



4G ROUTER (4GR) USER GUIDE

August 2nd, 2017

INTRODUCTION	2
Package Contents.....	2
System Requirements.....	2
4GR Overview	2
Remote Management Portal.....	3
HARDWARE OVERVIEW	4
I/O, LEDs, and Power	4
Mounting.....	5
GETTING STARTED	6
LED Indicator Guide	7
The Label.....	8
LOCAL CONFIGURATION APP	9
Logging in.....	9
Accessing the Configuration Pages.....	9
Default Settings	11
Changing Passwords	11
Network Configuration	13
<i>WiFi</i>	13
<i>Ethernet</i>	15
<i>Cellular</i>	16
<i>WAN Priority</i>	16
<i>Port Forwarding</i>	16
LAN Clients.....	18
Administration.....	18
<i>System</i>	18
<i>Firmware</i>	19
<i>Logs</i>	20
<i>Diagnostics</i>	21
FACTORY RESET	22
ADDITIONAL RESOURCES.....	22
CERTIFICATIONS, LICENSES AND WARNINGS.....	23

INTRODUCTION

Intwine's failover broadband services protect small businesses from the loss and disruption of revenue, productivity, and customer experience associated with losing Internet connectivity. Intwine's bundled solution offers customers a fully managed and seamless backup broadband solution that is plug-and-play for failover broadband and parallel networking. The entire solution is developed, configured, billed, and supported by Intwine and also includes a management portal for ongoing maintenance, deployment, and support.

Package Contents

- Intwine Connect 4G LTE Router
 - Embedded 4G LTE modem
 - Embedded 4G LTE Verizon SIM
 - 802.11b/g/n and 10/100/1000 Ethernet WAN/LAN
 - Metal or plastic enclosure options
- Two (2) 4G LTE paddle antennas
- Two (2) 2.4 GHz antennas
- 3 foot Ethernet cable
- 12 VDC power supply
- Quick Start Guide

System Requirements

- Windows 2000/XP/7+, MAC OS X, or Linux computer
- The following web browsers (earliest version in parenthesis): Chrome (43), Internet Explorer (IE11), or Firefox (38)

4GR Overview

The Intwine Connect 4G LTE Router (4GR) is a specialized networking device designed to ensure secure and reliable broadband connectivity for homes, small businesses, and commercial buildings alike. The ability to deploy, monitor, control, and automate primary and secondary 4G LTE broadband networks becomes a reality using the 4GR. With the 4GR users are able to leverage Verizon's Private LTE Network, which means that data never touches the "open Internet," and the security and reliability of the network are greatly enhanced. Intwine Connect's 4G Router bundled solution includes:

- Intwine Connect 4G LTE Router (4GR)
- Cellular activation
- Static cellular IP address
- Private cellular network access

- One-year hardware warranty
- Tier 1 technical and installation support
- Bundled data packages
- Remote Management Portal account

Remote Management Portal

Intwine's Remote Management Portal (RMP) enables users to centrally manage a network of 4G LTE routers in real time and from anywhere in the world. With the RMP, users can quickly deploy and manage networks of distributed hardware in order to increase productivity and reduce costs related to IT and customer support.

The RMP is a cloud-based network management application that provides instant scalability and increased visibility into your network including:

- Cellular online/offline status
- Data usage monitoring
- Network health indicators
- Advanced troubleshooting tools
- Remote firmware upgrades

To create an account and register your 4GR sign up at: rmp.intwineconnect.com

HARDWARE OVERVIEW

The 4GR includes all necessary hardware and accessories to deploy cellular connectivity in any home, office, or building with adequate cellular coverage.

4GR features:

- Embedded 4G LTE modem and SIM card
- 802.11b/g/n
- 10/100/1000 Ethernet port
- Verizon 4G LTE certified
- Verizon Private Network certified
- Plastic or rugged sheet metal enclosure
- 12 VDC input power (PoE optional)

I/O, LEDs, and Power



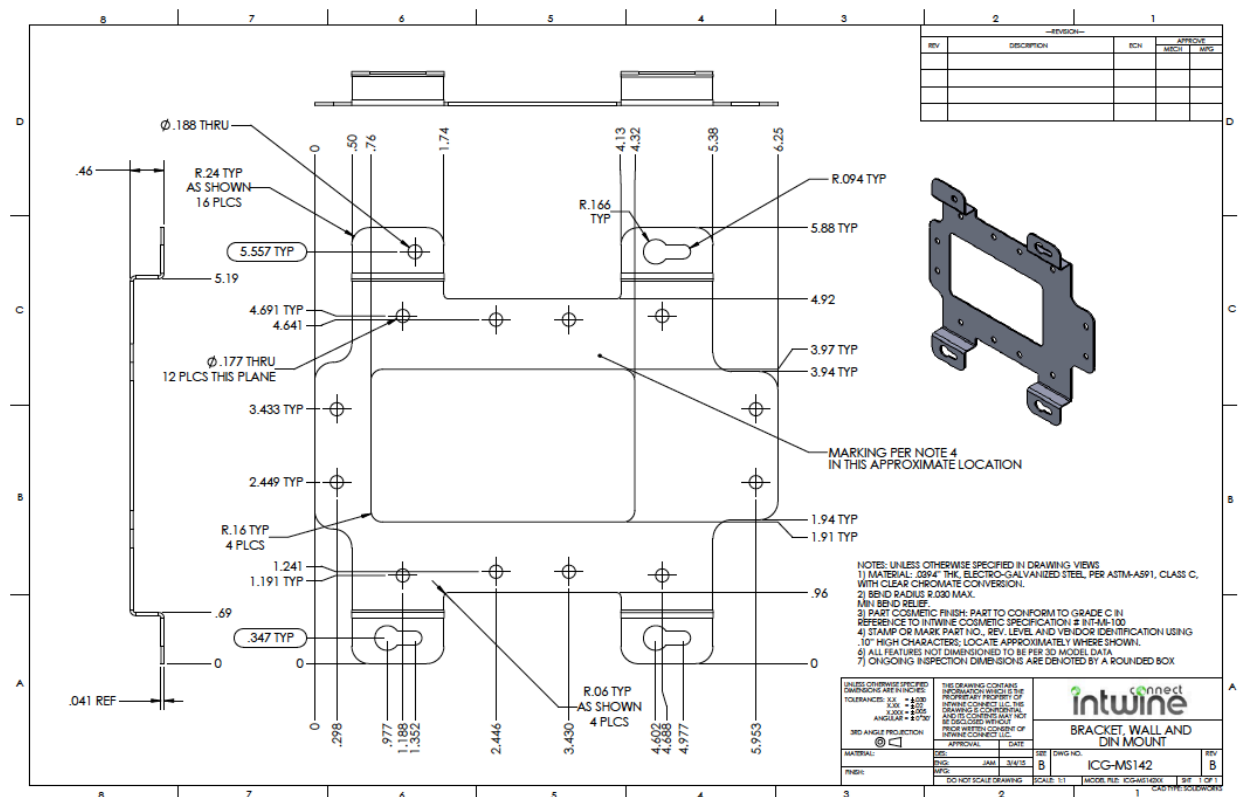
- ① 2 broad cellular antennas
- ② 2 circular 2.4GHz antennas
- ③ GB Ethernet port
- ④ USB 2.0 Host port
- ⑤ 12VDC Power supply input

1. The 4GR includes two high gain cellular antennas that are easy to attach and adjust for maximum reception. Warning: Antennas are only to be replaced by certified professionals. DO NOT use any external antennas that were not provided by Intwine Connect, LLC and installed by a certified professional.
2. The 4GR comes with two 2.4GHz antennas. If Wi-Fi is not being utilized the antennas can be removed, but should be replaced with 50 Ohm terminators.

- 10/100/1000 Ethernet port for WAN or LAN functionality. By default, the Ethernet port is configured as LAN. Access the Gateway configuration app to configure Ethernet settings.
- USB 2.0 port can be used as a standard USB host port.
- Please use the standard wall wart power source included in the box to power the 4GR.
- The reset button is recessed into the enclosure and can be pushed with a narrow screwdriver or a pen point. Press briefly to reset the system.

Mounting

The commercial (metal) version of the 4GR includes a wall mountable bracket.



To wall mount the 4GR, simply attach the bracket to the ICG using the four screws included in the box and mount to the wall using four additional screws.

GETTING STARTED

1. Hand-tighten the four antennas onto the threaded ports extending from the **4GR**.



NOTES:

- The broad antennas should be placed at the back of the **4GR**.
- For best coverage, position the broad antennas at a 45° angle from the base.
- Failure to properly attach the antennas **before** powering on the **4GR** to power could result in damage to the device.

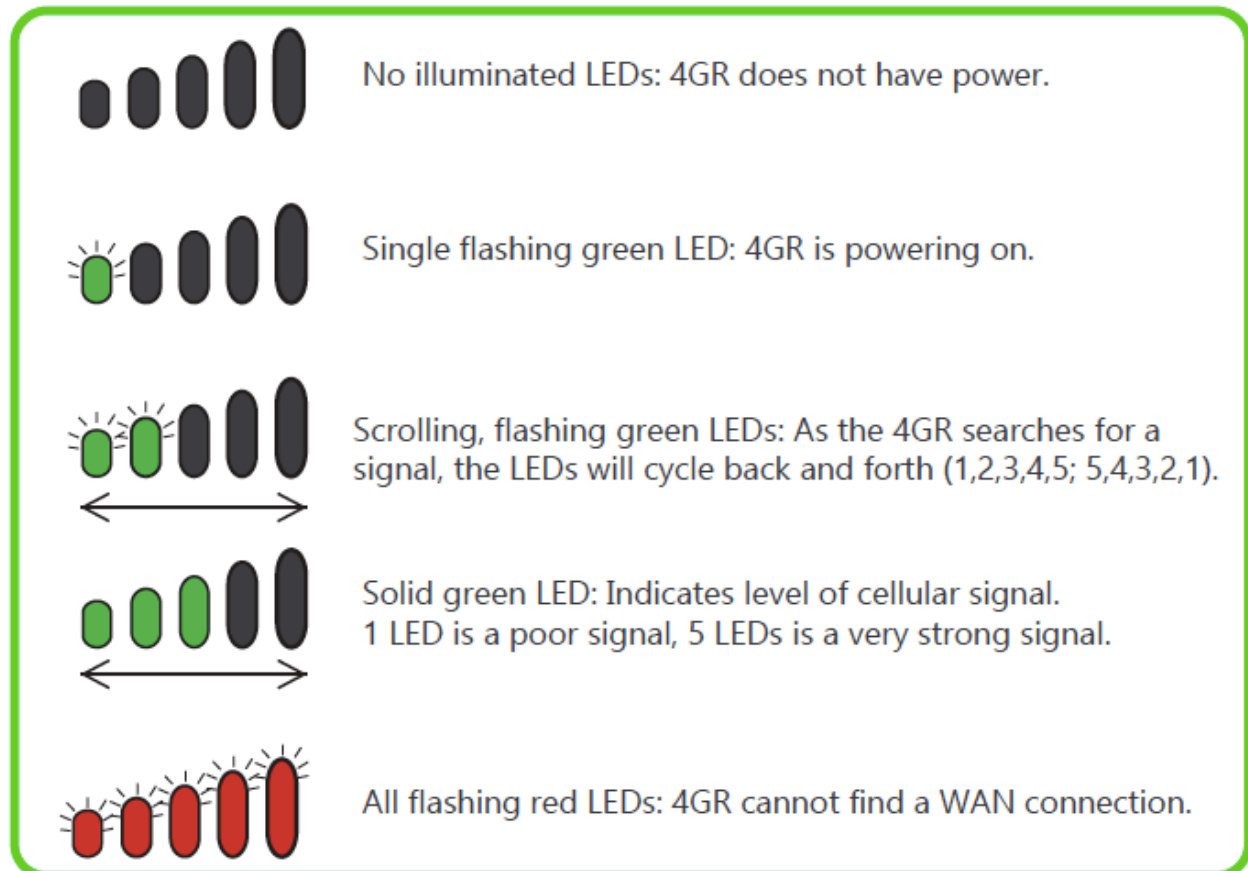
2. Attach the 12V DC power adapter to the **4GR** and plug it into a wall outlet.
3. The **4GR** will boot up automatically and connect to the 4G LTE network. This process may take up to 3 minutes.

NOTES:

Your **4GR** comes pre-equipped with a 4G LTE modem and SIM card.

LED Indicator Guide

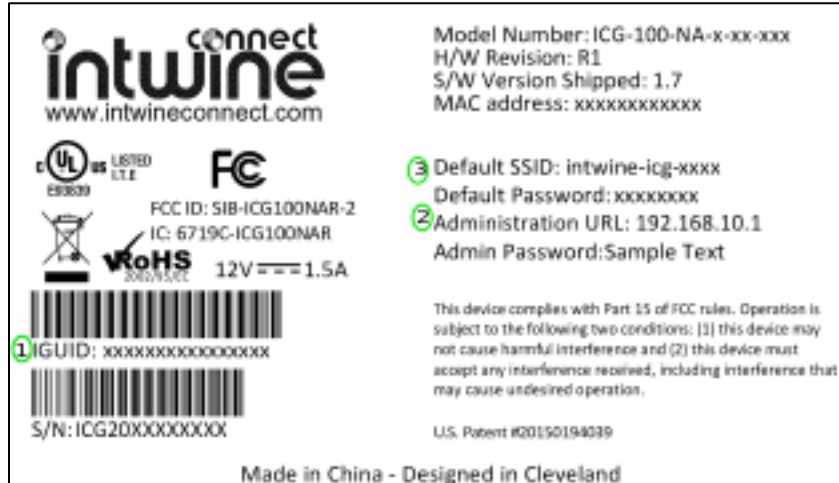
The LED indicators on the front panel of the 4GR are used to visually communicate the status of the 4GR. The below chart can be used to determine the state of the 4GR and cellular connection.



NOTES:

If your system is configured to have a secondary WAN interface, the LEDs will become orange-red when that interface is used to access the Internet.

The Label



A variant of the above pictured label ships on every production 4GR with both standard information and information that is specific to each individual Gateway. The label is full of pertinent information including the 4GR's FCC ID, UL number, MAC address, serial numbers, etc. The three most important pieces of information for configuring the 4GR are labeled above and described below:

1. **IGUID:** The IGUID stands for Intwine Globally Unique Identifier. The IGUID will allow you to register your Gateway to the Remote Management Portal and is the easiest and most assured way of identifying and tracking an individual Gateway.
2. **Admin URL/Password:** The admin URL (the same on each Gateway) is the local address at which users can access the local configuration pages (explained in **Logging In** section). The default username is **admin** and the default password is the unique string of characters that is printed on the label. The admin username and password can both be changed in the configuration pages, overriding these defaults, so **be sure to keep close track of any changes!**
3. **Default SSID/Password:** The default SSID is the wireless network name that will be broadcast by the 4GR. The default SSID is will always begin with **intwine-icg-** and the last four digits will be the last four of the IGUID. Since the default Wi-Fi access point is secured with WPA2 PSK encryption, the default password (pre-shared key) is the randomly generated string of characters printed on the label. The SSID and password can both be changed in the configuration pages, overriding these defaults, so **be sure to keep close track of any changes!**

LOCAL CONFIGURATION APP

The 4GR local configuration app is a web tool that allows users to customize the network configuration settings on their 4GR. The tool is useful for kitting, initial installation, and ongoing diagnostics/maintenance.

Logging in

To access the app and configure your 4GR simply connect to the 4GR's Wi-Fi SSID or Ethernet port from any Internet enabled device (e.g. phone, tablet, or PC).

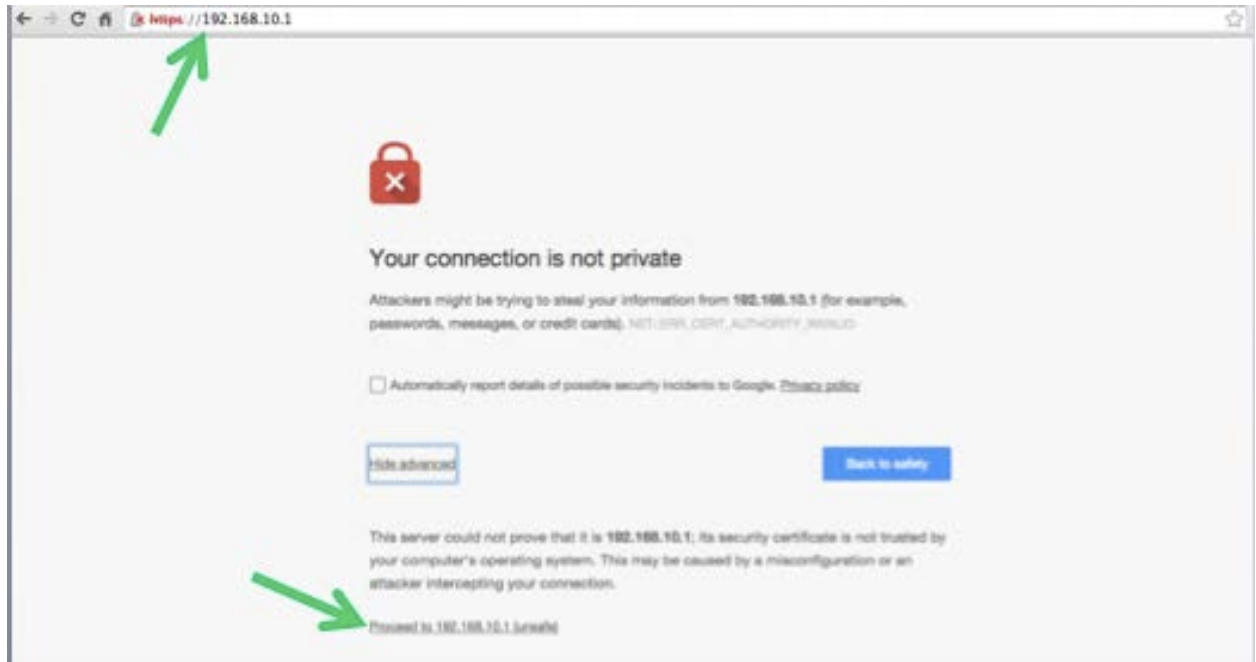
1. **Locate the network:** Using a Wi-Fi enabled device, open the window that shows available Wi-Fi networks. The 4GR's Wi-Fi network will appear on the list. Select the network (SSID) shown on the label.
2. **Connect to Wi-Fi:** After selecting the 4GR's Wi-Fi network, you will need to input the default password shown on the label. The password is the last eight digits of the device's IGUID.



Accessing the Configuration Pages

For most users, the 4GR can be used directly out of the box as a Wi-Fi/Ethernet to 4G LTE router and does not require any advanced configuration changes. For those that require custom changes, such as changing passwords, changing WAN/LAN settings, or accessing advanced networking features, you will need to log into the configuration pages.


1. To access the 4GR's configuration page, open up any standard web browser and browse to <http://192.168.10.1>. If you receive a security warning, dismiss it and proceed.



2. Enter **admin** as the username and the default password found on the label, then click the **LOGIN** button. It may take up to 30 seconds to login.



3. You are now able to configure your 4GR! You should now be on the **System Information** screen seen below. This screen shows pertinent 4GR settings, allows users to browse to advanced configuration settings, and shows real time 4G LTE data usage.




System Information

- System Information
- Network Configuration
- LAN Clients
- Administration
- Logout

4GR

Model	R1
Firmware Version	1.7.3
IGUID	yih5qhkbuori2r7z
System Time	2017-07-14 13:11:28
Uptime	1 day, 4:32:22

Cellular

Status	Powered On
Connection	Connected
Bars	
RSRP	-63 dBm
RSRQ	-7 dB
SINR	17 dBm
Data Usage	0.2 MB
IP Address	166.246.46.53
APN	mw01.VZWSTATIC
Cell IMEI	359692051112101
SIM ID	8914800000232292068
Phone Number	+13302170003

Interfaces

Interface	WAN/LAN	Priority	Status
Cellular	WAN	1	Online
WiFi	LAN		Online
Ethernet	LAN		Online

WiFi

IP Address	192.168.10.1
DHCP Server	Enabled
Station Type	Access Point
SSID	intwine-icg-yih5

Ethernet

IP Address	192.168.0.1
DHCP Server	Enabled

General Information:

- **Model Number:** R1
- **Modem Status:** Power on/off
- **Connection State:** Connected/ Disconnected (online/offline)
- **4G LTE Signal Strength:** Signal strength indicator, 1 (poor) through 5 (excellent)
- **4G LTE Data Usage:** XX MB
- **4G LTE WAN IP Address:** x.x.x.x
- **Interfaces:** Cellular/Wi-Fi/Ethernet – WAN/LAN – Online/Offline

Default Settings

Out of the box, the 4GR is configured as a Wi-Fi/Ethernet LAN to 4G LTE WAN router. All default usernames and passwords are printed on the label that can be seen on the bottom of the 4GR. Devices can be connected to the 4GR to access the Internet using these Wi-Fi credentials or by plugging in via Ethernet.

Changing Passwords

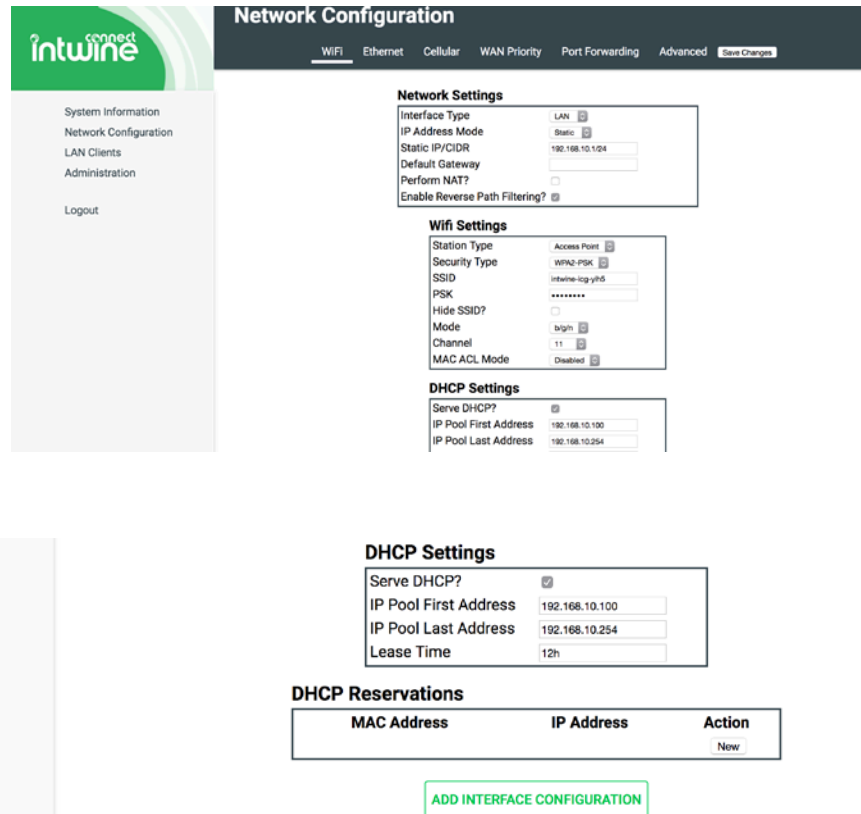
To change existing passwords and/or usernames, follow the steps above to log into the configuration pages, and then follow the below instructions. **NOTE:** Changing usernames/passwords will replace the information on the label. Be sure to **WRITE IT DOWN** and store in a **SECURE LOCATION**.

1. From the system information page, click on **Network Configuration** on the left hand of your browser and then **select the WiFi** tab.
2. To change your SSID and/or Wi-Fi password, edit the text in the current box and press **SAVE**.

NOTE:

Changes to the SSID and WPA2 key will kick you off of the network upon saving.

To log back in, repeat the **Logging In** steps above with your new information. Any changes that are saved are permanent until changed again and will **REPLACE** the information printed on the label.



The screenshot displays the 'Network Configuration' page with the 'WiFi' tab selected. The left sidebar shows navigation options: System Information, Network Configuration, LAN Clients, Administration, and Logout. The main content area is divided into three sections: Network Settings, Wifi Settings, and DHCP Settings.

Network Settings

- Interface Type: LAN
- IP Address Mode: Static
- Static IP/CIDR: 192.168.10.1/24
- Default Gateway:
- Perform NAT?: ☐
- Enable Reverse Path Filtering?: ☒

Wifi Settings

- Station Type: Access Point
- Security Type: WPA2-PSK
- SSID: intwine-4gr-yf8
- PSK:
- Hide SSID?: ☐
- Mode: bgn
- Channel: 11
- MAC ACL Mode: Disabled

DHCP Settings

- Serve DHCP?: ☒
- IP Pool First Address: 192.168.10.100
- IP Pool Last Address: 192.168.10.254
- Lease Time: 12h

DHCP Reservations

MAC Address	IP Address	Action
		New

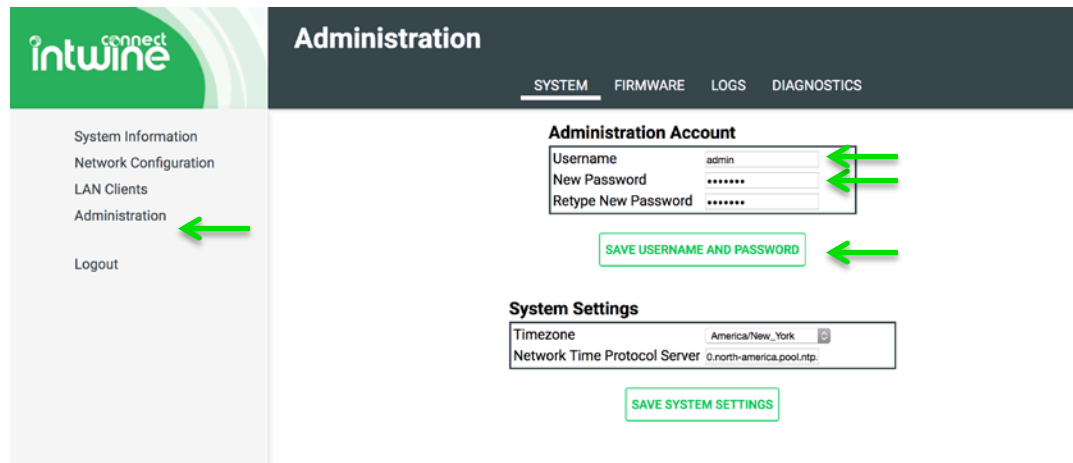
[ADD INTERFACE CONFIGURATION](#)

3. To change the administration username and password, click on the **Administration** tab on the left hand side of your browser. Change the username and password using the text boxes provided.

NOTE:

Changes to the admin username and password will keep you logged in, but will change upon logging out.

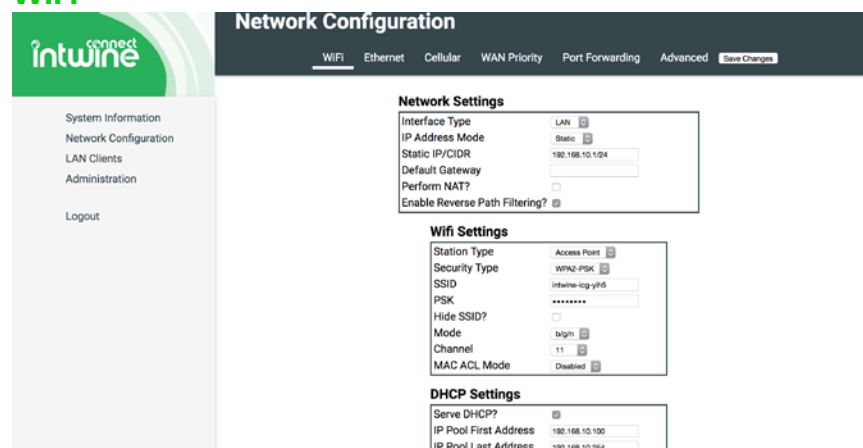
To log back in, repeat the **Logging In** steps above with your new information. Any changes that are saved are permanent until changed again and will **REPLACE** the information printed on the label.



Network Configuration

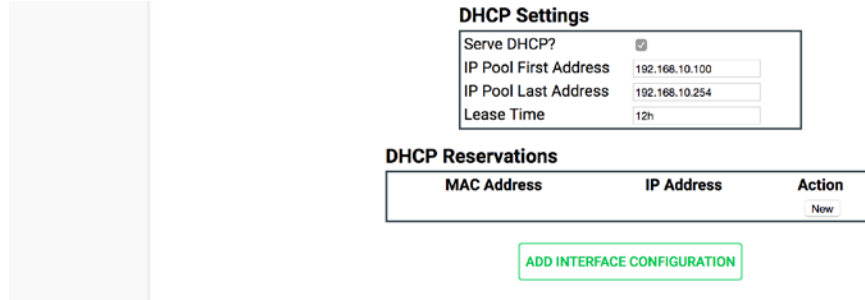
For those users that require more complex configurations, the below sections show the advanced settings of the 4GR and best practices to ensure appropriate configuration. All headings refer to a specific tab in the **Network Configuration** page and explain its function in detail.

WiFi



General Information:

- **SSID:** Customizable network identifier.
- **Wireless Mode:** b/g or b/g/n
- **Wi-Fi Radio Channel:** Auto or 1-11
- **Security:** WPA2-PSK or UNSECURED
- **Password:** WPA2 Key
- **IP Address Mode** Static or DHCP



DHCP Settings

Serve DHCP? ☒

IP Pool First Address 192.168.10.100

IP Pool Last Address 192.168.10.254

Lease Time 12h

DHCP Reservations

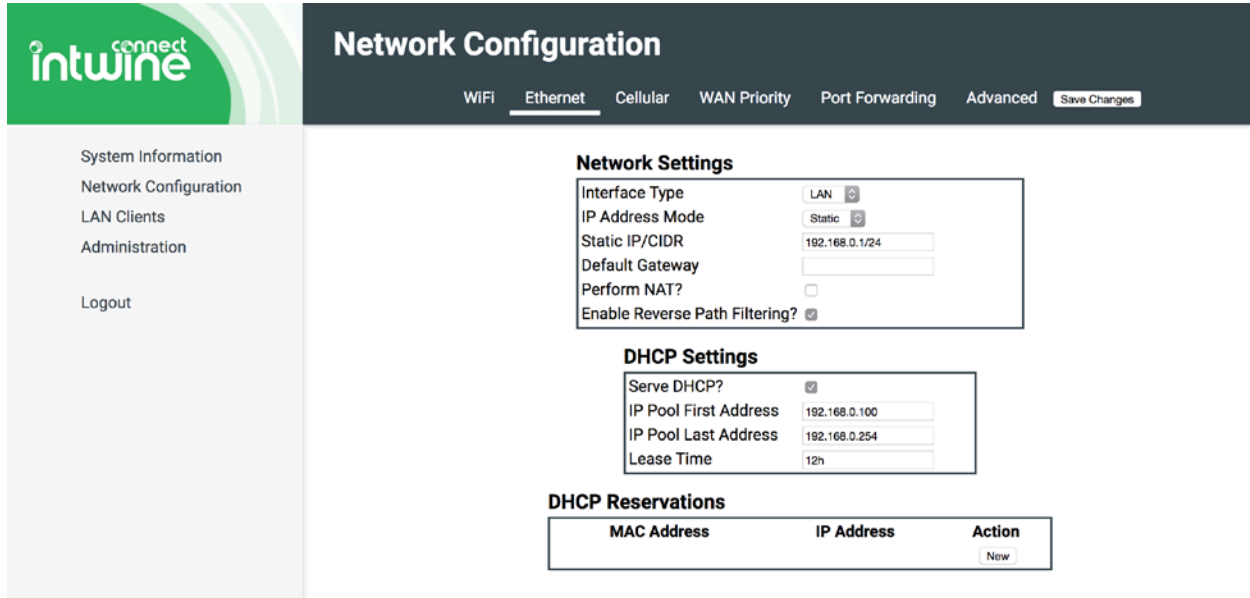
MAC Address	IP Address	Action
		New

ADD INTERFACE CONFIGURATION

To enable DHCP reservations:

1. Click **Enable DHCP Reservations** (check mark should be showing).
2. Click on New
3. Enter the MAC address of the device to which you would like to assign a specific IP address.
4. Enter the IP address that you would like to assign to the device (within the correct pool address range).
5. Click **Save Changes** at the top of the page.

Ethernet



The screenshot shows the 'Network Configuration' page for the intwine 4GR device. The 'Ethernet' tab is selected. The left sidebar contains links for System Information, Network Configuration, LAN Clients, Administration, and Logout. The main content area is divided into three sections: Network Settings, DHCP Settings, and DHCP Reservations.

Network Settings

Interface Type	LAN
IP Address Mode	Static
Static IP/CIDR	192.168.0.1/24
Default Gateway	
Perform NAT?	<input type="checkbox"/>
Enable Reverse Path Filtering?	<input checked="" type="checkbox"/>

DHCP Settings

Serve DHCP?	<input checked="" type="checkbox"/>
IP Pool First Address	192.168.0.100
IP Pool Last Address	192.168.0.254
Lease Time	12h

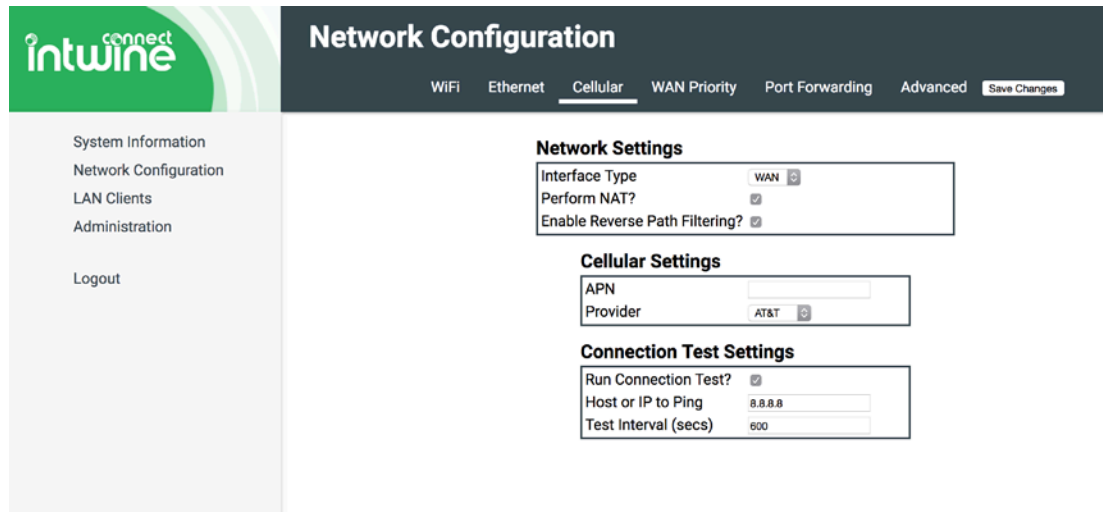
DHCP Reservations

MAC Address	IP Address	Action
		New

General Information:

- **Interface Type:** LAN or WAN
- **IP Address Mode:** Static or DHCP
- **Static IP/CIDR:** Local IP address/CIDR
- **Reverse Path Filtering:** Yes or No
- **Serve DHCP:** Yes or No
- **Lease Time:** Configurable by hour (default = 12 hours)
- New DHCP Reservations can be added or removed.
- **Changes will be applied once the Save Changes button is pressed. Use care when changing these settings.**

Cellular



The screenshot shows the 'Network Configuration' page with the 'Cellular' tab selected. The left sidebar contains links for System Information, Network Configuration, LAN Clients, Administration, and Logout. The main content area is divided into three sections: Network Settings, Cellular Settings, and Connection Test Settings.

Network Settings

Interface Type	WAN
Perform NAT?	<input checked="" type="checkbox"/>
Enable Reverse Path Filtering?	<input checked="" type="checkbox"/>

Cellular Settings

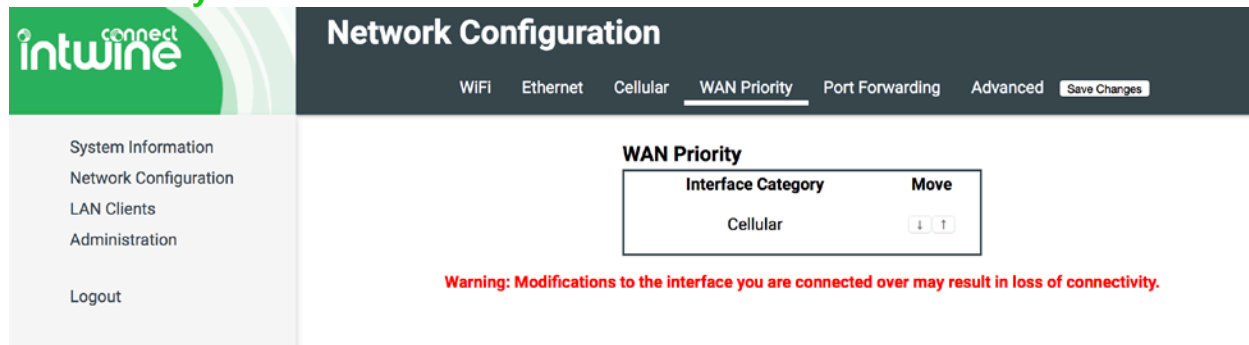
APN	
Provider	AT&T

Connection Test Settings

Run Connection Test?	<input checked="" type="checkbox"/>
Host or IP to Ping	8.8.8.8
Test Interval (secs)	600

The **Cellular** tab allows users to configure which interfaces are configured as **WAN/LAN**. The **APN** and the **Provider** can be changed.

WAN Priority



The screenshot shows the 'Network Configuration' page with the 'WAN Priority' tab selected. The left sidebar is the same as the Cellular page. The main content area shows the 'WAN Priority' section with a table for interface categories.

WAN Priority

Interface Category	Move
Cellular	<input type="button" value="↓"/> <input type="button" value="↑"/>


Warning: Modifications to the interface you are connected over may result in loss of connectivity.

Allows users to choose primary and secondary WAN connections. For example, in a typical cellular backup scenario, a user will want to configure Ethernet as the Primary WAN (priority 1) and Cellular as the backup WAN (priority 2), in case of a network outage.

Port Forwarding

Rules set under the **Port Forwarding** tab allow traffic from the Internet to reach a computer on the inside of your network. For example, a port-forwarding rule might be used to provide outside access to a local file server. Exercise caution when adding new rules, as they impact the security of your network.

WIFI Ethernet Cellular WAN Priority **Port Forwarding** Advanced Save Changes



- System Information
- Network Configuration
- LAN Clients
- Administration
- Logout

The rules on this page allow you to re-route network traffic destined for this gateway based on these factors:

- Inbound Interfaces:** Which interface the traffic arrives on. This can be one of wan, lan, eth, wifi, or cell, or a comma-separated list. wan refers to the current WAN interface—if the WAN interface fails over to a backup interface, or if the primary interface is restored, this rule will change automatically to match the new WAN interface. lan refers to all of the current LAN interfaces. If left blank, all interfaces match.
- Inbound Ports:** Which port or ports the traffic is destined for, if it is TCP or UDP. This is a comma-separated list of port ranges. For example, 561,1025-4096 matches ports 561 and ports 1025 through 4096 inclusive. This field is mandatory if forwarding TCP or UDP traffic.
- ICMP Types:** Which ICMP type or types the traffic is, if it is ICMP. Just like Inbound Ports, this is a comma-separated list of ICMP types. This field is mandatory if forwarding ICMP traffic.
- Protocol:** What kind of traffic it is (TCP, UDP, ICMP, IPSec ESP or IPSec AH). Note that when using IPSec forwarding, you must also forward UDP ports 500 and 4500.

Rules are checked in order. Anything after the first match is ignored. Any network traffic that matches a rule will be forwarded to the **Target Port** at the **Target IP Address**. If you don't want to change the **Target IP Address** or **Target Port**, leave the corresponding field empty.

WARNING: Changes made to these rules can drastically change the operation of your gateway and the devices connected to it, causing partial or total loss of functionality or even exposing new security vulnerabilities. Adding or removing rules here can lock you out of your gateway, preventing you or others from fixing its configuration. Never change this configuration without knowing exactly what you are doing, and always have a recovery plan.

Port Forwarding

Inbound Interfaces	Inbound Ports or ICMP Types	Protocol	Target IP Address	Target Port	Action
cell	2222	TCP ⌵	Unchanged	22	Remove
cell	22	TCP ⌵	Unchanged	2222	Remove
New					

To add a new port-forwarding rule:

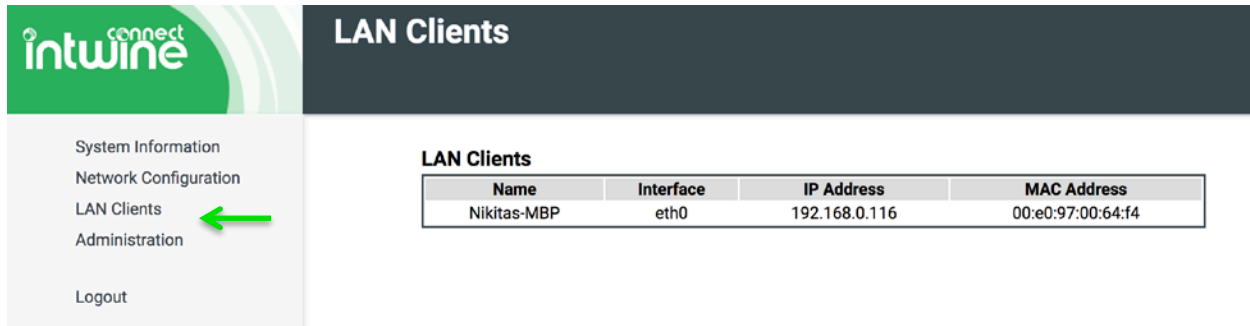
1. Type the inbound interface if desired. Possible values are wan, lan, eth, wifi, or cell. Only traffic on the selected interface will be forwarded to the desired destination.
2. Enter the Inbound Port numbers (can be specified as single value, comma separated list, or range).
3. Select the desired protocol (TCP/UDP/ICMP).
4. Enter the target IP address.
5. Enter the target port.
6. When complete, press the **Save Changes** button.

Port Forwarding Example

Your gateway is configured with an Ethernet connection to the Internet, with a 4G failover. You have a device connected to the Internet through the gateway, and have assigned it an IP address of 192.168.10.61 on a permanent basis through the WiFi settings page. Your device serves a web page on ports 80 (for HTTP) and 443 (for HTTPS), and you want to make it accessible to the Internet, on those ports. If you wish to keep your access to the gateway's web interface open, you need three rules. The first two rules open up ports 8080 and 8443 on the gateway, and expose the gateway's web interface on them, and the third rule forwards ports 80 and 443 to your device's web server as shown below:

Inbound Interfaces	Inbound Ports or ICMP Types	Protocol	Target IP Addresses	Target Port
Wan	8080	TCP		80
Wan	8443	TCP		443
Wan	80, 443	TCP	192.168.10.61	

LAN Clients



LAN Clients

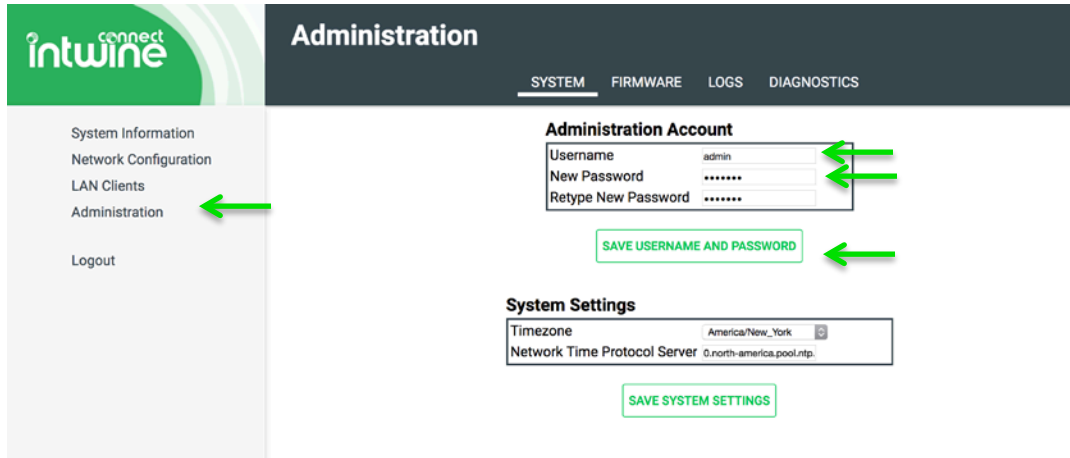
Name	Interface	IP Address	MAC Address
Nikita-MBP	eth0	192.168.0.116	00:e0:97:00:64:f4

The **LAN Clients** tab shows a complete listing of all Wi-Fi and/or Ethernet devices that are connected to the gateway. Each LAN client will show its **Interface** (Wi-Fi/Ethernet), **IP Address**, **MAC Address**, and for devices that have been assigned a **Name**, that will show as well.

Administration

The **Administration** tab enables users to perform general (non-networking) administrative tasks including setting the time zone, updating firmware, loading and saving network configurations, and reviewing logs.

System



Administration

SYSTEM FIRMWARE LOGS DIAGNOSTICS

System Information
Network Configuration
LAN Clients
Administration
Logout

Administration Account

Username: admin
New Password: *****
Retype New Password: *****

SAVE USERNAME AND PASSWORD

System Settings

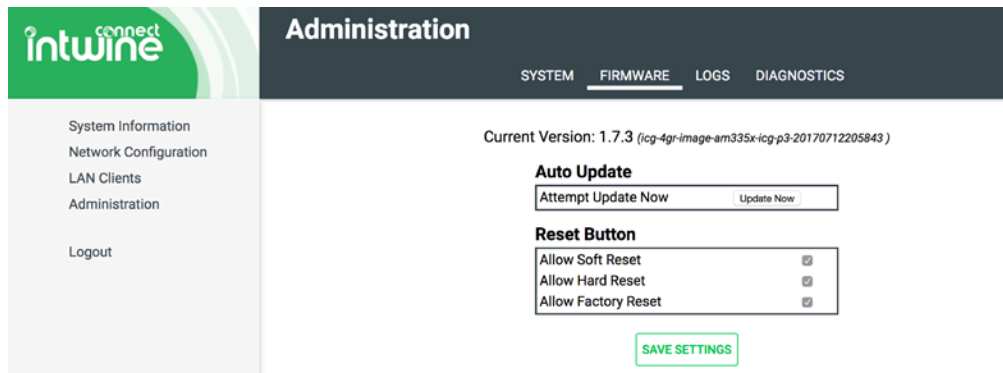
Timezone: America/New_York
Network Time Protocol Server: 0.north-america.pool.ntp.

SAVE SYSTEM SETTINGS

General Information:

- **Administration Account:** Change administrative username and password
- **System Settings:** Change time zone and NTP server.

Firmware



Administration

SYSTEM FIRMWARE LOGS DIAGNOSTICS

System Information
Network Configuration
LAN Clients
Administration
Logout

Current Version: 1.7.3 (icg-4gr-image-am335x-icg-p3-20170712205843)

Auto Update

Attempt Update Now Update Now


Reset Button

Allow Soft Reset ☒
Allow Hard Reset ☒
Allow Factory Reset ☒

SAVE SETTINGS

Shows current firmware version and allows the user to check for updates. The user can also configure the functionality of the reset button – the primary objective being to disable Factory Reset.

Logs



- System Information
- Network Configuration
- LAN Clients
- Administration
- Logout

Administration

- SYSTEM
- FIRMWARE
- LOGS**
- DIAGNOSTICS

Current Date and Time: 2017-07-14 14:27:45

Log File: [Download all logs \(.zip\)](#)

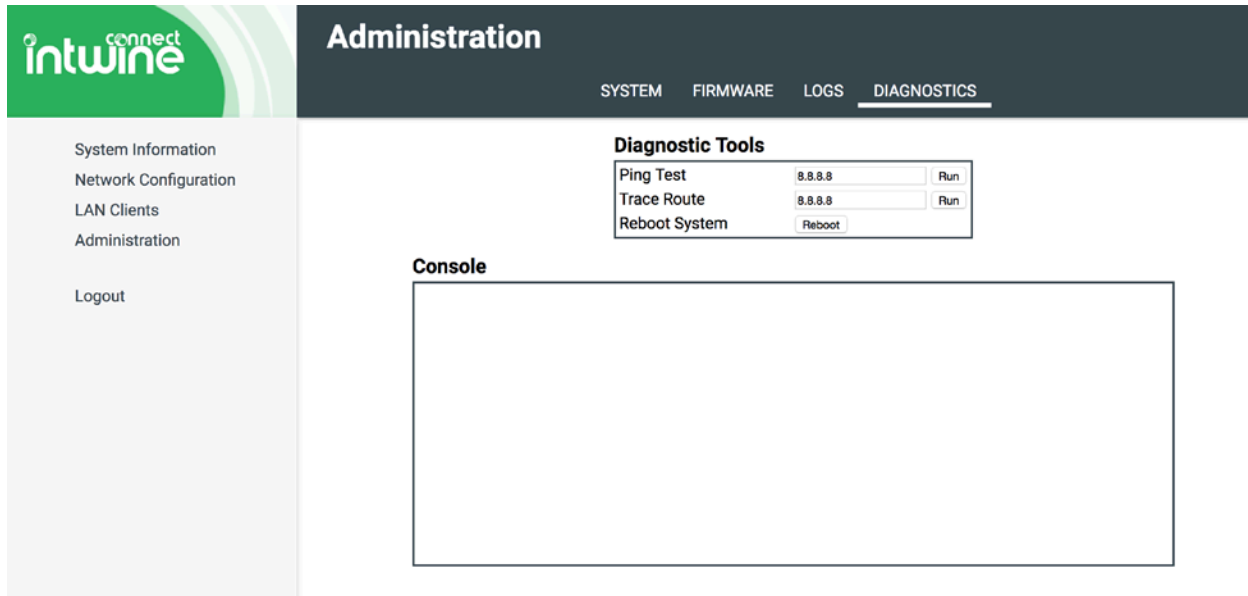
```

[128.028821] usb 1-1.2: Manufacturer: Realtek Semiconductor
[128.151174] cdc_ether 1-1.2:1.0 eth1: register 'cdc_ether' at usb-musb-hdrc2.auto-1.2, CDC Ethernet Device, 94:b9:b4:18:f6:4c
[128.178914] cdc_acm 1-1.2:1.2: This device cannot do calls on its own. It is not a modem.
[128.359022] cdc_acm 1-1.2:1.2: ttyACM0: USB ACM device
[155.810496] wicore: PHY firmware version: Rev 8.2.0.0.224
[155.732718] wicore: firmware booted (Rev 8.9.0.0.31)
[156.458252] net eth0: Initializing opsw version 1.12 (0)
[156.465803] net eth0: phy found : id is : 0x1cc916
[156.471133] net eth0: phy found : id is : 0x1cc916
[156.510310] 8021q: adding VLAN 0 to HW filter on device eth0
[157.198296] wicore: down
[158.458791] libphy: 4a101000.mdio:01 - Link is Up - 0/Half
[158.486480] libphy: 4a101000.mdio:01 - Link is Down
[159.969551] wicore: ERROR using 40Mhz AP in 2.4Ghz band - not officially supported
[160.050098] wicore: ERROR using 40Mhz AP in 2.4Ghz band - not officially supported
[195.295764] EXT4-fs (mmcblk0p0): mounted filesystem with ordered data mode. Opts: (null)
[221.028321] wicore: ERROR using 40Mhz AP in 2.4Ghz band - not officially supported
[100806.565327] libphy: 4a101000.mdio:00 - Link is Up - 1000/Full
[100806.595412] libphy: 4a101000.mdio:01 - Link is Up - 1000/Full

```

The **Logs** tab allows users to take a look at or download the logs. The available log files are – **System Log, Application Framework, Network Config daemon, ICG Log.**

Diagnostics



The screenshot shows the Intwine Connect Administration web interface. The top navigation bar includes 'SYSTEM', 'FIRMWARE', 'LOGS', and 'DIAGNOSTICS' (which is selected). The left sidebar contains links for 'System Information', 'Network Configuration', 'LAN Clients', 'Administration', and 'Logout'. The main content area is titled 'Diagnostic Tools' and contains three rows: 'Ping Test' with an IP input field set to '8.8.8.8' and a 'Run' button; 'Trace Route' with an IP input field set to '8.8.8.8' and a 'Run' button; and 'Reboot System' with a 'Reboot' button. Below these tools is a large empty box labeled 'Console'.

The **Diagnostics** tab allows users to **ping the gateway or reboot the system**.

FACTORY RESET

If you have had a problem with your 4GR after making configuration changes, you can use the Factory Reset capability. This function requires that the 4GR is running firmware 1.7.3 or newer and is not a pre-production system.

To perform the factory reset, press and hold the RESET button on the rear of the 4GR for 10 seconds or until the LEDs start flashing red; then release. The system will reboot, reinstall the operating system, and return all configurations to factory default (including all passwords to those shown on the bottom label).

For security purposes, this functionality can be disabled via the Local Configuration Page (Administration > Firmware).

ADDITIONAL RESOURCES

Contact tech support at (844) 259-3384 or support@intwineconnect.com.

CERTIFICATIONS, LICENSES AND WARNINGS

This Section contains safety, handling, disposal, regulatory, trademark, copyright, and software licensing information. Read all safety information below and operating instructions before using the 4GR device to avoid injury.

FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT

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 equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against such 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 provided by Intwine Connect, may cause harmful interference to radio communications. This device must accept any interference received, including interference that may cause undesired operations. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does 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 using one or more 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 or television technician for help.

Changes or modifications not expressly approved by Intwine Connect, LLC could void the user's authority to operate the product.

RSS-GEN COMPLIANCE: This device complies with RSS-GEN of the Industry Canada 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.

Ce dispositif est conforme à la norme CNR-GEN d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

This radio transmitter has been approved by Industry Canada to operate with the antenna types

listed below with the maximum permissible gain and required antenna impedance are strictly prohibited for use with this device.

Le présent émetteur radio a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

RADIATION EXPOSURE STATEMENT:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.

SAFETY AND HAZARDS - Under no circumstances should the 4GR device be used in any areas: (a) where explosives are being used ; (b) where explosive atmospheres may be present; or (c) that are proximate to any equipment which may be susceptible to any form of radio interference where such interference would result in harm of any kind. In such areas, the 4GR device **MUST BE POWERED OFF AT ALL TIMES** (since the device otherwise could transmit signals that might interfere with such equipment).

NOTE – The 4GR was not designed for safe in-vehicle use and, as such, it should not be used in any moving vehicle by the operator. In some jurisdictions, use of the 4GR device while driving or operating a vehicle constitutes a civil and/or criminal offense.

OPEN SOURCE SOFTWARE - This product contains software distributed under one or more of the following open source licenses: GNU General Public License Version 2, BSD License, and PSF License Agreement for Python 2.7. For more information on this software, including licensing terms and your rights to access source code, contact Intwine at info@intwineconnect.com.

WARRANTY INFORMATION - Intwine warrants this product against defects in materials and workmanship to the original purchaser (or the first purchaser in the case of resale by an authorized distributor) for a period of one (1) year from the date of shipment. This warranty is limited to a repair or replacement of the product, at Intwine's discretion as purchaser's sole and exclusive remedy. Intwine does not warrant that the operation of the device will meet your requirements or be error free. Within thirty (30) days of receipt should the product fail for any reason other than damage due to customer negligence, purchaser may return the product to the point of purchase for a full refund of the purchase price. If the purchaser wishes to upgrade or convert to another Intwine product within the thirty (30)

day period, purchaser may return the product and apply the full purchase price toward the purchase of another Intwine product. Any other return will be subject to Intwine's existing return policy.

LIMITATION OF INTWINE LIABILITY - The information contained in this Quick Start Guide is subject to change without notice and does not represent any commitment on the part of Intwine or its affiliates. INTWINE AND ITS AFFILIATES HEREBY SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL: (A) DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES, INCLUDING WITHOUT LIMITATION FOR LOSS OF PROFITS OR REVENUE OR OF ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE THE DEVICE, EVEN IF INTWINE AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND EVEN IF SUCH DAMAGES ARE FORESEEABLE; OR (B) CLAIMS BY ANY THIRD PARTY. Notwithstanding the foregoing, in no event shall the aggregate liability of Intwine and/or its affiliates arising under or in connection with the device, regardless of the number of events, occurrences, or claims giving rise to liability, exceed the price paid by the original purchaser of the device.

PRIVACY - Intwine collects general data pertaining to the use of Intwine products via the Internet including, by way of example, IP address, device ID, operating system, browser type and version number, etc. For more information, contact Intwine at info@intwineconnect.com.

OTHER BINDING DOCUMENTS, TRADEMARKS, COPYRIGHT - By activating or using your 4GR device, you agree to be bound by Intwine's Terms of Use, User License and other Legal Policies. For more information, contact Intwine at info@intwineconnect.com

© 2015 Intwine Connect, LLC. All rights reserved. Intwine is not responsible for omissions or errors in typography or photography. Intwine, 4GR and the Intwine logo are trademarks of Intwine Connect, LLC in the US and other countries. Other trademarks are property of their respective owners.

For a complete list of warnings, warranties, and other useful information about your 4GR, please visit www.intwineconnect.com.