶ WPS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ AP PIN	00020329 <input type="button" value="Generate New PIN"/>
▶ Config Mode	Registrar ▼
▶ Config Status	CONFIGURED <input type="button" value="Release"/>
▶ Config Method	Push Button ▼
▶ WPS status	NOUSED
<input type="button" value="Save"/> <input type="button" value="Trigger"/> <input type="button" value="Cancel"/>	

Wireless Client List

The list of wireless clients is shown here.

Wireless Clients List	
ID	MAC Address
1	00-60-64-24-0B-D3
2	00-60-64-25-D8-0E
<input type="button" value="Back"/> <input type="button" value="Refresh"/>	

Basic Setting > Change Password

On this page you can change the 3G25W-R web configuration password. Please type in your old password (the factory default password is admin) and then type in the new password. Type the same new password in the Reconfirm field.

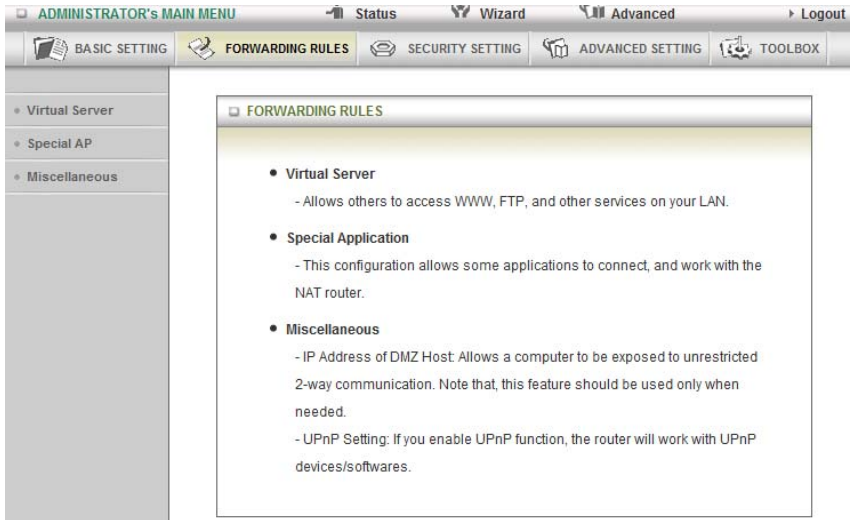
Change Password	
Item	Setting
Old Password	<input type="text"/>
New Password	<input type="text"/>
Reconfirm	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

Note: if you change the password, please make sure that you use the new password the next time you log into the web configuration.

Click "Save" to save the settings or "Undo" to cancel.

Forwarding Rules

The Forwarding Rules page allows you to configure the port forwarding management on the router. Click on any of the menu items on the left to access the respective settings page.



Forwarding rules are a necessary feature as by default NAT (Network Address Translation) will automatically block incoming traffic from the Internet to the LAN unless a specific port mapping exists in the NAT translation table. Because of this, NAT provides a level of protection for computers that are connected to your LAN. However, this also creates a connectivity problem when you want to make LAN resources available to Internet clients, which you may want to do to play network games or host network applications.

There are three ways to work around NAT and to enable certain LAN resources available from the Internet; Port Forwarding (in the Virtual Server page), Port Triggering (in the Special AP page) and DMZ Host (in the Miscellaneous page).

Forwarding Rules > Virtual Server

Virtual Server
[HELP]

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

Use schedule rule: --ALWAYS ON--

ID	Service Ports	Server IP	Enable	Schedule Rule#
1	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
9	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
10	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
11	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
12	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

A virtual server is defined as a Service Port, and all requests to this port will be redirected to the computer specified by the Server IP. Virtual Servers can also work with Scheduling Rules, and give you more flexibility on Access control. For detail instructions on scheduling rules, please refer to Advanced Setting > Scheduling.

For example, if you have an FTP server (default port is port 21) at 192.168.1.10, a Web server (default port is port 80) at 192.168.1.20, and a VPN server (default port is port 1723) at 192.168.1.60, then you need to specify the following virtual server mapping table:

Service.Port	Server.IP	Enable
21	192.168.1.10	Ticked
80	192.168.1.20	Ticked
1723	192.168.1.60	Ticked

Note: At any given time, only one IP address can bind to a particular Service Port.

Click "Save" to save the settings or "Undo" to cancel.

Forwarding Rules > Special AP

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Save Undo

Some applications like On-line games, Video conferencing and Internet telephony require multiple connections to the internet. Because of that, these applications cannot work with a pure NAT router such as the 3G25W-R. The Special Applications feature allows some of these applications to work with this router. If this fails to make the application work, try to set up that computer as the DMZ host instead. Please refer to Forwarding Rules > Miscellaneous section for assistance doing this.

The fields are explained as follows:

1. Trigger: the outbound port number that will be triggered by the application..
2. Incoming Ports: when the trigger packet is detected, the inbound packets sent to the specified port numbers will be allowed to pass through the firewall.

The 3G32VW also provides predefined settings for some popular applications. To use the predefined settings, select your application from the Popular application list, select an unused ID from the list and then click Copy to. After that the predefined settings will be added to the list.

Click "Save" to save the settings or "Undo" to cancel.

Forwarding Rules > Miscellaneous

Miscellaneous Items		[HELP]
Item	Setting	Enable
▶ IP Address of DMZ Host	<input type="text"/>	<input type="checkbox"/>
▶ UPnP setting		<input checked="" type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>		

DMZ (Demilitarized Zone) Host is a computer without the protection of firewall. It allows that particular computer to be exposed to unrestricted 2-way communication to the internet. It is mostly used for Internet games, Video conferencing, Internet telephony and other special applications.

To enable DMZ, enter the IP address of the PC and tick on Enable.

Note: This feature should be used only when necessary.

UPnP Setting, The device also supports this function. If the OS supports this function enable it.

Click "Save" to save the settings or "Undo" to cancel.

Security Setting

The Security Setting page allows you to configure the security management on the router such as Packet filters and MAC Control. Click on any of the menu items on the left to access the respective setting page.

The screenshot displays the Security Setting page in a router's web interface. The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this, a secondary menu shows 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING' (highlighted), 'ADVANCED SETTING', and 'TOOLBOX'. On the left, a vertical menu lists 'Status', 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Control', and 'Miscellaneous', with a red box highlighting the 'Status' item. The main content area contains three filter configuration sections, each with a table and a '[Modify]' link.

Outbound Filter [Modify]

Item	Status
Outbound Filter	Disable
Local Client	Only Allow Remote Host
Service	Working Time

Inbound Filter [Modify]

Item	Status
Inbound Filter	Disable
Remote Host	Deny Remote Host to access
Service	Working Time

Domain Filter [Modify]

Item	Status
Domain Filter	Disable
Domain	Access
All other Domains	Yes

[Refresh]

Security Setting > Packet Filters

The Packet Filter enables you to control what packets are allowed to pass through the router. There are two types of packet filter, Outbound Packet Filter which applies to all outbound packets and Inbound Packet Filter which only applies to packets that are destined for a Virtual Server or DMZ host only.

Outbound Packet Filter [HELP]				
Item		Setting		
▶ Outbound Packet Filter		<input type="checkbox"/> Enable		
<input checked="" type="radio"/> Allow all to pass except those match the following rules.				
<input type="radio"/> Deny all to pass except those match the following rules.				
ID	Source IP	Destination IP : Ports	Enable	Use rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Inbound Filter"/> <input type="button" value="MAC Level"/>				

To enable an Outbound Filter, please make sure to tick the Enable tick box on the top of the page. There are two type of filtering policies:

1. Allow all data traffic to pass except those that match the specified rules.
2. Deny all data traffic to pass except those that match the specified rules.

For each direction, you can specify up to 48 rules. For each rule you will need to define the following:

- Source IP address
- Source port
- Destination IP address
- Destination port
- Protocol: TCP or UDP or both.
- Use Schedule Rule#

For source or destination IP address, you can define a single IP address (192.168.1.1) or a range of IP addresses (192.168.1.100-192.168.1.200). Empty fields imply all IP addresses.

For source or destination port, you can also define a single port (80) or a range of ports (1000-1999). Use the prefix "T" or "U" to specify either the TCP or UDP protocol e.g. T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. An empty field implies all ports.

The Packet Filter also works with Scheduling Rules, and gives you more flexibility on Access control. For detailed instructions regarding scheduling rules, please refer to the Advanced Setting > Scheduling section.

Click "Save" to save the settings or "Undo" to cancel.

Inbound Filter:

To access the Inbound Packet Filter page, click on the "Inbound Filter" button on the bottom of the Outbound Filter page. All the settings on this page are similar to the one for the Outbound Filter.

Inbound Packet Filter		[HELP]		
Item		Setting		
▶ Inbound Packet Filter		<input type="checkbox"/> Enable		
<input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules.				
ID	Source IP	Destination IP : Ports	Enable	Use rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▼
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Outbound Filter"/> <input type="button" value="MAC Level"/>				

Click "Save" to save the settings or "Undo" to cancel.

Security Setting > Domain Filters

Domain Filters enable you to prevent users from accessing specific domain addresses.

Domain Filter		[HELP]	
Item	Setting		
Domain Filter	<input type="checkbox"/> Enable		
Log DNS Query	<input type="checkbox"/> Enable		
Privilege Host/NetMask	192.168.123.0	/	0
ID	Domain Suffix	Action	Enable
1	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
10	* (all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-
<input type="button" value="Save"/> <input type="button" value="Undo"/>			

To enable the Domain Filter please make sure to tick the Enable tick box on the top of the page.

Log DNS Query. Please tick the Enable tick box if you want to log when someone accesses specific URLs.

Privilege Host/Netmask. To set a group of computer that has privilege to access the internet without any restriction.

To set a Domain Filter, you need to specify the following:

- Domain Suffix: Please type the suffix of the URL that needs to be restricted. For example, ".com", "xxx.com".
- Action: The router action that you want when someone is accessing a URL that met the domain suffix. Tick on Drop to block the access and/or tick on Log to log this access.
- Enable. Tick to enable the rule.

Click "Save" to save the settings or "Undo" to cancel.

Security Setting > URL Blocking

URL Blocking will block LAN computers from connecting to a pre-defined website. The major difference between Domain Filter and URL Blocking is that Domain Filter require users to input a suffix (e.g. xxx.com, yyy.net) while URL Blocking only requires you to input a keyword.

Item		Setting
URL Blocking		<input type="checkbox"/> Enable
ID	URL	Enable
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>

To enable URL Blocking please make sure to tick on Enable tick box on the top of the page. To set a URL Blocking rule, you need to

specify the following:

- URL. If any part of the Website's URL matches the pre-defined word then the connection will be blocked. For example, you can use pre-defined word "sex" to block all websites if their URLs contain the pre- defined word "sex".
- Enable. Tick to enable the rule.

Click "Save" to save the settings or "Undo" to cancel.

Security Setting > MAC Control

MAC Control allows you to assign different access rights for different users and to assign a specific IP address to a specific MAC address.

MAC Address Control [HELP]					
Item	Setting				
MAC Address Control	<input type="checkbox"/> Enable				
<input type="checkbox"/> Connection control	Wireless and wired clients with C checked can connect to this device; and allow unspecified MAC addresses to connect.				
<input type="checkbox"/> Association control	Wireless clients with A checked can associate to the wireless LAN; and deny unspecified MAC addresses to associate.				
DHCP clients -- select one -- Copy to ID --					
ID	MAC Address	IP Address	Wake On Lan	C	A
1	<input type="text"/>	192.168.123. <input type="text"/>	<input type="button" value="Trigger"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.123. <input type="text"/>	<input type="button" value="Trigger"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.123. <input type="text"/>	<input type="button" value="Trigger"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.123. <input type="text"/>	<input type="button" value="Trigger"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Previous page"/> <input type="button" value="Next page"/> <input type="button" value="Save"/> <input type="button" value="Undo"/>					

To enable MAC Address Control please make sure to tick the Enable tick box on the top of the page. Two types of control are available:

- **Connection control.** Check Connection Control to control which clients (wired and wireless) can connect to the unit. If a client is denied to connect to this device, it means the client can not access to the Internet either. Choose allow or deny to allow or deny clients with MAC addresses that are not in the list to connect to this device.
- **Association control.** Check Association Control to control which wireless client can associate with the unit. If a client is denied to associate with the unit, it means the client can not send or receive any data via this device. Choose allow or deny to allow or deny the clients with MAC addresses that are not in the list to associate to the wireless LAN

Click the "Next Page" or the "Previous Page" buttons to see the entire list.

Click "Save" to save the settings or "Undo" to cancel.

Security Setting > Miscellaneous

This page allows you to change various miscellaneous security settings on the unit.

Miscellaneous Items		[HELP]
Item	Setting	Enable
▶ Administrator Time-out	300 seconds (0 to disable)	
▶ Remote Administrator Host : Port	<input type="text"/> / <input type="text"/> :	<input type="checkbox"/>
▶ Discard PING from WAN side		<input type="checkbox"/>
▶ DoS Attack Detection		<input type="checkbox"/>

Administrator Time-out

The period of time with no activity in the web configuration page to logout automatically, you may set it to zero to disable this feature.

Remote Administrator Host/Port

In general, only Intranet users can browse the built-in web pages to perform administration task. This feature enables you to perform administration tasks from a remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect to the router to perform administration tasks. You can use subnet mask bit (/nn) notation to specify a group of trusted IP addresses for example, "10.1.2.0/24".

NOTE: When Remote Administration is enabled, the web server port will be shifted to 80. You can also change the web server port.

Discard PING from WAN side

When this feature is enabled, your router will not respond to ping requests from remote hosts.

DoS Attack Detection

When this feature is enabled, the router will detect and log where the DoS attack comes from on the Internet. Currently, the router can detect the following DoS attack types: SYN Attack, WinNuke, Port Scan, Ping of Death and Land Attack, as well as others.

Click "Save" to save the settings or "Undo" to cancel.

Advanced Setting

The Advanced Setting page allows you to configure the advanced settings on the router such as the System log, Dynamic DNS and SNMP ports. Click on any of the menu items on the left to configure the access the respective setting page.

The screenshot shows a web interface for a router's configuration. At the top, there is a navigation bar with the following items: ADMINISTRATOR'S MAIN MENU, Status, Wizard, Advanced, and Logout. Below this is a secondary navigation bar with icons and labels for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING (which is highlighted), and TOOLBOX. On the left side, there is a vertical sidebar menu with the following items: Status, System Log, Dynamic DNS, QoS, System Time, and Scheduling. The main content area is titled 'ADVANCED SETTING' and contains a list of five items:

- **System Log**
 - Send system log to a dedicated host or email to specific receipts.
- **Dynamic DNS**
 - To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
- **QoS Rule**
 - Quality of Service can provide different priority to different users or data flows, or guarantee a certain level of performance.
- **System Time**
 - Allow you to set device time manually or consult network time from NTP server.
- **Schedule Rule**
 - Apply schedule rules to Packet Filters and Virtual Server.

Advanced Setting > System Log

This enables you to set up the system log features of the router. You can also choose to export the system log via email (SMTP) or send it to a remote syslog server (UDP).

System Log		[HELP]
Item	Setting	Enable
▶ IP address for syslogd	<input type="text"/>	<input type="checkbox"/>
▶ Setting of Email alert		<input type="checkbox"/>
● SMTP Server : port	<input type="text"/> : <input type="text"/>	
● SMTP Username	<input type="text"/>	
● SMTP Password	<input type="text"/>	
● E-mail addresses	<input type="text"/>	
● E-mail subject	<input type="text"/>	
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="View Log..."/> <input type="button" value="Email Log Now"/>		

IP Address for Syslogd

Host IP of destination where sys log will be sent to. Check Enable to enable this function.

Setting of Email alert

Check if you want to enable Email alert (send syslog via email). Check Enable to enable this function.

SMTP Server IP and Port

Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25. For example, "mail.your_url.com" or "192.168.1.100:26".

SMTP Username and password

Input a user account and password for the SMTP server.

E-mail address

The recipients who will receive these logs, you can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

E-mail Subject

The subject of email alert, this setting is optional.

View Log...

View the current system log.

Advanced Setting > Dynamic DNS

The Dynamic DNS feature enables users to have a static domain name for their internet connection even when their internet connection IP address is dynamic. By mapping the host name to the current public IP address of the router, users who want to connect to the router or any services behind the router from the internet can just use the Dynamic DNS hostname instead of the IP Address which might change every time the router connects to the Internet.

Dynamic DNS [HELP]	
Item	Setting
▶ DDNS	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
▶ Provider	DynDNS.org(Dynamic) ▼
▶ Host Name	<input type="text"/>
▶ Username / E-mail	<input type="text"/>
▶ Password / Key	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

Before you can use Dynamic DNS service, you need to register an account on one of the many supported Dynamic DNS provider such as DynDNS.org, TZO.com or dhs.org. After registering the account, the Dynamic DNS provider will provide you with the following details:

- Host Name
- Username/Email
- Password/Key.

To enable the Dynamic DNS feature on the unit, click the Enable check box, choose the respective Provider and enter the details from your provider.

Click "Save" to save the settings or "Undo" to cancel.

Advanced Setting > QoS

QoS Rule					
Item		Setting			
▶ QoS Control		<input type="checkbox"/> Enable			
▶ Bandwidth of Upstream		<input type="text"/> kbps (Kilobits per second)			
ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use rule#
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
2	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	(0) Always ▼
<input type="button" value="Save"/> <input type="button" value="Undo"/>					

QoS (Quality of Service) provides different priority to different users or data flows, or guarantees a certain level of performance.

QoS Control: This Item enables QoS function or not.

Bandwidth of Upstream: Set the limitation of upstream speed.

Local IP: Ports

Define the Local IP address and port to apply QoS to.

Remote IP: Ports

Define the Remote IP address and port to apply QoS to.

QoS Priority: This defines the priority level of the current Policy Configuration. Packets associated with this policy will be serviced based upon the priority level set. For critical applications High or Normal levels are recommended. For non-critical applications select a Low level.

User Rule#: The QoS rules can work in conjunction with Scheduling Rules. Please reference the section Advanced setting/schedule Rule section.

Click on "Save" to store your setting or "Undo" to discard your changes.

Advanced Setting > SNMP

SNMP Setting [HELP]	
Item	Setting
▶ Enable SNMP	<input type="checkbox"/> Local <input type="checkbox"/> Remote
▶ Get Community	<input type="text"/>
▶ Set Community	<input type="text"/>
▶ IP 1	<input type="text"/>
▶ IP 2	<input type="text"/>
▶ IP 3	<input type="text"/>
▶ IP 4	<input type="text"/>
▶ SNMP Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c
▶ WAN Access IP Address	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

SNMP (Simple Network Management Protocol) is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

Enable SNMP: You must check Local, Remote or both to enable SNMP function. If Local is checked, this device will only respond to requests from LAN connected hosts. If Remote is checked, this device will respond to requests from the WAN connection.

Get Community: Sets the community string your device will respond to for Read-Only access.

Set Community: Sets the community string your device will respond to for Read/Write access.

IP 1, IP 2, IP 3, IP 4: Input your SNMP Management host IP here. You will need to configure the address where the device should send SNMP Trap messages to.

SNMP Version: Please select proper SNMP Version that your SNMP Management software supports.

WAN Access IP Address: You can limit remote access to a specific IP address by entering it here.

Please note: If "Remote" access is enabled, the default setting of 0.0.0.0 means any IP obtain SNMP protocol information.

Click on "Save" to store your setting or "Undo" to discard your changes.

Advanced Setting > Routing

Routing Table [HELP]					
Item		Setting			
▶ Dynamic Routing		<input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2			
▶ Static Routing		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>					

Routing tables allow you to determine which physical interface address to use for outgoing IP data. If you have more than one router and subnet, you will need to configure the routing table to allow packets to find the proper routing path and allow different subnets to communicate with each other.

These settings are used to setup the static and dynamic routing features of the 3G25W-R.

Dynamic Routing:

Routing Information Protocol (RIP) will exchange information about different host destinations for working out routes throughout the network. Please only select RIPv2 if you have a different subnet in your network. Otherwise, please select RIPv1.

Static Routing:

For static routing, you can specify up to 8 routing rules.

You need to enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable the rule by clicking the Enable checkbox.

Click on "Save" to store your setting or "Undo" to discard your changes.

Advanced Setting > System Time

This page allows you to change the System time setting on the 3G25W-R.

Item	Setting
▶ Time Zone	(GMT+10:00) Australia
▶ Auto-Synchronization	<input checked="" type="checkbox"/> Enable Time Server (RFC-868): Auto

Save Undo

Sync Result

Sync with Time Server Sync with my PC (Monday July 05, 2010 18:30:18)

Time Zone

Select the time zone where this device is located.

Auto-Synchronization

Select the "Enable" checkbox to enable this function.

Time Server

Select a NTP time server to obtain the current UTC time from

Sync with Time Server

Select if you want to set Date and Time by NTP Protocol.

Sync with my PC

Select if you want to set Date and Time using your computers Date and Time

Click "Save" to save the settings or "Undo" to cancel.

Advanced Setting > Scheduling

Schedule Rule		[HELP]
Item	Setting	
▶ Schedule	<input type="checkbox"/> Enable	
Rule#	Rule Name	Action
1		<input type="button" value="New Add"/>
2		<input type="button" value="New Add"/>
3		<input type="button" value="New Add"/>
4		<input type="button" value="New Add"/>
5		<input type="button" value="New Add"/>
6		<input type="button" value="New Add"/>
7		<input type="button" value="New Add"/>
8		<input type="button" value="New Add"/>
9		<input type="button" value="New Add"/>
10		<input type="button" value="New Add"/>
<input type="button" value=" <<Previous"/> <input type="button" value="Next>>"/> <input type="button" value="Save"/> <input type="button" value="Add New Rule..."/>		

You can use scheduling to enable or disable a service at a specific time or on a specific day.

Select "Enable" and then click the "New Add" button.

Select a name for the rule and enter the details such as the day, start time or end time.

Click "Save" to save the settings or "Undo" to cancel.

Tool Box

The Tool Box page consists of various tools for the unit. Click on any of the menu items on the left to access the respective page.

The screenshot displays the administrator's main menu with the following navigation options: ADMINISTRATOR's MAIN MENU, Status, Wizard, Advanced, and Logout. Below these are tabs for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. The left sidebar contains a list of menu items: System Info, Firmware Upgrade, Backup Setting, Reset to Default, Reboot, and Miscellaneous. The main content area is titled 'TOOLBOX' and contains the following list of tools:

- **View Log**
 - View the system logs.
- **Firmware Upgrade**
 - Prompt the administrator for a file and upgrade it to this device.
- **Backup Setting**
 - Save the settings of this device to a file.
- **Reset to Default**
 - Reset the settings of this device to the default values.
- **Reboot**
 - Reboot this device.
- **Miscellaneous**
 - Domain Name or IP address for Ping Test: Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

Tool Box > System Info

From this page you can view the System log and the Routing Table information for the router.

System Information	
Item	Setting
▶ WAN Type	3G
▶ Display time	Mon, 05 Jul 2010 08:34:37 +0000
System Log	
Time	Log
Jul 5 00:16:10	kernel: klogd started: BusyBox v1.3.2 (2010-07-01 10:38:02 CST)
Jul 5 00:16:16	O3G/hotplug: tmp1=AT^M^M OK^M
Jul 5 00:16:16	commander: Write AP PinCode into CSID_S_WLANAP_WPS_AP_PINCODE
Jul 5 00:16:17	O3G/hotplug: tmp=AT+CGMM^M^M MC8700^M ^M OK^M
Jul 5 00:16:22	udhcpd[1517]: udhcpd (v0.9.9-pre) started
Jul 5 00:16:22	udhcpd[1517]: Unable to open /var/run/udhcpd.leases for reading
Jul 5 00:16:22	init: Starting pid 1564, console /dev/ttyS1: '/bin/ash'
Jul 5 00:16:22	commander: STOP LOCAL_WANTYPE_3G

Tool Box > Firmware Upgrade

You can upgrade the routers firmware by clicking the “Upgrade” button

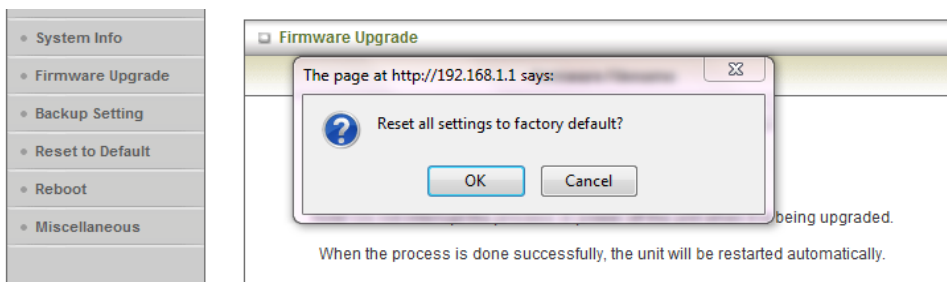
Firmware Upgrade
Firmware Filename
<input type="text"/> <input type="button" value="Browse..."/>
Current firmware version is V2.00a2 .
Note! Do not interrupt the process or power off the unit when it is being upgraded. When the process is done successfully, the unit will be restarted automatically.
<input type="checkbox"/> Accept unofficial firmware.
<input type="button" value="Upgrade"/> <input type="button" value="Cancel"/>

Tool Box > Backup Setting

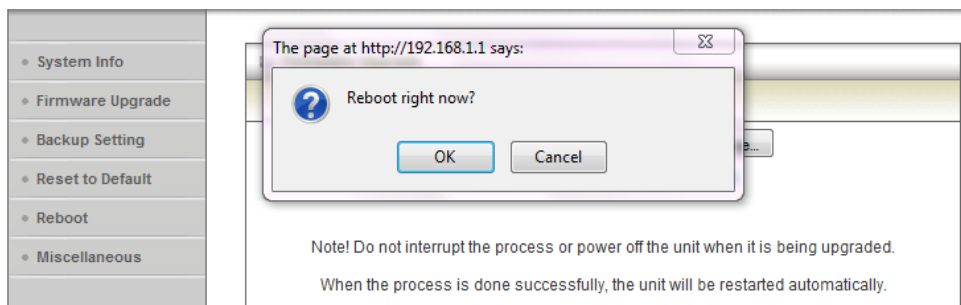


You can backup your current settings by clicking the **"Backup Setting"** button then and save it as a bin file. When you want to restore these settings, click the **"Firmware Upgrade"** button and use the bin file you saved.

Tool Box > Reset to Default



Tool Box > Reboot



Appendix A: WAN Failover

The WAN failover feature of the 3G25W-R is designed to provide a backup WAN connection in case your primary connection should fail. To use this feature, you will require both a regular WAN connection and a 3G WAN connection.

Please follow these steps to set up WAN failover on your 3G25W-R.

1. Set up a primary (non-3G) WAN connection by following the steps outlined in the Basic Setting > Primary Setup section of the User Guide.
2. Set up a secondary (3G) WAN connection by following the steps outlined in the Basic Setting > Primary Setup section of the User Guide.
3. Open your web browser (e.g. Internet Explorer/Firefox/Safari) and navigate to <http://192.168.1.1/>.
4. At the login screen, type in "admin" (without quotes) in the System Password field. Then click on Login.
5. Navigate to the Basic Setting > Primary Setup page. Select the Activate WWAN for Auto-Failover checkbox and enter a public IP address (for example 'www.google.com') into the remote host for keep alive box. The 3G25W-R will periodically check that it can connect to this address to determine if the WAN connection is still running.
6. In Basic Setting > Primary Setup, make sure that the selected WAN Type is your primary (non-3G) WAN connection and click Save. You are now ready to use the internet connection as normal.
7. When your primary (non-3G) WAN connection fails, the 3G25W-R will automatically failover to the secondary (3G) WAN connection. Please allow up to 2 minutes for this change to occur.
8. When your primary (non-3G) WAN connection reconnects, the 3G25W-R will automatically revert to this connection. Please allow up to 2 minutes for this change to occur.
9. To confirm that the process in Step 8 is complete, refresh the status page of the web interface after 1 minute.

Appendix B: Establishing your Wireless Connection

Windows XP service pack 2

1. Open Network Connections (Start -> Control Panel -> Network Connections):
2. Right-click on your Wireless Network Connection and select View Available Wireless Networks:
3. Select the wireless network you want to connect to and click Connect:
4. Enter the network key ("a1b2b3d4e5") and click Connect:
5. The connection will show Connected.

Windows Vista

1. Open Network and Sharing Center (Start > Control Panel > Network and Sharing center).
2. Click on "Connect to a network".
3. Choose "Connect to the Internet" and click on "Next".
4. Choose "NetComm n3G Series".
5. Click on the wireless network name and click "Connect".
6. Click on "Display Characters" and type in the network key. Then Click "Next".
7. Select the appropriate location. This will affect the firewall settings on the computer.
8. Click on both "Save this network" and "Start this connection automatically" and click "Next".

Windows 7

Follow these steps:

1. Open Network and Sharing Center (Start > Control Panel > Network and Sharing center).
2. Click on "Change Adapter settings" on the left-hand side.
3. Right-click on "Wireless Network Connection" and select "Connect / Disconnect".
4. You should see a network listed with the SSID of your 3G25W-R. Select your wireless network and click "Connect".
5. Type the following into the "Security key" section: a1b2c3d4e5 and click "OK".
6. You may then see a window that asks you to "Select a location for the 'wireless' network". Please select the "Home" location.
7. You may then see a window prompting you to setup a "HomeGroup". Click "Cancel" on this.
8. You can verify your wireless connection by clicking the "Wireless Signal" indicator in your system tray. After clicking on this, you should see an entry matching the SSID of your 3G25W-R with "Connected" next to it.

Mac OSX 10.6

Follow these steps:

1. Click on the Airport icon on the top right menu.
2. Click on the network name that you want to connect.
3. On the new window, tick on Show Password and type in the network key in the Password field. Click on OK.
4. To check the connection, click on the Airport icon and there should be a tick on the wireless name.

Notes: For other operating system (Windows 98SE, Windows ME, Windows 2000 etc) or if you use the wireless adaptor utility to configure your wireless connection, please consult the wireless adaptor documentation for additional information.

Appendix C: Troubleshooting

Using LEDs to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

Power LED

The Power LED does not light up.

Step	Correct Action
1	Make sure that the 3G25W-R power adaptor is connected to the device and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the 3G25W-R and the power source are both turned on and device is receiving sufficient power.
3	Turn the 3G25W-R off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

Web Configuration

I cannot access the web configuration.

Step	Correct Action
1	Make sure you are using the correct IP address of the 3G25W-R. Check the IP address of the device.
2	Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it.
3	Your computer's and the 3G25W-R's IP addresses must be on the same subnet for LAN access.
4	If you changed the devices WLAN IP address, then enter the new one as the URL.

The web configuration does not display properly.

Step	Correct Action
1	Delete the temporary web files and log in again. In Internet Explorer, click Tools, Internet Options and then click the Delete Files ... button. When a Delete Files window displays, select Delete all offline content and click OK. (Steps may vary depending on the version of your Internet browser.)

Login Username and Password

I forgot my login username and/or password.

Step	Correct Action
1	If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This will erase all custom configurations and restore all of the factory defaults including the password.
2	Press the Reset button for ten seconds, and then release it. When the LINK LED begins to blink, the defaults have been restored and the 3G25W-R restarts.
3	The default username is "admin". The default password is "admin". The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing.
4	It is highly recommended to change the default username and password. Make sure you store the username and password in a safe place.

WLAN Interface

I cannot access the 3G25W-R from the WLAN or ping any computer on the WLAN.

Step	Correct Action
1	Check the WiFi LEDs on top of the unit
2	Make sure that the IP address and the subnet mask of the NB14WN and your computer(s) are on the same subnet.

Internet Access

I cannot access the Internet.

Step	Correct Action
1	Make sure the 3G25W-R is turned on and connected to the network.
2	Verify your 3G settings

Internet connection disconnects.

Step	Correct Action
1	Check the schedule rules.
2	Contact your 3G SIM provider

Legal and Regulatory Information

FCC Statement:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation.

Important Note:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.

The transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Industry Canada RF exposure requirements

In order to ensure compliance with the RF exposure requirements specified in Health Canada Safety Code 6, this device may be operated while held in the hand, but not when held close to the body, carried in a pocket or holster, or similar configuration that allows close proximity to the body."

NOTE: THE MANUFACTURER IS NOT RESPONSIBLE FOR ANY RADIO OR TV INTERFERENCE CAUSED BY UNAUTHORIZED MODIFICATIONS TO THIS EQUIPMENT. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

This device complies with Industry Canada licence-exempt RSS standard(s).

Operation is subject to the following two conditions:

(1) this device may not cause interference

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Son Fonctionnement est soumis aux deux conditions suivantes :

(1) Le matériel ne peut être source D'interférences et

(2) Doit accepter toutes les interférences reques, Y compris celles pouvant provoquer un fonctionnement indésirable.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

This device has been designed to operate with the antennas listed below, and having a maximum gain of [4]dB.

Antennas not included in this list or having a gain greater than [4]dB are strictly prohibited for use with this device. The required antenna impedance is [50] ohms.

CANADIAN CLASS B STATEMENT: This digital device does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications. Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par le ministre des Communications.

MODIFICATION: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the device. Toute modification non approuvée explicitement par le fournisseur de licence de l'appareil peut entraîner l'annulation du droit de l'utilisateur à utiliser l'appareil.

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please refer to the GNU General Public License below to check the detailed terms of this license.

The following parts of this product are subject to the GNU GPL, and those software packages are copyright by their respective authors.

Linux-2.6.21 system kernel

busybox_1_00_rc2

bridge-utils 0.9.5

dhcpcd-1.3

ISC DHCP V2 P5

syslogd spread from busybox

wireless tools

ntpclient of NTP client implementation

GNU Wget

Availability of source code

Please visit our web site or contact us to obtain more information.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be

on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

Accompany it with the information you received as to the offer to distribute corresponding source code.

(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a

consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply

in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,

INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS