# Residential Gateway

USER GUIDE

Rev. A06

ONT-7259G

# CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# 1. PREFACE

This Residential Gateway is one part of a GPON (gigabit passive optical network). It allows communications between your home and your service provider using a high-speed (gigabit) optical fiber network, while distributing the signals to the various devices in your home via standard Ethernet, wireless, or coax (for cable TV). Taking advantage of optical network technology allows greater bandwidth and speeds than were previously possible, while also increasing reliability. The Residential Gateway also acts as a router by converting the optical signals into data packets – and vice versa – that can traverse both upstream and downstream in the network. With this Residential Gateway, downstream traffic can travel at rates up to 2.5 Gbps, and upstream traffic can travel at rates of up to 1.2 Gbps.

*Note: Before you can use high-speed internet access, cable TV or telephone service with this device, you must already have set up an account with your service provider for these services.*

## Conventions Used

The conventions used throughout this document are as follows:

Blue annotations (circles, arrows, etc.) on images draw your attention to a particular area.

ⓘ Signifies a tip or useful information.

⚠ Signifies the user should proceed with caution.

**WARNING** Signifies a warning, where injury to the user, the Residential Gateway, or any of the connected devices may result.

Text the user should enter from the keyboard is highlighted in **white on black**. Care should be taken to type the text exactly as written, including upper/lower case.

### Important Notice

This document contains examples of screens (web pages) which are shown for illustration purposes only. Your pages/screens may differ slightly. The settings and configurations depicted on the screens represent default or sample values. Your settings and configurations will be different. Finally, the Residential Gateway device itself is available in different models with different hardware/software options. Thus, the functionality described in this document may not always exactly match your particular device, model, or software version.

## Care of Your Residential Gateway

- Do not clean with any liquid, aerosol or static cleaning solution. Clean only with a dry cloth. Keep free from dust and water.

- Install the device following *all* recommendations (refer to *Physical Setup*).
- Use caution when routing wires and cables. Avoid severe bending and routing over sharp edges. Use grommet material when possible to avoid wear on cable insulation.
- Unplug the device when it is not used for a prolonged time.
- Do not use if the unit becomes damaged or wet.
- Keep the device away from heat sources, wetness, and excessive humidity.
- Operate the unit only from an AC electrical outlet having input voltages of 100-240V and frequency of 50/60 Hz, utilizing the supplied power cord, unless using a suitable UPS device.

## Product Safety

**WARNING** Elevated voltages are present at specific points in this electrical equipment. Some of the parts may also have elevated operating temperatures. Care must be taken in order to avoid personal injury and/or property damage. Only trained and qualified personnel may install and service the system. There are no user-serviceable parts.

⚠ Installation: Follow all precautions stated in this manual for care of the device and physical setup.

**WARNING** Laser: This equipment uses fiber optics employing powerful lasers. Do not look into the ends of optical fibers. Exposure to invisible laser radiation may cause serious retinal damage or blindness.

### RF Interference

RF frequency ranges of this device comprise a spectrum from 54 MHz to 1000 MHz. This equipment generates, uses, and can radiate radio frequency energy and may cause interference with radio communications, radio and TV reception, and/or RF-controlled devices such as garage door openers or baby monitors, at particular installations. If this happens, you can correct the problem by employing one or more of these measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the Residential Gateway and the device.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Contact your service provider for assistance.

## Compliance

This is a Class B device regulated under FCC Rules Part 15, Subpart B. This Residential Gateway complies with the requirements for Class B digital devices per Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This product uses a Class 1 LASER according to FDA Rules. This product conforms to all applicable requirements of 21 CFR 1040.

This device is CSA Certified for use in the U.S. and Canada (UL/CSA 60950). It complies with the standard EN 60950-1 / IEC 60950-1. All equipment connected to the Residential Gateway has to comply with the applicable safety standards.

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme á la norme NMB-003 du Canada.

This device supports tones, cadences and ring patterns for the following countries: USA, Canada, Brazil, Mexico, Germany, Kuwait, Switzerland, China, Saudi Arabia, United Arab Emirates, Ukraine, Poland, India, and Russia.

### Standards

This device supports or complies with many telecommunications and data standards, among them are as follows (not an exhaustive list):

- Ethernet bridging/switching as per IEEE 802.1D/802.1Q
- Ethernet interface meets IEEE 802.3 specifications
- 802.3n flow control
- Wireless meets 802.11n specifications
- QoS with four traffic classes as per IEEE 802.1p
- Full IEEE 802.1Q VLAN ID processing per port
- SIP, H.248, MGCP
- Meets GR-909 transmission requirements
- Meets GR1089 AC power cross and lightning protection
- Echo cancellation as per ITU-T G.168 (up to 16 ms tail end)
- Fax Transmission: G.711 Direct & Indirect Media, T.38 Direct & Indirect Media
- Supports receiving and sending media using the G.711 Codec and G.729 Codec
- Supports DTMF as specified in RFC2833

## Service & Support

**WARNING** This device has no user-serviceable parts. Only authorized service personnel should attempt to install, service, and/or repair this equipment. Opening the device will void the warranty and could cause injury to the user, the device, and/or connected devices. All service must be performed by a qualified technician or by the manufacturer.

For support with the hardware or software or for service, please contact your service provider:

Service provider will write or insert a sticker here
containing their customer support phone number

# 2. INSTALLATION

## Physical Setup

Select an appropriate and safe location to install your Residential Gateway, taking care to observe these important caveats:

- Select a location which is close to an AC electrical outlet and an active fiber-optic cable connection, not in direct sunlight, not near water, and free from extreme temperatures and excessive humidity.
- Do not block ventilation openings, place things on top of it, or place the device in an enclosure.
- Do not allow cords or cables into or out of the device to become pinched or kinked.

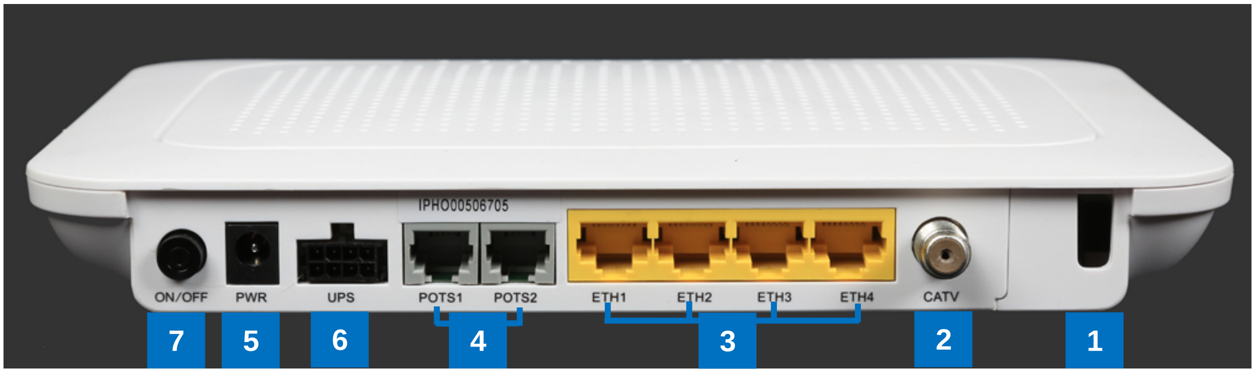
The Residential Gateway may sit on a flat surface or may be mounted vertically using optional wall mount kit. Refer to mounting instructions included with the kit.

### Connecting Devices

Before powering up the Residential Gateway, make the following connections on the back of the device.

*Note: Depending on your model, you may have a slightly different port configuration.*

**Figure 2-1. Back of Residential Gateway showing port connections.**



1. Fiber-optic connection: The active fiber-optic cable from your service provider should extend out from the fiber-optic connector at the back right corner of the Residential Gateway.
2. Cable TV connection: Connect one end of a coax cable to the CATV connector at the back of the Residential Gateway, and connect the other end to your TV, set top box, or DVR. To connect more than one coax device, a splitter (not provided) will be needed.
3. Ethernet LAN connections: Connect one end of an Ethernet cable to an Ethernet port at the back of the Residential Gateway and connect the other end to your Ethernet device – usually a PC or an Ethernet hub or switch. Depending on your Residential Gateway's configuration, you may have multiple Ethernet ports, allowing you to connect multiple devices.
4. Telephone/fax connections: Connect one end of an RJ-11 cable to one of the POTS ports

at the back of the Residential Gateway, and connect the other end to your telephone or fax machine. Depending on your Residential Gateway's configuration, you may have multiple POTS ports, allowing you to connect multiple telephones or fax machines. Note: If you are using a VoIP phone, it would plug into one of the Ethernet ports rather than one of the POTS ports.

5. Power: Attach the AC power cord provided to the back of the Residential Gateway and plug the other end of the power cord (containing the power adapter) into an AC electrical outlet.
6. UPS connection (optional): If you have a UPS (uninterruptible power supply), it may be plugged into the Molex port labeled 'UPS' at the back of the Residential Gateway. Although having a UPS is not mandatory, it is desirable and recommended. Not only will it protect the Residential Gateway from power spikes, but it will allow the phone, LAN and CATV connections to continue operation during a power failure to your home (length of time varies depending on your UPS equipment). For more about connecting the UPS refer to the *Battery/UPS Operation* section.

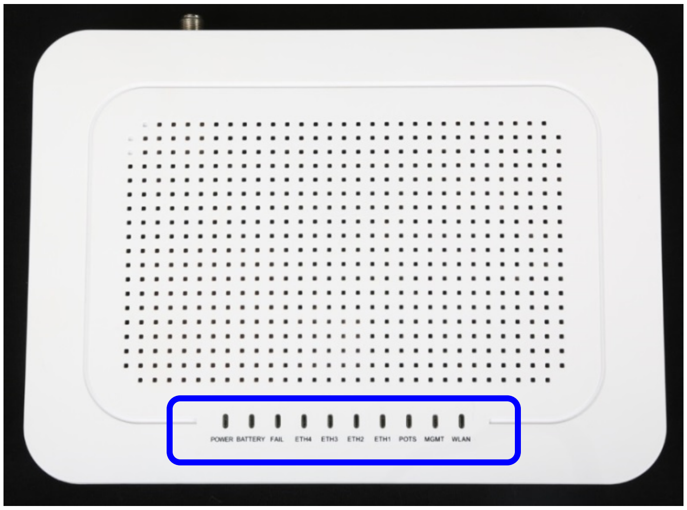
*Note: While the Residential Gateway device is plugged into a UPS, it does not need to be simultaneously plugged into an AC electrical outlet (item #5 above).*

7. On/Off switch: When pushed in, the unit is powered on. Pushing in the button a second time will cause the button to pop back out and this will power off the device.

## Powering Up the Residential Gateway

To switch on the device, press the power button at the back of the Residential Gateway. Refer to item 7 in Figure 2-1 above. You should see the green power light display on the front of the Residential Gateway (refer to Figure 2-2). Wait a couple of minutes, during which time various lights will flash. After about 2 to 5 minutes, the lights should stop flashing, and you should see a solid green light for power, Eth1 (or whatever Ethernet connections you have made), and WLAN (if it senses any active wireless devices) .

**Figure 2-2. Front/top of Residential Gateway showing location of lighted indicators.**



## LED Descriptions

From left to right, the lighted indicators are described in Table 2-1 below.

**Table 2-1. LED Descriptions**

| LED | Description |
|---|---|
| POWER | • Glows steady green when the power is on (from a valid AC or UPS source).<br>• Flashes when the unit is ranging.<br>• Off when the power is off. Note: Even though the power light is not illuminated, the device may still be plugged in (connected to the power source). |
| BATTERY | • Glows steady green when the external battery/UPS is charged and the unit is operating on external power.<br>• Flashes slowly when the unit is running off battery power only (no AC power).<br>• Flashes quickly when battery power is low and the unit is about to turn off.<br>• Off when battery is missing or defective.<br>• Refer to the section below on *Battery/UPS Operation* for further details. |
| FAIL | • Glows red to indicate no optical signal present.<br>• Flashes slowly when there is a weak optical signal or the fiber connection needs cleaning. If this occurs, contact your service provider.<br>• Flashes quickly when software upgrade has failed. If this occurs, contact your service provider.<br>• Off when the optical signal is present and functioning normally. |
| ETH1 – ETH4 | • Glows steady green when Ethernet connection is operational.<br>• Flashes to indicate data transmission in progress.<br>• Off means there is no Ethernet connection (link is down) or the system is not equipped with this feature. |
| POTS | • Glows red to indicate an active telephone call (off-hook).<br>• Flashes slowly to indicate an incoming call (ringing).<br>• Off indicates no call in process (on-hook) or the system is not equipped with this feature. |
| MGMT | • Glows green when the management channel (OMCI) is active.<br>• Off when not active or there is no link present. |
| WLAN | • Glows green when the Wi-Fi function is active.<br>• Flashes to indicate data transmission in progress.<br>• Off when Wi-Fi is not active or the system is not equipped with this feature. |

Refer to this table of LED descriptions (above) when trouble-shooting your Residential Gateway device.

## Battery/UPS Operation

It is highly recommended that you provide an uninterruptible power supply (UPS) in order to provide power to the device in the event of an AC power outage. Such a battery backup device is also useful in providing continuous surge suppression and power filtering which will prolong the life of the equipment as well as all its connected devices.

⚠ Without a UPS or backup battery supply, telephones will cease to operate during a power failure to your home.

Connecting the Battery/UPS**:** Use the following steps and refer to the diagram below when connecting the UPS.

1. Select a UPS that can provide 14.24W continuous power at 12VAC to the Residential Gateway device.

2. Select a location for the UPS, following all the manufacturer's requirements and

specifications for temperature, humidity, airflow, etc.

3. Fully charge the battery inside the UPS before attaching it to the Residential Gateway device, by attaching it to an AC power source (i.e., a wall electrical outlet).
4. Plug the UPS into the Residential Gateway device via a Molex 46235-5002 connector to the appropriate port on the back of the Residential Gateway device (refer to item #6 in Figure 2-1 in the section on *Connecting Devices*).
5. While the Residential Gateway is plugged into a UPS, there is no need to plug the Residential Gateway into an AC wall outlet simultaneously.

**Diagram A:** with UPS:

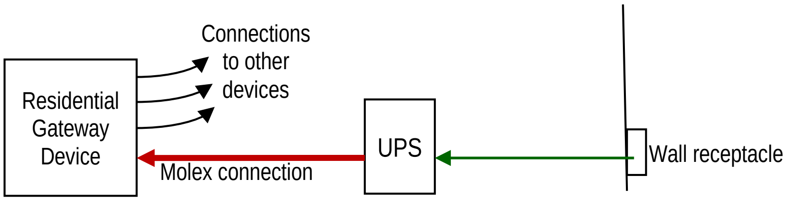
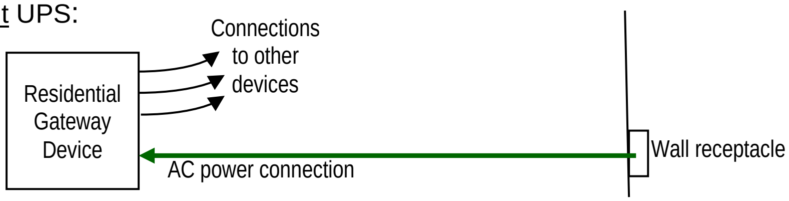


**Diagram B:** without UPS:



UPS Interface: When the UPS is functioning normally, the 'Battery' light on the front of the Residential Gateway will glow a steady green (Diagram A setup). If there is no UPS present, the 'Battery' light on the front of the Residential Gateway will be off (Diagram B setup). The Residential Gateway also provides the following alarm reporting for the UPS:

- On-Battery – AC power lost, now operating on the backup battery power within the UPS. 'Battery' light on the front of the Residential Gateway flashes slowly.
- Battery Missing – No UPS connected (similar to Diagram B). 'Battery' light on the front of the Residential Gateway will be off.
- Low Battery – Battery inside the UPS is weak (drained) and will go down soon. 'Battery' light on the front of the Residential Gateway will flash quickly.

## Logging Into the Residential Gateway

The software used for setting up and configuring the device may be accessed using any operating system (Windows, Mac OS, Linux, etc.) that supports an html-compliant web browser. Supported browsers include, but are not limited to: Internet Explorer 9.0 and up, Mozilla FireFox 3.6 and up, Google Chrome, myOpra, etc. It may also be accessed from a SmartPhone such as Android, Apple iOS using the Safari browser, or with the Dolphin browser.

*For initial setup, it is recommended that you use a PC (rather than a SmartPhone) that can be* *directly connected to one of the Ethernet ports.*

Using a PC connected to the device, open a web browser and type the Residential Gateway's default IP address in the address bar of the browser:

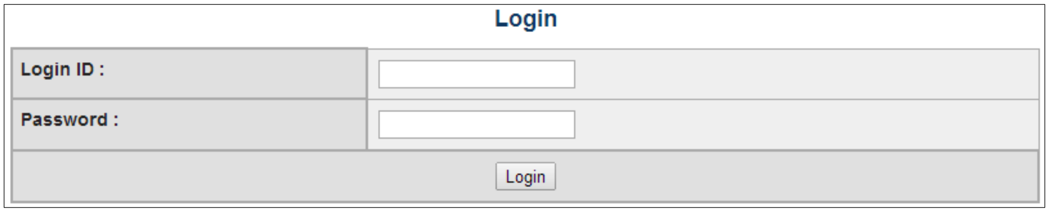
**https://192.168.1.1/**

*Note: The Residential Gateway's default IP address as configured from the factory is 192.168.1.1. This cannot be changed.*

The first time you enter this, your browser may give you a security warning. For example, in Google Chrome, it might say "This site's security certificate is not trusted." In Mozilla Foxfire, it might say "This connection is untrusted." If this happens, select the option that allows you continue to the site. For example, in Google Chrome, you would click "Proceed anyway" and in Mozilla Foxfire, you would click "I understand the risks." Whatever your browser may be, select the equivalent option.

A login page will appear similar to that shown below:

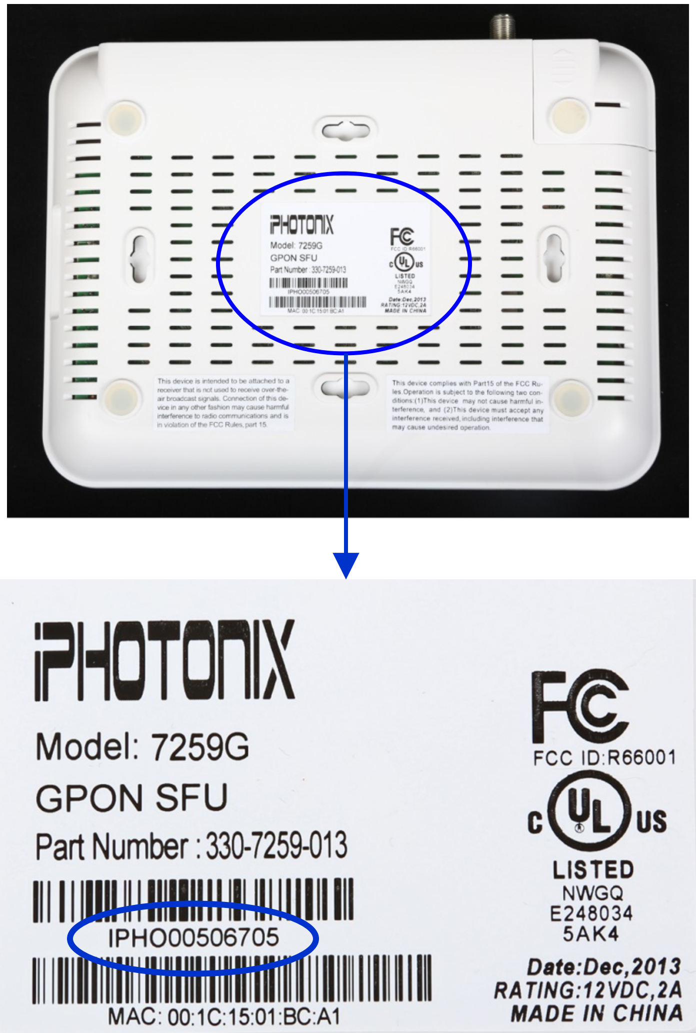
**Figure 2-3. Login screen.**



Enter the default Login ID: **admin**.
*Note: This can be changed later, if desired. Refer to the section on User Administration.*

Enter the default password. This is your Residential Gateway's serial number. It can be found on a sticker on the bottom of the Residential Gateway, along with the model, part number, and MAC address. The serial number is below the first barcode and starts with 'IPHO' as shown in the example below (refer to Figure 2-4 below).

**Figure 2-4. Bottom of Residential Gateway and Sticker showing location of Serial Number.**



Enter the entire serial number - all letters and numbers - for the password, taking care to correctly type the letter "O" (4th character of the serial number) and the number "0" (zero). Then click on the login button.

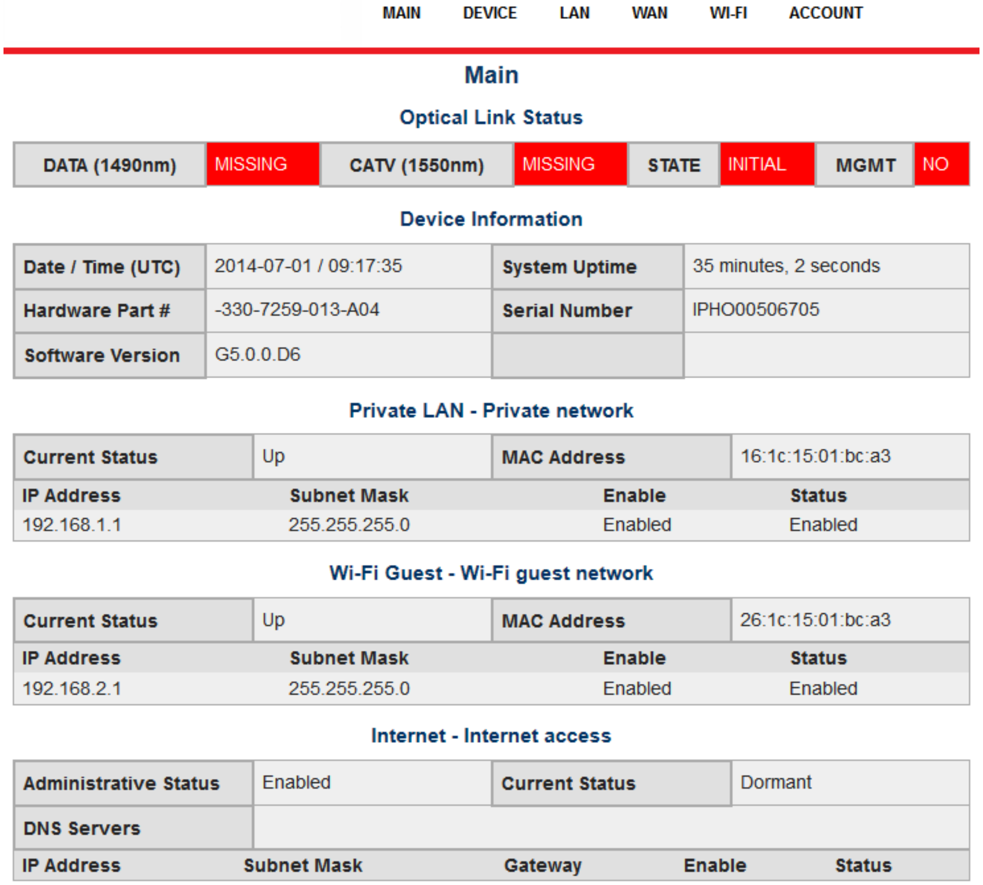
*Note: We recommend you change the password for the administrator account to better safeguard your Residential Gateway from hacking. Refer to the section on User Administration.*

After logging in, the Main page will be displayed, showing current status information.

### The Main Page

Shown below is a sample of the Main page. It reports the status of the various parts of the Residential Gateway. The exact details shown on your Main page will differ.

Figure 2-5. Main Page.



Main

Optical Link Status

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| DATA (1490nm) | MISSING | CATV (1550nm) | MISSING | STATE | INITIAL | MGMT | NO |

Device Information

| | | | |
|---|---|---|---|
| Date / Time (UTC) | 2014-07-01 / 09:17:35 | System Uptime | 35 minutes, 2 seconds |
| Hardware Part # | -330-7259-013-A04 | Serial Number | IPHO00506705 |
| Software Version | G5.0.0.D6 | | |

Private LAN - Private network

| | | | |
|---|---|---|---|
| Current Status | Up | MAC Address | 16:1c:15:01:bc:a3 |
| IP Address | Subnet Mask | Enable | Status |
| 192.168.1.1 | 255.255.255.0 | Enabled | Enabled |

Wi-Fi Guest - Wi-Fi guest network

| | | | |
|---|---|---|---|
| Current Status | Up | MAC Address | 26:1c:15:01:bc:a3 |
| IP Address | Subnet Mask | Enable | Status |
| 192.168.2.1 | 255.255.255.0 | Enabled | Enabled |

Internet - Internet access

| | | | | |
|---|---|---|---|---|
| Administrative Status | Enabled | Current Status | Dormant | |
| DNS Servers | | | | |
| IP Address | Subnet Mask | Gateway | Enable | Status |

The sections displayed on the Main page are as follows:

Optical Link Status**:** Ideally, the status reported would be normal (connected) and the fields will be colored green. In the example above (Figure 2-5), there was no fiber optic connection; thus it reports missing and is colored red.

Device Information: Your Residential Gateway's serial number and software version is reported here, as is the Residential Gateway's hardware part number, system uptime and current date and time.

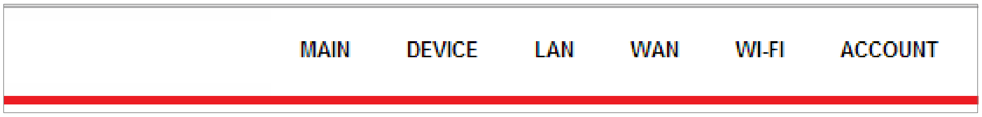
Private LAN: The status of the connected Ethernet LAN is shown, with its internal IP address, MAC address, and subnet mask. Ideally, the current status should be "Up" (the connection is working) and the ports should be enabled. If it reports "Down" then the Ethernet connection is not working.

Wi-Fi Guest: Your Residential Gateway may be equipped with a separate guest network that allows visitors to your home wireless access to the Internet without having access to the other devices on your home's network. The IP address, MAC address, and subnet mask (different from the LAN subnet) are displayed. The Wi-Fi Guest access point is delivered disabled by default and must be enabled by the user. Ideally, the current status should be "Up," the port should be enabled, and your user-defined SSID (the name you assigned to the wireless access point) will be displayed. Refer to the section titled *Configuring the Wi-Fi* for setting up these details.

## Navigation

Displayed in the header of the Main page (and all pages) are the names of the various menus. These are also referred to as the first line tabs. Clicking on these displays the configuration information and options for that particular function of your Residential Gateway.

Figure 2-6. First Line Tabs displayed in the header of each page.



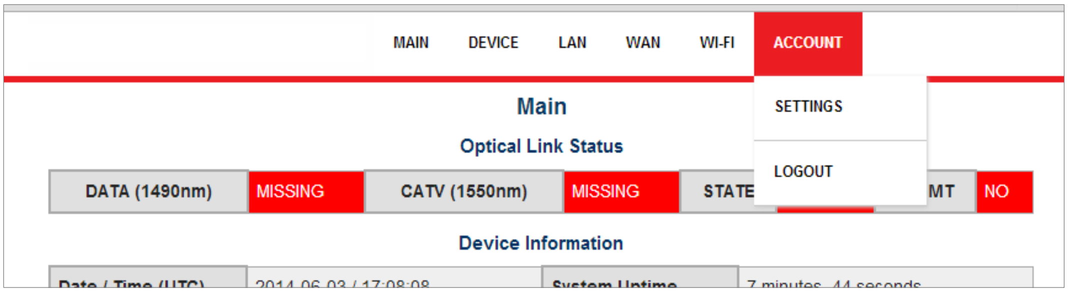
An explanation of the functionality within each of the first line tabs can be found in Table 2-2 below.

Table 2-2. First Line Tabs (menus).

| Menu | Description |
|---|---|
| MAIN | Takes you back to the Main page, where the status information for the Residential Gateway is displayed. |
| DEVICE | Displays a summary page, and allows the user to reboot/restart the system. |
| LAN | Displays the configuration information for the Ethernet and Wi-Fi portion of the Residential Gateway, and allows the user to edit it. |
| WAN | Allows user to view network settings and do some Internet connection trouble-shooting. |
| Wi-Fi | Displays configuration information for the wireless network(s) and allows the user to edit it. |
| ACCOUNT | Allows the adding and deleting of users, and changing of user names and passwords. |

Hovering the mouse over the menu name in the header will display additional sub-menus below them. In the example below, hovering over 'Account' displays the 'Settings' and 'Logout' sub-menu options.

Figure 2-7. Account hover menu.



Main

Optical Link Status

| DATA (1490nm) | MISSING | CATV (1550nm) | MISSING | STATE | | MT | NO |
|---|---|---|---|---|---|---|---|

Device Information

| Date / Time (UTC) | 2014-06-03 / 17:08:08 | System Uptime | 7 minutes, 44 seconds |
|---|---|---|---|

## Logging Out

To log out, simply click on 'Logout' on the Account sub-menu. This option is shown on the Account hover menu (refer to Figure 2-7 above). If you remain logged in without any activity, the system will automatically log you out after 30 minutes.

It is a good idea never to leave the system logged in.  Someone could come behind you during that 30 minute window and alter the settings and leave your system and/or devices non-operational.

## Getting Started

The typical tasks a user will need to do upon initial installation are as follows:

1. Log in using the admin account and change the admin password.  Refer to *Changing Your Password*.
2. If you have a wireless network, set up the Wi-Fi SSID and security protocols you wish to use.  Refer to *Wi-Fi – Private LAN*.
3. If you are setting up a guest wireless network, set up its Wi-Fi SSID and security protocols. Refer to *Wi-Fi – Wi-Fi Guest*.
4. To view or trouble-shoot your connection to the Internet, refer to *The WAN Connection* section.

# 3. USER ADMINISTRATION

The Residential Gateway can be configured to allow multiple users to log in and administer it. Each user will have a password of their choosing and will be assigned a role. User administration can be done through the 'Settings' option on the Account sub-menu.

Hover the mouse on 'Account' in the first line tab. A drop-down menu with two options as shown in Figure 2-7 above will display. Select the 'Settings' option. Using this option, you can add and delete users, change user names and change passwords.

## Changing Your Password

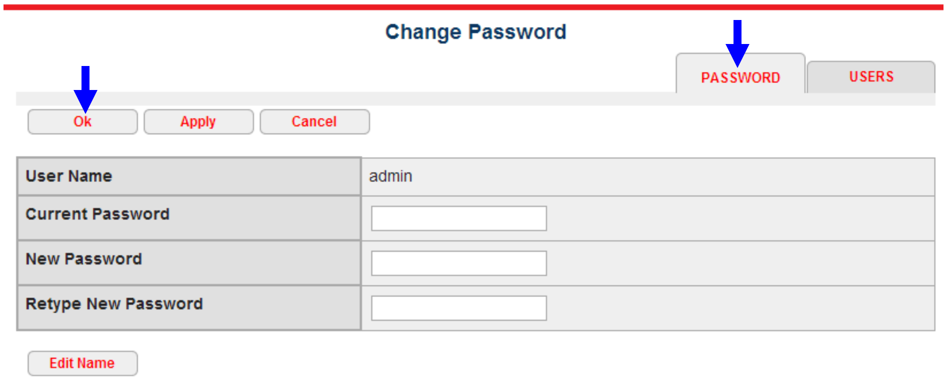
Initially, when you first log in, the only active user account is the admin account (see *Logging Into the Residential Gateway*) and you logged in with a default password (i.e., the device's serial number). It is highly recommended that you change the password for the admin account as soon as possible to safeguard your Residential Gateway from hacking and unauthorized use. To do so, follow these steps:

1. Click on the 'Settings' option on the 'Account' sub-menu.
2. Click on the 'Password' tab (highlighted in Figure 3-1 below) in the upper right.
3. The currently logged in user name will be displayed – in this case, admin. Refer to the screen shown in Figure 3-1 below.
   - Enter the current password. If this is your first log in, it will be the default password (i.e., the serial number of your Residential Gateway).
   - In the next field, enter a new password (see *Password Tips* below). The password will not display on the screen as you type it, in order to prevent others from seeing it.
   - In the next field, re-type the new password. This is necessary since you cannot see the characters echoed back on the screen as you typed them. Both password entries must match *exactly*.
4. When all fields have been entered, click on the 'OK' button (highlighted in Figure 3-1 below) or 'Apply' button in the upper left.

Note: When you click 'Apply' your screen remains on the same page. When you click 'OK' you are taken back to the former page or Main page, so you can begin a new task. Either way, the change in password will take effect the next time you log in. If you decide not to change the password, you can click 'Cancel' and the change will not take effect (*provided* you have not already clicked 'Apply').

After you have reset the password for the admin account, you can set up additional user accounts (refer to *Adding Users* below). From time to time, it is a good idea to change passwords to prevent hacking and unauthorized access.

**Figure 3-1. Change Password screen.**



| | |
|---|---|
| User Name | admin |
| Current Password | |
| New Password | |
| Retype New Password | |

### Password Tips

1. Passwords must be a minimum of 8 characters, and ideally should contain numbers as well as letters (the best passwords include special characters, too!), and are not easy to guess. For example, your birthdate or a pet's name would not be ideal passwords. You may also use a pass phrase of up to 64 characters, which contains spaces and other punctuation. For example, "Red cars go FAST!" or something meaningful to you that would be easy to remember.
2. Once you have changed the password, write it down some place you will be sure to remember. Lost passwords cannot be recovered and can only be reset to the factory default by your service provider. However, resetting to the factory default will also wipe out all of your other configurations on the device.
3. Each user can only change his/her own password. Although the admin user can add additional users to the system and in so doing, sets an initial password (refer to the *Adding Users* section), the admin user cannot change another user's password. The user must log in with their initial password and then can change their password, following the steps listed here.

## Adding Users

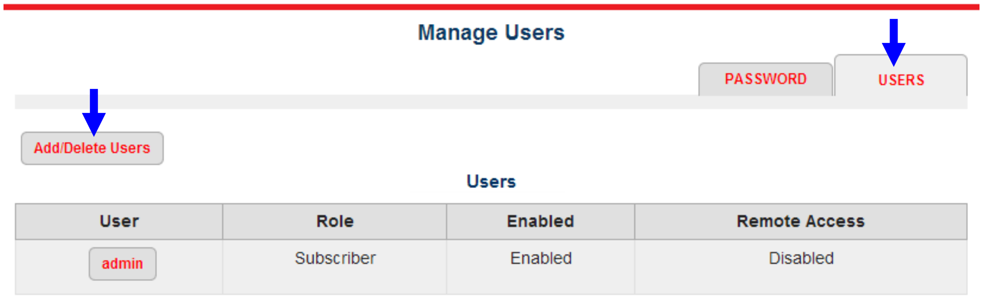
If you want additional users – other than the admin account – to be able to manage the Residential Gateway, set up a separate login and password for each of them. To do so, follow these steps:

1. Hover over 'Account' in the first line tabs, and select 'Settings' from the sub-menu.
2. Click on the 'Users' tab (highlighted in Figure 3-2 below) in the upper right.
3. The Manage Users screen will display as shown in Figure 3-2.

In the example below, there is only the single admin account already set up. If you had other users, their user names would also display in the grid. The grid also shows each user's role, whether the user has been enabled, and whether the user has been granted remote access capabilities.

At any time while on the Manage Users screen, you can click on the button displaying the user name to see a detailed view of that user, including being able to change the user's status. Refer to *Change User Settings*.

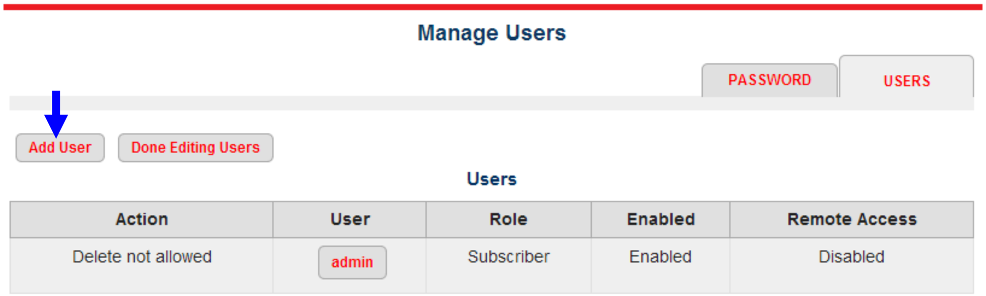
Figure 3-2. Manage Users screen.



| User | Role | Enabled | Remote Access |
|---|---|---|---|
| admin | Subscriber | Enabled | Disabled |

To add a user, click on the 'Add/Delete Users' button (highlighted in  Figure 3-2 above) in the upper left.  The Manage Users screen now displays with Add/Delete capabilities as shown in Figure 3-3 below.  Note that the admin account cannot be deleted at this point, since it is the only user account.  However, if you had already set up other users on the system, they would show with the delete option in the grid (refer to *Deleting Users* section).

Figure 3-3. Add/Delete Users screen.



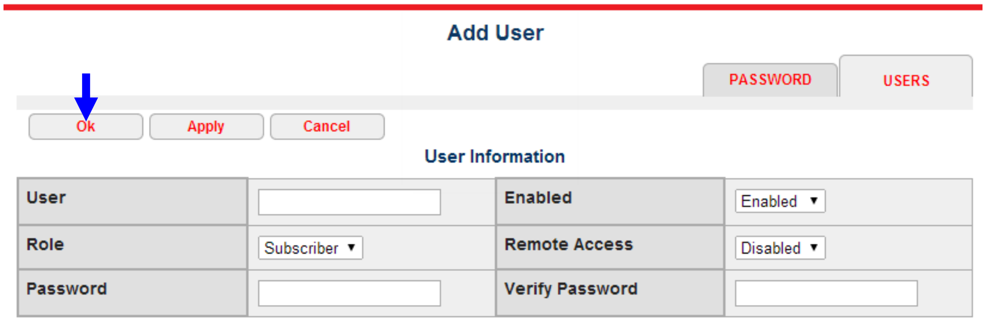
| Action | User | Role | Enabled | Remote Access |
|---|---|---|---|---|
| Delete not allowed | admin | Subscriber | Enabled | Disabled |

At any time while on the Add/Delete Users screen, you can click on the button displaying the user name to see a detailed view of that user, including being able to change the user's status. Refer to *Change User Settings*.

*Note that initially, since the admin account is the only account in the system, you cannot delete it!  See Deleting Users for further details.*

To add a user, click on the 'Add User' button (highlighted in Figure 3-3 above) in the upper left. The Add User detail screen will display as shown in Figure 3-4 below.

**Figure 3-4. Add User detail screen.**



User Information

| | | | |
|---|---|---|---|
| User | | Enabled | Enabled ▾ |
| Role | Subscriber ▾ | Remote Access | Disabled ▾ |
| Password | | Verify Password | |

## The Add User Screen

Fill in the required information on the Add User screen:

User: Enter a unique user name. Some names – like "admin" – may already be in use by the system even though they are not displayed in the list of users (some system names are hidden). If you try to assign a new user one of these system names, or another user name already in use, it will tell you that it is not unique and you can try again with a new name. User names must be at least 3 characters in length, and no more than 64 characters long.

Enabled: Select either "Enabled" or "Disabled" from the list. Only enabled users will be able to log into the system. The system will lock out all disabled users.

Whether a user is enabled or disabled has nothing to do with the user's Internet access. It only applies to the ability to login and manage the Residential Gateway through this management software. For example, a user may be disabled here but may still access the Internet, TV, or phone through any devices that are plugged into the Residential Gateway.

Role: The role of a user dictates what menus and functions they have access to. As a subscriber, the only other users you may add are other subscribers or "lower" roles (i.e., roles that have more restrictive access). The list of roles you may assign to a user will display when you click on the small down arrowhead in this field.

Remote Access: Select either "Enabled" or "Disabled" from the list. Only enabled users will be able to log into the system remotely from a device that is not directly plugged into it. For example, suppose you had the ability to log into your home network while at work (using a computer on your employer's network). In order to deter would-be hackers from breaking into your home network, it is highly suggested that you *not* grant remote access to your device to anyone, including the admin account.

Password: Enter a password for this new user following the previously stated *Password Tips*. The user will log into the Residential Gateway with this password, but will be able to change their password if they desire after that (refer to *Changing Your Password*). Ideal passwords or pass phrases contain a mixture of letters, numbers, and special characters, and are between 8 and 64 characters in length. The password will not display on the screen as you type it, in order to prevent others from seeing it.

Verify Password: Re-type the password you just typed in the previous field. This is necessary since you cannot see the characters echoed back on the screen as you typed them. Both the 'Password' and the 'Verify Password' entries must match exactly.

*Saving the New User entry*
When you have completed the above entries, click on either the ‘Apply’ button or the ‘OK’ button at the top left of the screen. When you click ‘Apply’ your screen remains on the same page. When you click ‘OK’ you are taken back to the former page (the Manage Users screen), so you can begin a new task. Either way, the new user you just created is now immediately effective.

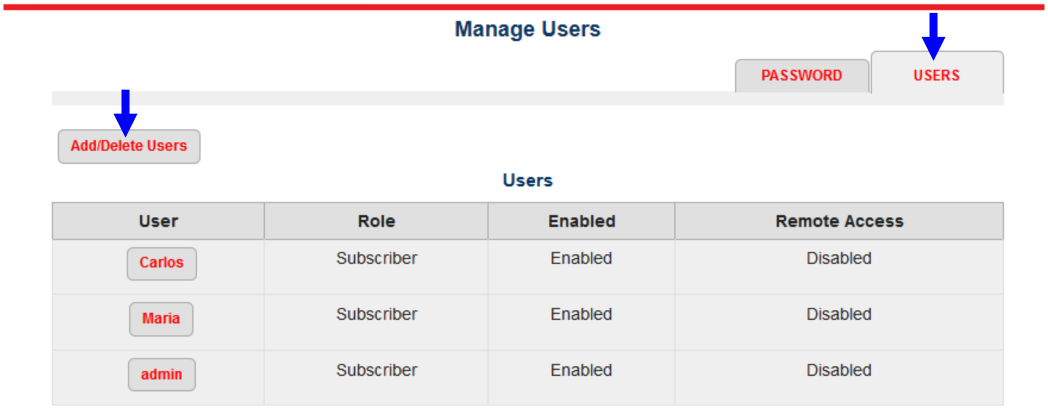
*Discarding the New User entry*
If you decide not to add this user, or want to “start over” without saving your changes, you can click the ‘Cancel’ button at the top left of the screen and the new user will not be added (provided you have not already clicked ‘Apply’).

## Deleting Users

If you want delete an existing user, and are starting from the Main page, follow these steps:

1. From the ‘Account’ menu, select ‘Settings’.
2. Click on the ‘Users’ tab (highlighted in Figure 3-5).
3. On the Manage Users screen you will see a grid containing the list of users configured in the system (see example in Figure 3-5 below). In addition to the user name, the grid also shows each user’s role, whether the user has been enabled, and whether the user has been granted remote access capabilities.

**Figure 3-5. Manage Users screen.**



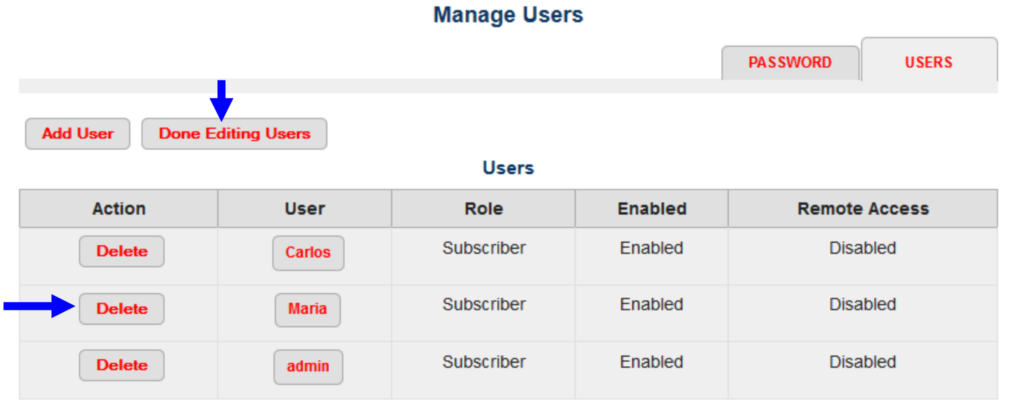
Users

| User | Role | Enabled | Remote Access |
|---|---|---|---|
| Carlos | Subscriber | Enabled | Disabled |
| Maria | Subscriber | Enabled | Disabled |
| admin | Subscriber | Enabled | Disabled |

At any time while on the Manage Users screen, you can click on the button displaying the user name to see a detailed view of that user, including being able to change the user’s status. Refer to *Change User Settings*.

To delete a user, click on the ‘Add/Delete Users’ button (highlighted in Figure 3-5 above) in the upper left. The Manage Users screen now displays with delete capabilities as shown in Figure 3-6 below.

Figure 3-6. Delete Users screen.



Users

| Action | User | Role | Enabled | Remote Access |
|---|---|---|---|---|
| Delete | Carlos | Subscriber | Enabled | Disabled |
| Delete | Maria | Subscriber | Enabled | Disabled |
| Delete | admin | Subscriber | Enabled | Disabled |

Find the user name you want to delete. Then click on the 'Delete' button to the left of that user name. In the example in Figure 3-6, we would click on the 'Delete' button highlighted (see arrow) in order to remove the user Maria. Once deleted, all details of that user are removed from the Residential Gateway, the user will no longer show up in the list/grid, and the user will no longer be able to log in.

⚠ *Do not delete the last (or only) enabled subscriber account! Initially, since there is only an admin account defined, you cannot delete the admin account. But if you created another user account (for example, "Carlos") and disabled the admin account, and later deleted the Carlos account, you would no longer be able to log in.*

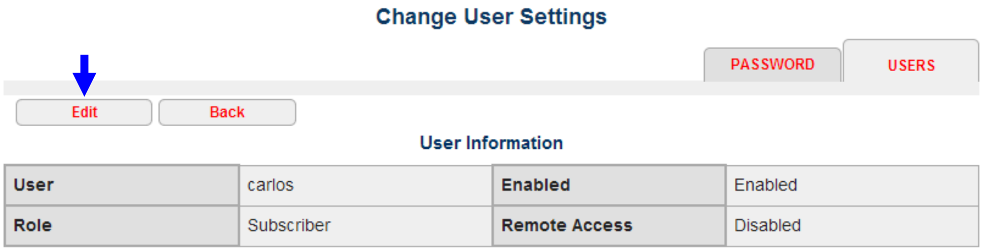
At any time while on the Delete Users screen, you can click on the button displaying the user name to see a detailed view of that user, including being able to change the user's status. Refer to *Change User Settings*.

When you have finished making the deletions, click on the 'Done Editing Users' button in the upper left, highlighted in Figure 3-6.

## Change User Settings

User settings include a user's role, enabled/disabled status, and remote access capabilities. Many of the screens throughout the various user administration functions offer access to the Change User Settings screen (see 'Manage User' screen throughout the *Adding Users* and *Deleting Users* sections above). Any time you click on the user name when it is shown as a "button," you will see the Change User Settings screen. See example in Figure 3-7 below.

**Figure 3-7. Change User Settings screen.**



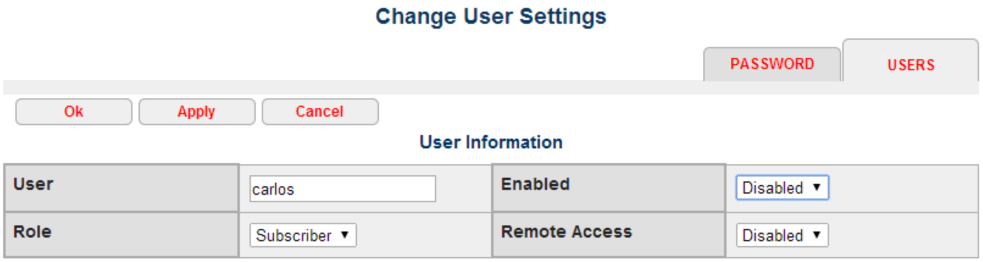
Change User Settings

User Information

| | | | |
|---|---|---|---|
| User | carlos | Enabled | Enabled |
| Role | Subscriber | Remote Access | Disabled |

Initially, this screen is displayed in view-only mode (editable fields are greyed out). You can return to the previous screen by clicking the ‘Back’ button, or you can open this screen in edit mode by clicking the ‘Edit’ button in the upper left (highlighted in Figure 3-7). When opened in edit mode, the editable fields will no longer be greyed out as shown below in Figure 3-8.

**Figure 3-8. Change User Settings screen – Edit mode.**



Change User Settings

User Information

| | | | |
|---|---|---|---|
| User | carlos | Enabled | Disabled ▾ |
| Role | Subscriber ▾ | Remote Access | Disabled ▾ |

Edit any of the fields on the Change User Settings as required:

User: Edit the user name. This can also be done via the *Change/Edit Name* function (discussed below).

Enabled: Select either “Enabled” or “Disabled” from the list. Disabled users can no longer log into the system. However unlike deleted users, disabled users still show up in user lists/grids and can be easily re-enabled.

Whether a user is enabled or disabled has nothing to do with the user’s Internet access. It only applies to the ability to login and manage the Residential Gateway through this management software. For example, a user may be disabled here but may still access the Internet, TV, or phone through any devices that are plugged into the Residential Gateway.

Role: Based on the role of the currently-logged in user, you can only assign other users to a similar or “lower” role (i.e., roles that have more restrictive access). The list of roles you may assign to a user will display when you click on the small down arrowhead in this field.

Remote Access: Select either “Enabled” or “Disabled” from the list. Only enabled users will be able to log into the system remotely from a device that is not directly plugged into it. In order to deter would-be hackers from breaking into your home network, it is highly suggested that you *not* grant remote access to anyone, including the admin account.

*Saving the Changed Settings*

When you have completed the above changes, click on either the ‘Apply’ button or the ‘OK’ button at the top left of the screen. When you click ‘Apply’ your screen remains on the same page. When you click ‘OK’ you are taken back to the former page, so you can begin a new task. Either way, the changes you made are immediately effective.

*Discarding the Changes*

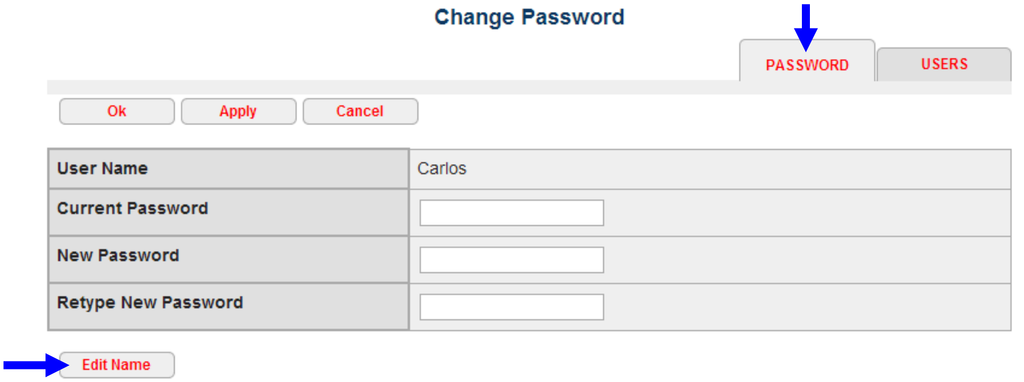
If you decide not to make any changes, or want to “start over” without saving any changes you already made, you can click the ‘Cancel’ button at the top left of the screen and the changes will not take effect (provided you have not already clicked ‘Apply’).

## Change/Edit User Name

Changing your user name is similar to changing your password. To change your user name using this feature, you must log in with the existing user name you wish to change. To do so follow these steps:

1. Click on the ‘Settings’ option on the ’Account’ menu.
2. Click on the ‘Password’ tab (highlighted in Figure 3-9 below) in the upper right.
3. The currently logged in user name will be displayed – in this example, Carlos. Refer to the screen shown in Figure 3-9 below.
4. Click on the ‘Edit Name’ button below the data entry fields (highlighted in Figure 3-9 below).

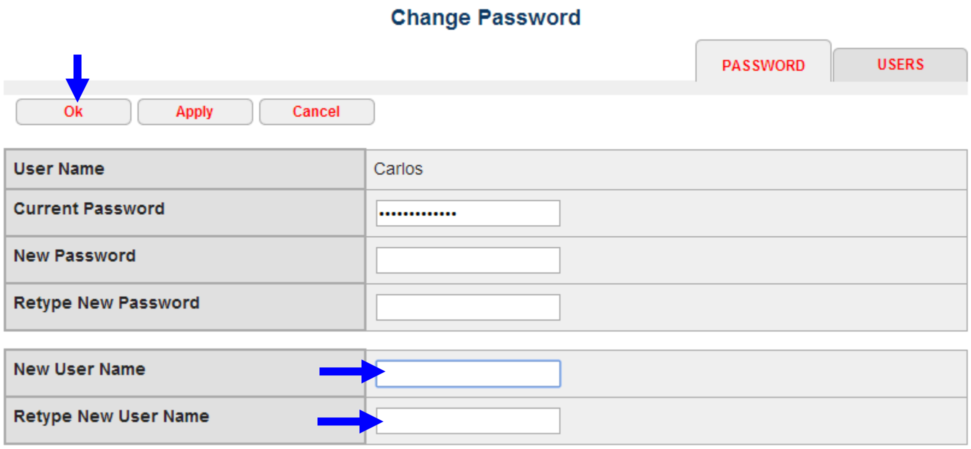
**Figure 3-9. Change Password screen – Edit Name functionality.**



| | |
|---|---|
| User Name | Carlos |
| Current Password | |
| New Password | |
| Retype New Password | |

Additional fields will display below the password screen to allow you to enter the new user name, as shown in Figure 3-10 below.

**Figure 3-10. Edit Name screen.**



Change Password

| | |
|---|---|
| User Name | Carlos |
| Current Password | ••••••••••••• |
| New Password | |
| Retype New Password | |
| New User Name | |
| Retype New User Name | |

Enter the new user name (see field marked with arrow in Figure 3-10). In the next field re-enter the new user name. Both user name entries must match *exactly*. Click on the 'OK' button (highlighted in Figure 3-10) or 'Apply' button in the upper left. When you click 'Apply' your screen remains on the same page. When you click 'OK' you are taken back to the former page or Main page, so you can begin a new task. Either way, the new name will take effect immediately.

User names must be between 3 and 64 characters in length. The next time you log in, remember to do so using the new user name, as the former one will no longer work. All the former settings will "follow along" and the new name will now be displayed in user lists/grids.

If you decide not to change the user name, you can click the 'Cancel' button and the change will not take effect (*provided* you have not already clicked 'Apply').

# 4. CONFIGURING THE LAN

The word “LAN” which stands for Local Area Network refers to your internal home network. This section provides information on how to configure your Residential Gateway to work with your home’s Ethernet and wireless devices. There are essentially two networks – one wired and one wireless – that are bridged together. This enables wired and wireless devices to communicate with each other on the same subnet. Wired devices include items such as a PC plugged into an Ethernet port (or Ethernet hub) on your Residential Gateway. Wireless devices include items such as a SmartPhone or wireless printer that communicate using one of the 802.11 protocols.

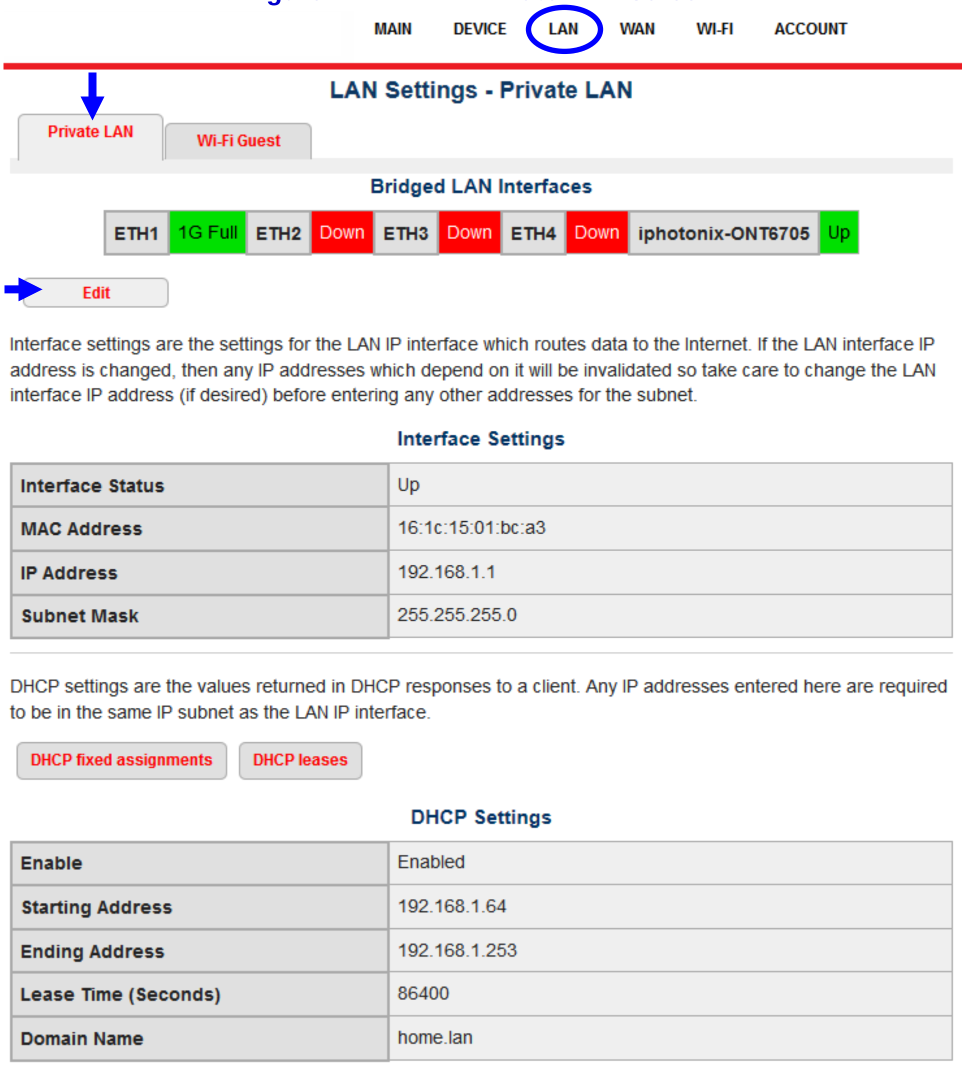
Be sure the wireless and LAN devices you wish to connect are powered up prior to configuring your Residential Gateway.

## The Private LAN Page

To access your home’s LAN interface, follow these steps:

1. From the Main page, click on ‘LAN’ in the first line tabs.
2. Click on the ‘Private LAN’ tab (highlighted in Figure 4-1 below) in the upper left.
3. A three-part screen will be displayed, similar to that shown in Figure 4-1.

**Figure 4-1. LAN - Private LAN screen.**



LAN Settings - Private LAN

Bridged LAN Interfaces

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ETH1 | 1G Full | ETH2 | Down | ETH3 | Down | ETH4 | Down | iphotonix-ONT6705 | Up |

Interface settings are the settings for the LAN IP interface which routes data to the Internet. If the LAN interface IP address is changed, then any IP addresses which depend on it will be invalidated so take care to change the LAN interface IP address (if desired) before entering any other addresses for the subnet.

Interface Settings

| | |
|---|---|
| Interface Status | Up |
| MAC Address | 16:1c:15:01:bc:a3 |
| IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |

DHCP settings are the values returned in DHCP responses to a client. Any IP addresses entered here are required to be in the same IP subnet as the LAN IP interface.

DHCP Settings

| | |
|---|---|
| Enable | Enabled |
| Starting Address | 192.168.1.64 |
| Ending Address | 192.168.1.253 |
| Lease Time (Seconds) | 86400 |
| Domain Name | home.lan |

The three sections of this screen are discussed individually below.

## Bridged LAN Interfaces

The first section of this screen reports the status of the bridged LAN interfaces. Up to four Ethernet ports and one wireless access point are bridged to comprise your “private LAN”. Note: Depending on your model of Residential Gateway, you may have a different number of ports available.

This section is view-only and cannot be edited. The status of each port is displayed in words – ‘Up’ or ‘Down’ – as well as in color:

- Green means the connection is working.
- Yellow means the connection may be working (if it says ‘Up’) but that it is not achieving high speeds – for example, the device may only be functioning at 10Mbps or 100Mbps, instead of at maximum possible speeds (in the Gbps range). This may be because the network card in the device is not rated for higher speeds.

- Red means the connection is missing (not plugged into any device) or is not working.

### Interface Settings

The middle section of the screen displays more detail about the LAN interface, including its status, MAC address, IP address, and subnet mask. The IP address shown here is the IP address that all client devices on your private LAN will use to gain access to the Internet. As the instructions on the screen state, be sure to change this IP address first (if necessary), before configuring any client devices. Refer to *Editing the LAN Settings*.

### DHCP Settings

Your Residential Gateway acts as a DHCP server, which means it can automatically assign individual unique IP addresses to each device on your network. This section of the screen displays:

- the status of the DHCP server (whether it is enabled or disabled),
- the starting IP address it will use when assigning IP addresses to each client device,
- the ending IP address that can be used,
- the length of time a device may keep the same IP address before it will be “recycled,”
- and the domain name for your private LAN.

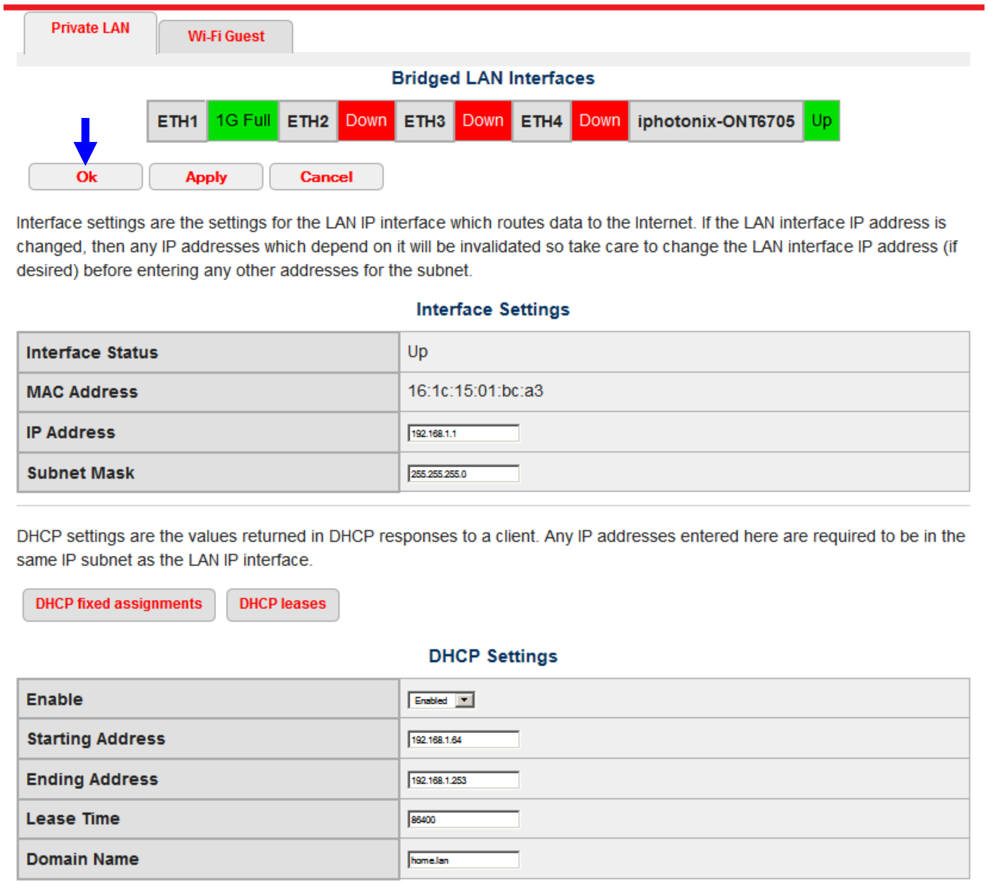
To edit any of these settings, refer to *Editing the LAN Settings* below.

### Editing the LAN Settings

To make changes in the Interface Settings or DHCP Settings, click on the ‘Edit’ button (highlighted in Figure 4-1 above). The screen shown in Figure 4-2. will display. You can edit the Interface IP address and subnet mask, if needed, and also each of the DCHP settings, if needed. *Generally, the default values or values provided by your service provider do not require editing.*

⚠ If you are not familiar with the configuration details in this section, contact your service provider before changing the default settings of your Residential Gateway.

**Figure 4-2. LAN - Private LAN screen in Edit mode.**



Bridged LAN Interfaces

| ETH1 | 1G Full | ETH2 | Down | ETH3 | Down | ETH4 | Down | iphotonix-ONT6705 | Up |
|---|---|---|---|---|---|---|---|---|---|

Interface settings are the settings for the LAN IP interface which routes data to the Internet. If the LAN interface IP address is changed, then any IP addresses which depend on it will be invalidated so take care to change the LAN interface IP address (if desired) before entering any other addresses for the subnet.

Interface Settings

| | |
|---|---|
| Interface Status | Up |
| MAC Address | 16:1c:15:01:bc:a3 |
| IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |

DHCP settings are the values returned in DHCP responses to a client. Any IP addresses entered here are required to be in the same IP subnet as the LAN IP interface.

DHCP Settings

| | |
|---|---|
| Enable | Enabled |
| Starting Address | 192.168.1.64 |
| Ending Address | 192.168.1.253 |
| Lease Time | 86400 |
| Domain Name | home.lan |

*Interface Settings:*

The Interface Status and MAC Address are not editable (view-only).

IP Address: Enter an IP address, or use the default (recommended).

Subnet Mask: Enter the subnet mask, or use the default (recommended).

*DHCP Settings:*

Enable: If you want to allow your Residential Gateway to act as a DHCP server, select "Enable" (recommended). If not, select "Disable."

Starting Address: Enter a starting IP address. The system will begin making IP assignments to devices on your network starting with this IP address. It should not overlap with the IP address used for the Interface Settings. Using the default value is recommended.

Ending Address: Enter an ending IP address. It must be within the same subnet as the Starting Address, and must allow for the maximum number of devices you may have on your network at any given time. Using the default value is recommended.

Lease Time: This is the length of time in seconds that a client device may keep an IP address before it is recycled (goes back into the IP pool). When a device on the network is turned off and the lease time has expired, then when the device is again turned on (booted) it may be assigned a different IP address from the pool from the one it had earlier.

However, as long as the device remains on, it will keep the same IP address even if the lease time has expired; it will merely renew that lease automatically. Additionally, if the Residential Gateway itself is rebooted, all new leases will be assigned to all devices. All of this happens transparently to user. Having long lease durations decreases network traffic and is ideal for networks that don't have many transient users coming in and going out. Using the default value is recommended.

Domain Name: Enter the name you want to assign to your network domain, being sure to adhere to Network Naming Rules below. Example (the default): home.lan

Network Naming Rules: A domain name, often referred to as a DNS (domain name system), is a way to be able to refer to your network with a name rather than an IP address. A domain name can be descriptive for your residence if you choose. However, it must conform to the rules below:

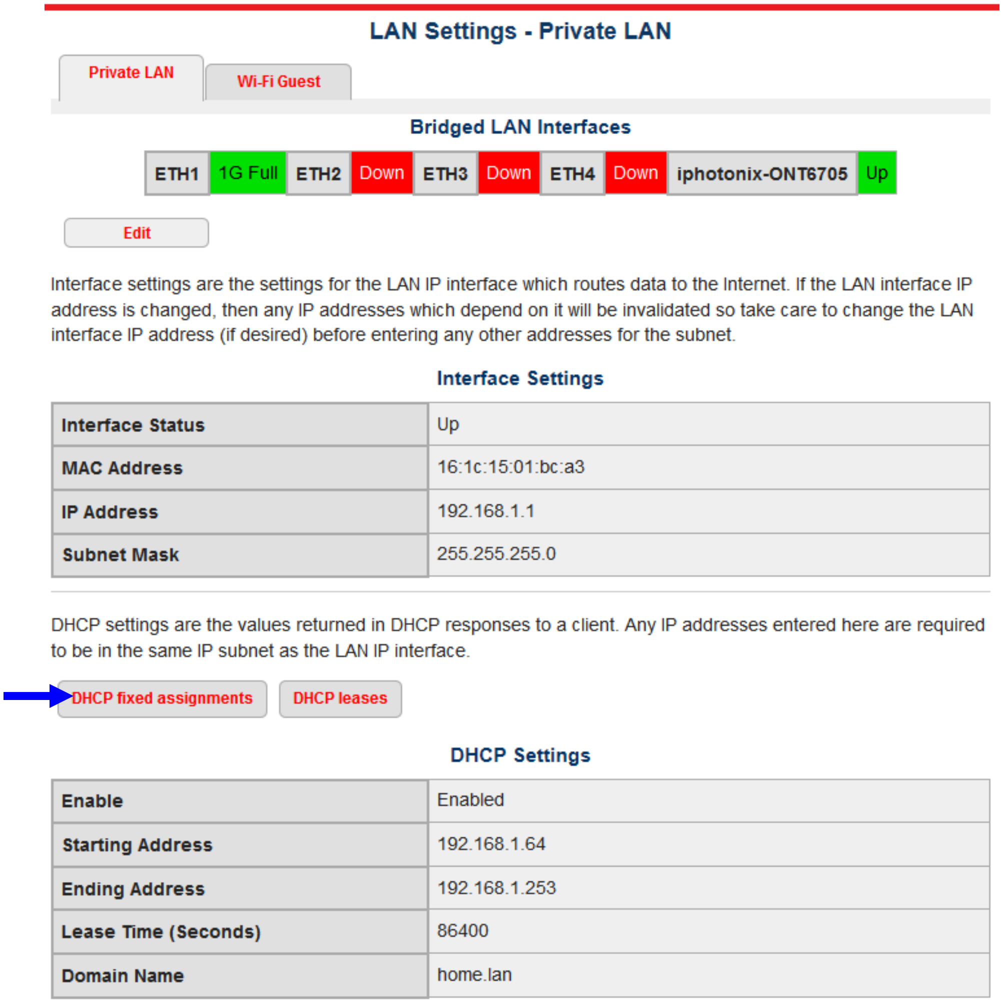
- Use only letters in the alphabet (a through z, and A through Z) or numbers (0 through 9) or a hyphen (-).
- It must be at least 3 characters long and must not exceed 63 characters in length.
- It cannot be comprised solely of numbers. It cannot begin or end with a hyphen. It must not have any spaces.
- It should have a dot/period (.) followed by at least two more characters.

After you have made changes to the Interface Settings and DHCP Settings, click 'OK' (highlighted in Figure 4-2 above) or 'Apply' to save your changes. When you click 'Apply' your screen remains on the same page and you can continue making edits. When you click 'OK' you are taken back to the former page, so you can begin a new task. If you decide not to make any changes or to discard the changes you made, you can click the 'Cancel' button and the changes will not take effect (*provided* you have not already clicked 'Apply').

## Configuring Static IP Addresses

In some cases, you may have a client device that needs to have a fixed IP address all the time, and not have its lease expire or its IP address "recycled." This is called a static IP address because it will never change. To configure this, access the Private LAN screen as shown above, and click on 'DHCP fixed assignments' in the DHCP Settings portion of the screen (highlighted in Figure 4-3 below).

**Figure 4-3. LAN - Private LAN screen.**



LAN Settings - Private LAN

Bridged LAN Interfaces

| ETH1 | 1G Full | ETH2 | Down | ETH3 | Down | ETH4 | Down | iphotonix-ONT6705 | Up |
|---|---|---|---|---|---|---|---|---|---|

Interface settings are the settings for the LAN IP interface which routes data to the Internet. If the LAN interface IP address is changed, then any IP addresses which depend on it will be invalidated so take care to change the LAN interface IP address (if desired) before entering any other addresses for the subnet.

Interface Settings

| | |
|---|---|
| Interface Status | Up |
| MAC Address | 16:1c:15:01:bc:a3 |
| IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |

DHCP settings are the values returned in DHCP responses to a client. Any IP addresses entered here are required to be in the same IP subnet as the LAN IP interface.

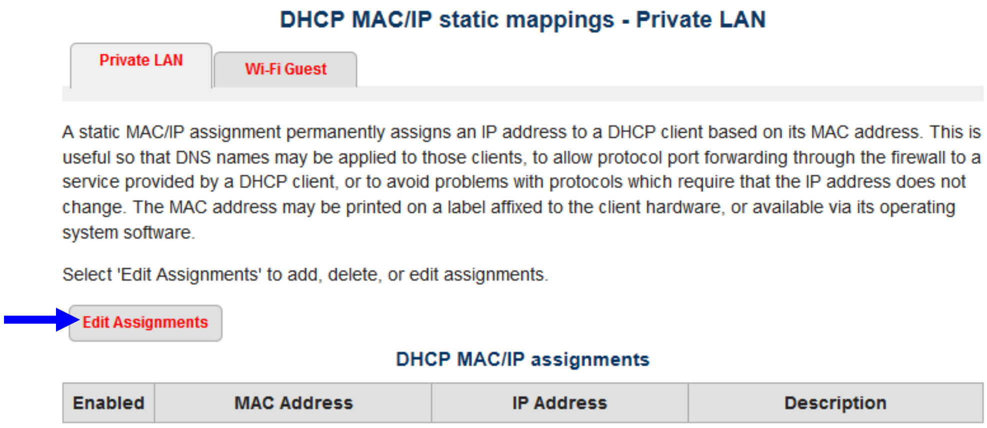
DHCP Settings

| | |
|---|---|
| Enable | Enabled |
| Starting Address | 192.168.1.64 |
| Ending Address | 192.168.1.253 |
| Lease Time (Seconds) | 86400 |
| Domain Name | home.lan |

## DHCP Fixed Assignments

You can assign a static (permanent) IP address to a client device on your network based on its MAC address. When you click on ‘DHCP fixed assignments,’ you will see the list of static IP addresses that have already been assigned. Initially, there will not be any DHCP fixed assignments configured and your screen may look similar to Figure 4-4 below.

**Figure 4-4. DHCP Static Mapping screen.**



DHCP MAC/IP static mappings - Private LAN

A static MAC/IP assignment permanently assigns an IP address to a DHCP client based on its MAC address. This is useful so that DNS names may be applied to those clients, to allow protocol port forwarding through the firewall to a service provided by a DHCP client, or to avoid problems with protocols which require that the IP address does not change. The MAC address may be printed on a label affixed to the client hardware, or available via its operating system software.

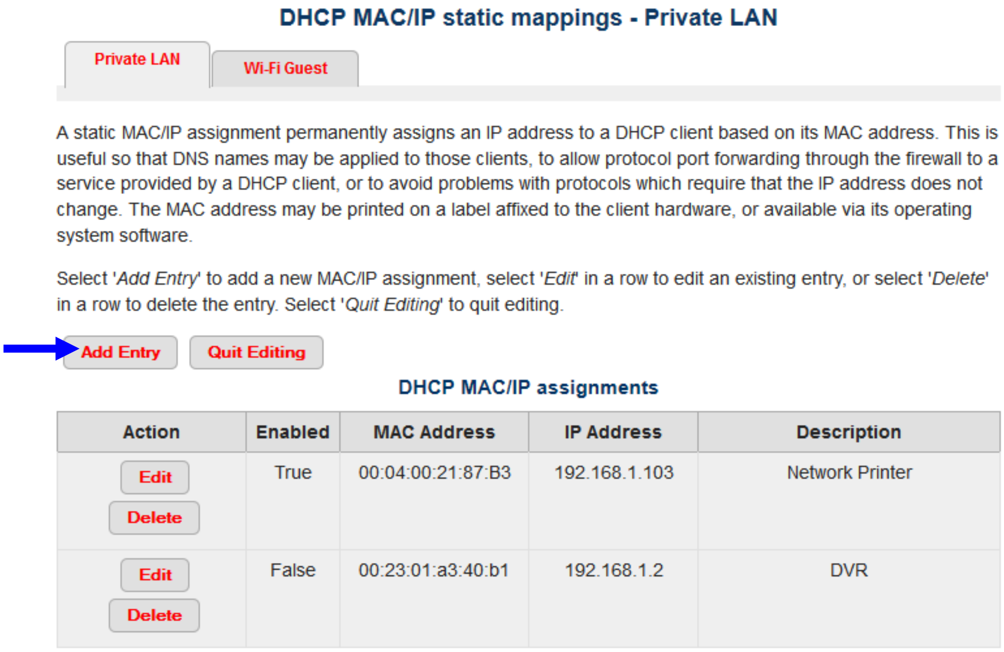
Select 'Edit Assignments' to add, delete, or edit assignments.

DHCP MAC/IP assignments

| Enabled | MAC Address | IP Address | Description |
|---|---|---|---|

To add a new fixed assignment, click on ‘Edit Assignments’ (highlighted in Figure 4-4 above). A new screen, shown in Figure 4-5 below will be displayed. If there were any assignments previously made, they would be displayed in the grid; if not, this grid may be blank.

**Figure 4-5. DCHP Static Mapping screen – Edit mode.**
*(Example: Two fixed assignments displayed.)*



DHCP MAC/IP static mappings - Private LAN

A static MAC/IP assignment permanently assigns an IP address to a DHCP client based on its MAC address. This is useful so that DNS names may be applied to those clients, to allow protocol port forwarding through the firewall to a service provided by a DHCP client, or to avoid problems with protocols which require that the IP address does not change. The MAC address may be printed on a label affixed to the client hardware, or available via its operating system software.

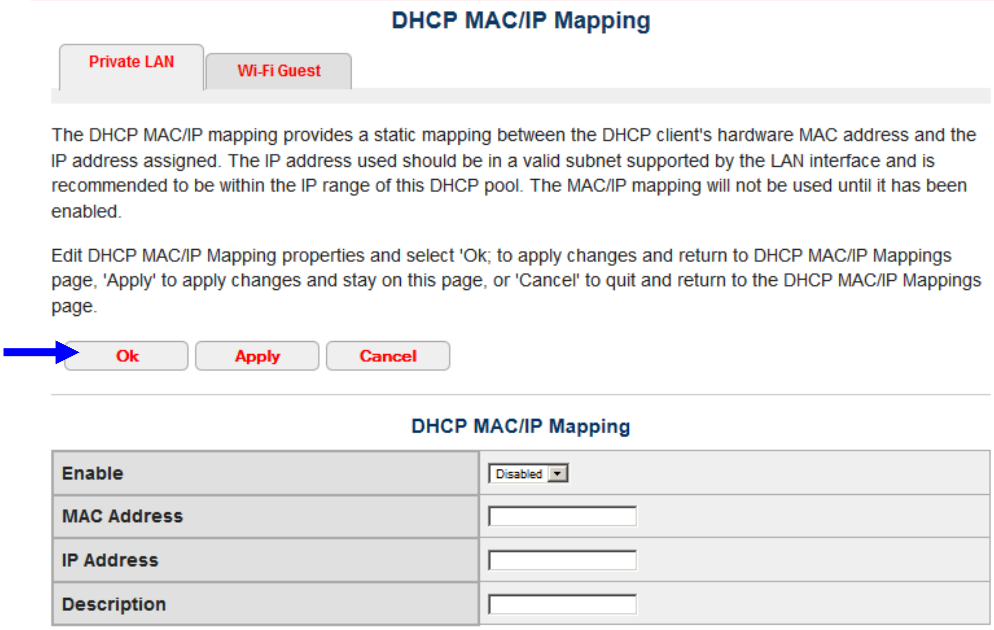
Select '*Add Entry*' to add a new MAC/IP assignment, select '*Edit*' in a row to edit an existing entry, or select '*Delete*' in a row to delete the entry. Select '*Quit Editing*' to quit editing.

DHCP MAC/IP assignments

| Action | Enabled | MAC Address | IP Address | Description |
|---|---|---|---|---|
| Edit<br>Delete | True | 00:04:00:21:87:B3 | 192.168.1.103 | Network Printer |
| Edit<br>Delete | False | 00:23:01:a3:40:b1 | 192.168.1.2 | DVR |

To add a fixed IP address, click ‘Add Entry’ (highlighted in Figure 4-5 above). The data entry screen shown in Figure 4-6 will be displayed.

Figure 4-6. DHCP Static Mapping screen - Data Entry mode.



DHCP MAC/IP Mapping

The DHCP MAC/IP mapping provides a static mapping between the DHCP client's hardware MAC address and the IP address assigned. The IP address used should be in a valid subnet supported by the LAN interface and is recommended to be within the IP range of this DHCP pool. The MAC/IP mapping will not be used until it has been enabled.

Edit DHCP MAC/IP Mapping properties and select 'Ok; to apply changes and return to DHCP MAC/IP Mappings page, 'Apply' to apply changes and stay on this page, or 'Cancel' to quit and return to the DHCP MAC/IP Mappings page.

DHCP MAC/IP Mapping

| | |
|---|---|
| Enable | Disabled |
| MAC Address | |
| IP Address | |
| Description | |

*DHCP MAC/IP Mapping fields:*

Enable: Select whether you want to enable or disable this MAC/IP mapping. If you enable it, it becomes a static IP address. If you disable it, it reverts back to the DHCP pool of addresses.

MAC Address: Enter the MAC address of the client device whose IP address you want to remain static. The MAC address may be found on a sticker on the back of the client device or it may be accessible via the client's operating system software. Generally, it is comprised of numbers and letters written in 6 sets of two, with each set separated by a colon (for example: 00:12:0A:9D:40:B2). However, it may be printed as just a 12-character alphanumeric string on your particular device.

IP Address: Enter the fixed IP address you want to assign to this device. Keep in mind, the IP address must be within the Private LAN subnet. Refer to Figure 4-2, under *DHCP Settings*, the fields *Starting Address* and *Ending Address*. The IP address you enter here must be a number between these starting and ending addresses.

Description: Enter a word or phrase describing this device. This is helpful so you can pick it out in a grid displaying the fixed IP assignments (refer to Figure 4-5) if you need to edit it at a later date.

When you have finished your edits, click on 'OK' (highlighted in Figure 4-6 above) or 'Apply' to save. When you click 'Apply' your screen remains on the same page and you can continue making edits. When you click 'OK' you are taken back to the former page. If you decide not to make any changes or to discard the changes you made, you can click the 'Cancel' button and the changes will not take effect (provided you have not already clicked 'Apply').

Once back at the DHCP Mapping screen (see Figure 4-5), you can:

- Add additional static IP entries by clicking on 'Add Entry' (highlighted in Figure 4-5).
- Delete an existing fixed assignment by clicking on 'Delete' in the corresponding row in the

grid. That row and the static MAC/IP Mapping will be removed from the system.

- Edit an existing fixed assignment by clicking on 'Edit' in the corresponding row in the grid. The data entry screen will then display (see Figure 4-6), where you can edit any of the fields.

When you are finished making all necessary additions/edits/deletions, click on 'Done Editing DHCP MAC/IP Assignments' and you will be returned to the starting Private LAN screen.

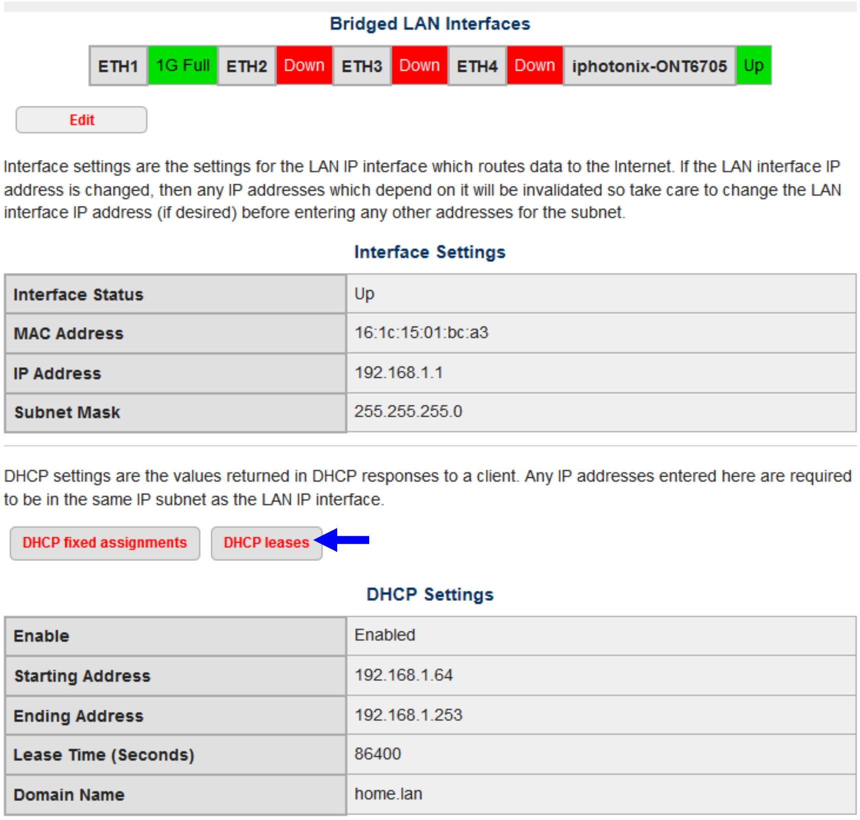
## DHCP Leases

Your Residential Gateway acts as a DHCP server, and will automatically assign each device on your network a unique IP address as it is added or booted up on the network. But the IP address is only leased for a fixed length of time. After that time, the next time that device is turned on, it might be assigned a different IP address from what it had previously. You may configure the lease length to make it a shorter or longer length of time (refer to *Lease Time* above); however the default value rarely needs to be edited.

To view the current leases on your network, follow these steps:

1. From the Main page, click on 'LAN' in the first line tabs.
2. Click on the 'Private LAN' tab in the upper left.
3. A three-part screen will be displayed, similar to that shown in Figure 4-7. In the lower section on DHCP Settings, click on the 'DHCP Leases' button (highlighted in Figure 4-7 below).

**Figure 4-7. LAN - Private LAN screen.**



Bridged LAN Interfaces

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ETH1 | 1G Full | ETH2 | Down | ETH3 | Down | ETH4 | Down | iphotonix-ONT6705 | Up |

Interface settings are the settings for the LAN IP interface which routes data to the Internet. If the LAN interface IP address is changed, then any IP addresses which depend on it will be invalidated so take care to change the LAN interface IP address (if desired) before entering any other addresses for the subnet.

Interface Settings

| | |
|---|---|
| Interface Status | Up |
| MAC Address | 16:1c:15:01:bc:a3 |
| IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |

DHCP settings are the values returned in DHCP responses to a client. Any IP addresses entered here are required to be in the same IP subnet as the LAN IP interface.

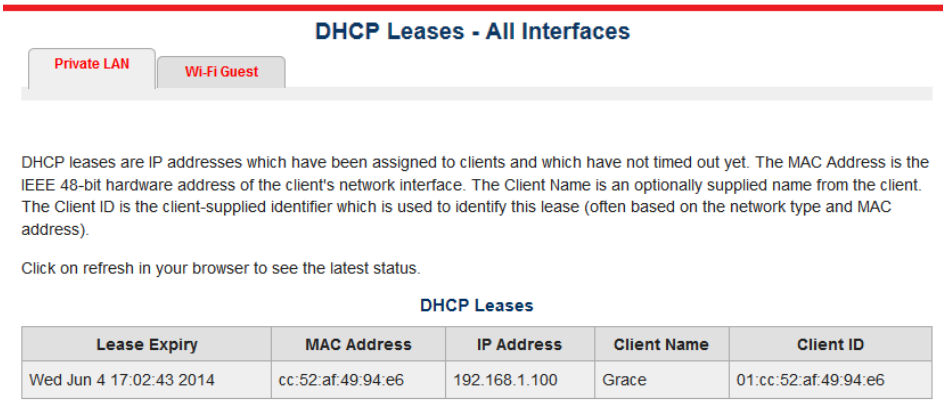
DHCP Settings

| | |
|---|---|
| Enable | Enabled |
| Starting Address | 192.168.1.64 |
| Ending Address | 192.168.1.253 |
| Lease Time (Seconds) | 86400 |
| Domain Name | home.lan |

After clicking on ‘DHCP Leases’ (highlighted above), the following screen, shown in Figure 4-8 below, will display. It will show all the active devices on your network, with their MAC address, IP address, client name and ID, and the date and time at which their lease will expire. It is important to note that it displays all leases, regardless of whether they are on your Private LAN (Ethernet attached) or on your Wi-Fi Guest (wireless) portion of the network.

Devices which may be physically attached to your network but are not turned on (booted up) will not display in this list. Therefore, be sure you have turned on all devices. Then refresh your browser to see what IP address has been assigned to that device and when it will expire.

**Figure 4-8. DHCP Leases screen.**



DHCP Leases - All Interfaces

DHCP leases are IP addresses which have been assigned to clients and which have not timed out yet. The MAC Address is the IEEE 48-bit hardware address of the client's network interface. The Client Name is an optionally supplied name from the client. The Client ID is the client-supplied identifier which is used to identify this lease (often based on the network type and MAC address).

Click on refresh in your browser to see the latest status.

DHCP Leases

| Lease Expiry | MAC Address | IP Address | Client Name | Client ID |
|---|---|---|---|---|
| Wed Jun 4 17:02:43 2014 | cc:52:af:49:94:e6 | 192.168.1.100 | Grace | 01:cc:52:af:49:94:e6 |

For each device attached to your network, this screen will display:

- Lease expiration date (date and time stamp),
- MAC address of the device,
- IP address of the device, regardless of whether it is from the pool or a static IP address,
- Client name (computer name),
- Client ID – a unique identifier comprised of the network number and the MAC address.

This data is displayed for informational purposes only and is non-editable. If you want to change the length of time for leases, details of changing the lease duration can be found in the section on Editing the LAN Settings under Lease Time.

## Wi-Fi Guest

Your home LAN is comprised of two different subnets:

- the Private LAN (discussed above) – which is comprised of your wired and wireless devices that can intercommunicate with each other as well as with the Internet, and
- the Wi-Fi Guest network (discussed below) – which allows public access to the Internet by guests (casual or transient users) in your home, without allowing intercommunication with

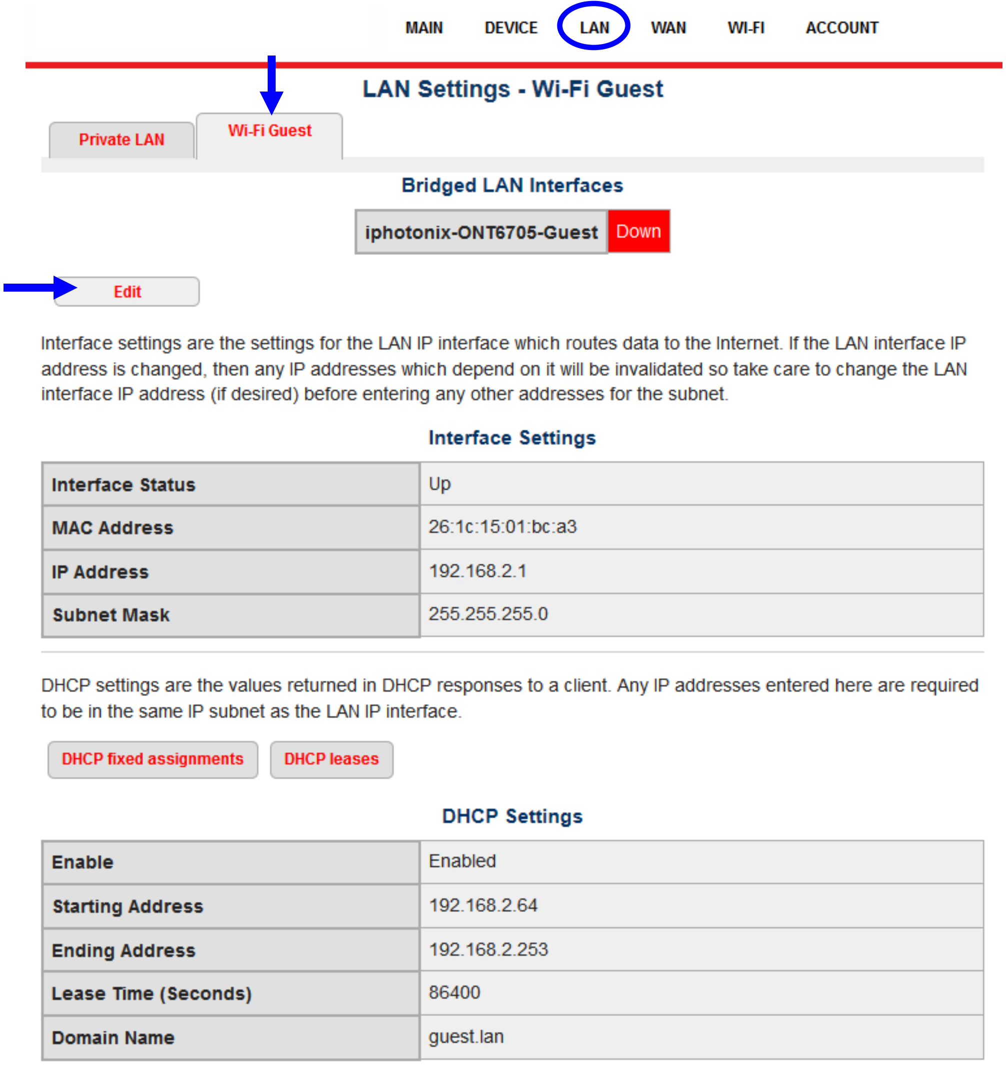
your Private LAN directly. However, all users on the Wi-Fi Guest network can intercommunicate with each other directly unless you have access point isolation turned on. Contact your service provider if you require this.

Having each of these networks assigned to different subnets enables them to operate independently of one another, while both are sharing the same high-speed, fiber optic connection to your service provider.

To view and configure the Wi-Fi network settings, follow these steps:

1. From the Main page, click on 'LAN' in the first line tabs.
2. Click on the 'Wi-Fi Guest' tab in the upper left (highlighted in Figure 4-9.
3. A three-part screen will be displayed, similar to that shown in Figure 4-9.

**Figure 4-9. LAN - The Wi-Fi Guest screen.**



LAN Settings - Wi-Fi Guest

Bridged LAN Interfaces

| iphotonix-ONT6705-Guest | Down |
|---|---|

Interface settings are the settings for the LAN IP interface which routes data to the Internet. If the LAN interface IP address is changed, then any IP addresses which depend on it will be invalidated so take care to change the LAN interface IP address (if desired) before entering any other addresses for the subnet.

Interface Settings

| | |
|---|---|
| Interface Status | Up |
| MAC Address | 26:1c:15:01:bc:a3 |
| IP Address | 192.168.2.1 |
| Subnet Mask | 255.255.255.0 |

DHCP settings are the values returned in DHCP responses to a client. Any IP addresses entered here are required to be in the same IP subnet as the LAN IP interface.

DHCP Settings

| | |
|---|---|
| Enable | Enabled |
| Starting Address | 192.168.2.64 |
| Ending Address | 192.168.2.253 |
| Lease Time (Seconds) | 86400 |
| Domain Name | guest.lan |

The three sections of this screen are discussed individually below.

### Bridged LAN Interfaces

The first section of this screen is view-only and cannot be edited. It reports the status of the wireless access point for the guest network. The status is displayed in words ('Up' or 'Down') as well as color:

- Green means the connection is working.
- Yellow means the connection may be working (if it says 'Up') but that it is not achieving optimal speeds. This may be because the network card in the device is not rated for higher speeds or there is a network problem.
- Red means the connection is missing or is not working.

Notice that the default condition of the Wi-Fi Guest network is "Down" even though the interface is up. You must specifically enable the Wi-Fi Guest via the Wi-Fi menu. Refer to the section on *Configuring the Wi-Fi*.

### Interface Settings

The middle section of the screen displays more detail about the Wi-Fi Guest interface, including its status, MAC address, IP address, and subnet mask. The IP address shown here is the IP address that all client devices on your Wi-Fi Guest network will use to gain access to the Internet. As the instructions on the screen state, be sure to change this IP address first (if necessary), before configuring any client devices. Refer to *Editing the Wi-Fi Guest Settings.*

### DHCP Settings

Your Residential Gateway acts as a DHCP server, which means it can automatically assign individual unique IP addresses to each wireless device on your guest network. This section of the screen displays:

- the status of the DHCP server (whether it is enabled or disabled),
- the starting IP address it will use when assigning IP addresses to each client device,
- the ending IP address that can be used,
- the length of time a device may keep the same IP address before it will be "recycled,"
- the domain name for your Wi-Fi Guest network.

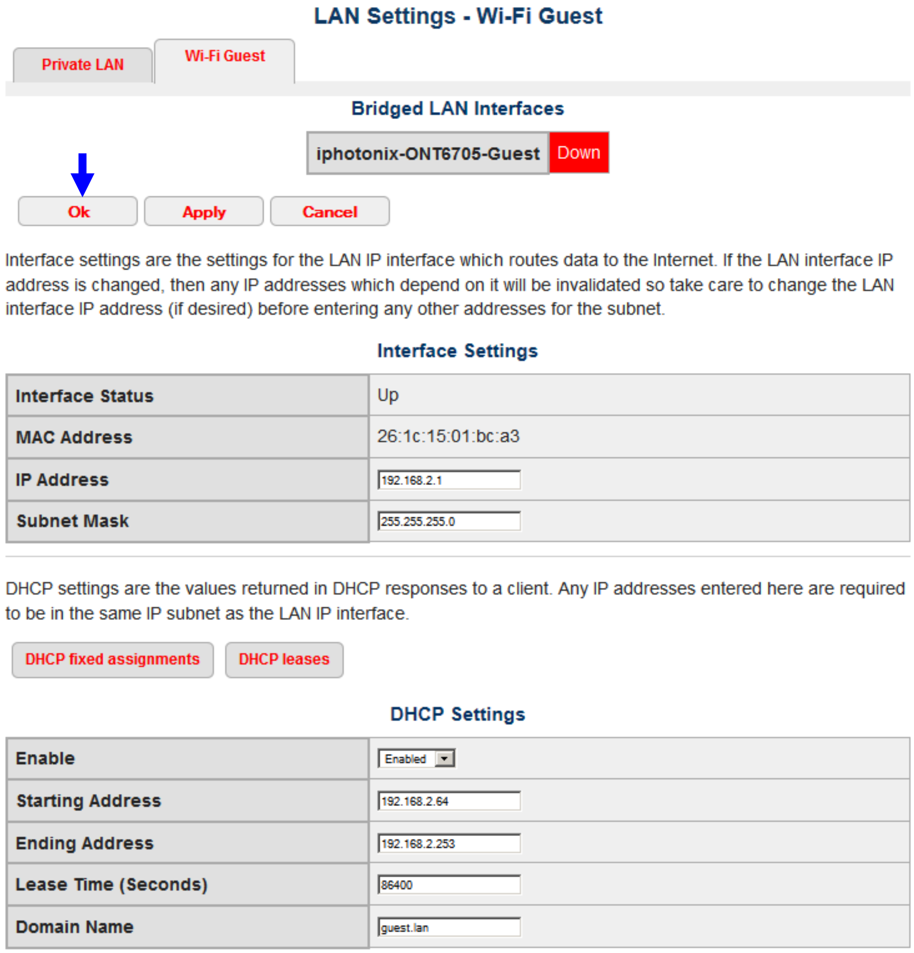
All the IP addresses used for both the Interface Settings and the DHCP Settings must use a *different subnet* from the Private LAN. For example, if the Private LAN contains IP addresses of 192.168.**1**.x (where x can be any number from 1 to 254), the Wi-Fi Guest network contains IP addresses of 192.168.**2**.x (where x can be any number from 1 to 254).

To edit any of the DHCP settings, refer to *Editing the Wi-Fi Guest Settings* below.

### Editing the Wi-Fi Guest Settings

To make changes in the Interface Settings or DHCP Settings, click on the 'Edit' button (highlighted in Figure 4-9 above). The screen shown in Figure 4-10 will display. You can edit the Interface IP address and subnet mask, if needed, and as well as each of the DCHP settings, if needed. Generally, the default values or values provided by your service provider do not require editing.

**Figure 4-10. LAN - Wi-Fi Guest screen - Edit mode.**



**LAN Settings - Wi-Fi Guest**

**Bridged LAN Interfaces**

| | |
|---|---|
| iphotonix-ONT6705-Guest | Down |

Interface settings are the settings for the LAN IP interface which routes data to the Internet. If the LAN interface IP address is changed, then any IP addresses which depend on it will be invalidated so take care to change the LAN interface IP address (if desired) before entering any other addresses for the subnet.

**Interface Settings**

| | |
|---|---|
| Interface Status | Up |
| MAC Address | 26:1c:15:01:bc:a3 |
| IP Address | 192.168.2.1 |
| Subnet Mask | 255.255.255.0 |

DHCP settings are the values returned in DHCP responses to a client. Any IP addresses entered here are required to be in the same IP subnet as the LAN IP interface.

**DHCP Settings**

| | |
|---|---|
| Enable | Enabled |
| Starting Address | 192.168.2.64 |
| Ending Address | 192.168.2.253 |
| Lease Time (Seconds) | 86400 |
| Domain Name | guest.lan |

If you are not familiar with the configuration details in this section, contact your service provider before changing the default settings of your Residential Gateway.

*Interface Settings:*

The Interface Status and MAC Address are not editable (view-only).

IP Address: Enter an IP address, or use the default (recommended). Keep in mind this must be in a different subnet from your Private LAN.

Subnet Mask: Enter the subnet mask, or use the default (recommended).

*DHCP Settings:*

Enable: If you want to allow your Residential Gateway to act as a DHCP server for your Wi-Fi Guest network, select “Enable” (recommended). If not, select “Disable.”

Starting Address: Enter a starting IP address. The system will begin making IP assignments to wireless devices on your Guest network starting with this IP address. It should not overlap with the IP address used for the Interface Settings (above), but should be within the same subnet. Using the default value is recommended.

Ending Address: Enter an ending IP address. It must be within the same subnet as the

Starting Address, and must allow for the maximum number of devices you may have on your Wi-Fi Guest network at any given time. Using the default value is recommended.

Lease Time: This is the length of time in seconds that a client device may keep an IP address before it is recycled (goes back into the IP pool). When a device on the Guest network is turned off and the lease time has expired, then when the device is again turned on (booted) it may be assigned a different IP address from the one it had earlier. However, as long as the device remains on, it will keep the same IP address even if the lease time has expired; it will merely renew that lease automatically. Additionally, if the Residential Gateway itself is rebooted, all new leases will be assigned to all devices. All of this happens transparently to user. Having shorter lease durations may be ideal if your Wi-Fi Guest network experiences many transient users who typically use the connection for less than a day at a time.

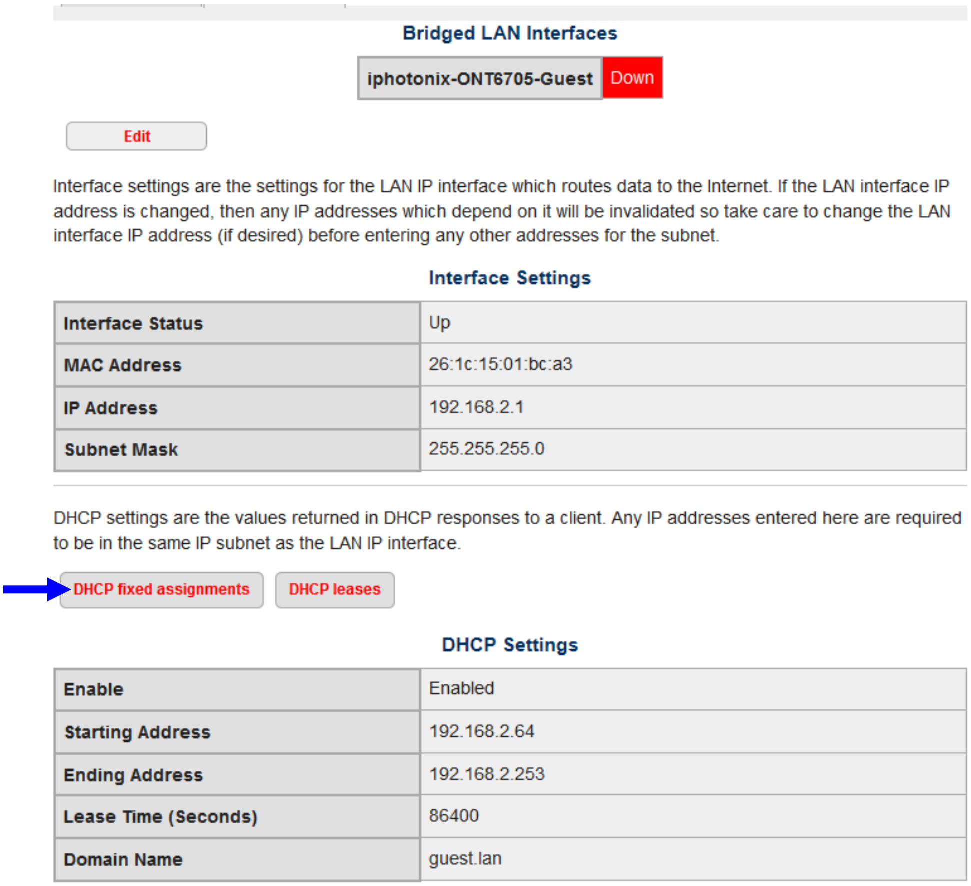
Domain Name: Enter the name you want to assign to your Wi-Fi Guest network domain, being sure to adhere to the *Network Naming Rules* specified earlier. Example (the default): Guest.lan

After you have made changes to the Interface Settings and DHCP Settings, click 'OK' (highlighted in Figure 4-10 above) or 'Apply' to save your changes. When you click 'Apply' your screen remains on the same page and you can continue making edits. When you click 'OK' you are taken back to the former page, so you can begin a new task. If you decide not to make any changes or to discard the changes you made, you can click the 'Cancel' button and the changes will not take effect (*provided* you have not already clicked 'Apply').

### Configuring Static IP Addresses on the Guest Network

If you have a guest device that needs to have a fixed IP address all the time, then you will use this section to create static IP addresses within the Guest network. To configure this, access the Wi-Fi Guest screen as shown above, and click on 'DHCP fixed assignments' in the DHCP Settings portion of the screen (highlighted in Figure 4-11 below).

**Figure 4-11. LAN - Wi-Fi Guest screen.**



**Bridged LAN Interfaces**

| iphotonix-ONT6705-Guest | Down |
|---|---|

Interface settings are the settings for the LAN IP interface which routes data to the Internet. If the LAN interface IP address is changed, then any IP addresses which depend on it will be invalidated so take care to change the LAN interface IP address (if desired) before entering any other addresses for the subnet.

**Interface Settings**

| | |
|---|---|
| Interface Status | Up |
| MAC Address | 26:1c:15:01:bc:a3 |
| IP Address | 192.168.2.1 |
| Subnet Mask | 255.255.255.0 |

DHCP settings are the values returned in DHCP responses to a client. Any IP addresses entered here are required to be in the same IP subnet as the LAN IP interface.

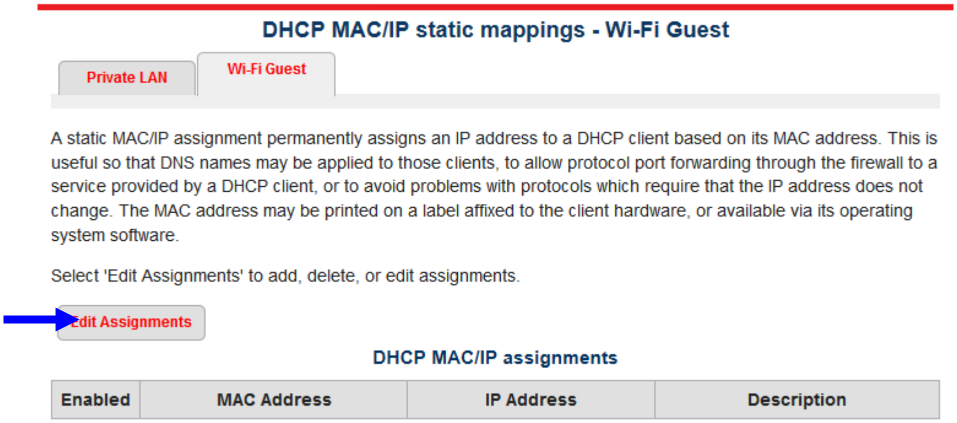
**DHCP Settings**

| | |
|---|---|
| Enable | Enabled |
| Starting Address | 192.168.2.64 |
| Ending Address | 192.168.2.253 |
| Lease Time (Seconds) | 86400 |
| Domain Name | guest.lan |

## DHCP Fixed Assignments

You can assign a static (permanent) IP address to a client device on the Guest network based on its MAC address. When you click on 'DHCP fixed assignments,' you will see the list of static IP addresses that have already been assigned. Initially, there will not be any DCHP fixed assignments configured and your screen may look similar to Figure 4-12 below.

**Figure 4-12. Wi-Fi Guest DHCP Static Mapping screen.**



**DHCP MAC/IP static mappings - Wi-Fi Guest**

A static MAC/IP assignment permanently assigns an IP address to a DHCP client based on its MAC address. This is useful so that DNS names may be applied to those clients, to allow protocol port forwarding through the firewall to a service provided by a DHCP client, or to avoid problems with protocols which require that the IP address does not change. The MAC address may be printed on a label affixed to the client hardware, or available via its operating system software.

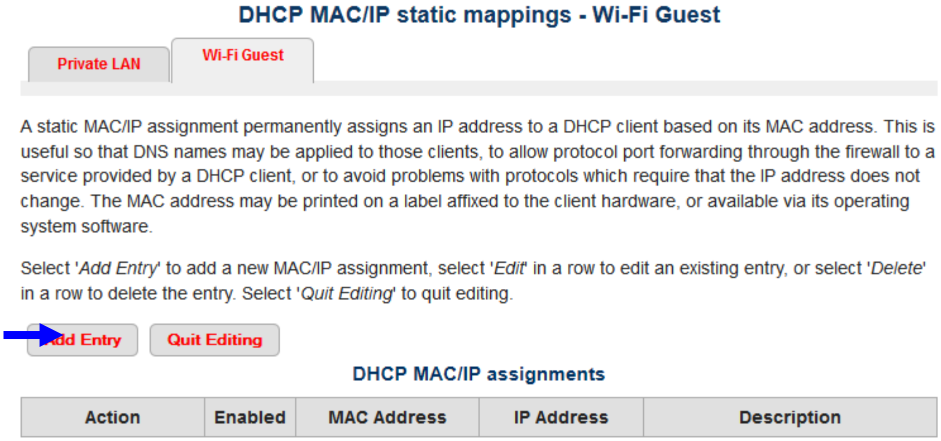
Select 'Edit Assignments' to add, delete, or edit assignments.

**DHCP MAC/IP assignments**

| Enabled | MAC Address | IP Address | Description |
|---|---|---|---|

To add a new fixed assignment, click on 'Edit Assignments' (highlighted in Figure 4-12 above). A new screen, shown in Figure 4-13 below will be displayed. If there were any assignments previously made, they would be displayed in the grid; if not, this grid may be blank (as shown).

**Figure 4-13. Wi-Fi Guest DCHP Static Mapping screen – Edit mode.**



DHCP MAC/IP static mappings - Wi-Fi Guest

A static MAC/IP assignment permanently assigns an IP address to a DHCP client based on its MAC address. This is useful so that DNS names may be applied to those clients, to allow protocol port forwarding through the firewall to a service provided by a DHCP client, or to avoid problems with protocols which require that the IP address does not change. The MAC address may be printed on a label affixed to the client hardware, or available via its operating system software.

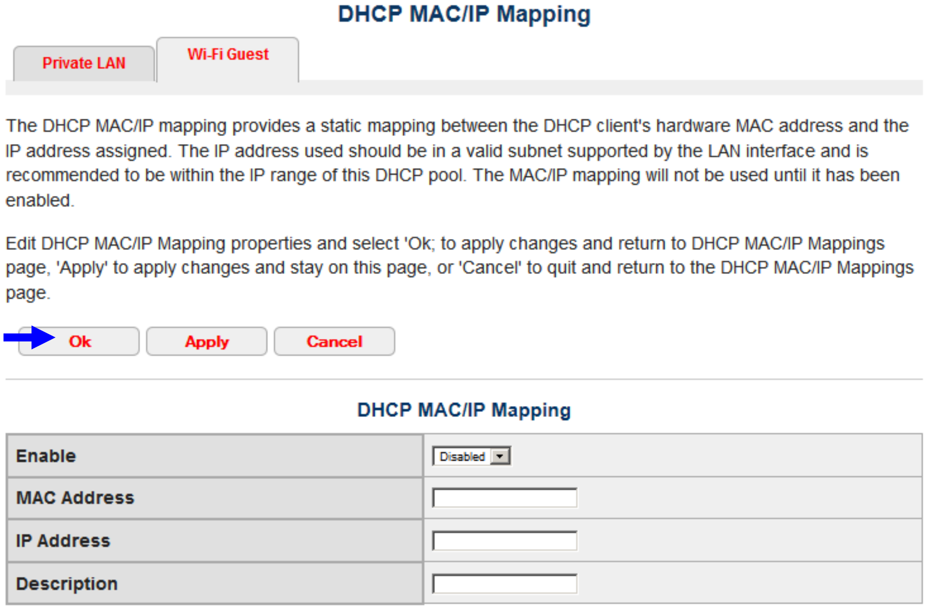
Select '*Add Entry*' to add a new MAC/IP assignment, select '*Edit*' in a row to edit an existing entry, or select '*Delete*' in a row to delete the entry. Select '*Quit Editing*' to quit editing.

DHCP MAC/IP assignments

| Action | Enabled | MAC Address | IP Address | Description |
|---|---|---|---|---|

To add a new fixed assignment, click on 'Add Entry' (highlighted in Figure 4-13 above). The data entry screen shown in Figure 4-14 will be displayed.

**Figure 4-14. Wi-Fi Guest DHCP MAC/IP Mapping – Data Entry screen.**



DHCP MAC/IP Mapping

The DHCP MAC/IP mapping provides a static mapping between the DHCP client's hardware MAC address and the IP address assigned. The IP address used should be in a valid subnet supported by the LAN interface and is recommended to be within the IP range of this DHCP pool. The MAC/IP mapping will not be used until it has been enabled.

Edit DHCP MAC/IP Mapping properties and select 'Ok; to apply changes and return to DHCP MAC/IP Mappings page, 'Apply' to apply changes and stay on this page, or 'Cancel' to quit and return to the DHCP MAC/IP Mappings page.

DHCP MAC/IP Mapping

| | |
|---|---|
| Enable | Disabled |
| MAC Address | |
| IP Address | |
| Description | |

*DHCP MAC/IP Mapping fields:*

<u>Enable</u>: Select whether you want to enable or disable this MAC/IP mapping. If you enable it, it becomes a static IP address. If you disable it, it reverts back to the DHCP pool of addresses.

MAC Address: Enter the MAC address of the guest device whose IP address you want to remain static. The MAC address may be found on a sticker on the back of the client device or it may be accessible via the client's operating system software. Generally, it is comprised of numbers and letters written in 6 sets of two, with each set separated by a colon (for example: 00:12:0A:9D:40:B2). However, it may be printed as just a 12-character alphanumeric string on your particular device.

IP Address: Enter the fixed IP address you want to assign to this device. Keep in mind, the IP address must be within the Wi-Fi Guest subnet. Refer to Figure 4-10, under the DHCP Settings, the fields *Starting Address* and *Ending Address*. The IP address you enter here must be a number between these starting and ending addresses.

When you have finished your edits, click on 'OK' (highlighted in Figure 4-14 above) or 'Apply' to save. When you click 'Apply' your screen remains on the same page and you can continue making edits. When you click 'OK' you are taken back to the former page. If you decide not to make any changes or to discard the changes you made, you can click the 'Cancel' button and the changes will not take effect (*provided* you have not already clicked 'Apply').

Once back at the DHCP Mapping screen (similar to Figure 4-5), you can:

- Add additional static IP entries by clicking on 'Add Entry' (highlighted in Figure 4-5).
- Delete an existing fixed assignment by clicking on 'Delete' in the corresponding row in the grid. That row and the static MAC/IP Mapping will be removed from the system.
- Edit an existing fixed assignment by clicking on 'Edit' in the corresponding row in the grid. The data entry screen will then display (see Figure 4-6), where you can edit any of the fields.

When you are finished making all necessary additions/edits/deletions, click on 'Done Editing DHCP MAC/IP Assignments' and you will be returned to the starting Wi-Fi Guest screen. Or, you may click on the 'WiFi Guest' tab in the upper left.

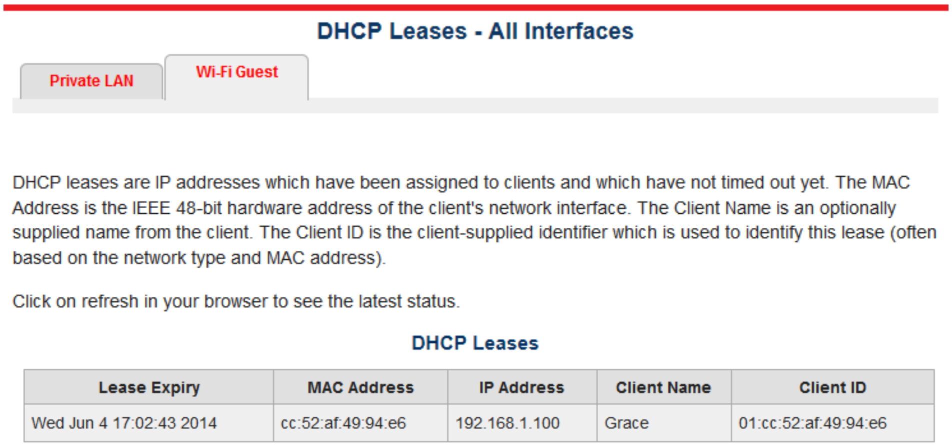
## DHCP Leases

Your Residential Gateway acts as a DHCP server and will automatically assign each guest wireless device a unique IP address as it is added or booted up on the network. But the IP address is only leased for a fixed length of time. After that time, the next time that device is turned on, it might be assigned a different IP address from what it had previously. You may configure the lease length to make it a shorter or longer length of time (refer to *Lease Time* above); however the default value rarely needs to be edited.

To view the current leases on your network, follow these steps:

1. From the Main page, click on 'LAN' in the first line tabs.
2. Click on the 'Wi-Fi Guest' tab in the upper left.
3. A three-part screen will be displayed, similar to that shown in Figure 4-9. In the lower section on DHCP Settings, click on the 'DHCP Leases' button. A screen similar to that shown in Figure 4-15 will be displayed.

**Figure 4-15. DHCP Leases screen.**



DHCP Leases - All Interfaces

DHCP leases are IP addresses which have been assigned to clients and which have not timed out yet. The MAC Address is the IEEE 48-bit hardware address of the client's network interface. The Client Name is an optionally supplied name from the client. The Client ID is the client-supplied identifier which is used to identify this lease (often based on the network type and MAC address).

Click on refresh in your browser to see the latest status.

DHCP Leases

| Lease Expiry | MAC Address | IP Address | Client Name | Client ID |
|---|---|---|---|---|
| Wed Jun 4 17:02:43 2014 | cc:52:af:49:94:e6 | 192.168.1.100 | Grace | 01:cc:52:af:49:94:e6 |

Devices which may be physically attached to your network but are not turned on (booted up) will not display in this list. Therefore, be sure you have turned on all devices. Then refresh your browser to see what IP address has been assigned to that device and when it will expire.

It is important to note that it displays *all* leases, regardless of whether they are on your Private LAN (Ethernet attached) or on your Wi-Fi Guest (wireless) portion of the network. For each device attached to your network, this screen will display:

- Lease expiration (date and time stamp),
- MAC address of the device,
- IP address of the device, regardless of whether it is from the pool or a static IP address,
- Client name (computer name),
- Client ID – a unique identifier comprised of the network number and the MAC address.

This data is displayed for informational purposes only and is non-editable. If you want to change the length of time for leases, details of changing the lease duration can be found in the section on *Editing the Wi-Fi Guest Settings* under *Lease Time*.

# 5. CONFIGURING THE WI-FI

There are two different wireless access points – each with its own SSID - that are configurable via your Residential Gateway device. [Note: the number of wireless access points available may be different depending upon your model.] One Wi-Fi access point belongs to the Private LAN subnet and allows wireless devices to co-exist with your wired devices (attached to the Ethernet ports) on the same network. The other Wi-Fi access point belongs to the Wi-Fi Guest subnet. Because each of these exists on different subnets, they can and must be configured independently of one another.

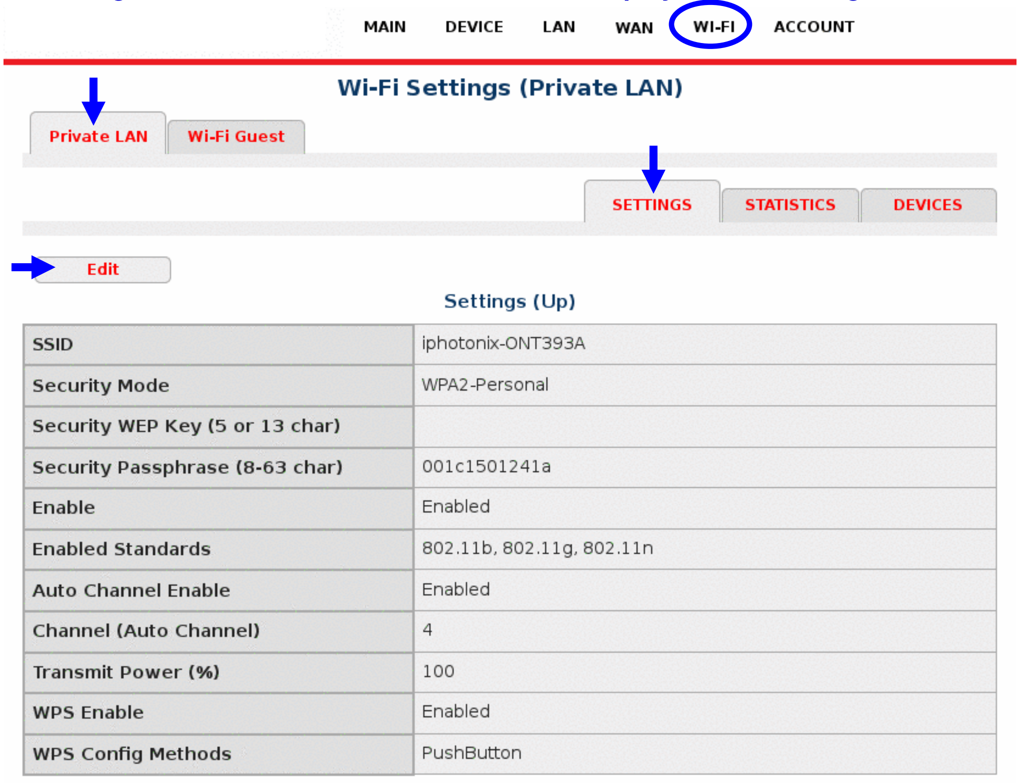
To begin configuring the wireless portion of your Residential Gateway, click on 'Wi-Fi' in the first line tabs. Then click on either the 'Private LAN' tab (to configure the wireless on the Private LAN) or the 'Wi-Fi Guest' tab (to configure the guest wireless), and follow the instructions in the appropriate section below.

## Wi-Fi - Private LAN

To configure the wireless connected to your Private LAN, follow these steps:

1. From the Main page, click on 'Wi-Fi' in the first line tabs, highlighted in Figure 5-1 below.
2. Click on the 'Private LAN' tab in the upper left, highlighted in Figure 5-1 below.
3. Click on the 'Settings' tab in the upper right, highlighted in Figure 5-1 below.

Figure 5-1. Wi-Fi - Private LAN screen, displaying the Settings tab.



Wi-Fi Settings (Private LAN)

Settings (Up)

| | |
|---|---|
| SSID | iphotonix-ONT393A |
| Security Mode | WPA2-Personal |
| Security WEP Key (5 or 13 char) | |
| Security Passphrase (8-63 char) | 001c1501241a |
| Enable | Enabled |
| Enabled Standards | 802.11b, 802.11g, 802.11n |
| Auto Channel Enable | Enabled |
| Channel (Auto Channel) | 4 |
| Transmit Power (%) | 100 |
| WPS Enable | Enabled |
| WPS Config Methods | PushButton |

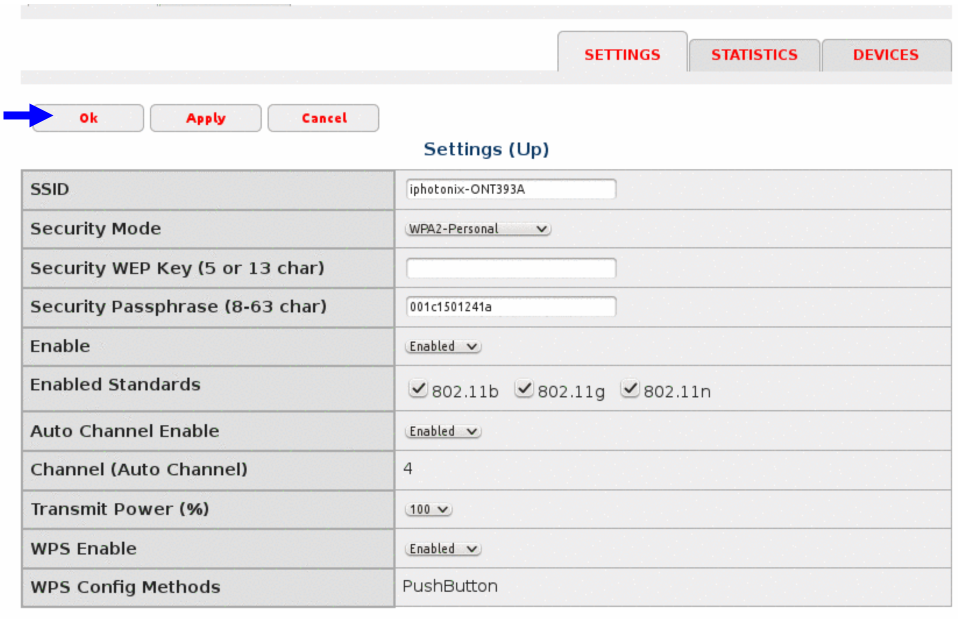
Note: There are three tabs displayed along the upper right. Clicking on each one will display a different page. Each of these is described in detail below. Most configuration tasks will be done using the *Settings* tab. The *Statistics* and *Devices* tabs are view-only and do not require configuration.

## Settings

On the Settings tab, you will notice the status information - “Up” or “Down” - displayed beside the page title. This tells you whether the wireless access point is working (‘Up’) or is missing or not working (‘Down’).

To edit the fields on the Settings page, click the ‘Edit’ button (highlighted in Figure 5-1) in the upper left, and a screen similar to Figure 5-2 will be displayed. You may then edit the fields as desired. A description of each of the fields follows below.

Figure 5-2. Wi-Fi - Private LAN screen, Settings tab - Edit mode.



Settings (Up)

| | |
|---|---|
| SSID | iphotonix-ONT393A |
| Security Mode | WPA2-Personal |
| Security WEP Key (5 or 13 char) | |
| Security Passphrase (8-63 char) | 001c1501241a |
| Enable | Enabled |
| Enabled Standards | ☑ 802.11b ☑ 802.11g ☑ 802.11n |
| Auto Channel Enable | Enabled |
| Channel (Auto Channel) | 4 |
| Transmit Power (%) | 100 |
| WPS Enable | Enabled |
| WPS Config Methods | PushButton |

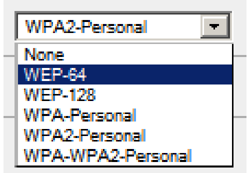
If you are not familiar with the configuration details in this section, contact your service provider before changing the default settings of your Residential Gateway.

*Wi-Fi Settings fields:*

SSID: This stands for Service Set Identifier. This is a unique name for your wireless network, similar to a workgroup name. It can be up to 32 characters in length and ideally should be something meaningful and/or easy to remember. You may use any combination of numbers, letters, and special characters. Example: Magic_Volcano.

Setting up a unique SSID for each wireless subnet is one of the first configuration tasks you will need to do. This is important from a security perspective, as many wireless devices have ranges that overlap (yours and your neighbor’s, for example, as well as the Private LAN’s wireless and Guest LAN’s wireless). Therefore, you need to differentiate the appropriate connection points from one another.

Security Mode: Click on the dropdown arrow to see a list of choices (example shown). These refer to the type of encryption that you want applied to this access point. WEP is a weaker security mode than WPA (128-bit encryption), and WPA2 is the strongest as it supports the full 802.11i standard as well as AES-based encryption. Some older wireless network cards do not support the newer WPA2 standard, and so the combination WPA-WPA2 option is available to allow for downward compatibility.



Security WEP Key: WEP stands for Wired Equivalent Privacy. The WEP Key is a code that will allow devices connected on the same network (the Private LAN, in this case) to exchange messages openly between one another while still remaining hidden to users outside the network. To implement this, the same key you set here (on the Residential Gateway) needs to also be set on each device on your Private LAN – both the wired and wireless devices. The key is comprised of letters (A through F) and numbers (0 through 9) and may be either 5 or 13 characters in length. Example: 1A648C9FE271D. Note: If you are using the WPA2 security mode (see above), there is no need to set a WEP key here. However, they are typically used with the less secure WEP security mode to increase encryption strength.

Security Passphrase: This is a word or words from which a WEP key can be derived. A passphrase may be easier to setup and remember, and acts like a long password. The passphrase can be from 8 to 63 characters in length, and may contain letters, numbers, and special characters. Note: Some operating systems do not support passwords longer than 14 characters. Generally, the longer the passphrase, the stronger the encryption will be (harder for someone to hack). Do not use easy-to-guess phrases, your user name, birthdate, family name, etc. Instead, use an intentional misspelling or something more cryptic. Example: iLuv2playG@lf. A passphrase is typically only used with the less secure WEP security mode to increase encryption strength. Not all network cards support the use of passphrases, and different manufacturers may use different algorithms for translating the phrase into a WEP key.

Enable: This is the setting for enabling or disabling the wireless access point. Note that the status may be ‘Up’ but if it is not enabled, no device will be able to connect to the network via this access point.

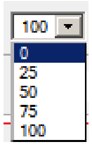
Enabled Standards: Put a checkmark beside each standard you want to enable on the wireless network by clicking in the box beside it. The different standards refer to the bandwidth, data rates, and error-correction that are supported. For example, 802.11b supports up to 11Mb/s, while 802.11g supports up to 54Mb/s but is backwards compatible. Not all network cards will support all standards. Verify the standards supported by each of your devices and set this accordingly. The default is to check all to allow for maximum flexibility.

Auto Channel Enable: You can enable or disable auto channel selection. The Residential Gateway has the ability to randomly select the best channel on which to communicate. It will check for interference (i.e., signal overlap) from other devices and automatically move to a different channel. You can optionally disable Auto Channel and instead set the Residential Gateway to a “fixed” channel (see below) that you know has good throughput due to lack of interference.

Devices such as garage-door openers, your neighbor's wireless network, baby monitors, and even microwave ovens, can cause interference on some channels. Many wireless devices ship with a default channel pre-set. If you experience interference, slow connection speeds, or find you are frequently losing connectivity to the network, try setting the channel to something different (see below).

Channel (Auto Channel): If Auto Channel (see above) is enabled, this field is greyed and does not allow edits. It merely displays the channel currently in use. To set a fixed channel, you would need to disable Auto Channel (above), and then this field becomes editable. Enter the number corresponding to the channel you want to use, from 1 to 11.

Transmit Power: This refers to the percentage of maximum transmit power, and is selectable from 1% to 100%. Click on the dropdown arrow to see a list of choices (example shown). A higher transmit power may provide a better signal long distances from the Residential Gateway.



WPS Enable: You can enable or disable WPS. WPS stands for Wi-Fi Protected Setup and is a type of home wireless network security which allows a user to connect to the network without knowing the network's SSID or passphrase. However, the wireless device you are attempting to connect must support WPS. Your Residential Gateway has a default setup allowing push-button control (see WPS Config Methods below). The push-button control method of authenticating to the network is discussed in Push-Button Control below.

WPS Config Methods: This defaults to 'PushButton' and is only used if the WPS Enable field is set to "Enabled" (see above). When enabled, it makes connecting a wireless device to the network easy and quick. Refer to instructions in the section on *Push-Button Control* below.

When you have finished your edits, click on 'OK' (highlighted in Figure 5-2) or 'Apply' to save. When you click 'Apply' your screen remains on the same page and you can continue making edits. When you click 'OK' you are taken back to the former page. If you decide not to make any changes or to discard the changes you made, you can click the 'Cancel' button and the changes will not take effect (*provided* you have not already clicked 'Apply').

### Push-Button Control

The process of joining the network is called authentication. Your Residential Gateway comes with an easy method of automatically allowing wireless devices to authenticate to the network without knowing the SSID or passphrase, and without having to configure a WEP security key. Rather, it is simply the push of a button, thus the name "Push-Button Control." To use this feature, the WPS Enable field must be set to "Enabled" (discussed above). Here's how the push-button control works:

1. Put the wireless device (the laptop, cell phone, or whatever you are trying to connect) in close proximity to the Residential Gateway. Ideally, it should be within 20-feet (6 meters) to ensure a strong signal.

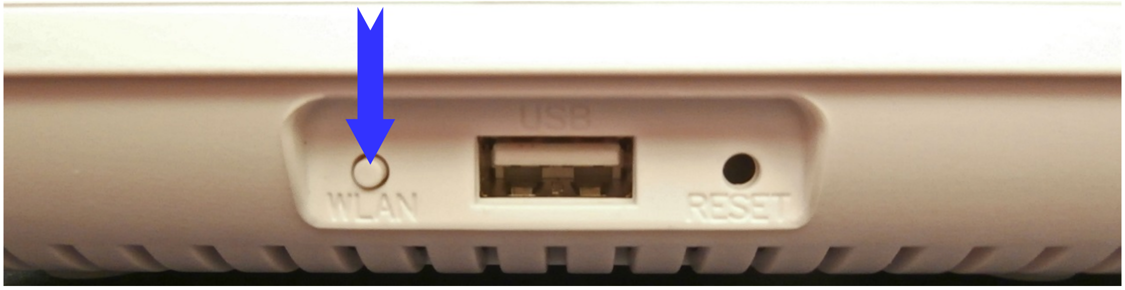
The wireless device you are attempting to connect must support WPS or be WPS-enabled. This is a newer technology and not all devices support it.

2. Make sure the wireless device is powered on, then press the button on the side of the Residential Gateway marked 'WLAN' (shown in Figure 5-3 below) for 2 seconds, and then

release. The WLAN light on the front of the device (refer to *LED Descriptions*) will begin to blink on and off, about once per second. This indicates that the wireless access point is in the WPS mode.

3. Activate the WPS Wi-Fi link on the client wireless device. This may be a button or a setting (the "connect via WPS" option) on the wireless device. This must be done *within two minutes* of pressing the 'WLAN' button on the Residential Gateway.
4. Information allowing the client wireless device to connect (the network's SSID and passphrase) will automatically be sent to the wireless device. On the wireless device, you can choose to store this so that your device "remembers" how to connect again in the future.
5. As soon as the client device has successfully connected, or after two minutes (whichever comes first), the blinking on the front of the Residential Gateway will cease and the Residential Gateway will exit WPS mode.

**Figure 5-3. Side of Residential Gateway, showing location of WPS PushButton.**



The main advantage of using WPS and the Push-Button Control method is that there are no SSIDs, passphrases, or difficult-to-remember hexadecimal security keys to type in.

*Important Caveats about the Push-Button Control Method:*

- The button on the Residential Gateway and the button/setting on your wireless device must be pressed within *two minutes* of each other.
- Only *one* device may establish a connection in this manner at a time. To attach another wireless device to the network, follow the above steps again, or use a different authentication method.
- Since using the Push-Button Control method of authentication by-passes setting up a more elaborate network security method and can be used without any knowledge of the network (i.e., without knowing the SSID), it can be easily hacked. For example, when you press the Residential Gateway's push-button, ANY device – even your neighbor's or a stranger in close enough proximity to pick up the signal or a hacker who has been monitoring your network – may connect. Conversely, when you hit the WPS button (or setting) on your wireless device, it will attach to the first access point it sees, which may or may not be your Private LAN, as intended.

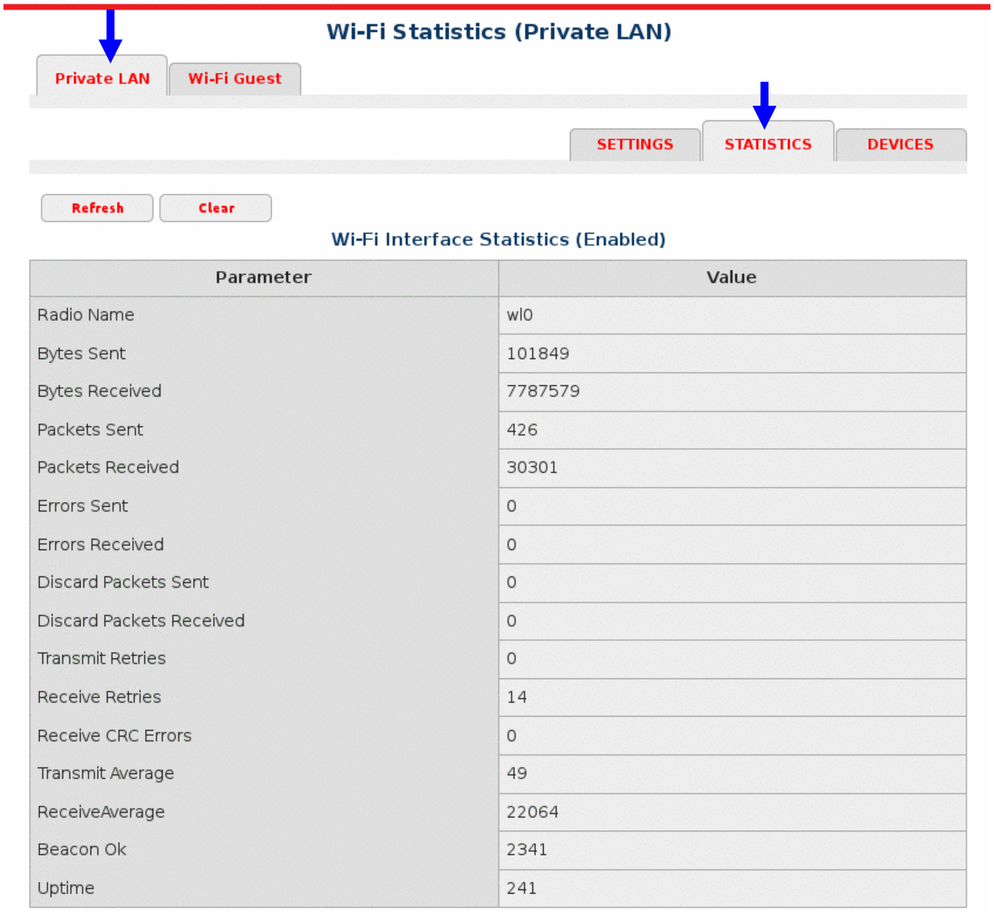
## Statistics

To view the wireless network statistics, follow these steps:

- From the Main page, click on 'Wi-Fi' in the first line tabs.
- Click on the 'Private LAN' tab in the upper left, highlighted in Figure 5-4 below.

- Click on the ‘Statistics’ tab in the upper right, highlighted in Figure 5-4 below.

**Figure 5-4. Wi-Fi - Private LAN, displaying the Statistics tab.**



Wi-Fi Interface Statistics (Enabled)

| Parameter | Value |
|---|---|
| Radio Name | wl0 |
| Bytes Sent | 101849 |
| Bytes Received | 7787579 |
| Packets Sent | 426 |
| Packets Received | 30301 |
| Errors Sent | 0 |
| Errors Received | 0 |
| Discard Packets Sent | 0 |
| Discard Packets Received | 0 |
| Transmit Retries | 0 |
| Receive Retries | 14 |
| Receive CRC Errors | 0 |
| Transmit Average | 49 |
| ReceiveAverage | 22064 |
| Beacon Ok | 2341 |
| Uptime | 241 |

This screen is view-only and is used for informational purposes only. It provides statistics about your wireless transmissions, including the number of bytes and packets sent and received, any discarded packets, errors, and the amount of time the wireless network has been up, among other things. There are only two possible actions on this screen:

- Refresh: This will refresh the statistics reported on the screen with the latest values.
- Clear: This will clear all the past statistics (i.e., reset all values to zero) and begin gathering new statistics from this point in time forward.

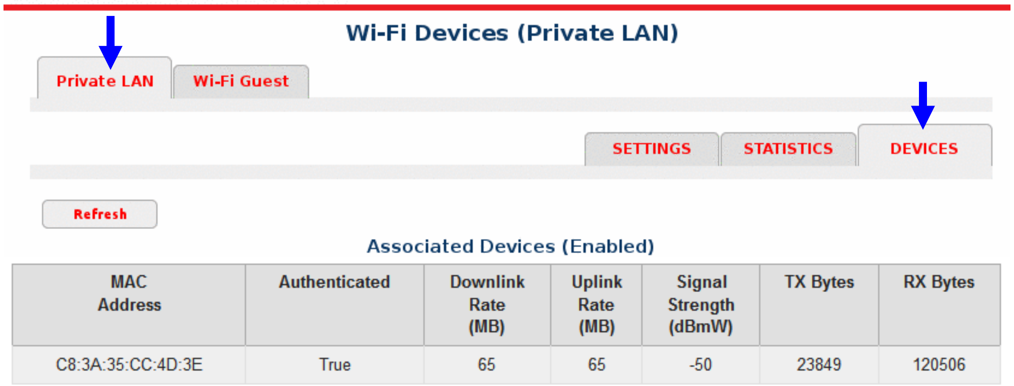
Click on the ‘Refresh’ or ‘Clear’ button in the upper left, as needed.

## Devices

To view the devices currently connected to the wireless network, follow these steps:

- From the Main page, click on ‘Wi-Fi’ in the first line tabs.
- Click on the ‘Private LAN’ tab in the upper left, highlighted in Figure 5-5 below.
- Click on the ‘Devices’ tab in the upper right, highlighted in Figure 5-5 below.

**Figure 5-5. Wi-Fi – Private LAN, displaying the Devices tab.**



Wi-Fi Devices (Private LAN)

Associated Devices (Enabled)

| MAC Address | Authenticated | Downlink Rate (MB) | Uplink Rate (MB) | Signal Strength (dBmW) | TX Bytes | RX Bytes |
|---|---|---|---|---|---|---|
| C8:3A:35:CC:4D:3E | True | 65 | 65 | -50 | 23849 | 120506 |

If there are no devices displayed in the list, then you have not succeeded in connecting to the wireless network from your user device. Follow the instructions for your user device (either within the operating system or with the network card in your user device) for attaching to a wireless network. Be sure you have connected to the correct SSID and have employed the same type of security (for example, WEP key or passphrase, if appropriate) on all devices.

The list of devices displays:

- The MAC address of each wireless device,
- Whether the device has successfully authenticated to the network (True = successful authentication, False = not authenticated),
- The downstream and upstream data rates in megabytes (MB),
- The signal strength in decibel milliwatts (dBmW),
- The number of bytes that have been transmitted (TX) and received (RX).

This screen is view-only. The only action that can be taken is to refresh the list (and statistics associated with each device). To do so, click the ‘Refresh’ button in the upper left.

## Wi-Fi – Wi-Fi Guest

To begin configuring the Guest network’s wireless access point, click on ‘Wi-Fi’ in the first line tabs. Then click on the ‘Wi-Fi Guest’ tab, and follow the instructions in the appropriate section below.

### Wi-Fi Guest — Settings

To configure the wireless connected to your Wi-Fi Guest network, follow these steps:

1. From the Main page, click on ‘Wi-Fi’ in the first line tabs, highlighted in Figure 5-1.
2. Click on the ‘Wi-Fi Guest’ tab in the upper left.
3. Click on the ‘Settings’ tab in the upper right.
4. The screen that will be displayed will be similar to Figure 5-1. All fields and instructions are the same as that described for the Private LAN – Settings page, except that the “WPS

Enable" and "WPS Config Method" are not available on the Wi-Fi Guest network. Thus, the push-button control method of authenticating to the guest network cannot be used.

### Wi-Fi Guest ─ Statistics

To view the wireless network statistics for your Wi-Fi Guest network, follow these steps:

1. From the Main page, click on 'Wi-Fi' in the first line tabs, highlighted in Figure 5-1.
2. Click on the 'Wi-Fi Guest' tab in the upper left.
3. Click on the 'Statistics' tab in the upper right.
4. The screen that displays will look similar to Figure 5-4. Follow the instructions as described in the *Private LAN – Statistics* section, knowing that the statistics you are viewing are applicable to the Wi-Guest network only.

### Wi-Fi Guest ─ Devices

To view the devices currently connected to the Wi-Fi Guest network, follow these steps:

1. From the Main page, click on 'Wi-Fi' in the first line tabs, highlighted in Figure 5-1.
2. Click on the 'Wi-Fi Guest' tab in the upper left.
3. Click on the 'Devices' tab in the upper right.
4. The screen that displays will look similar to Figure 5-5. Follow the instructions as described in the *Private LAN – Devices* section, knowing that the devices you are viewing are applicable to the Wi-Guest network only.

# 6. THE WAN CONNECTION

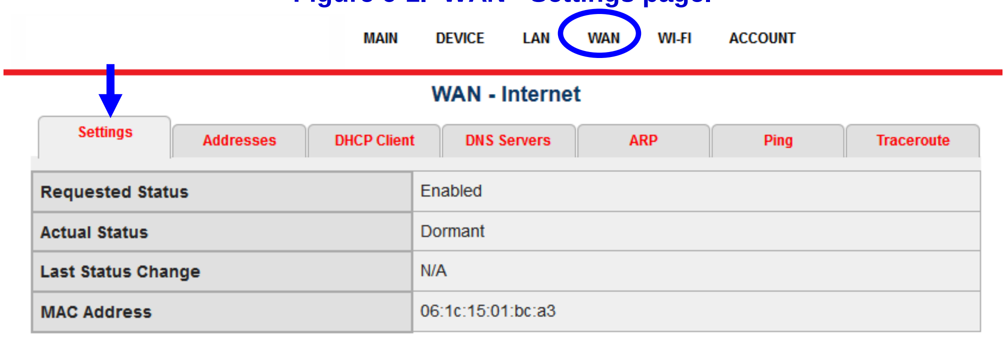
The WAN refers to the Wide Area Network. This portion of the system allows you to view your connection to the outside world (i.e., the Internet) and to diagnose Internet connection problems. Inside your Residential Gateway is a router and DCHP server. You can think of these as having two "sides." The side that is inward-facing and assigns IP addresses to devices on your private network is called the LAN side, and is discussed in the section *Configuring the LAN*. The side that is outward-facing and controls the traffic between you and your Internet service provider is called the WAN side, and is discussed in this chapter. All of the pages and screens in the WAN portion of the device are either informational (view-only) and cannot be edited, or they are used for trouble-shooting connection issues. There are not fields requiring configuration.

## Settings

To view the WAN settings for your Residential Gateway, follow these steps:

1. From the Main page, click on 'WAN' in the first line tabs, highlighted in Figure 6-1 below.
2. Click on the 'Settings' tab in the upper left, highlighted in Figure 6-1 below.
3. The screen that displays will look similar to Figure 6-1.

Figure 6-1. WAN - Settings page.



| | |
|---|---|
| Requested Status | Enabled |
| Actual Status | Dormant |
| Last Status Change | N/A |
| MAC Address | 06:1c:15:01:bc:a3 |

This screen is for informational purposes only and cannot be edited. The fields displayed are:

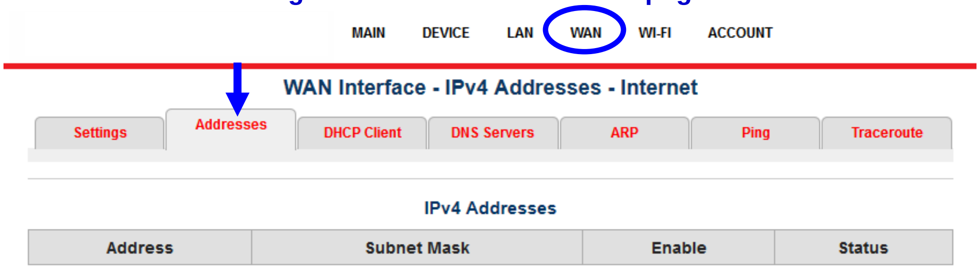
- *Requested Status*: If you have signed up for Internet service from your Internet service provider, the status here should be "Enabled." Otherwise, the status will be disabled.
- *Actual Status*: If the WAN side of the Residential Gateway can "see" the Internet, this status will be "Up." Otherwise, if it cannot see the Internet or cannot make a connection outside of your private LAN, the status will be "Dormant."
- *Last Status Change*: If there was status change – for example, your service provider just turned on or off your Internet capabilities, the date and time of that change would be reported here.
- *MAC Address*: This is the MAC address of the WAN side of your Residential Gateway.

## Addresses

To view the address assignments on the WAN side of your Residential Gateway, follow these steps:

1. From the Main page, click on ‘WAN’ in the first line tabs, highlighted in Figure 6-2 below.
2. Click on the ‘Addresses’ tab, highlighted in Figure 6-2 below.
3. The screen that displays will look similar to Figure 6-2.

**Figure 6-2. WAN - Addresses page.**



| Address | Subnet Mask | Enable | Status |
|---|---|---|---|

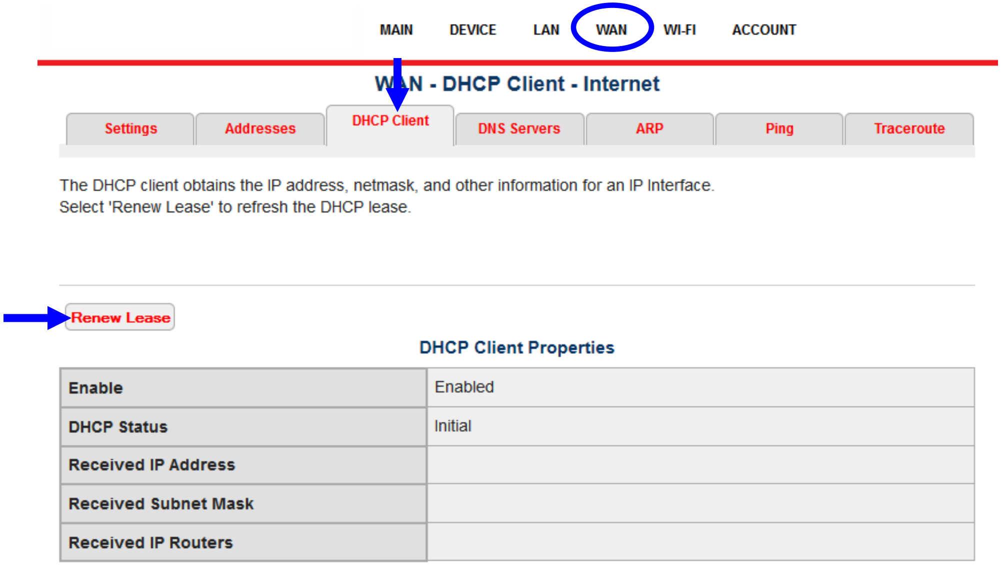
If your service provider has assigned a static IP address to the WAN side of your gateway, it will be displayed here. However, it is more common to use the DHCP server within the device to assign the IP address, and if that is case, this will be blank (as shown).

## DHCP Client

To view the assignments the DCHP server has made, follow these steps:

1. From the Main page, click on ‘WAN’ in the first line tabs, highlighted in Figure 6-3 below.
2. Click on the ‘DHCP Client’ tab, highlighted in Figure 6-3 below.
3. The screen that displays will look similar to Figure 6-3.

**Figure 6-3. WAN - DHCP Client page.**



The DHCP client obtains the IP address, netmask, and other information for an IP Interface.
Select 'Renew Lease' to refresh the DHCP lease.

| | |
|---|---|
| Enable | Enabled |
| DHCP Status | Initial |
| Received IP Address | |
| Received Subnet Mask | |
| Received IP Routers | |

This screen is for informational purposes only and cannot be edited. The fields displayed are:

- *Enable*: This will be "Enabled" when the DHCP server is responsible for assigning the IP address on the WAN side. This will be "Disabled" if your service provider has assigned a static IP address to the WAN side of your Residential Gateway.

- *DHCP Status*: If the Residential Gateway has connected to the Internet using the assigned IP address, this status will be "Found." Otherwise, if it cannot connect to the Internet, its status will be "Initial."

- *Received IP Address, Subnet Mask, and IP Routers*: These are the assignments that the DHCP server has made to the WAN side of your Residential Gateway.

When a DHCP server assigns an IP address, it picks one from a "pool" of IP addresses, and that address is leased for a certain length of time. You can re-request a new IP address with a new lease by clicking on the 'Renew Lease' button (upper left), highlighted in Figure 6-3 above. As is often the case, it still may "pick" the same IP address it had before; however the lease will be renewed.

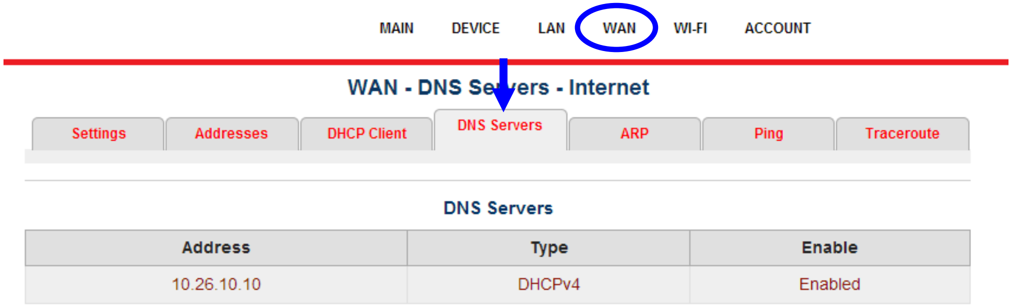
The DHCP server and lease used on the WAN side is *not* the same as that discussed earlier, which is used on the LAN side.

## DNS Servers

To view the IP address of your service provider's DNS server(s), follow these steps:

1. From the Main page, click on 'WAN' in the first line tabs, highlighted in Figure 6-4 below.
2. Click on the 'DNS Servers' tab, highlighted in Figure 6-4 below.
3. The screen that displays will look similar to Figure 6-4.

**Figure 6-4. WAN - DNS Servers page.**



DNS Servers

| Address | Type | Enable |
|---|---|---|
| 10.26.10.10 | DHCPv4 | Enabled |

This screen reports the IP address of your Internet service provider's DNS server. There can be more than one, if, for example, your service provider also has a backup DNS server. This screen is for informational purposes only and has no editable fields.

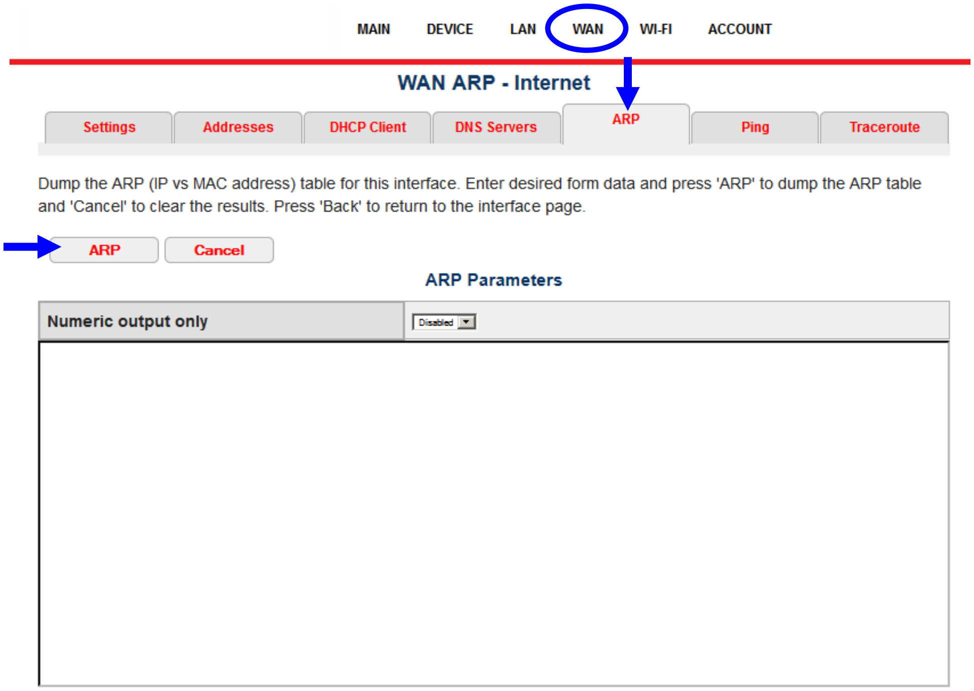
## ARP

ARP stands for Address Resolution Protocol. It provides a method for mapping IP addresses to MAC addresses. To view the IP address paired to the MAC address for your service provider's router, follow these steps:

1. From the Main page, click on 'WAN' in the first line tabs, highlighted in Figure 6-5 below.

2. Click on the ‘ARP’ tab, highlighted in Figure 6-5 below.
3. The screen that displays will look similar to Figure 6-5.

Figure 6-5. WAN - ARP page.



WAN ARP - Internet

Dump the ARP (IP vs MAC address) table for this interface. Enter desired form data and press 'ARP' to dump the ARP table and 'Cancel' to clear the results. Press 'Back' to return to the interface page.

ARP Parameters

| | |
|---|---|
| Numeric output only | Disabled |

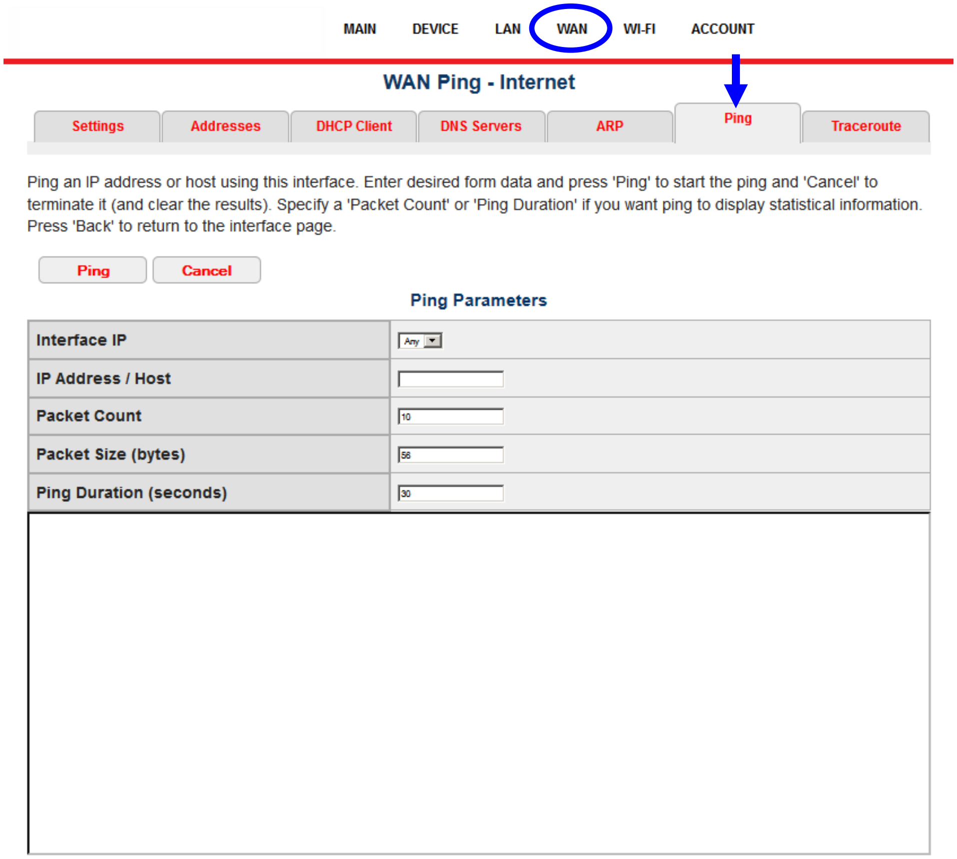
Select the type of output you want to see. If ‘Numeric output only’ is set to ”Enabled,” you will see IP addresses with corresponding MAC addresses. If ‘Numeric output only’ is set to “Disabled,” you will see the names (e.g., website names, such as “yahoo.com’) corresponding to the IP addresses as well. Once you have selected the type of output you want to see, click the ‘ARP’ button near the upper right (highlighted in Figure 6-5 above). Typically, the IP addresses that will be displayed here (with corresponding MAC addresses and/or names) refer to your service provider’s router(s). This page is for informational purposes only and has no editable fields.

## Ping

Often, while troubleshooting a problem, it is helpful to query another computer on the WAN, and see if it responds. If so, that validates that the two are connected and that their signals are reaching one another (e.g., they can communicate). To use the ping tool to query another computer on the WAN, follow these steps:

1. From the Main page, click on ‘WAN’ in the first line tabs, highlighted in Figure 6-6 below.
2. Click on the ‘Ping’ tab, highlighted in Figure 6-6 below.
3. The screen that displays will look similar to Figure 6-6.

**Figure 6-6. WAN - Ping page.**



WAN Ping - Internet

Ping an IP address or host using this interface. Enter desired form data and press 'Ping' to start the ping and 'Cancel' to terminate it (and clear the results). Specify a 'Packet Count' or 'Ping Duration' if you want ping to display statistical information. Press 'Back' to return to the interface page.

Ping Parameters

| | |
|---|---|
| Interface IP | Any |
| IP Address / Host | |
| Packet Count | 10 |
| Packet Size (bytes) | 56 |
| Ping Duration (seconds) | 30 |

This ping tool will only ping other computers from the WAN-side of the Residential Gateway outward towards the Internet. It will not allow pinging of individual devices on your internal Private LAN.

Enter the following fields:

Interface IP: This defaults to "Any."

IP Address/Host: Enter the IP address of the device you want to ping. Often this will be a computer or router within your service provider's network.

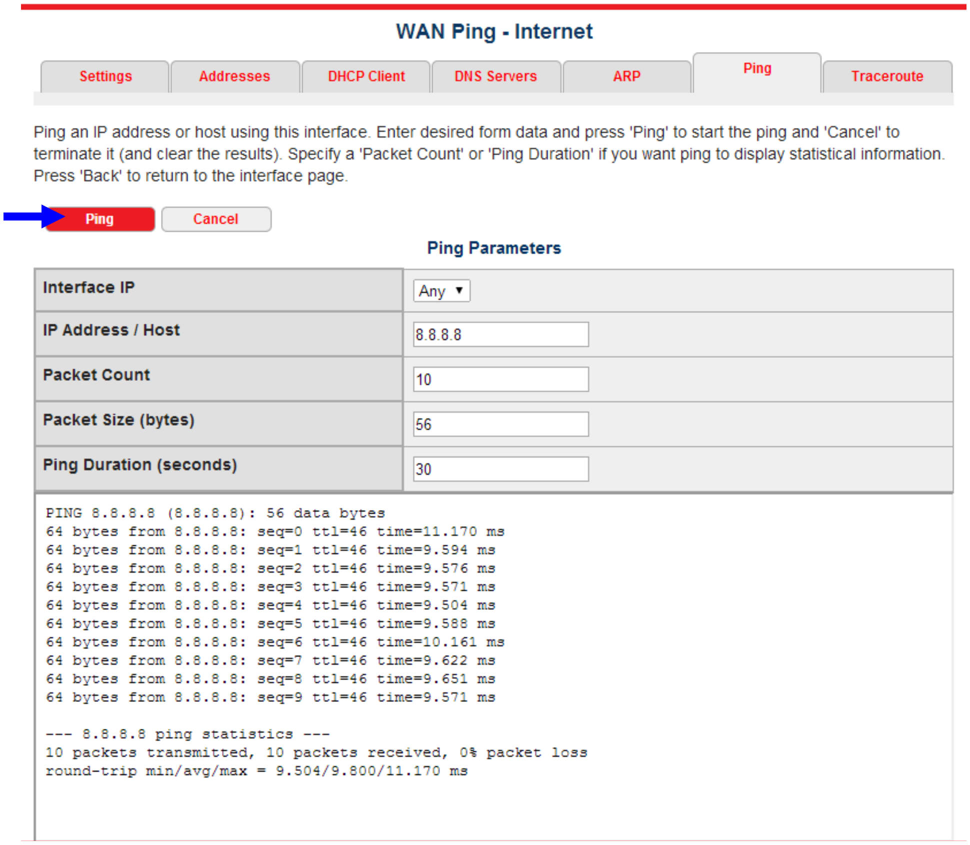
Packet Count: This refers to the number of packets of information you want to send to the IP address/Host above. Typically, the default is adequate.

Packet Size (bytes): This refers to the amount of information in each packet, in bytes. Typically, the default is adequate.

Ping Duration (seconds): This refers to how long (in seconds) you want to keep querying this other computer to see if it responds. Typically, the default is adequate.

After entering all fields, click the 'Ping' button in the upper left, highlighted in Figure 6-7 below.

Figure 6-7.  WAN - Ping example.



WAN Ping - Internet

Ping an IP address or host using this interface. Enter desired form data and press 'Ping' to start the ping and 'Cancel' to terminate it (and clear the results). Specify a 'Packet Count' or 'Ping Duration' if you want ping to display statistical information. Press 'Back' to return to the interface page.

Ping Parameters

| | |
|---|---|
| Interface IP | Any ▾ |
| IP Address / Host | 8.8.8.8 |
| Packet Count | 10 |
| Packet Size (bytes) | 56 |
| Ping Duration (seconds) | 30 |

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=46 time=11.170 ms
64 bytes from 8.8.8.8: seq=1 ttl=46 time=9.594 ms
64 bytes from 8.8.8.8: seq=2 ttl=46 time=9.576 ms
64 bytes from 8.8.8.8: seq=3 ttl=46 time=9.571 ms
64 bytes from 8.8.8.8: seq=4 ttl=46 time=9.504 ms
64 bytes from 8.8.8.8: seq=5 ttl=46 time=9.588 ms
64 bytes from 8.8.8.8: seq=6 ttl=46 time=10.161 ms
64 bytes from 8.8.8.8: seq=7 ttl=46 time=9.622 ms
64 bytes from 8.8.8.8: seq=8 ttl=46 time=9.651 ms
64 bytes from 8.8.8.8: seq=9 ttl=46 time=9.571 ms

--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 9.504/9.800/11.170 ms
```

Figure 6-7 shows an example of what the ping results will look like when the ping is successful. In the above example, we sent 10 packets of information to IP address 8.8.8.8, and see that each of the 10 packets received a response in under 12 milliseconds with no loss of data.

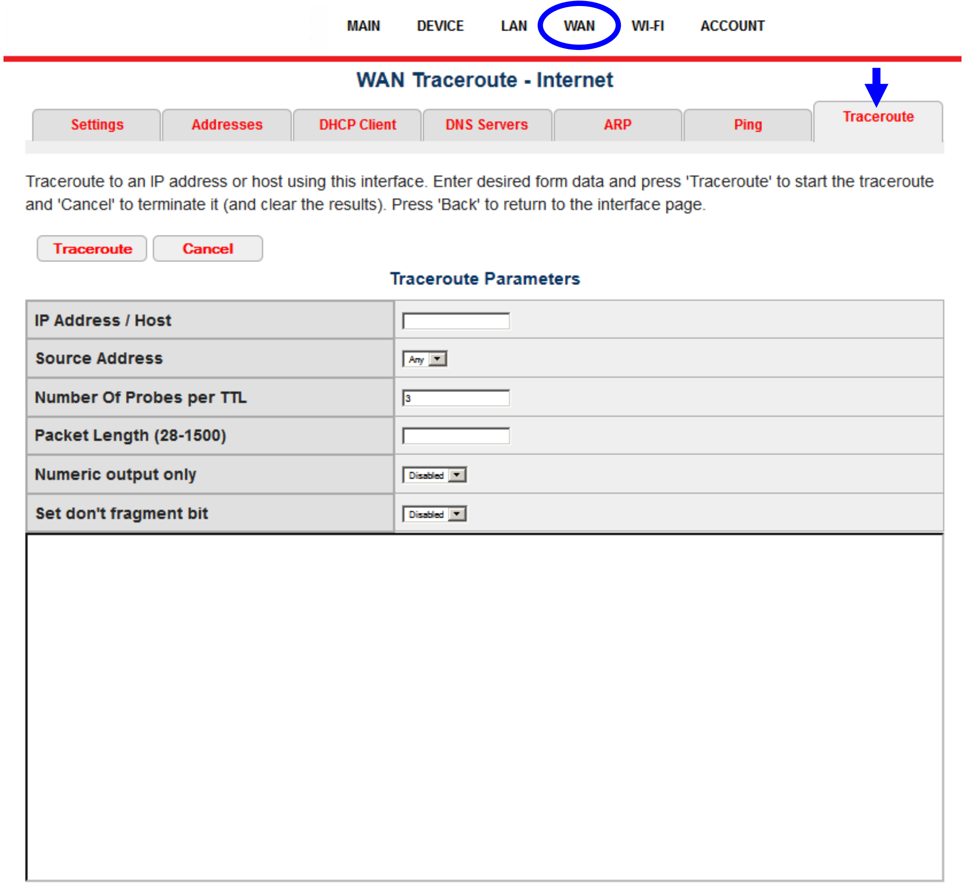
## Traceroute

Traceroute is a tool that allows you see the various “hops” a signal makes between your Residential Gateway and a given destination (another computer or website), including all the delays along the path.  In contrast, ping just gives the round-trip times between the two endpoints.  Knowing where the delays are in the network can be a useful trouble-shooting tool.

To use the traceroute tool, follow these steps:

1. From the Main page, click on ‘WAN’ in the first line tabs, highlighted in Figure 6-8 below.
2. Click on the ‘Traceroute’ tab, highlighted in Figure 6-8 below.
3. The screen that displays will look similar to Figure 6-8.

**Figure 6-8. WAN - Traceroute page.**



WAN Traceroute - Internet

Traceroute to an IP address or host using this interface. Enter desired form data and press 'Traceroute' to start the traceroute and 'Cancel' to terminate it (and clear the results). Press 'Back' to return to the interface page.

Traceroute Parameters

| | |
|---|---|
| IP Address / Host | |
| Source Address | Any |
| Number Of Probes per TTL | 3 |
| Packet Length (28-1500) | |
| Numeric output only | Disabled |
| Set don't fragment bit | Disabled |

Enter the following traceroute parameters:

IP Address/Host: Enter the IP address of the destination computer.

Source Address: This defaults to "Any."

Number of Probes per TTL: Enter the number of probes (messages) to send to each hop. The default is 3, but values can range from 1 to 64. TTL stands for time to live. An internal counter or timer is placed in each packet of information. The TTL prevents a message that has been delayed excessively or has gone through too many hops from circulating indefinitely. After the TTL limit is reached, the message "expires" and is discarded.

Packet Length: Enter the length, in bytes, of the packet of information you want to send. Any integer between 28 and 1500 is acceptable.

Numeric output only: If this is enabled, it shows the IP and MAC addresses of each computer the packet of information traversed on its way to its destination. If this is disabled, then it also shows the website names of the computer(s) it traversed.

Set don't fragment bit: This is only applicable for very large packets of information. If the 'don't fragment bit' is enabled, then the packet will have to be transmitted in its entirety successfully at each hop. If it is disabled, then large packets of information may be broken up into smaller fragments. Each fragment may traverse a different set of hops on its way to its destination, and then the message is reassembled at the end.

When each of these parameters has been entered, click on the ‘Traceroute’ button in the upper left to start sending the message and tracing the route it takes to its destination. The output – shown in the lower portion of the screen - will contain the time (usually in milliseconds) at each hop and each hop’s IP address, among other things. The probe status will report ‘successful’ – meaning it arrived at its destination without exceeding the TTL limit – or ‘unsuccessful’ – meaning the packet of information did not arrive at its destination. This can signify a connection problem or sometimes, a network traffic congestion problem.

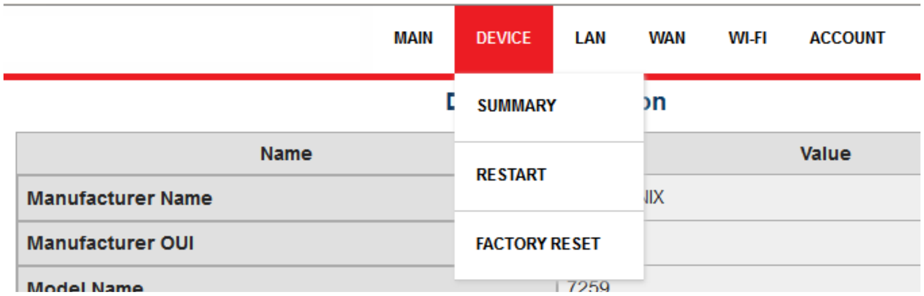
# 7. Periodic Maintenance

This section covers tasks that you might do or encounter infrequently, if at all. Most of the time, if you experience something out of the ordinary, you will contact your service provider.

## The Device Menu

In the first line tabs (menu in the header), if you hover over the Device menu, you will see a submenu containing the options Summary Restart, and Factory Reset (refer to Figure 7-1). These are discussed below.

Figure 7-1. Device hover menu, showing sub-menu.

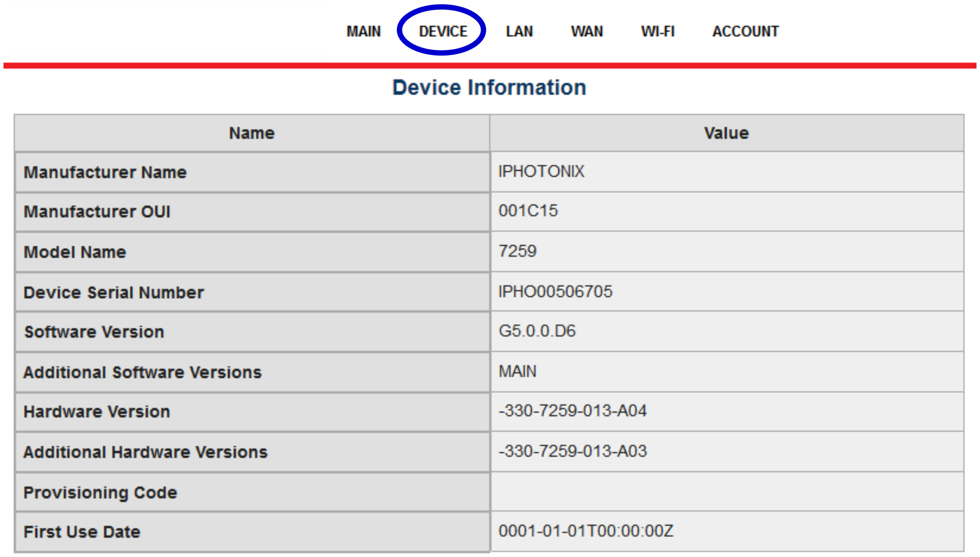


| Name | Value |
|---|---|
| Manufacturer Name | IX |
| Manufacturer OUI | |
| Model Name | 7259 |

### Summary

From the Device menu, click on 'Summary' to view a summary about your Residential Gateway device. See example in Figure 7-2 below (your device information will differ).

Figure 7-2. Device Information page.



Device Information

| Name | Value |
|---|---|
| Manufacturer Name | IPHOTONIX |
| Manufacturer OUI | 001C15 |
| Model Name | 7259 |
| Device Serial Number | IPHO00506705 |
| Software Version | G5.0.0.D6 |
| Additional Software Versions | MAIN |
| Hardware Version | -330-7259-013-A04 |
| Additional Hardware Versions | -330-7259-013-A03 |
| Provisioning Code | |
| First Use Date | 0001-01-01T00:00:00Z |

When you have a problem with your device, your service provider may ask you for some information from this page, such as the serial number, software version, or hardware version. There are no editable fields on this screen; it is for informational purposes only (view-only).

### Restart

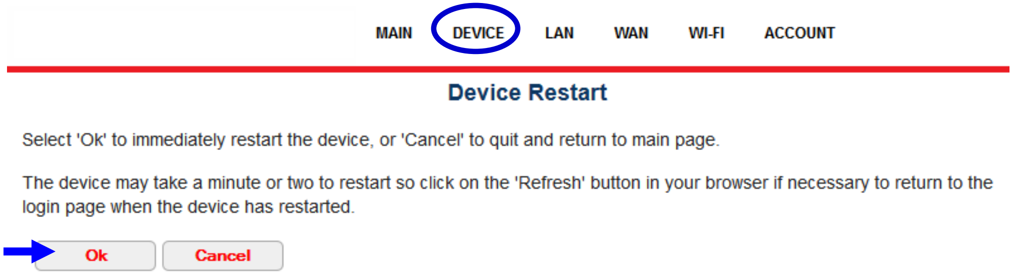
In rare cases, if your Residential Gateway device is “hung” (ceases to operate), you may be able to resolve the problem by restarting (also called rebooting) your Residential Gateway. Additionally, your service provider may ask that you do this while trouble-shooting a problem.

⚠ Doing a restart will close all Residential Gateway connections for a short period of time. During this period, all Ethernet and wireless will be disconnected from the Internet, and all CATV and phones will ceases to work. Make sure that no operations are on-going that could be adversely affected (such as downloading a file from the Internet, recording a TV show, etc.) before doing a restart.

There are two ways to restart your Residential Gateway:

- Via the Device menu, select the ‘Restart’ option, shown in Figure 7-3.
- Via the On/Off button on the back of your Residential Gateway device, shown in Figure 2-1.

**Figure 7-3. Device Restart page.**



Device Restart

Select 'Ok' to immediately restart the device, or 'Cancel' to quit and return to main page.

The device may take a minute or two to restart so click on the 'Refresh' button in your browser if necessary to return to the login page when the device has restarted.

Device Restart: After selecting the ‘Restart’ submenu option on the Device menu, you will see the screen above (Figure 7-3). The device will not actually restart until you click on ‘OK’ (highlighted in Figure 7-3). You may opt to click ‘Cancel’ to avoid a restart and return to the previous page.

With either method you use to restart the Residential Gateway, keep in mind that the restarting process may take up to 5 minutes. The lights on the front will flash, and after about 2 to 5 minutes when the lights stop flashing, you will need to log back into the device again, and all devices will need to re-establish their connection to the device.

ⓘ Restarting does not change any existing settings or configurations. However, it causes all new leases to be issued to connected devices, and all statistics (for example, see Figure 5-4) and error logs will be cleared and begin accumulating anew.

### Factory Reset

If there appears to be corruption, hanging, or a failed software upgrade, or if you can no longer log into the system (for example, if the only ‘enabled’ user has lost or forgotten their password) you may be forced to reset your Residential Gateway to its factory default programs in order to clear the fault(s), and/or log back in with the factory default password (serial number).

**WARNING** This option should be used with **great caution**, as it will **erase all settings and configurations** you have made, including your SSID name, users, security settings, and LAN configurations. All connectivity will be lost and you would need to start again from scratch to configure the device, which may take some time.

There are two ways to do a factory reset:

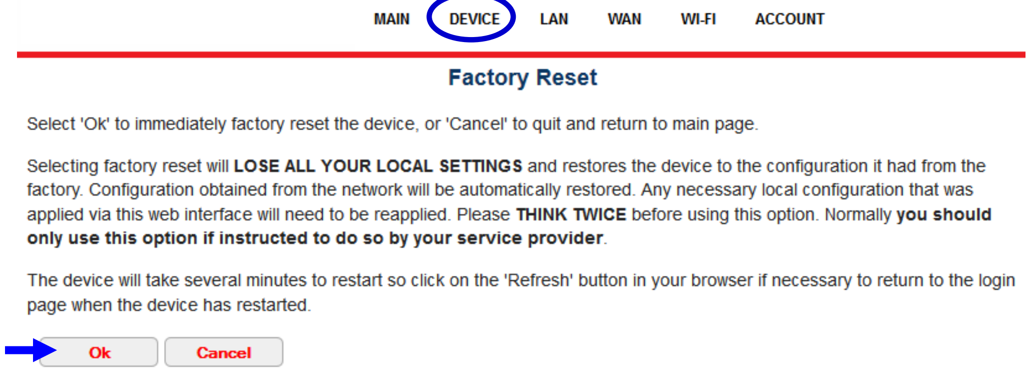
- Via software, using the Device menu.
- Via hardware, pressing the 'Reset' button.

If the Residential Gateway is hung in such a way that the software is not accessible, the hardware method may need to be used. Either should only be done as a last resort, and after consulting with your service provider.

⚠ Before doing a factory reset, be sure all users and connected devices are disengaged from using the system. During a factory reset, all Ethernet and wireless will be disconnected from the Internet, and all CATV and phones will ceases to work. Make sure that no operations are on-going that could be adversely affected (such as downloading a file from the Internet, recording a TV show, etc.) before doing a factory reset.

Device Menu – Factory Reset: Select the 'Factory Reset' option from the Device menu. The screen shown in Figure 7-4 will be displayed. *Read the warning carefully on this screen*. You may opt to click 'Cancel' to avoid a resetting your Residential Gateway and return to the previous page. Only when you are *sure* you want to proceed with doing a factory reset, or if told to do so by your service provider, click the 'OK' button highlighted in Figure 7-4.

**Figure 7-4. Device - Factory Reset page.**



Factory Reset

Select 'Ok' to immediately factory reset the device, or 'Cancel' to quit and return to main page.

Selecting factory reset will **LOSE ALL YOUR LOCAL SETTINGS** and restores the device to the configuration it had from the factory. Configuration obtained from the network will be automatically restored. Any necessary local configuration that was applied via this web interface will need to be reapplied. Please **THINK TWICE** before using this option. Normally **you should only use this option if instructed to do so by your service provider**.

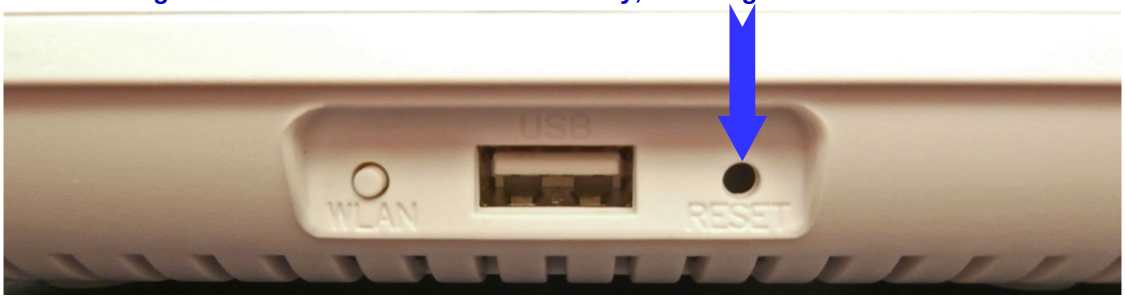
The device will take several minutes to restart so click on the 'Refresh' button in your browser if necessary to return to the login page when the device has restarted.

Factory Reset Button: Using this hardware method of doing a factory reset may be required if your Residential Gateway software is hung or corrupted in such a way that the Device menu is inaccessible, or if the only enabled user has lost or forgotten their password and is unable to log in. To use this method, you will need a small, thin implement, such as an unkinked paper clip.

On the side of the Residential Gateway is small hole marked 'Reset' (refer to Figure 7-5 below). Insert the end of the paper clip into the hole marked 'Reset, highlighted in Figure 7-5 below.

Hold the end of the paper clip pressing inside this hole for at least 3 seconds. Then release.

**Figure 7-5. Side of Residential Gateway, showing the 'Reset' button.**



After doing a Factory Reset - regardless of which method you used - the Residential Gateway's lights will flash, and after about 2 to 5 minutes when the lights stop flashing, you should be able to log back into the device again. However, you will need to log back in using the factory default user "admin" and factory default password (the serial number). Refer to the instructions on Logging Into the Residential Gateway. You will also need to re-do all your settings and configuration, including resetting your SSID name, users, security settings, and LAN configurations. All devices will need to re-establish their connection to the device.

## Software Updates

As new software is released, your service provider may need to apply software updates to your Residential Gateway. This is usually done during a maintenance window so as not to inconvenience the subscribers. Maintenance windows usually occur during off hours - such as between 2am and 5am – and your service provider may announce this beforehand. The downloading of software to your Residential Gateway occurs transparently. However, after new software is downloaded, the system will automatically reboot for the new software to take effect. If you happen to be using the Residential Gateway at the time of the reboot, you would experience a brief interruption of service. This is normal.

If the software update failed, your Residential Gateway may not come back online, and the 'Fail' light on the front of the unit will be red and flashing quickly (refer to Figure 2-2 and Table 2-1). If this happens contact your service provider.