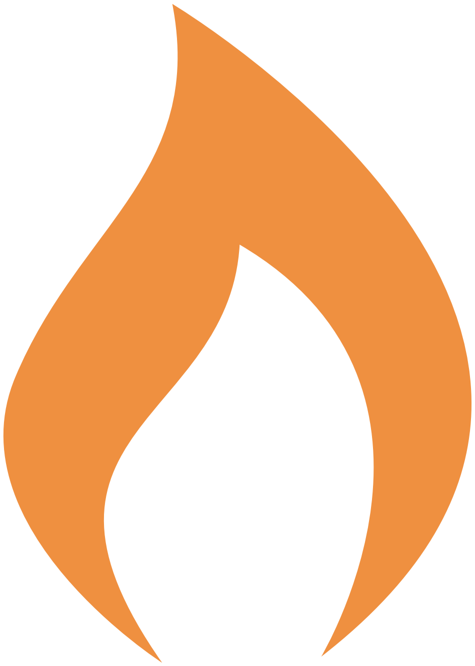
User Manual

MetroLinq^{TM}

Software Release v1.2.0 & v2.1.0



www.ignitenet.com

User Manual

IgniteNet MetroLinq^{TM}

Cloud-Enabled 60 GHz Outdoor Point-to-Point
and Point-to-Multipoint Wireless Bridges

MetroLinq™ 60 PTP

MetroLinq™ 2.5G 60 PTP

MetroLinq™ 2.5G 60 PTMP

MetroLinq™ 60 LW

MetroLinq™ 5 LW

MetroLinq™ 10G Tri-Band Omni

FW2.1.0
E062018-KS-R03
150200001394A

How to Use This Guide

This guide includes detailed information on IgniteNet MetroLinq wireless bridge software, including how to operate and use the management functions of the wireless bridge. To deploy wireless bridges effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all software features.

Who Should Read This Guide?

This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks), the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

How This Guide is Organized

The organization of this guide is based on the wireless bridge's web management interface. An introduction and initial configuration information is also provided.

The guide includes these sections:

- Section I "Getting Started" — Includes an introduction to wireless bridge management and initial configuration settings.
- Section II "Web Configuration" — Includes all management options available through the web interface.
- Section III "Appendices" — Includes information on troubleshooting wireless bridge management access.

Related Documentation

This guide focuses on wireless bridge software configuration, it does not cover hardware installation of an wireless bridge. For specific information on how to install an wireless bridge, see the following guide:

Quick Start Guide

For all safety information and regulatory statements, see the following documents:

Quick Start Guide
Safety and Regulatory Information

Conventions

The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warning: Alerts you to a potential hazard that could cause personal injury.

Revision History

This section summarizes the changes in each revision of this guide.

Table 1: Revision History

Revision	Date	Change Description
1.2.0 & 2.1.0	06/2018	**New:** ◆ “Stand-alone Mode Only” on page 14 ◆ “Welcome” on page 20 ◆ “2.4 GHz Wireless Status” on page 30 ◆ “Traffic Control Settings” on page 36 ◆ “Radio#1 or #4 — 2.4 GHz Settings” on page 50 ◆ “Ping” on page 65 ◆ “Traceroute” on page 66 ◆ “Nslookup” on page 66 ◆ “Speed Test” on page 67 ◆ “Operational and Performance Issues” on page 70 ◆ “MetroLinq Omni 10G Sectors” on page 73 ◆ “Device Discovery Tool” on page 74 **Updated:** ◆ “Configuration Options” on page 14 ◆ “Connecting to the Web Interface” on page 16 ◆ “Setup Wizard” on page 17 ◆ “The Dashboard” on page 19 ◆ “Common Web Page Buttons” on page 20 ◆ “General Status” on page 24 ◆ “Interface Information” on page 26 ◆ “5 GHz Wireless Status” on page 27 ◆ “60 GHz Wireless Status” on page 29 ◆ “Radio Settings Overview” on page 37 ◆ “Radio#0 — 5 GHz Settings” on page 38 ◆ “Radio#1, #2 or #3 — 60 GHz Settings” on page 44 ◆ “System Settings” on page 55 ◆ “Upgrading Firmware” on page 58 ◆ “SNMP” on page 63

Table 1: Revision History

Revision	Date	Change Description
2.0.1	01/2018	**New:** ◆ "5 GHz Wireless Status" on page 27 ◆ "60 GHz Wireless Status" on page 29 ◆ "PING Watchdog" on page 64 **Updated:** ◆ "Dashboard" on page 17 ◆ "General Status" on page 24 ◆ "Internet Status" on page 25 ◆ "Interface Information" on page 26 ◆ "Wireless Status" on page 27 ◆ "Internet Settings" on page 33 ◆ "Ethernet Settings" on page 35 ◆ "Wireless Settings" on page 37
1.1.5	04/2017	**New:** ◆ "SNMP" on page 63 ◆ "Failure Count— Total consecutive ping failures before the watchdog service reboots the wireless bridge. (Default: 5)" on page 64 **Updated:** ◆ "Radio#0 — 5 GHz Settings" on page 38
1.1.2	04/2016	Initial release

Contents

Figures

Tables

Section I

Getting Started

This section provides an overview of the wireless bridge, and introduces some basic concepts about wireless networking. It also describes the basic settings required to access the management interface.

This section includes these chapters:

1 Introduction

The wireless bridge runs software that includes a network management agent. The agent offers a variety of management options, including a web-based interface. The wireless bridge can also be accessed via Telnet or SSH for configuration using a command line interface (CLI).

Stand-alone Mode Only

This manual describes the configuration interface for **stand-alone** mode. The wireless bridge can be completely configured for full operations, through the local management agent. It may also be necessary at times to access the device's stand-alone management interface to perform certain configuration and troubleshooting procedures. In stand-alone mode, there are procedures to perform antenna alignments, Internet diagnostics, and link performance testing.

Initial Cloud Configuration

The MetroLinq wireless bridge is by default cloud-enabled. If you want to configure and administer the MetroLinq using the IgniteNet Cloud Controller, the wireless bridge is already 'out-of-the-box' configured to be managed from the cloud controller.

Simply connect the wireless bridge directly to a network with both DHCP and Internet service available. Once the hardware identification parameters for your wireless bridge are added to the cloud controller database, the cloud controller will be able to add and configure the device without any local device configuration necessary. Refer to the IgniteNet Cloud Controller User Manual for information on configuring the wireless bridge through the cloud interface.

Configuration Options

The wireless bridge's web agent allows you to configure wireless bridge parameters, monitor wireless connections, and display statistics using a standard web browser such as Internet Explorer 9.x or later, Mozilla Firefox 32 or later, and Google Chrome 35 or later. The wireless bridge's web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed remotely by a Telnet or Secure Shell (SSH) connection over the network. The CLI is used primarily for technical support.

The wireless bridge's web interface allows you to perform management functions such as:

- Set management access user names and passwords
- Setup multiple services and set system settings
- Configure IP and Ethernet settings
- Configure 60 GHz, 5 GHz, and 2.4 GHz radio settings
- Control access through wireless security settings
- Download system firmware
- Download or upload configuration files
- Display system information and statistics
- Conduct network tests

Network Connections

Prior to accessing the wireless bridge's management agent through a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using the web interface, or the DHCP protocol.

The wireless bridge is by default in DHCP mode but it also has a static fallback default management address of 192.168.1.20 and a subnet mask of 255.255.255.0. If the wireless bridge's default IP address is not compatible with your network or a DHCP server is not available, the wireless bridge's IP address must be configured manually through the web interface.

First connect to the wireless bridge's LAN port and log in to the web interface, as described in "Connecting to the Web Interface" on page 16. Follow the steps described in "Setup Wizard" on page 17 to select your country and specify one of the configuration methods. Then configure the wireless bridge with an IP address that is compatible with your network, as described under "Internet Settings" on page 33.

Once the wireless bridge's IP settings are configured for your network, you can access the wireless bridge's management agent from anywhere within the attached network. The wireless bridge can be managed by any computer using a web browser.

Connecting to the Web Interface

The wireless bridge offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer 9.x or later, Mozilla Firefox 32 or later, and Google Chrome 35 or later.

You may want to make initial configuration changes by connecting a PC directly to the wireless bridge's LAN port. The wireless bridge's RJ-45 LAN port is set to operate by default in DHCP mode. If no DHCP server is available on the connected LAN, the wireless bridge has a fall-back management IP address of 192.168.1.20 with a subnet mask of 255.255.255.0. You must set your PC IP address to be on the same subnet as the wireless bridge (that is, the PC and wireless bridge addresses must both start with 192.168.1.x).

To access the wireless bridge's web management interface, follow these steps:

1. If your device is connected to a LAN with a DHCP server, you can use IgniteNet's Device Discovery Tool to find your device's IP and open the management interface in your web browser - See "Device Discovery Tool" on page 74.

   - otherwise -

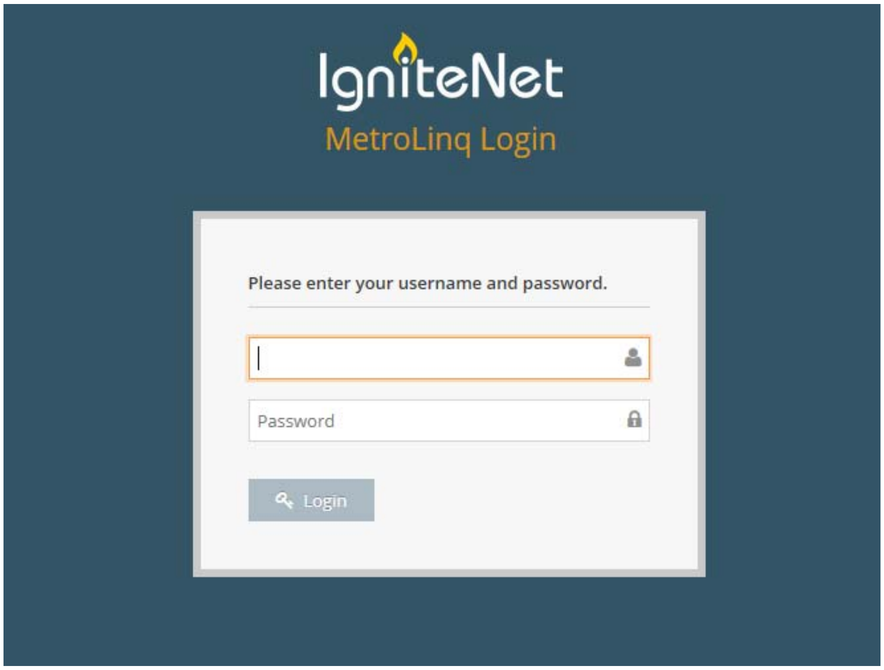
   If there is no DHCP server, use your web browser to connect to the management interface using the default IP address of 192.168.1.20.

2. Log in to the interface by entering the default user name "root" with the password "admin123", then click Login.

Note: It is strongly recommended to change the default user name and password the first time you access the web interface. For information on changing user names and passwords, see "User Accounts" on page 59.

Note: When connecting a computer directly to the wireless bridge's Ethernet port and no external DC power source is provided, it is recommended to use the PoE power injector included with the wireless bridge.

Figure 1: Login Page



Please enter your username and password.

Setup Wizard

Before using the wireless bridge for the first time or after a reset, the Setup Wizard configures the management mode of the wireless bridge.

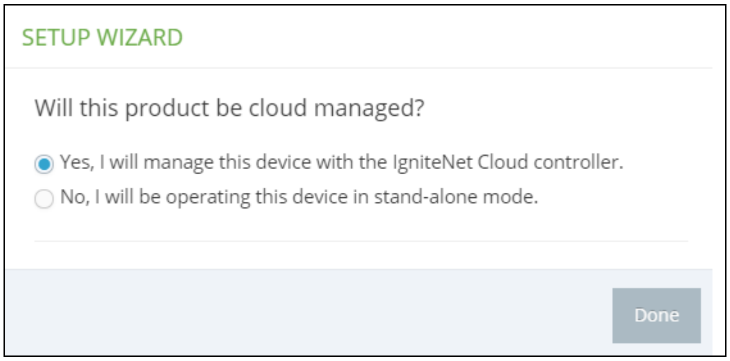
Management Mode

Select to Cloud Manage wireless bridge — To manage the wireless bridge using the IgniteNet Cloud controller, select either:

- "Yes, I will manage this device with the IgniteNet Cloud controller." - or -
- "No, I will be operating this device in stand-alone mode."

Click “Done” to complete the Setup Wizard.

Figure 2: Select Cloud Managed



SETUP WIZARD

Will this product be cloud managed?

● Yes, I will manage this device with the IgniteNet Cloud controller.
○ No, I will be operating this device in stand-alone mode.

After you select to manage the wireless bridge using the IgniteNet Cloud controller, go to **cloud.ignitenet.com** to register your wireless bridge. Log in and select **Devices** from the menu. Click **Add Device** and enter the wireless bridge serial number and MAC address to register the wireless bridge with your cloud network. The serial number and MAC address can be found on the product packaging or label.

Note: This manual describes the configuration interface for stand-alone mode. Refer to the IgniteNet Cloud Controller User Manual for information on configuring the wireless bridge through the cloud interface.

Note: If the wireless bridge will only be configured from the IgniteNet Cloud Controller, it is unnecessary to perform the above procedure. Refer to “Initial Cloud Configuration” on page 14.

Note: For certain maintenance procedures such as for example, antenna alignment, the wireless bridge may be cloud-enabled but the procedure will still use the local management agent interface.

Main Menu

The web interface Main Menu provides access to all the configuration settings available for the wireless bridge.

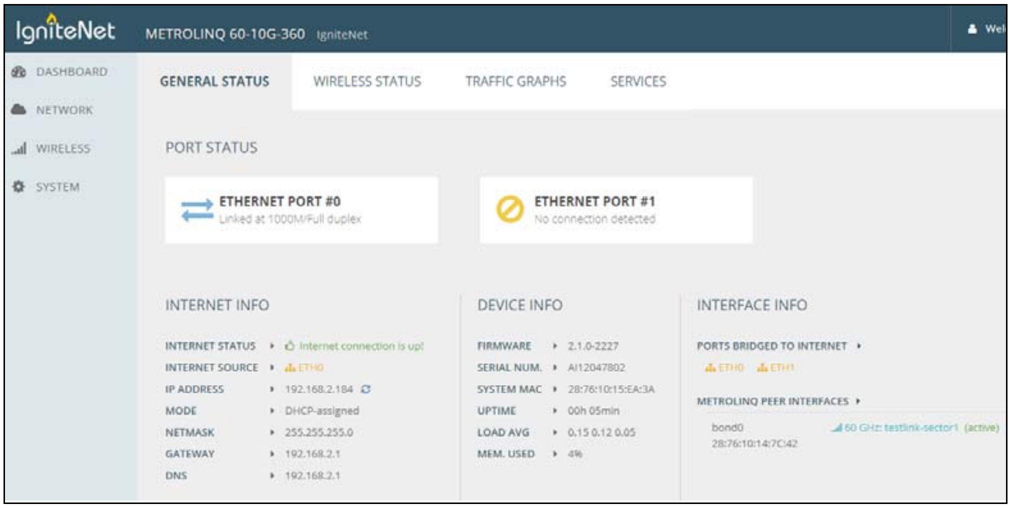
To configure settings, click the relevant Main Menu item. Each Main Menu item is summarized below with links to the relevant section in this guide where the configuration parameters are described in detail:

- **Dashboard** — The dashboard shows basic settings for the wireless bridge, including Internet status, local network settings, wireless radio status, traffic graphs and services. See "Status Information" on page 23.
- **Network** — Configures Internet and Ethernet settings. See "Network Settings" on page 33.
- **Wireless** — Configures 5 GHz and 60 GHz radio settings. See "Wireless Settings" on page 37
- **System** — Configures System (designation and location), Maintenance (such as view log, firmware upgrade, and reset), User Accounts, Services (management access methods), and Diagnostics (Ping, Traceroute, and Nslookup). See "System Settings" on page 54

Dashboard

After logging in to the web interface, the dashboard screen is displayed. The dashboard shows basic settings for the wireless bridge, including Internet status, local network settings, wireless radio status, traffic graphs, and services.

Figure 3: The Dashboard



PORT STATUS

ETHERNET PORT #0
Linked at 1000M/Full duplex

ETHERNET PORT #1
No connection detected

INTERNET INFO

INTERNET STATUS ▸ Internet connection is up!
INTERNET SOURCE ▸ ETH0
IP ADDRESS ▸ 192.168.2.184
MODE ▸ DHCP-assigned
NETMASK ▸ 255.255.255.0
GATEWAY ▸ 192.168.2.1
DNS ▸ 192.168.2.1

DEVICE INFO

FIRMWARE ▸ 2.1.0-2227
SERIAL NUM. ▸ AI12047802
SYSTEM MAC ▸ 28:76:10:15:EA:3A
UPTIME ▸ 00h 05min
LOAD AVG ▸ 0.15 0.12 0.05
MEM. USED ▸ 4%

INTERFACE INFO

PORTS BRIDGED TO INTERNET ▸
ETH0 ETH1

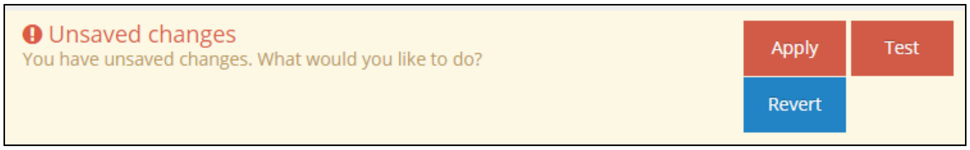
METROLINQ PEER INTERFACES ▸
bond0 28:76:10:14:7C:42 60 GHz: testlink-sector1 (active)

Common Web Page Buttons

The list below describes the common buttons found on most of the web management pages:

- **Save** – Applies the new parameters and saves them to temporary RAM memory. Also displays a message at the top of the screen to inform you that the changes have not yet been saved to Flash memory. The running configuration will **not** be saved upon a reboot unless you click the “Apply” button.

Figure 4: Set Configuration Changes

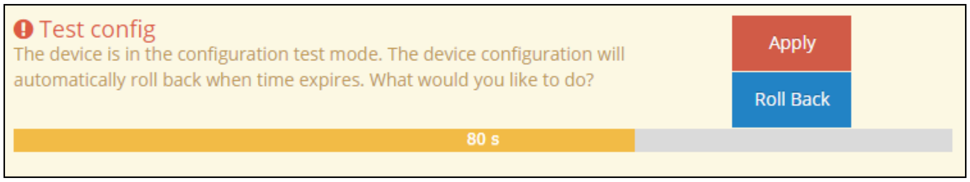


Unsaved changes

You have unsaved changes. What would you like to do?

- **Apply** – Saves the current configuration so that it is retained after a restart.
- **Revert** – Cancels the newly entered settings and restores the originals.
- **Test** – Applies the new configuration changes temporarily for 120 seconds to use as a test period to check the effect of the changes. During the 120 seconds a new dialog box with a countdown timer (Figure 5) presents you the option to click an “**Apply**” button to save the changes permanently or click a “**Roll Back”** button to revert to the previous configuration settings. If the “**Apply**” or “**Roll Back”** buttons are not clicked during the 120 second wait period, the configuration will automatically revert to previous configuration settings.

Figure 5: Test Config



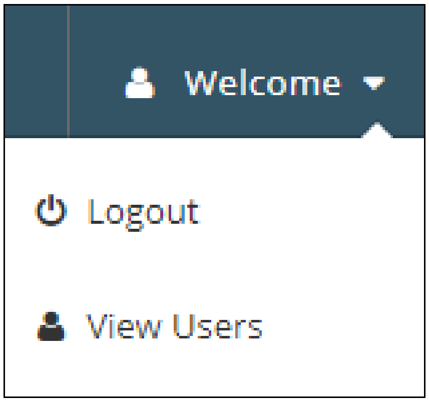
Test config

The device is in the configuration test mode. The device configuration will automatically roll back when time expires. What would you like to do?

Welcome

In the upper right corner of Wireless Bridge web interface you can find the menu item “Welcome” click it to view the options as described below.

Figure 6: Welcome Menu



- **Welcome > Logout** – Open the Welcome list and click Logout to end the web management session.
- **Welcome > View Users** – Open the Welcome list and click View Users to open the User Accounts menu.

Section II

Web Configuration

This section provides details on configuring the wireless bridge using the web browser interface.

This section includes these chapters:

2 Status Information

The Dashboard displays information on the current system configuration, including Internet status, local network settings, wireless radio status, traffic graphs, and services.

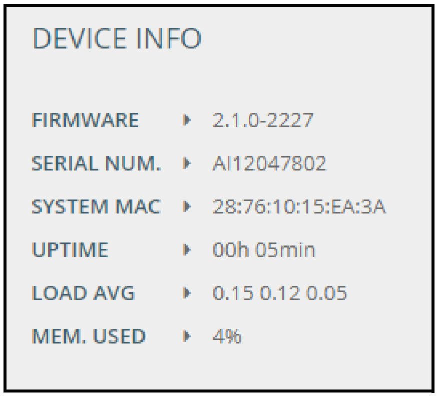
Status Information includes the following sections:

- “General Status” on page 24
- “Internet Status” on page 25
- “Port Status” on page 26
- “Interface Information” on page 26
- “Wireless Status” on page 27
- “Traffic Graphs” on page 31
- “Services” on page 32

General Status

The General Status section shows descriptive information about the wireless bridge under the Device Info heading.

Figure 7: Device Information



DEVICE INFO

FIRMWARE	2.1.0-2227
SERIAL NUM.	AI12047802
SYSTEM MAC	28:76:10:15:EA:3A
UPTIME	00h 05min
LOAD AVG	0.15 0.12 0.05
MEM. USED	4%

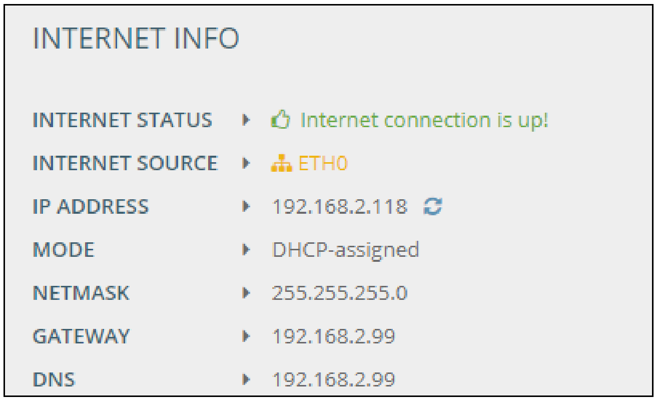
The following items are displayed in this section:

- The firmware version number.
- The serial number of the physical wireless bridge.
- The system MAC address of the wireless bridge.
- Length of time the management agent has been activated.
- The last 1-minute, 5-minute and 15-minute CPU load averages.
- The percentage of memory consumed by the running system software.

Internet Status

The Internet Info section shows information about the Internet connection.

Figure 8: Internet Status



INTERNET INFO

INTERNET STATUS	Internet connection is up!
INTERNET SOURCE	ETH0
IP ADDRESS	192.168.2.118
MODE	DHCP-assigned
NETMASK	255.255.255.0
GATEWAY	192.168.2.99
DNS	192.168.2.99

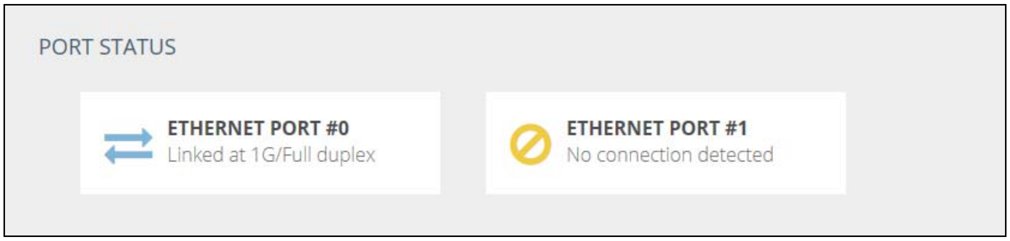
The following items are displayed in this section:

- **Internet Status** — The current up or down condition of the connection to the internet.
- **Internet Source** — The Ethernet port connected to the Internet. By default, this is Ethernet Port 0.
- **IP Address** — IP address of the Internet connection.
- **Mode** — Shows if the IP address is configured by a static setting or DHCP.
- **Netmask** — The subnet mask of the IP address.
- **Gateway** — The IP address of the gateway router that is used when a destination address is not on the local subnet.
- **DNS** — The IP address of the Domain Name Server on the network. A DNS maps numerical IP addresses to domain names and is used to identify network hosts by familiar names instead of the IP addresses.

Port Status

The Port Status section shows information about Ethernet port connections.

Figure 9: Port Status



PORT STATUS

ETHERNET PORT #0
Linked at 1G/Full duplex

ETHERNET PORT #1
No connection detected

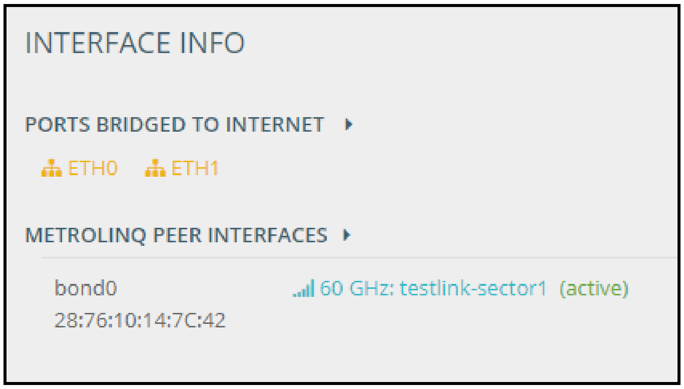
The following items are displayed in this section:

- **Ethernet Port #0** — Shows the status of the RJ-45 Ethernet port, including link-up state, speed, and duplex mode.
- **Ethernet Port #1** — Shows the status of the SFP+ Ethernet port, including link-up state, speed, and duplex mode.

Interface Information

The Interface Info section shows information about additional interfaces connected to the Internet.

Figure 10: Interface Information



INTERFACE INFO

PORTS BRIDGED TO INTERNET ▸

ETH0 ETH1

METROLINQ PEER INTERFACES ▸

bond0
28:76:10:14:7C:42

60 GHz: testlink-sector1 (active)

The following items are displayed in this section:

- **Ports Bridged to Internet** — Additional interfaces attached directly to the Internet. Lists interfaces attached to the uplink network (that is, the Internet). The MetroLinq bridges all wired and wireless interfaces and this configuration cannot be modified.

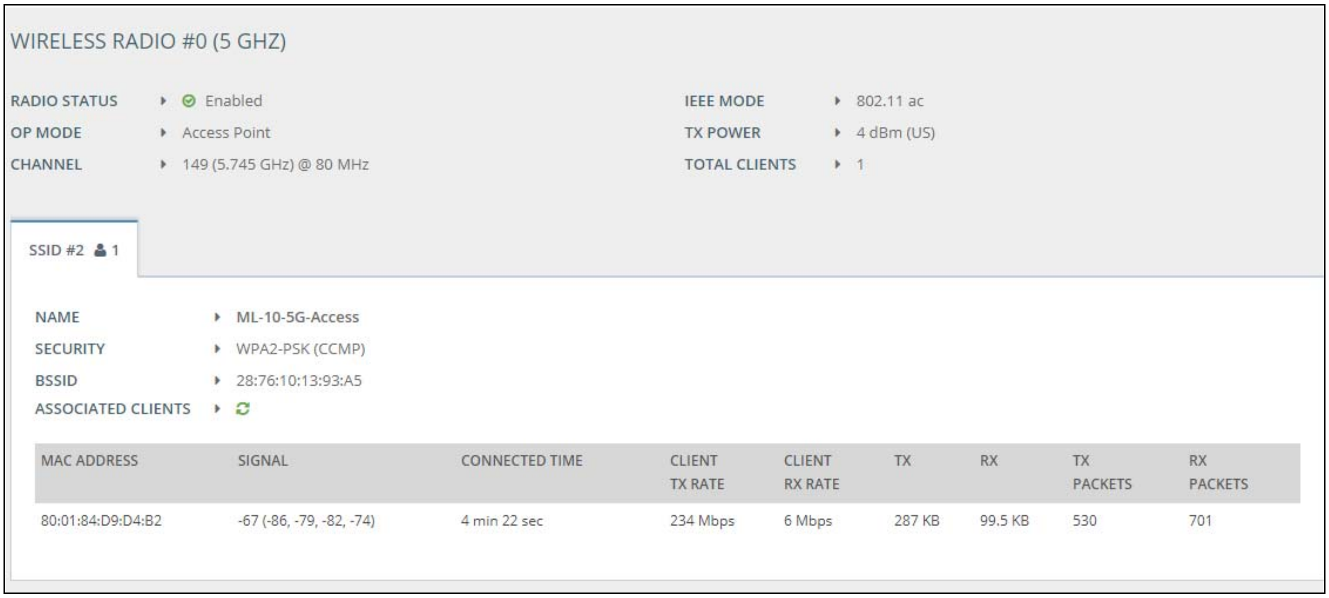
- **MetroLinq Peer Interfaces** — Active MetroLinq wireless connections i.e. wireless bonds with other MetroLinq units listing the SSID of the link, frequency and the remote MetroLinq MAC address.

Wireless Status

The Wireless Status section shows information about the radio settings and link status of 2.4 GHz, 5 GHz, and 60 GHz wireless interfaces.

Note: The frequencies and number of radios shown is dependent on the MetroLinq model.

Figure 11: Wireless Status 5 Ghz Radio



WIRELESS RADIO #0 (5 GHZ)

RADIO STATUS	✓ Enabled	IEEE MODE	802.11 ac
OP MODE	Access Point	TX POWER	4 dBm (US)
CHANNEL	149 (5.745 GHz) @ 80 MHz	TOTAL CLIENTS	1

SSID #2 1

NAME	ML-10-5G-Access
SECURITY	WPA2-PSK (CCMP)
BSSID	28:76:10:13:93:A5
ASSOCIATED CLIENTS	

MAC ADDRESS	SIGNAL	CONNECTED TIME	CLIENT TX RATE	CLIENT RX RATE	TX	RX	TX PACKETS	RX PACKETS
80:01:84:D9:D4:B2	-67 (-86, -79, -82, -74)	4 min 22 sec	234 Mbps	6 Mbps	287 KB	99.5 KB	530	701

5 GHz Wireless Status

The following items are displayed under **Wireless Radio #0 5 GHz**:

- Radio Status — Shows if the wireless interface is enabled or disabled.
- Op Mode — Shows if the wireless interface is configured to operate in master or client mode.
- Channel — The radio channel selected and its frequency.
- IEEE Mode — The 802.11 protocol mode configured for wireless host-client communications.
- TX Power — The radio power level setting in dBm

- Total Clients — The number of 802.11 wireless clients attached.

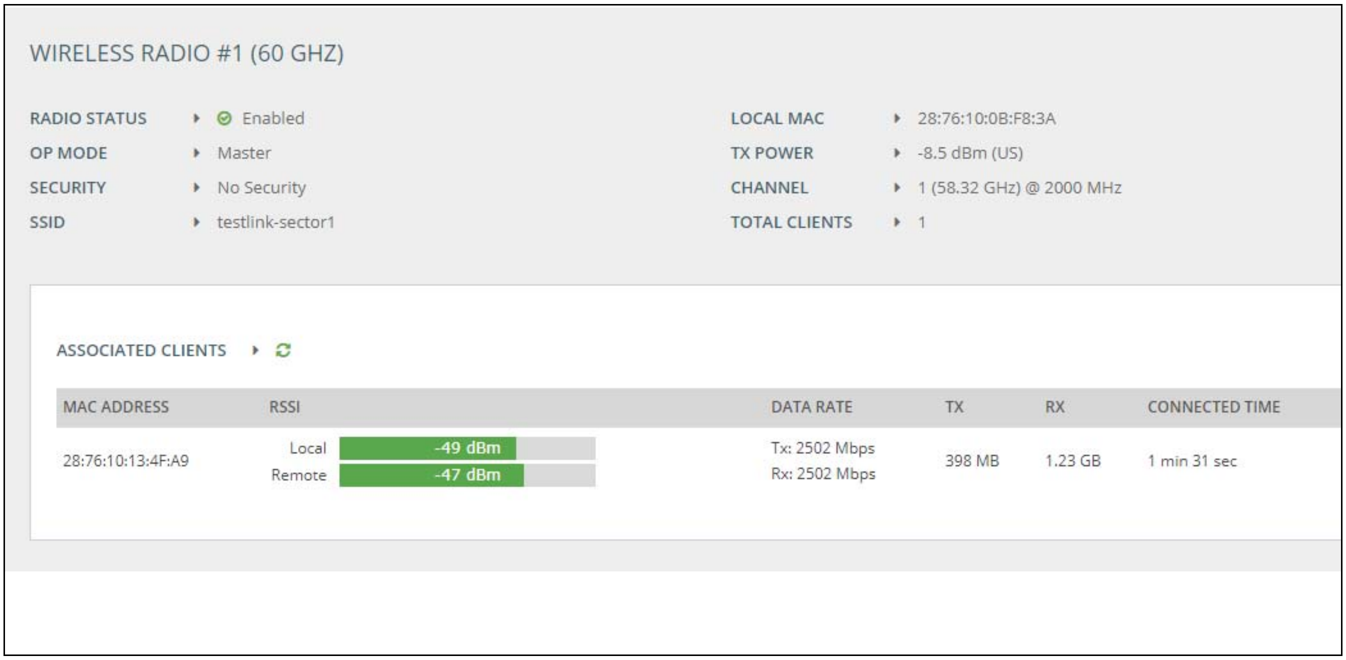
The following items are displayed under **SSID #**:

- Name — The configured SSID name broadcasted to wireless clients.
- Security — Shows whether or not security has been enabled.
- BSSID — The Basic Service Set Identifier derived from the wireless bridge MAC address.

The following items are displayed under **ASSOCIATED CLIENTS**:

- Name — The wireless client's host name.
- MAC Address — The MAC address used by the wireless client MAC layer.
- Signal — The average WiFi radio signal level measured from the client in dBm.
- Duration — The wireless client connection time.
- Client TX Rate — The current wireless data transmission rate to the client.
- Client RX Rate — The current wireless data reception rate from the client.
- TX — Total data amount transmitted to the client.
- RX — Total data amount received from the client.
- TX Packets — Total number of IP packets transmitted to the client.
- RX Packets — Total number of IP packets received from the client.

Figure 12: Wireless Status 60 Ghz Radio



WIRELESS RADIO #1 (60 GHZ)

RADIO STATUS	✓ Enabled	LOCAL MAC	28:76:10:0B:F8:3A
OP MODE	Master	TX POWER	-8.5 dBm (US)
SECURITY	No Security	CHANNEL	1 (58.32 GHz) @ 2000 MHz
SSID	testlink-sector1	TOTAL CLIENTS	1

ASSOCIATED CLIENTS

MAC ADDRESS	RSSI	DATA RATE	TX	RX	CONNECTED TIME
28:76:10:13:4F:A9	Local -49 dBm Remote -47 dBm	Tx: 2502 Mbps Rx: 2502 Mbps	398 MB	1.23 GB	1 min 31 sec

60 GHz Wireless Status

The following items are displayed under **Wireless Radio #1, 2 or 3 60 GHz**:

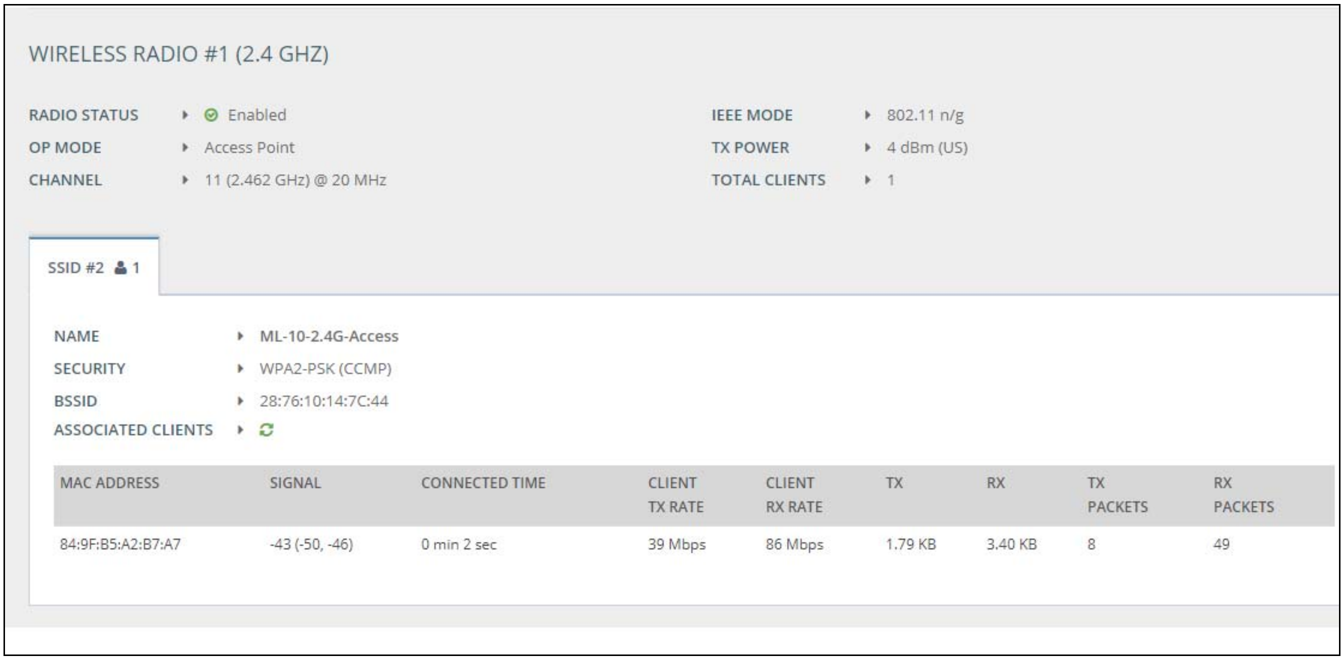
- Radio Status — Shows if the wireless interface is enabled or disabled.
- Op Mode — Shows if the wireless interface is configured to operate in Master or Client mode.
- Security — Shows whether or not security has been enabled.
- Local MAC Address — The MAC address used by 60 GHz Radio of the wireless bridge.
- TX Power — The radio power level setting in dBm
- Channel — The radio channel selected and its frequency.

The following items are displayed under **ASSOCIATED CLIENTS**:

- MAC Address — The MAC address used by the master or client associated wireless bridge.
- RSSI— The received signal strength indicator measurement of the received signal from the associated wireless bridge in dBm.
- Data Rate — The current wireless data transmission rate on the link to the associated wireless bridge.

- TX — Total data amount transmitted to the associated wireless bridge.
- RX — Total data amount received from the associated wireless bridge.
- Connected Time — The connection time of the wireless link.

Figure 13: Wireless Status 2.4 Ghz Radio



WIRELESS RADIO #1 (2.4 GHZ)

RADIO STATUS	✓ Enabled	IEEE MODE	802.11 n/g
OP MODE	Access Point	TX POWER	4 dBm (US)
CHANNEL	11 (2.462 GHz) @ 20 MHz	TOTAL CLIENTS	1

NAME ▸ ML-10-2.4G-Access
SECURITY ▸ WPA2-PSK (CCMP)
BSSID ▸ 28:76:10:14:7C:44
ASSOCIATED CLIENTS ▸

MAC ADDRESS	SIGNAL	CONNECTED TIME	CLIENT TX RATE	CLIENT RX RATE	TX	RX	TX PACKETS	RX PACKETS
84:9F:B5:A2:B7:A7	-43 (-50, -46)	0 min 2 sec	39 Mbps	86 Mbps	1.79 KB	3.40 KB	8	49

2.4 GHz Wireless Status

The following items are displayed under **Wireless Radio #1 or 4 2.4 GHz**:

- Radio Status — Shows if the wireless interface is enabled or disabled.
- Op Mode — Shows if the wireless interface is configured to operate in master or client mode.
- Channel — The radio channel selected and its frequency.
- IEEE Mode — The 802.11 protocol mode configured for wireless host-client communications.
- TX Power — The radio power level setting in dBm
- Total Clients — The number of 802.11 wireless clients attached.

The following items are displayed under **SSID #**:

- Name — The configured SSID name broadcasted to wireless clients.
- Security — Shows whether or not security has been enabled.

- BSSID — The Basic Service Set Identifier derived from the wireless bridge MAC address.

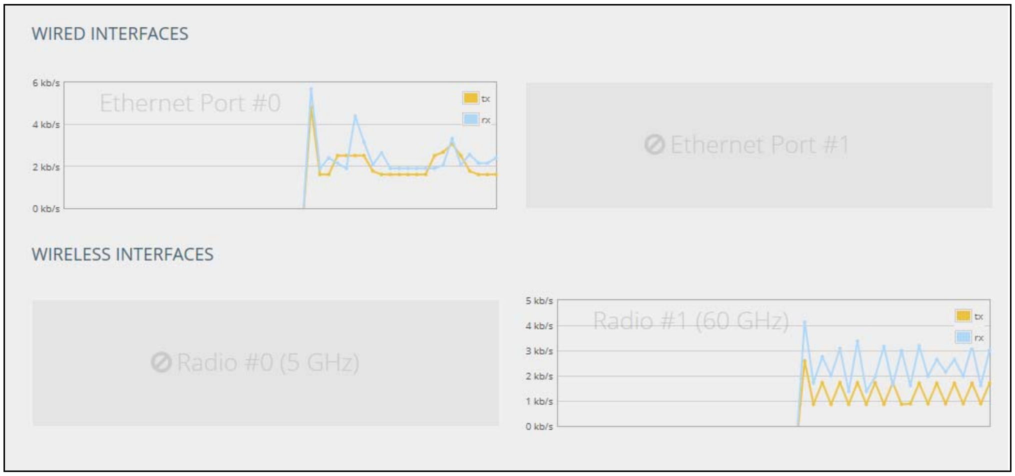
The following items are displayed under **ASSOCIATED CLIENTS**:

- Name — The wireless client's host name.
- MAC Address — The MAC address used by the wireless client MAC layer.
- Signal — The average WiFi radio signal level measured from the client in dBm.
- Duration — The wireless client connection time.
- Client TX Rate — The current wireless data transmission rate to the client.
- Client RX Rate — The current wireless data reception rate from the client.
- TX — Total data amount transmitted to the client.
- RX — Total data amount received from the client.
- TX Packets — Total number of IP packets transmitted to the client.
- RX Packets — Total number of IP packets received from the client

Traffic Graphs

The Traffic Graphs section shows the data rate for the Ethernet ports and wireless interfaces.

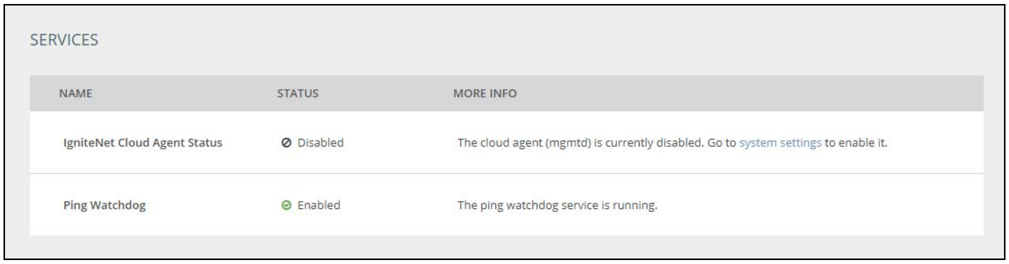
Figure 14: Traffic Graphs



Services

The Services section shows the status of the IgniteNet cloud management agent (See "System Settings" on page 55) and the Ping Watchdog (See "PING Watchdog" on page 64).

Figure 15: Services



SERVICES

NAME	STATUS	MORE INFO
IgniteNet Cloud Agent Status	⊘ Disabled	The cloud agent (mgmtd) is currently disabled. Go to system settings to enable it.
Ping Watchdog	✓ Enabled	The ping watchdog service is running.

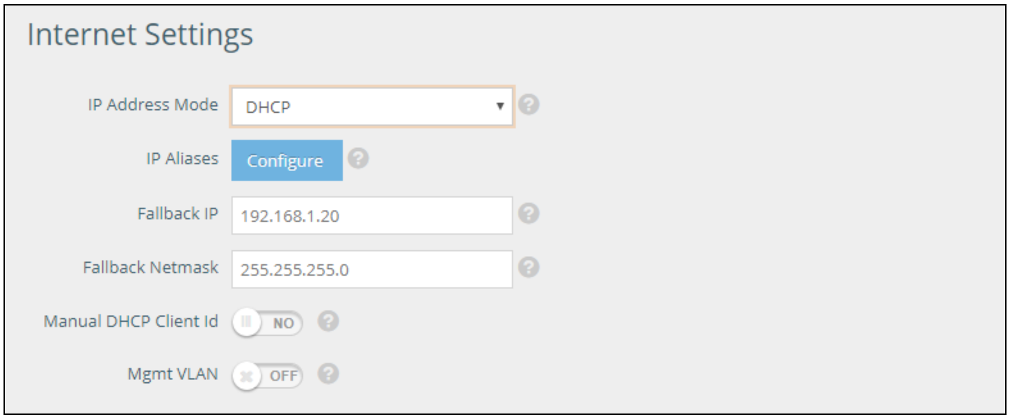
3 Network Settings

This chapter describes basic network settings on the wireless bridge. It includes the following sections:

Internet Settings

The Internet Settings page configures the basic Internet settings for the wireless bridge, such as the IP address mode, Falback IP address and IP aliases.

Figure 16: Internet Settings



Internet Settings

IP Address Mode: DHCP

IP Aliases: Configure

Fallback IP: 192.168.1.20

Fallback Netmask: 255.255.255.0

Manual DHCP Client Id: NO

Mgmt VLAN: OFF

The following items are displayed on this page:

- **IP Address Mode** — The method used to provide an IP address for the Internet access port. (Default: DHCP; Options: DHCP, static IP)
  - **DHCP** — Configuration options displayed for DHCP are shown in Figure 16, "Internet Settings", on page 33.
  - **Static IP** — To configure a static IP address for the selected Ethernet interface, the following items must be specified.

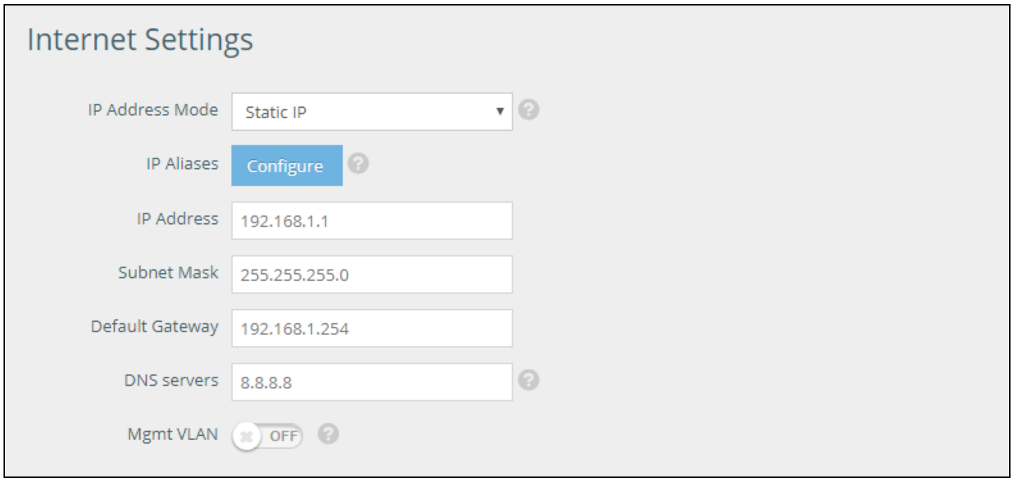
- **Fallback IP** — The IPv4 address used when a DHCP server is unavailable. (Default: 192.168.1.20)

- **Fallback Netmask** — The subnet mask used for the Fallback IP address. (Default: 255.255.255.0)

- **Manual DHCP Client ID** — Turn this on to enter a custom DHCP client host name.

- **Mgmt VLAN** — If your network uses a specific management VLAN for management traffic turn this on and then enter the VLAN ID for your management network (Range: 0-4094).

Figure 17: IP Address Mode – Static IP



Internet Settings

IP Address Mode: Static IP

IP Aliases: Configure

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

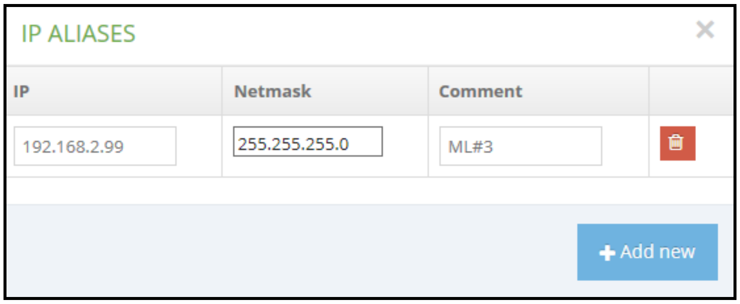
Default Gateway: 192.168.1.254

DNS servers: 8.8.8.8

Mgmt VLAN: OFF

- **IP Aliases** — Adds a static IPv4 address under which the wireless bridge can also be reached.

Figure 18: IP Alias



IP ALIASES

IP	Netmask	Comment
192.168.2.99	255.255.255.0	ML#3

- **IP Address** — Specifies an IP address for the wireless bridge. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.1.1)

- **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)

- **Default Gateway** — The IP address of the default gateway, which is used if the requested destination address is not on the local subnet.

  If you have management stations, DNS, RADIUS, or other network servers located on another subnet, type the IP address of the default gateway router in the text field provided.

- **DNS Servers** — The IP address of Domain Name Servers on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

  If you have a DNS servers located on the local network, type the IP addresses in the text field provided. Up to four IP addresses can be entered, each separated by spaces.

Note: Before enabling a management VLAN on the wireless bridge, be sure to configure the attached network switch port to support tagged VLAN frames for the VLAN ID configured on the wireless bridge. Otherwise, connectivity to the wireless bridge will be lost when you enable the VLAN feature.

Ethernet Settings

The Ethernet Settings page configures the network behavior of the Ethernet ports, indicating that a port provides an Internet connection.

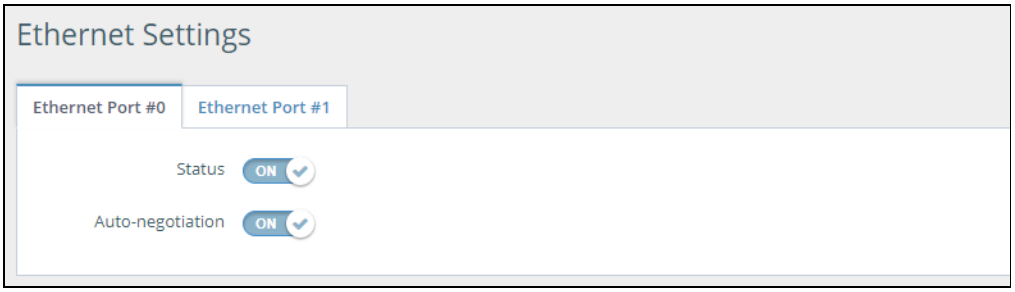
The following items are common for all pages under Ethernet Settings:

- **Status** — Enables or disables this port. (Default: ON)

- **Auto-negotiation** — Enables or disables auto-negotiation for a given interface. (Default: ON)

  1000BASE-T or higher rates do not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T or higher rate port.

Figure 19: Ethernet Port #0 Settings



Ethernet Settings

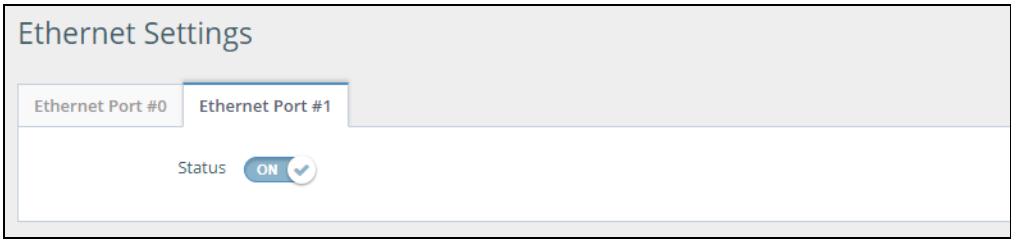
Status: ON

Auto-negotiation: ON

Ethernet Port#1 Settings

Ethernet Port#1 only supports the Status switch to enable or disable the port.

Figure 20: Ethernet Settings – Network Behavior



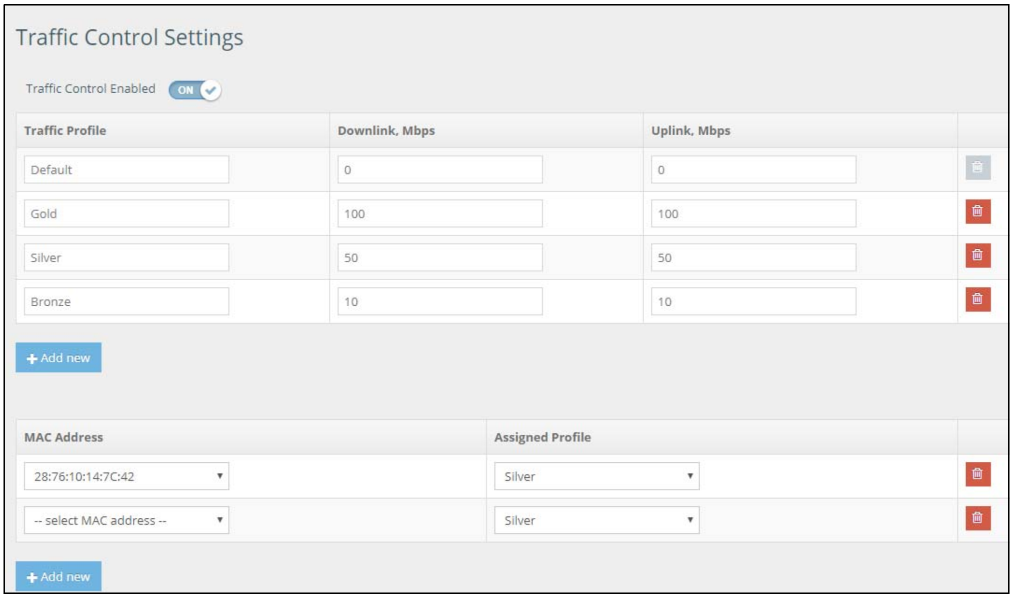
Status ON

Traffic Control Settings

Use the Traffic Control settings to limit the uplink and downlink speeds of specified devices. First create a Traffic Profile which specifies a name and the downlink and uplink speed limit for the profile. Click the + Add new button to add a profile by entering the profile name and limits.

Once a profile is added you can then configure a device MAC address in the MAC address field and assign one of your Traffic Profiles to the MAC address. Click the + Add new button under MAC Address and assign a Traffic Profile to either a custom or existing MAC address. The device's uplink and downlink data transfer speed will be limited to the speeds specified in the profile.

Figure 21: Traffic Control Settings



Traffic Control Enabled ON

Traffic Profile	Downlink, Mbps	Uplink, Mbps
Default	0	0
Gold	100	100
Silver	50	50
Bronze	10	10

MAC Address	Assigned Profile
28:76:10:14:7C:42	Silver
-- select MAC address --	Silver

4 Wireless Settings

This chapter describes wireless settings on the wireless bridge. It includes the following sections:

Radio Settings Overview

The IEEE 802.11 wireless interfaces include configuration options for radio signal characteristics and wireless security features.

The wireless bridges can operate in up to three different radio modes, 802.11n at 2.4 Ghz, 802.11ac at 5 GHz and a 60 GHz PTP/PTMP wireless bridge protocol (IgniteNet ML60G). The modes and bands supported are dependent on the MetroLinq model. Refer to Table 2 for the modes supported.

Note that some models can operate using all three bands at the same time with the 5 GHz radio operating as the 60 GHz backup and or alternatively only the 5 GHz radio and or 2.4 GHz radio (Omni and LW models only) can be enabled with the 60 GHz radio(s) disabled.

Radio Operation by Band

The 5 GHz radio can also be enabled as either an Access Point with Auto-WDS or a WDS Client.

If supported, the 2.4 GHz radio operates only as an Access Point.

The 60 GHz radio(s) operates as the primary point-to-point radio(s) and can be set as either the master or the client (Omni 10G 60 GHz radios support master only).

The web interface identifies the radio configuration pages specifically for each MetroLinq model as shown in Table 2:

Table 2: MetroLinq Models vs. Supported Radio Modes

Model	Radio#0 Mode		Radio#1 Mode		Radio#2 Mode		Radio#3 Mode		Radio#4 Mode	
	Band	Protocol	Band	Protocol	Band	Protocol	Band	Proto-col	Band	Protocol
MetroLinq Omni 10G	5 GHz	802.11ac	60 GHz	ML60G[*]	60 GHz	ML60G	60 GHz	ML60G	2.4 GHz	802.11n
MetroLinq 60 LW	5 GHz	802.11ac	2.4 GHz	802.11n	60 GHz	ML60G	—	—	—	—
MetroLinq 5 LW	5 GHz	802.11ac	2.4 GHz	802.11n	—	—	—	—	—	—
MetroLinq 2.5G 60 PTMP	5 GHz	802.11ac	60 GHz	ML60G	—	—	—	—	—	—
MetroLinq 2.5G 60 PTP	5 GHz	802.11ac	60 GHz	ML60G	—	—	—	—	—	—
MetroLinq 60 PTP	5 GHz	802.11ac	60 GHz	ML60G	—	—	—	—	—	—

[*] ML60G refers to IgniteNet's proprietary radio link protocol, used for wireless bridge links in PTP or PTMP settings.

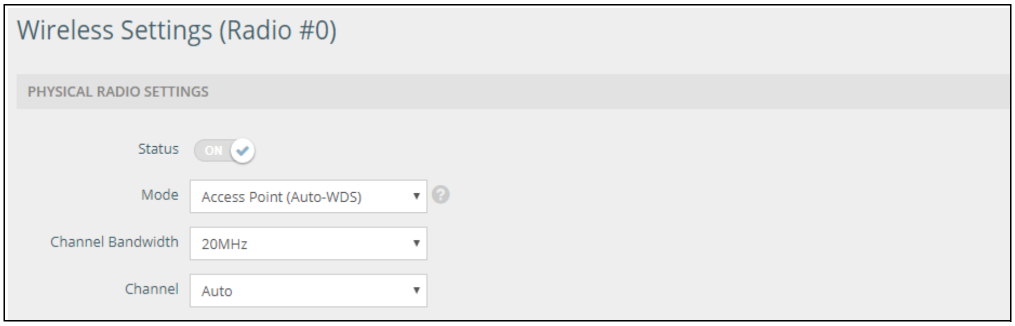
Backup

The 5 GHz interface is available as a backup for the 60 GHz interface. If there is a link failure on the 60 GHz interface, traffic is automatically forwarded to the 5 GHz interface. When the 60 GHz link is restored, traffic reverts back to the 60 GHz interface.

Radio#0 — 5 GHz Settings

Physical Radio Settings

Figure 22: Radio Settings (5 GHz Physical Radio Settings)



Wireless Settings (Radio #0)

PHYSICAL RADIO SETTINGS

Status: ON

Mode: Access Point (Auto-WDS)

Channel Bandwidth: 20MHz

Channel: Auto

The following items are displayed on this page:

- **Status** — This button is disabled.
- **Mode** — Selects the mode in which the wireless bridge will function (unavailable in the Metro Linq Omni 10G).

  - **Access Point (Auto-WDS)** — Operates as a standard access point with auto-WDS enabled. If any of the 60 GHz radios are enabled then the 5 GHz radio mode will automatically switch over to act as a backup if there is a link failure on the 60 GHz link.

  - **Client (WDS)** — (Outdoor wireless bridges only) Sets the 5 GHz radio to only operate as the backup wireless bridge client in a point-to-point wireless link between two IgniteNet units.

- **Channel Bandwidth** — The options for the 5 GHz channel bandwidths include 20, 40 and 80 MHz. Using a larger channel bandwidth setting provides a higher connection speed. (5 GHz Default: 20 MHz; 5 GHz Range: 20 MHz, 40 MHz, 80MHz)

- **Channel** — The radio channel that the wireless bridge uses to communicate on the point-to-point link. Note that the wireless bridge at the other end of the link must be set to the same channel and channel bandwidth. (The available channels are dependent on the band, Channel Bandwidth and Country regulations.) Table "Radio Channels" shows the available channels that can be set for all radios.

  Selecting Auto (5 GHz) enables the wireless bridge to automatically select an unoccupied radio channel. (5 GHz Default: Auto)

Table 3: Radio Channels

	Radio#0 (5 GHz)		Radio#1, #2 or #3 (60 GHz)		Radio#1 or #4 (2.4 GHz)	
UNII Band[*]	Radio Channels[†]	Frequency (GHz)	Radio Channels	Frequency (GHz)	Radio Channels	Frequency (GHz)
—	Auto scan	—	1	58.32	1	2.412
U-NII 1	36	5.180	2	60.48	2	2.417
	40	5.200	3	62.64	3	2.422
	44	5.220	4	64.80	4	2.427
	48	5.240			5	2.432
U-NII 2C	100	5.500			6	2.437
	104	5.520			7	2.442
	108	5.540			8	2.447
	112	5.560			9	2.452
	116	5.580			10	2.457
	120	5.600			11	2.462
	124	5.620				
	128	5.640				
	132	5.660				
	136	5.680				
	140	5.700				
U-NII-3	149	5.745				
	153	5.765				
	157	5.785				
	161	5.805				
	165	5.825				

[*] UNII Band support is dependent on the operating region.

[†] Supported channels depend on the channel bandwidth.

Wireless Networks Settings

For the 5 GHz radio the Wireless Networks settings pages are displayed when operating in the Access Point mode. For client mode operation see the "5GHz Client Configuration Settings" on page 39.

5 GHz Backup

The following items are displayed in the 5 GHz Backup tab of the Wireless Networks Settings page:

- **General Settings**
  - **Status** — For the backup SSID this button is disabled. In access point mode the 5 GHz radio is always available to switch over as a backup link for the 60 GHz link.

- **SSID** — The name of the basic service set provided by the 5 GHz backup link interface. APs at each end of a point-to-point link must set to the same SSID. (Default: IgniteNet0-1-5G-Backup)

- **Scan** — Click the scan button to have the radio scan the available SSIDs that can be seen by the 5 GHz radio receiver.

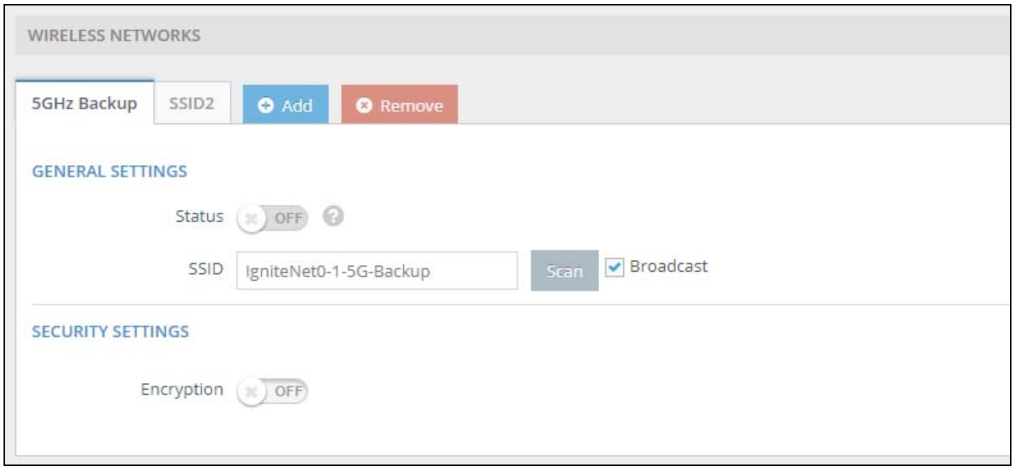
- **Security Settings**

  - **Encryption** — Sets the wireless security method for the interface. (Default: Off)

    - Off (No Security) — When the Encryption is set to off, there is no security on the wireless link.

    - On (WPA2-PSK): APs in the point-to-point link use WPA2 security with a Pre-shared Key for authentication and encryption.

Figure 23: 5 GHz Backup SSID - Wireless Networks Settings- Access Point Mode



WIRELESS NETWORKS

5GHz Backup | SSID2 | Add | Remove

GENERAL SETTINGS

Status: OFF

SSID: IgniteNet0-1-5G-Backup | Scan | ☑ Broadcast

SECURITY SETTINGS

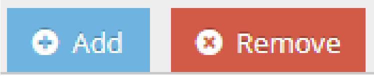
Encryption: OFF

SSID(2 - 8)

The following items are displayed in the SSID(2-8) tabs of the Wireless Networks Settings tab.

Note: SSID2 tab is available by default. To add SSID tabs 2 to 8 click on the blue Add tab (button). SSID tabs are added in ascending order from 2 to 8. To remove SSID tabs 2 to 8 click on the red Remove tab (button). SSID tabs are removed in descending order from 8 to 2.

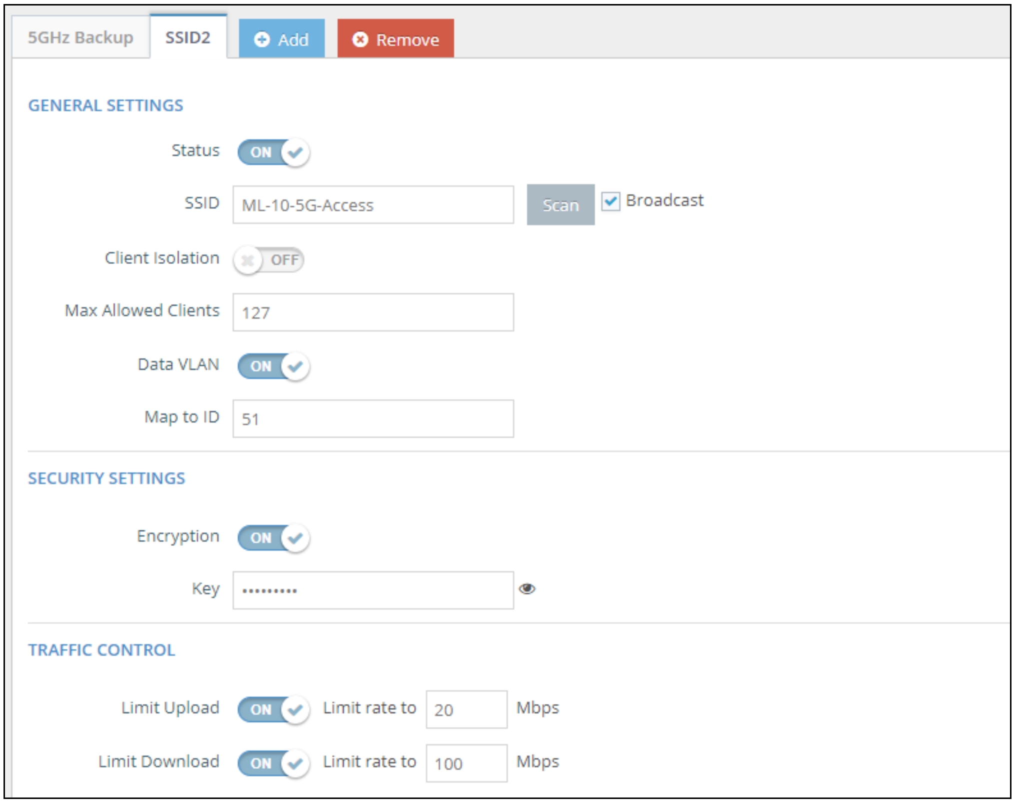
Figure 24: SSID Add and Remove Tab Buttons



- **General Settings**
  - **Status** — Click this button to enable or disable (ON/OFF) the SSID.
  - **SSID** — The name of the basic service set provided by the 5 GHz radio operating as a general access point. (Default: IgniteNet0-2-Pro)
  - **Scan** — Click the scan button to have the radio scan the available SSIDs that can be seen by the 5 GHz radio receiver.
  - **Client Isolation** — Click this to ON to prevent Clients from directly communicating to each other through the wireless bridge LAN. Any Client to Client traffic must first pass via the wireless bridge WAN.
  - **Max Allowed Clients** — The maximum number of clients that can setup an 802.11 WiFi link with the wireless bridge 5 GHz radio in Access Point mode. (Range:1-127, Default:127)
  - **Data VLAN** — When set to ON, the setting tags the 5 GHz access traffic with the VLAN ID set in the **Map to ID** input box (VLAN ID range 2 to 4094).
- **Security Settings**
  - **Encryption** — Sets the wireless security method for the interface. (Default: Off)
    - Off (No Security) — When the Encryption is set to off, there is no security on the wireless link.
    - On (WPA2-PSK): The wireless bridge uses WPA2 security with a Pre-shared Key for authentication and encryption with WiFi clients.

- **Traffic Control**
  - **Limit Upload** — Sets the maximum uplink rate to a value between 1 and 1000 Mbps (Default: Off)
  - **Limit Download** — Sets the maximum downlink rate to a value between 1 and 1000 Mbps (Default: Off)

Figure 25: SSID(2-8) Wireless Networks Settings - Access Point Mode



GENERAL SETTINGS

Status: ON
SSID: ML-10-5G-Access [Scan] ☑ Broadcast
Client Isolation: OFF
Max Allowed Clients: 127
Data VLAN: ON
Map to ID: 51

SECURITY SETTINGS

Encryption: ON
Key: •••••••••

TRAFFIC CONTROL

Limit Upload: ON Limit rate to 20 Mbps
Limit Download: ON Limit rate to 100 Mbps

Advanced Radio Settings

These settings can be applied under the Advanced Radio Settings

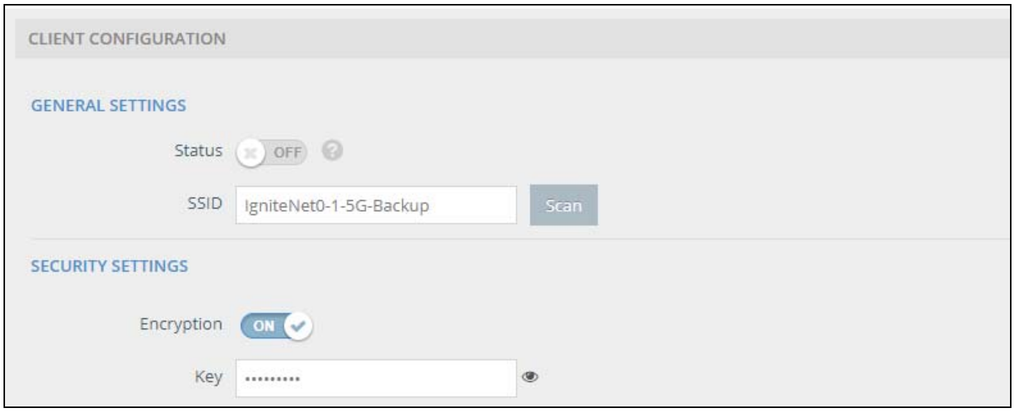
- **MCS Rate** — The minimum data rate at which the wireless bridge transmits packets on the wireless interface. The setting is hard-coded 173.3 Mbps for the 5 GHz radio.
- **Tx Power** — Adjusts the power of the radio signals transmitted from the wireless bridge. As the transmission power increases the transmission range generally also increases. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the wireless bridge model, radio band, the Country setting, and the client device radio characteristics.)

- **Multicast Enhancement** — Use the switch to enable or disable (ON/OFF) the multicast enhancement. (Not available when the 5 GHz radio is set to Client mode)

Client Configuration Settings

When the 5 GHz radio is set to operate in Client mode then the Client Configuration settings are presented in the Wireless Settings for Radio#0. The settings are identical to the SSID setting for 5 GHz backup describe in "5 GHz Backup" on page 40.

Figure 26: Client Configuration - 5 GHz Client Mode



CLIENT CONFIGURATION

GENERAL SETTINGS

Status: OFF

SSID: IgniteNet0-1-5G-Backup

SECURITY SETTINGS

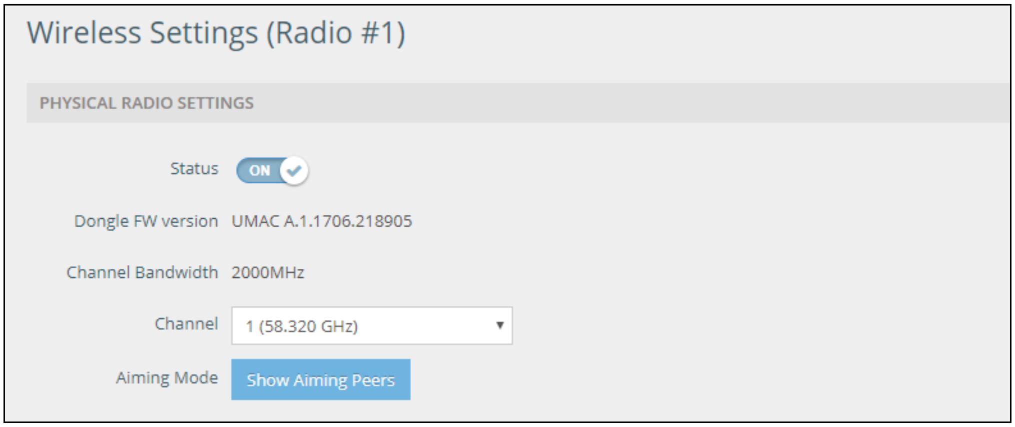
Encryption: ON

Key: •••••••••

Radio#1, #2 or #3 — 60 GHz Settings

Physical Radio Settings

Figure 27: 60 GHz Radio Settings (Physical Radio Settings)



Wireless Settings (Radio #1)

PHYSICAL RADIO SETTINGS

Status: ON

Dongle FW version: UMAC A.1.1706.218905

Channel Bandwidth: 2000MHz

Channel: 1 (58.320 GHz)

Aiming Mode

Note: Depending on the MetroLinq wireless bridge used, the 60 GHz Radio settings menu could be numbered either 1, 2 or 3.

The following items are displayed on the 60 GHz radio page:

- **Status** — Click the button to enable or disable (ON/OFF) the 60 GHz radio.
- **Dongle FW Version** — The firmware version of the 60 GHz radio.
- **Mode** — Selects the mode in which the wireless bridge will function.
  - **Master** — (Outdoor wireless bridges only) Sets the wireless bridge radio as the Master in a point-to-point or point to multi-point wireless link between two or more IgniteNet units. Point-to-point wireless links require one unit set as Master and the other(s) set to Client. Links to any non-IgniteNet units will not work.
  - **Client** — (Outdoor wireless bridges only) Sets the wireless bridge radio as a client in a point-to-point or point-to-multipoint wireless link between two IgniteNet units.
- **Channel Bandwidth** — For the 60 GHz radio, the channel bandwidth is fixed at 2000 MHz.
- **Channel** — The radio channel that the wireless bridge uses to communicate on a point-to-point or point-to-multipoint link(s). Note that the wireless bridge(s) at the other end of the link(s) must be set to the same channel and channel bandwidth. (The available channels are dependent on the 802.11 band, Channel Bandwidth, and Country Code settings.) Table "Radio Channels" shows the available channels that can be set for both radios. (60 GHz Default: 1)
- **Aiming Mode** — Opens the antenna alignment tool for 60 GHz point-to-point links. You can set the tool to operate in a transmit or receive mode. In transmitter mode, the wireless bridge continuously sends a signal. In receiver mode, you can visually monitor the received signal strength from the web interface while adjusting the antenna alignment.

  For Aiming Mode to operate normally, one side has to be the Master, and the other side has to be the Client. The Client side is the side that starts the internal Aiming Mode process, and while the Master side will display the relevant signal information when the Aiming Mode is started on that side, the Client side is what drives the operation. (This operation is described in detail in the 60 GHz PTP/PTMP Aiming Mode & App – Linq Assist™ blog on the IgniteNet web site.)

  Before beginning alignment, configure the radios and make sure the channels on both sides are the same, the SSIDs are the same, leave encryption off for now, set the data rate to MCS1, and ensure the ACK settings are set for the appropriate distance.

  - **PTP Alignment** — Set one side to Client and the other side to Master. On the Client side, click on the Open Aiming Tool. Once the Aiming Mode page pops up, press Start and it will start scanning for Master units. Once the Client sees a Master unit, it will display the MAC of the Master, the Local and

Remote RSSI and SNR values, and a signal bar that shows the current signal strength and the highest level. If the Client sees two Master units in the scan, both will be displayed with corresponding MAC addresses and signal bars.

When logged into the GUI on the Master, you can also see this alignment information. Please note again that the Aiming Mode on the Master will not display any information until the Aiming Mode on the Client unit has been started. It looks quite similar to the Client information, but this time showing the MAC of the Client radio.

When the Aiming Mode is operational, begin making your alignment adjustments. Be sure to make small adjustments, and mark or remember the positioning when you first start to see link numbers reported so you can always return to that point if you lose alignment.

- **PTMP Alignment** — The Aiming Mode usage in PTMP modes is quite similar to PTP modes. The PTMP Client is identical to the PTP Client. The PTMP Master is slightly different however, in that instead of displaying a signal bar for a single Client, it can show multiple Aiming Peers at one time. This is done so that you can monitor multiple Client devices being aimed at the Master from the Master side at the same time. (This operation is described in detail in the 60 GHz PTP/PTMP Aiming Mode blog on the IgniteNet web site.)

Linq Assist™

The Linq Assist™ app (available for iOS and Android operating systems), allows you to use your mobile device to quickly and easily make alignment adjustments. Connect a bluetooth USB dongle from your phone to the MetroLinq radio to be aligned. Linq Assist is able to communicate with the MetroLinq radio to poll and display local and remote signals in real time.

To use Linq Assist, open the app and look for the 60 GHz interface MAC address of the MetroLinq device into which you have installed the bluetooth USB dongle. Click on the desired radio and the connection will establish and the app will display alignment information from the radio.

The app will display the local signal, remote signal, and a combined signal strength. It will also sound an audio tone (the faster the tone interval, the stronger the signal). Once alignment is finished, leave the app, turn off Aiming Mode in the GUI, and your link will establish and can pass data across it.

If you are using the app on a Client that sees multiple Masters on the same channel, that GUI will display all Masters but the app will only display a single Master that has the strongest signal.

Note: The bluetooth USB dongle used is a standard bluetooth 4.0 USB dongle you can purchase from a number of sources. Most units tested from common sources such as the one from Amazon work well.

Wireless Networks Settings

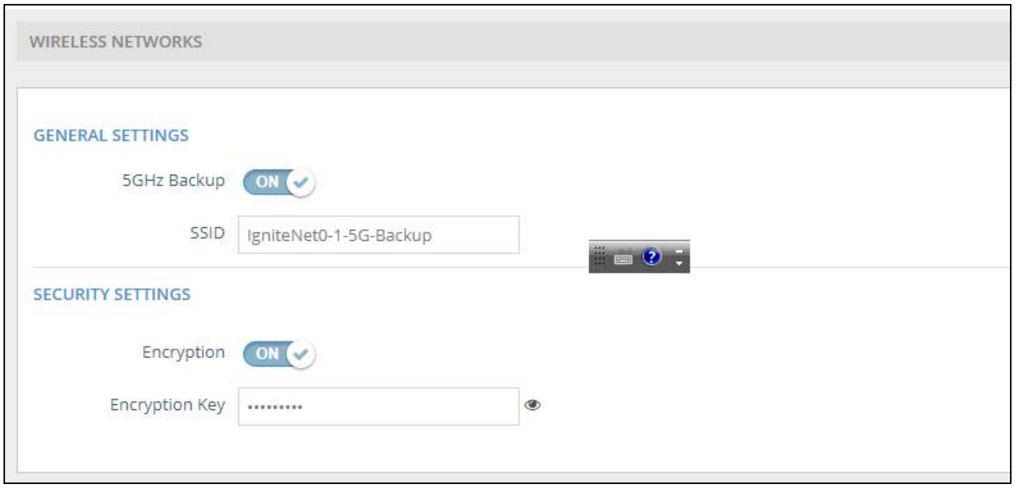
Master Mode

When the 60 GHz physical radio mode is set to Master mode, the settings interface will show the following settings:

Note: The MetroLinq Omni 10G 60 GHz radios are permanently configured to operate in the Master Mode.

- **General Settings**
  - **5 GHz Backup** — If the 60 GHz link fails, this switch enables or disables (ON/OFF) the ability to backup the link to a 5 GHz link using Radio#0.
  - **SSID** —Input a distinct name representing the service set identifier of the 60 GHz link interface. APs at each end of a point-to-point link must be set to the same SSID. (Range: 1—32 characters)
- **Security Settings**
  - **Encryption** — Sets the wireless security method for the interface. (Default: Off)
    - Off (No Security) — When the Encryption is set to off, there is no security on the wireless link.
    - On (WPA2-PSK): APs in the point-to-point link use WPA2 security with a Pre-shared Key for authentication and encryption.

Figure 28: Wireless Network Settings- 60 GHz Master Mode



WIRELESS NETWORKS

GENERAL SETTINGS

5GHz Backup: ON

SSID: IgniteNet0-1-5G-Backup

SECURITY SETTINGS

Encryption: ON

Encryption Key: •••••••••

Client Configuration

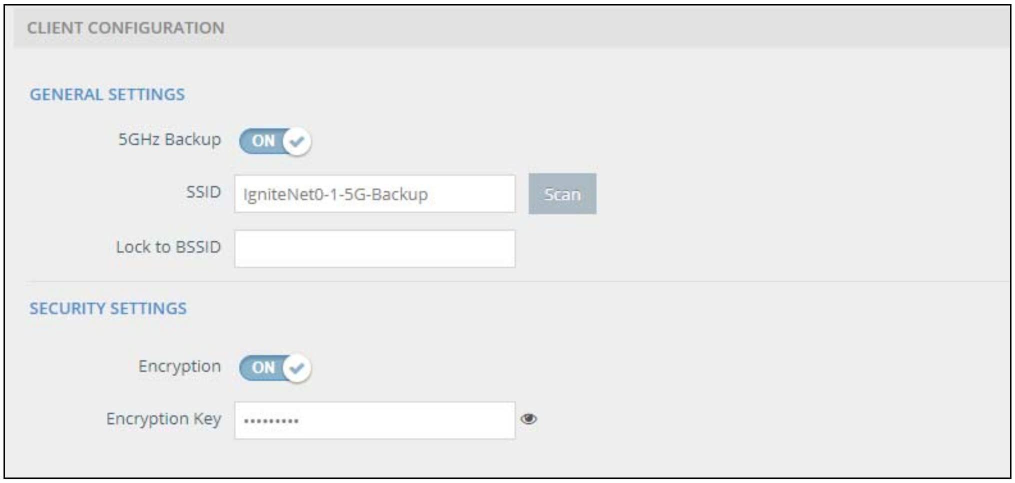
Client Mode

When the 60 GHz physical radio mode is set to Client mode the settings interface will show one configuration item not shown in the Master mode.

- **General Settings**
  - **Lock to BSSID** — Locks the Radio to the specified BSSID.

For all other settings, refer to the settings described under "Master Mode" on page 47.

Figure 29: Client Configuration- 60 GHz Client Mode



CLIENT CONFIGURATION

GENERAL SETTINGS

5GHz Backup: ON

SSID: IgniteNet0-1-5G-Backup

Lock to BSSID:

SECURITY SETTINGS

Encryption: ON

Encryption Key: •••••••••

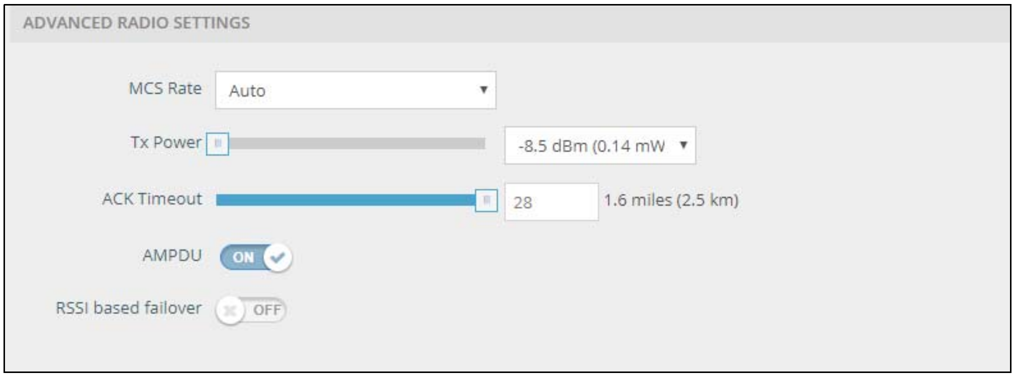
Advanced Radio Settings

Master Mode and Client Mode (Except for the MetroLinq Omni 10G)

The following items are displayed in this section of the Wireless Settings page when the 60 GHz radio is set to Master or Client mode. (For the MetroLinq Omni 10G see "MetroLinq Omni 10G Advanced Radio Settings" on page 50.)

Note: Radio#1 Client mode does not support the RSSI based failover settings.

Figure 30: Advanced Radio Settings - Radio#1 60 GHz Master Mode



ADVANCED RADIO SETTINGS

MCS Rate: Auto

Tx Power: -8.5 dBm (0.14 mW

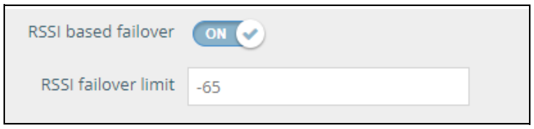
ACK Timeout: 28 1.6 miles (2.5 km)

AMPDU: ON

RSSI based failover: OFF

- **MCS Rate** — The minimum data rate at which the wireless bridge transmits packets on the wireless interface. A setting of "Auto" sets the rate depending on the signal strength.
- **Tx Power** — Adjusts the power of the radio signals transmitted from the wireless bridge. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the wireless bridge model, radio band, and the Country setting.)
- **ACK Timeout** — Sets the acknowledgment timeout, which is used primarily for long-distance connections. This timeout is used to make an adjustment for link distance. It is based on the amount of time, in microseconds, that it should take to transmit a frame to the other end of the link, be processed by the receiving device, and have the ACK frame created and returned to the sending device. (5 GHz Range: 32-255 microseconds; Default: 64 microseconds, 60 GHz Range: 10-28 microseconds; Default: 10 microseconds)
- **AMPDU** — Enables or disables the use of Aggregated MAC Protocol Data Units. Physical layer (PHY) data rate improvements do not increase real throughput beyond a point because of 802.11 protocol overheads. The main media access control feature that provides a performance improvement is aggregation. Aggregation of MAC protocol data units (MPDUs) is referred to as MPDU aggregation or (A-MPDU). (Default: Enabled)
- **RSSI based failover** —Enable this to turn on RSSI failover. When the Received Signal Strength Indicator (RSSI) of the 60 GHz link goes below the value set here in dBm then the link will failover to the 5 GHz backup link.(Default:-65, Range: -95 to -25)

Figure 31: RSSI Based Failover setting



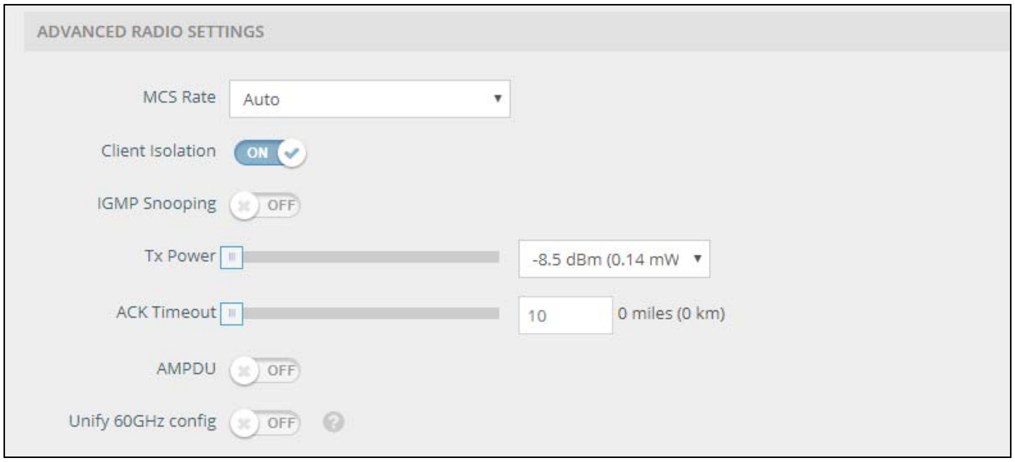
RSSI based failover ON ✓

RSSI failover limit -65

MetroLinq Omni 10G Advanced Radio Settings

For the MetroLinq Omni 10G, the following further items are displayed in this section of the Wireless Settings page of the 60 GHz radios.

Figure 32: Omni 10G Advanced Radio Settings



ADVANCED RADIO SETTINGS

MCS Rate: Auto
Client Isolation: ON
IGMP Snooping: OFF
Tx Power: -8.5 dBm (0.14 mW
ACK Timeout: 10 0 miles (0 km)
AMPDU: OFF
Unify 60GHz config: OFF

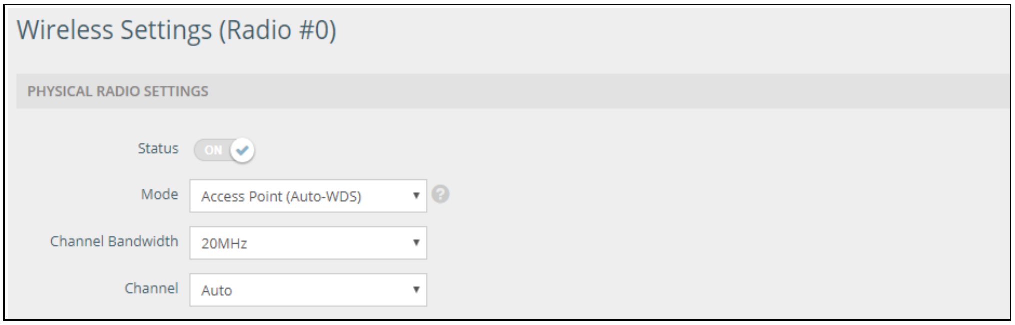
- **IGMP Snooping** — Enabled IGMP snooping to manage any multicast streams over the three separate air interfaces.
- **Unify 60 GHz config** —Sets the advanced radio parameters of the three 60 GHz radio sectors to the same values.

For items not described here, refer to “MetroLinq Omni 10G Advanced Radio Settings” on page 50.

Radio#1 or #4 — 2.4 GHz Settings

Physical Radio Settings

Figure 33: Radio Settings (5 GHz Physical Radio Settings)



Wireless Settings (Radio #0)

PHYSICAL RADIO SETTINGS

Status: ON
Mode: Access Point (Auto-WDS)
Channel Bandwidth: 20MHz
Channel: Auto

The following items are displayed on this page:

- **Status** — Slide the button to ON to enable 2.4 GHz access point operation.

- **Channel Bandwidth** — The access point options for 2.4 GHz channel bandwidths include 20 and 40 MHz. Using a larger channel bandwidth setting provides a higher connection speed. (2.4 GHz Default: 20 MHz)

- **Channel** — The radio channel that the access point uses to communicate on its radio links. (The available channels are dependent on the 802.11 band, Channel Bandwidth, and Country Code settings.) Table "Radio Channels" shows the available channels that can be set for all radios.

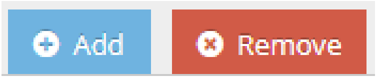
  Selecting Auto (2.4 GHz) enables the access point to automatically select an unoccupied radio channel. (2.4 GHz Default: Auto) Wireless Networks Settings

2.4 GHz Wireless Network Settings

The 2.4 GHz radio access point if supported, shows the following under Wireless Networks when accessing the Wireless Networks Settings menu item. The items are displayed in the SSID(1-8) tabs of the Wireless Networks Settings tab.

Note: The SSID1 tab is available by default. To add SSID tabs 2 to 8 click on the blue Add tab (button). SSID tabs are added in ascending order from 2 to 8. To remove SSID tabs 2 to 8 click on the red Remove tab (button). SSID tabs are removed in descending order from 8 to 2.

Figure 34: SSID Add and Remove Tab Buttons

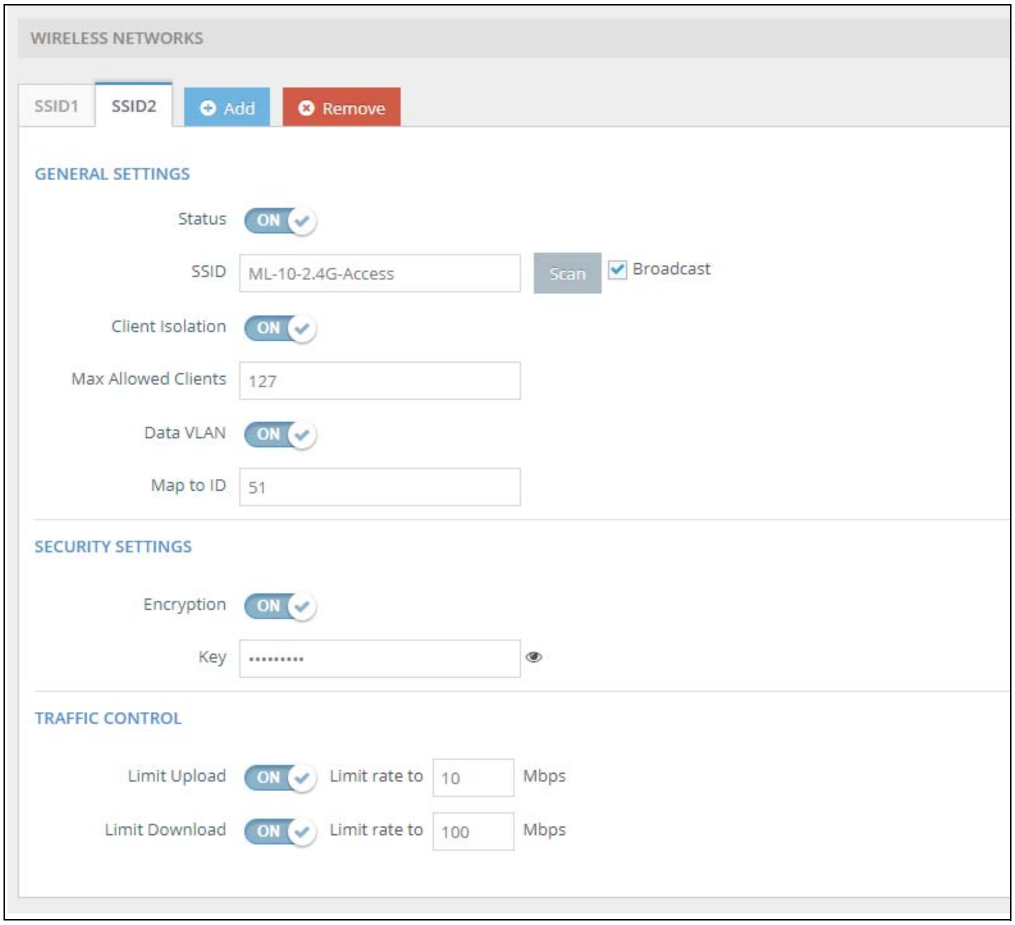


SSID 1 to 8

- **General Settings**
  - **Status** — Click this button to enable or disable (ON/OFF) the SSID.
  - **SSID** — The name of the basic service set provided by the 2.4 GHz radio operating as a general access point. (Default: IgniteNet0-2-Pro)
  - **Scan** — Click the scan button to have the radio scan the available SSIDs that can be seen by the 2.4 GHz radio receiver.
  - **Client Isolation** — Click this to ON to prevent Clients from directly communicating to each other through the wireless bridge LAN. Any Client to Client traffic must first pass via the wireless bridge WAN.
  - **Max Allowed Clients** — The maximum number of clients that can setup an 802.11 WiFi link with the 2.4 GHz access point. (Range:1-127, Default:127)
  - **Data VLAN** — When set to ON, the setting tags the 2.4 GHz access traffic with the VLAN ID set in the **Map to ID** input box (VLAN ID range 2 to 4094).

- **Security Settings**
  - **Encryption** — Sets the wireless security method for the interface. (Default: Off)
    - Off (No Security) — When the Encryption is set to off, there is no security on the wireless link.
    - On (WPA2-PSK): APs in the point-to-point link use WPA2 security with a Pre-shared Key for authentication and encryption.
- **Traffic Control**
  - **Limit Upload** — Sets the maximum uplink rate to a value between 1 and 1000 Mbps (Default: Off)
  - **Limit Download** — Sets the maximum downlink rate to a value between 1 and 1000 Mbps (Default: Off)

Figure 35: 2.4 GHz Tabs 1-8 - Wireless Networks Settings



WIRELESS NETWORKS

GENERAL SETTINGS

Status: ON ✓

SSID: ML-10-2.4G-Access Scan ☑ Broadcast

Client Isolation: ON ✓

Max Allowed Clients: 127

Data VLAN: ON ✓

Map to ID: 51

SECURITY SETTINGS

Encryption: ON ✓

Key: ••••••••• 👁

TRAFFIC CONTROL

Limit Upload: ON ✓ Limit rate to 10 Mbps

Limit Download: ON ✓ Limit rate to 100 Mbps

Advanced Radio Settings

These settings can be applied under the Advanced Radio Settings

- **MCS Rate** — The minimum data rate at which the access point transmits packets on the wireless interface. The setting is hard-coded 173.3 Mbps for the 2.4 GHz radio.

- **Tx Power** — Adjusts the power of the radio signals transmitted from the access point. As the transmission power increases the transmission range generally also increases. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the wireless bridge model, radio band, the Country setting, and the client device radio characteristics.)

- **Multicast Enhancement** — Use the switch to enable or disable (ON/OFF) the multicast enhancement. (Not available when the 5 GHz radio is set to Client mode.)

5

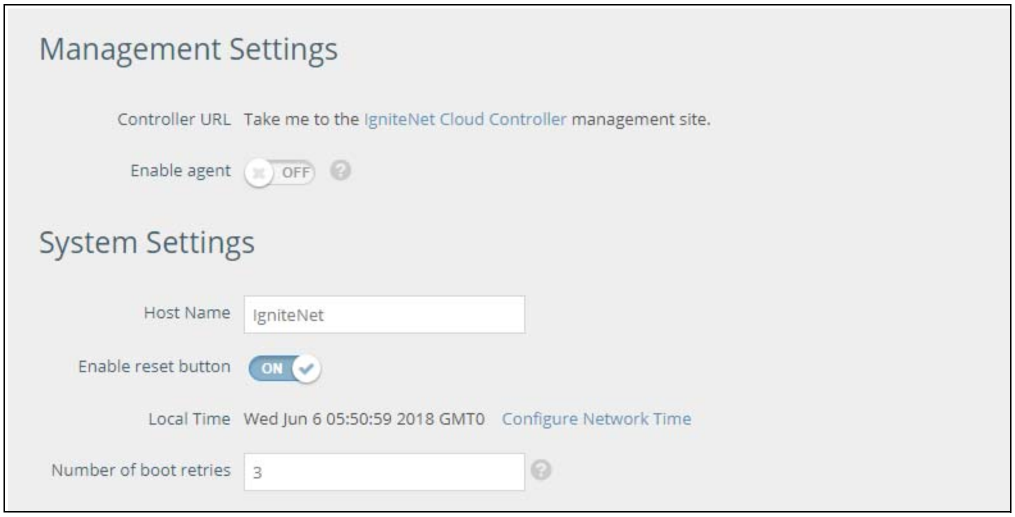
System Settings

This chapter describes maintenance settings on the wireless bridge. It includes the following sections:

System Settings

The System Settings page can be used to enable the wireless bridge to be managed from the IgniteNet Cloud controller and configure general descriptive information about the wireless bridge, such as the system identification name and local time.

Figure 36: System Settings



Management Settings

Controller URL Take me to the IgniteNet Cloud Controller management site.

Enable agent OFF

System Settings

Host Name IgniteNet

Enable reset button ON

Local Time Wed Jun 6 05:50:59 2018 GMT0 Configure Network Time

Number of boot retries 3

The following items are displayed on this page:

- **Enable agent** — Set to "On" to manage this wireless bridge from the IgniteNet Cloud controller. Click on the link to **cloud.ignitenet.com** where you can create an account and register your wireless bridge.
- **Host Name** — An alias for the wireless bridge, enabling the device to be uniquely identified on the network. (Default: IgniteNet; Range: 0-50 characters)

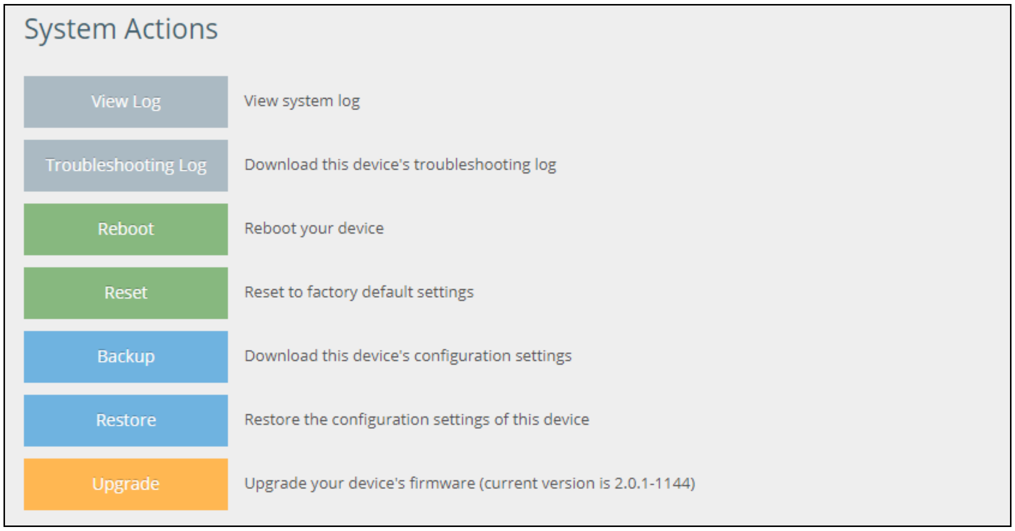
Note: The Host Name field is unavailable if the cloud agent is enabled.

- **Enable reset button** — Enables or disables the hardware reset button.
- **Local Time** — The local time, given as day of week, month, time, year.
- **Configure Network Time** — Links to the Network Time (NTP) section on the Services page.
- **Number or boot retries** — Number of boot retries before switching to next boot bank.

Maintenance

The Maintenance page supports general maintenance tasks including displaying the system log or troubleshooting log, rebooting the device, restoring factory defaults, backing up or restoring configuration settings, and upgrading firmware.

Figure 37: Maintenance



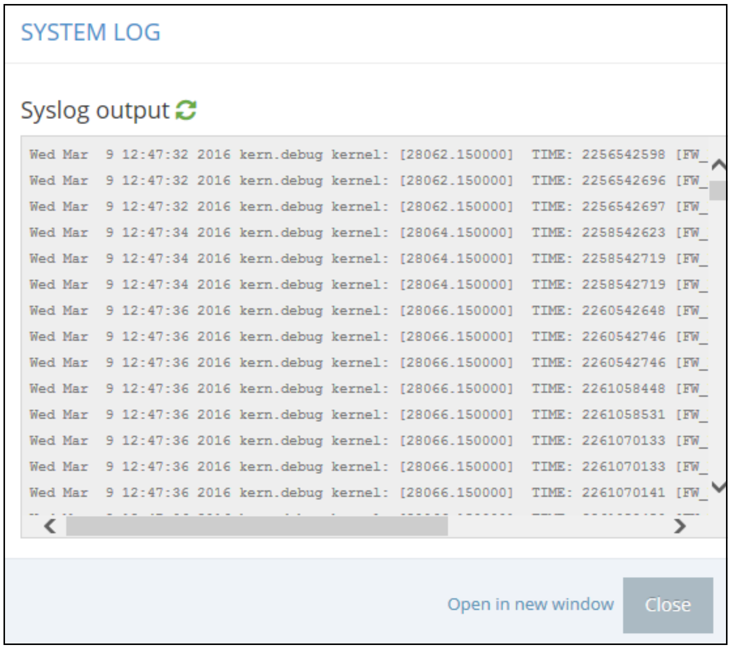
System Actions

View Log	View system log
Troubleshooting Log	Download this device's troubleshooting log
Reboot	Reboot your device
Reset	Reset to factory default settings
Backup	Download this device's configuration settings
Restore	Restore the configuration settings of this device
Upgrade	Upgrade your device's firmware (current version is 2.0.1-1144)

Viewing the System Logs

The wireless bridge saves event and error messages to a local system log database. The log messages include the date and time, device name, message type, and message details.

Figure 38: System Log



SYSTEM LOG

Syslog output

```
Wed Mar  9 12:47:32 2016 kern.debug kernel: [28062.150000]  TIME: 2256542598 [FW_
Wed Mar  9 12:47:32 2016 kern.debug kernel: [28062.150000]  TIME: 2256542696 [FW_
Wed Mar  9 12:47:32 2016 kern.debug kernel: [28062.150000]  TIME: 2256542697 [FW_
Wed Mar  9 12:47:34 2016 kern.debug kernel: [28064.150000]  TIME: 2258542623 [FW_
Wed Mar  9 12:47:34 2016 kern.debug kernel: [28064.150000]  TIME: 2258542719 [FW_
Wed Mar  9 12:47:34 2016 kern.debug kernel: [28064.150000]  TIME: 2258542719 [FW_
Wed Mar  9 12:47:36 2016 kern.debug kernel: [28066.150000]  TIME: 2260542648 [FW_
Wed Mar  9 12:47:36 2016 kern.debug kernel: [28066.150000]  TIME: 2260542746 [FW_
Wed Mar  9 12:47:36 2016 kern.debug kernel: [28066.150000]  TIME: 2260542746 [FW_
Wed Mar  9 12:47:36 2016 kern.debug kernel: [28066.150000]  TIME: 2261058448 [FW_
Wed Mar  9 12:47:36 2016 kern.debug kernel: [28066.150000]  TIME: 2261058531 [FW_
Wed Mar  9 12:47:36 2016 kern.debug kernel: [28066.150000]  TIME: 2261070133 [FW_
Wed Mar  9 12:47:36 2016 kern.debug kernel: [28066.150000]  TIME: 2261070133 [FW_
Wed Mar  9 12:47:36 2016 kern.debug kernel: [28066.150000]  TIME: 2261070141 [FW_
```

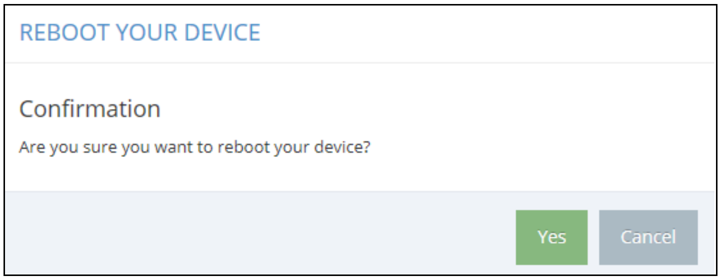
Downloading the Troubleshooting Log

Click “Troubleshooting Log” to download the log file to the management workstation. In Windows, a GNU Zip (*.tar.gz) file is stored in the Downloads folder. The troubleshooting log file contains information that can help IgniteNet resolve technical issues with the wireless bridge.

Rebooting the Wireless Bridge

The Reboot page allows you to reboot the wireless bridge.

Figure 39: Rebooting the Wireless Bridge



REBOOT YOUR DEVICE

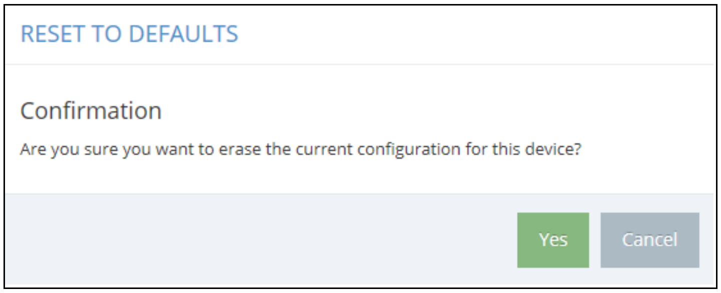
Confirmation

Are you sure you want to reboot your device?

Resetting the Wireless Bridge

The Reset page allows you to reset the wireless bridge to the factory defaults. Note that all user configured information will be lost. You will have to re-enter the default user name and password to re-gain management access to this device.

Figure 40: Resetting to Defaults



RESET TO DEFAULTS

Confirmation

Are you sure you want to erase the current configuration for this device?

Note: It is also possible to reboot or reset the wireless bridge by inserting a pin in the pin hole labeled “Reset” on the connector panel of the wireless bridge and:

- press 2 seconds to reboot the wireless bridge;
- press 5 seconds to reset the wireless bridge to the factory defaults.

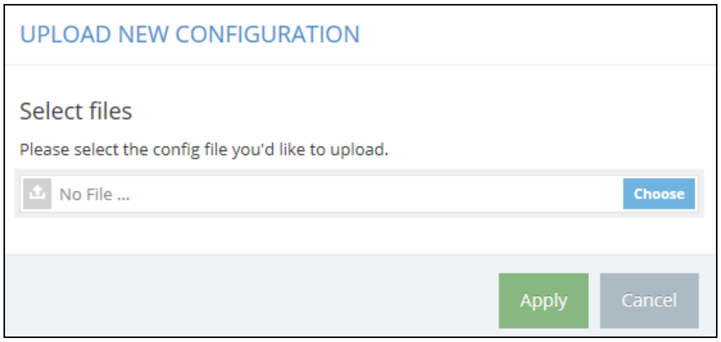
Backing Up Configuration Settings

The Backup function allows you to back up the wireless bridge's configuration to a management workstation. In Windows, a GNU Zip (*.tar.gz) file will be stored in the Downloads folder. This is a sample file name: backup-IgniteNet-2018-01-11.tar.gz

Restoring Configuration Settings

The Restore page allows you to upload configuration settings from a management workstation. The specified file must be one that was previously backed up from the wireless bridge.

Figure 41: Restoring Configuration Settings



UPLOAD NEW CONFIGURATION

Select files

Please select the config file you'd like to upload.

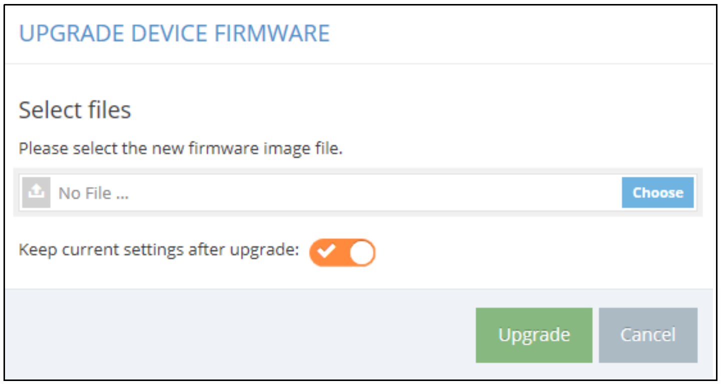
No File ...

Upgrading Firmware

You can upgrade new wireless bridge software from a local file on the management workstation. New software may be provided periodically from IgniteNet.

After upgrading new software, you must reboot the wireless bridge to implement the new code. Until a reboot occurs, the wireless bridge will continue to run the software it was using before the upgrade started. The wireless bridge supports dual software images, so if newly loaded software is corrupted, the alternate image will be used on the next reboot. Configuration settings are stored separately from the software, so the current settings will always be used for any new software. However, note that if the current configuration settings are corrupted, the system defaults will be used.

Figure 42: Upgrading Firmware



UPGRADE DEVICE FIRMWARE

Select files

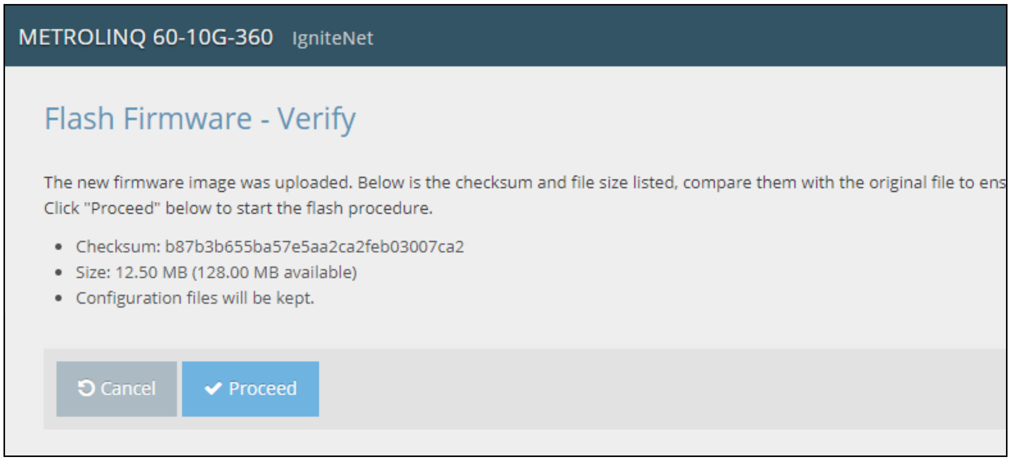
Please select the new firmware image file.

No File ...

Keep current settings after upgrade: ✓

Caution: Before proceeding with the upgrade, be sure to verify the new firmware's MD5 Checksum and File Size that the MetroLinq reports after selecting the file. SeeFigure 43.

Figure 43: Flash Firmware - Verify Checksum



Flash Firmware - Verify

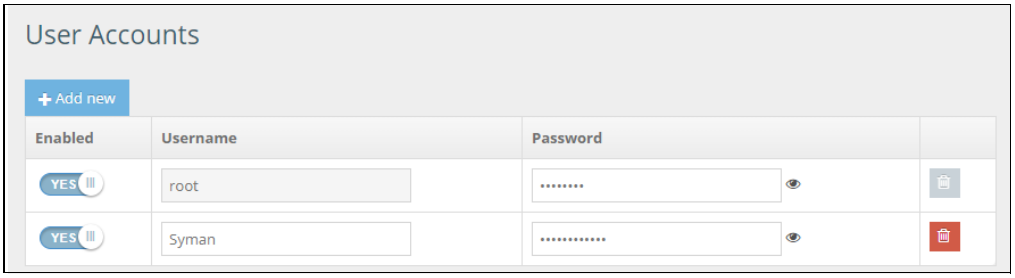
The new firmware image was uploaded. Below is the checksum and file size listed, compare them with the original file to ens
Click "Proceed" below to start the flash procedure.

- Checksum: b87b3b655ba57e5aa2ca2feb03007ca2
- Size: 12.50 MB (128.00 MB available)
- Configuration files will be kept.

User Accounts

The User Accounts page allows you to control management access to the wireless bridge based on manually configured user names and passwords.

Figure 44: User Accounts



User Accounts

Enabled	Username	Password	
YES	root	••••••••	
YES	Syman	••••••••••••	

The following items are displayed on this page:

- **Enabled** — Click to enable or disable the user account.
- **Username** — The name of the user. (Range: 3-15 ASCII characters, no special characters)

Password — The user password. (Range: 3-15 ASCII characters, case sensitive, no special characters)

Note: A maximum of 10 user accounts can be supported.

Services

The Services page allows you to control remote management access to the wireless bridge and configure NTP time servers.

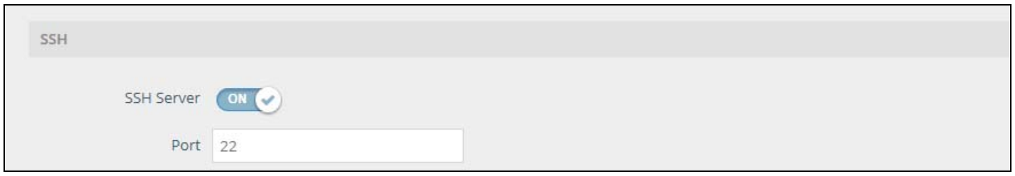
The Telnet and Web management interfaces are enabled and open to access from the Internet. To provide more security, specific services can be disabled and management access prevented from the Internet.

SSH

The Secure Shell (SSH) can act as a secure replacement for Telnet. The SSH protocol uses generated public keys to encrypt all data transfers passing between the wireless bridge and SSH-enabled management station clients and ensures that data traveling over the network arrives unaltered. Clients can then securely use the local user name and password for access authentication.

Note that SSH client software needs to be installed on the management station to access the wireless bridge for management via the SSH protocol.

Figure 45: SSH Server Settings



SSH

SSH Server ON ✓

Port 22

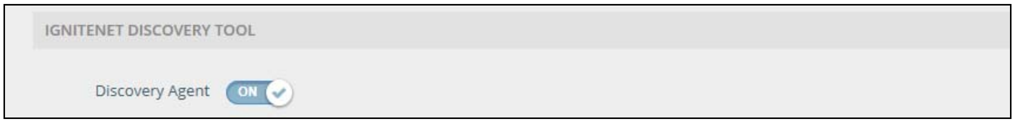
The following items are displayed on this page:

- **SSH Server** — Enables or disables SSH access to the wireless bridge. (Default: Enabled)
- **Port** — Sets the TCP port number for the SSH server on the wireless bridge. (Range: 1-65535; Default: 22)

IgniteNet Discovery Tool

The IgniteNet Discovery agent allows the wireless bridge to be discovered by other devices on the local network or over the Internet.

Figure 46: IgniteNet Discovery Tool Settings



IGNITENET DISCOVERY TOOL

Discovery Agent ON ✓

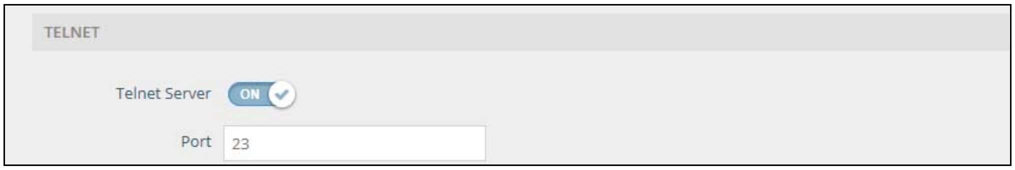
The following items are displayed on this page:

- **Discovery Agent** — Enables or disables IgniteNet Discovery. (Default: Enabled)

Telnet

Telnet is a remote management tool that can be used to configure the wireless bridge from anywhere in the network. However, note that Telnet is not secure from hostile attacks.

Figure 47: Telnet Server Settings



TELNET

Telnet Server: ON ✓

Port: 23

The following items are displayed on this page:

- **Telnet Server** — Enables or disables Telnet access to the wireless bridge. (Default: Enabled)

- **Port** — Sets the TCP port number for the Telnet server on the wireless bridge. (Range: 1-65535; Default: 23)

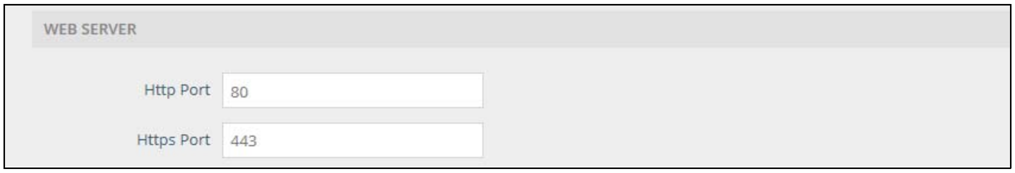
Web Server

A Web browser provides the primary method of managing the wireless bridge. Both HTTP and HTTPS service can be accessed independently. If you enable HTTPS, you must indicate this in the URL: https://[device:port_number]

When you start HTTPS, the connection is established in this way:

- The client authenticates the server using the server's digital certificate.
- The client and server negotiate a set of security protocols to use for the connection.
- The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
- A padlock icon should appear in the status bar for most browsers.

Figure 48: Web Server Settings



WEB SERVER

Http Port: 80

Https Port: 443

The following items are displayed on this page:

- **HTTP Port** — The TCP port to be used by the HTTP Web browser interface. (Range: 1-65535; Default: 80)

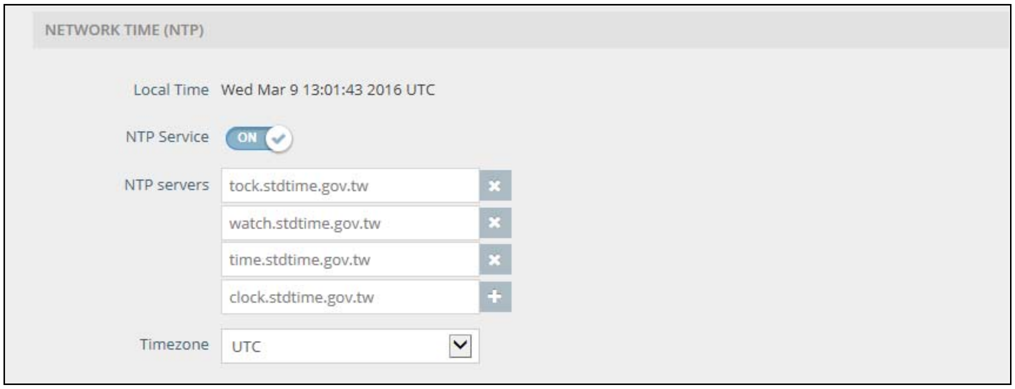
- **HTTPS Port** — The TCP port to be used by the HTTPS Web browser interface. (Range: 1-65535; Default: 443)

Network Time

Network Time Protocol (NTP) allows the wireless bridge to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the wireless bridge enables the system log to record meaningful dates and times for event entries. If the clock is not set, the wireless bridge will only record the time from the factory default set at the last bootup.

The wireless bridge acts as an NTP client, periodically sending time synchronization requests to specified time servers. The wireless bridge will attempt to poll each server in the configured sequence to receive a time update.

Figure 49: NTP Settings



NETWORK TIME (NTP)

Local Time Wed Mar 9 13:01:43 2016 UTC

NTP Service ON

NTP servers tock.stdtime.gov.tw
watch.stdtime.gov.tw
time.stdtime.gov.tw
clock.stdtime.gov.tw

Timezone UTC

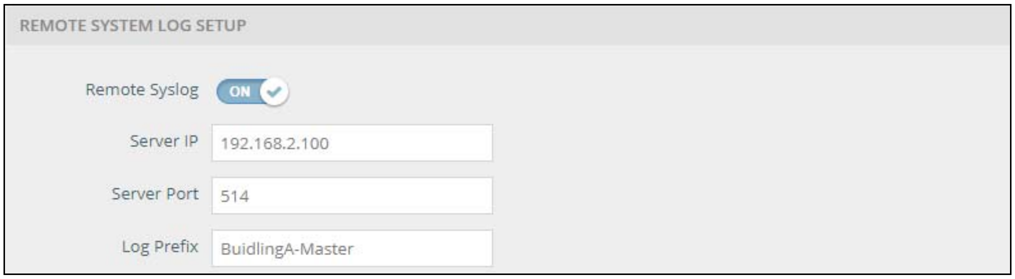
The following items are displayed on this page:

- **Local Time** — Displays the local time as day of week, month, hour:minute:second, year, based on Universal Time Coordinates.
- **NTP Service** — Enables or disables sending of requests for time updates. (Default: Enabled)
- **NTP Servers** — Sets the host names for time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence. To configure additional servers, click the "+" button to open a new edit field.
- **Timezone** — To display a time corresponding to your local time, choose one of the predefined time zones from the scroll-down list.

Remote System Log Setup

Use this feature to send log messages to syslog servers or other management stations.

Figure 50: Remote Log Settings



REMOTE SYSTEM LOG SETUP

Remote Syslog: ON ✓
Server IP: 192.168.2.100
Server Port: 514
Log Prefix: BuidlingA-Master

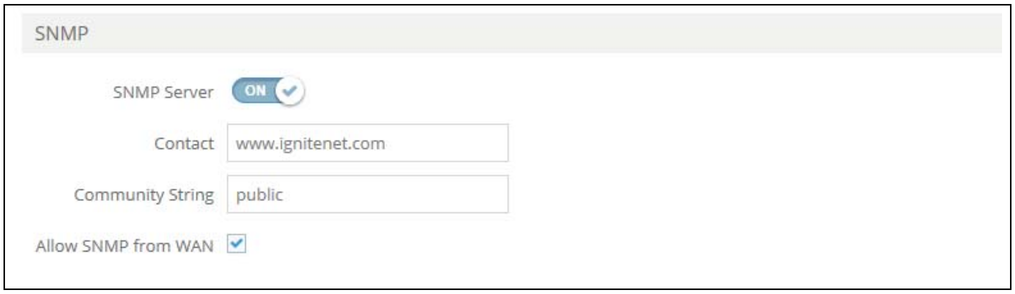
The following items are displayed on this page:

- **Remote Syslog** — Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Server IP** — Specifies the IP address of a remote server which will be sent syslog messages.
- **Server Port** — Specifies the UDP port number used by the remote server. (Range: 1-65535)
- **Log Prefix** — Sets the prefix for the log file sent to the specified server. The file suffix "log" is used.

SNMP

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. It is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Figure 51: SNMP Settings



SNMP

SNMP Server: ON ✓
Contact: www.ignitenet.com
Community String: public
Allow SNMP from WAN: ☑

The following items are displayed on this page:

- **SNMP Server** — Enables or disables SNMP (version 1/ 2) on the wireless bridge. (Default: Enabled)
- **Contact** — Administrator responsible for the wireless bridge.

- **Community String** — A community string that acts like a password and permits access to the SNMP protocol. (Range: 1-32 characters, case sensitive; Default: public)

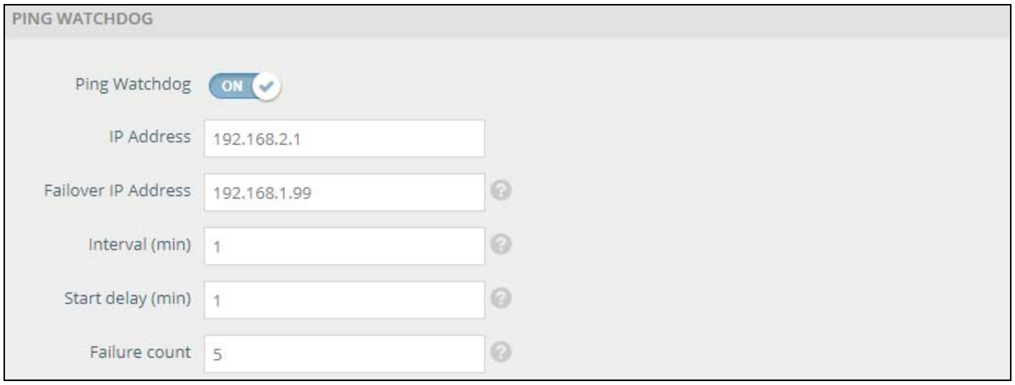
  The default string "public" provides read-only access to the wireless bridge's Management Information (MIB) database.

- **Allow SNMP from WAN** — Allows SNMP management access from the WAN.

PING Watchdog

A ping watchdog can be setup to cause the wireless bridge to reboot automatically.

Figure 52: PING Watchdog Settings



PING WATCHDOG

Ping Watchdog	ON ✓
IP Address	192.168.2.1
Failover IP Address	192.168.1.99
Interval (min)	1
Start delay (min)	1
Failure count	5

The following items are displayed on this page:

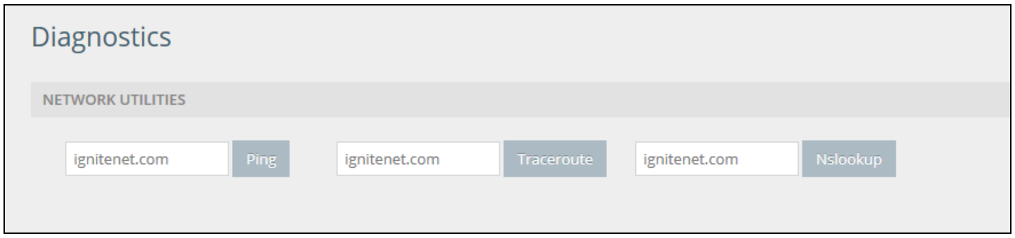
- **Ping Watchdog**— Enables or disables a Ping Watchdog on the wireless bridge. (Default: Disabled)
- **IP Address**— Primary IP address to ping.
- **Failover IP Address**— Secondary IP address to ping if the primary fails. If this address responds to the ping the failure count is reset.
- **Interval (min)**— Interval in minutes between pings. (Default: 1)
- **Start delay**— The wait time in minutes after wireless bridge startup. (Default: 0)
- **Failure Count**— Total consecutive ping failures before the watchdog service reboots the wireless bridge. (Default: 5)

Diagnostics

The Diagnostics page provides Ping, Traceroute, and Nslookup tools for troubleshooting connectivity problems.

Enter a hostname or IP address and click to run the tool.

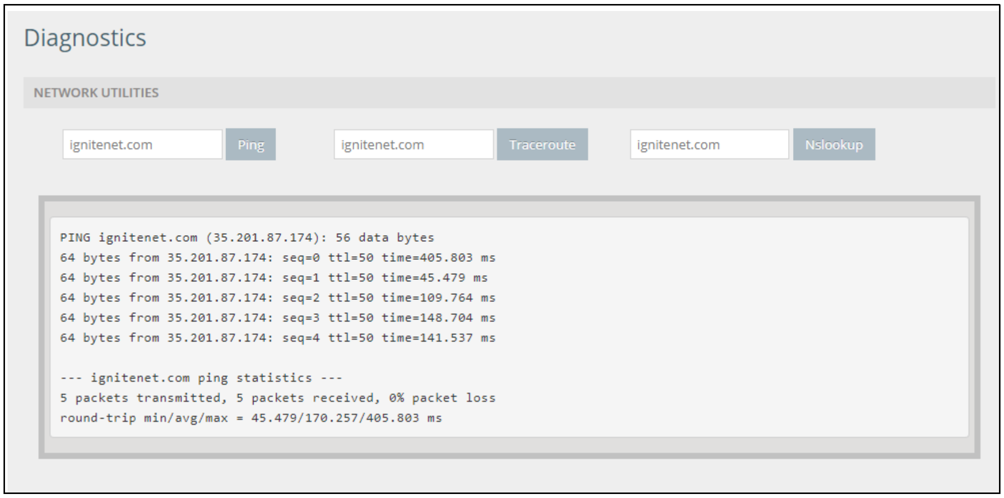
Figure 53: Diagnostics



Ping

Input either an IP address or URL and click the PING button. A successful PING output will be as in Figure 54.

Figure 54: Ping - Successful Result



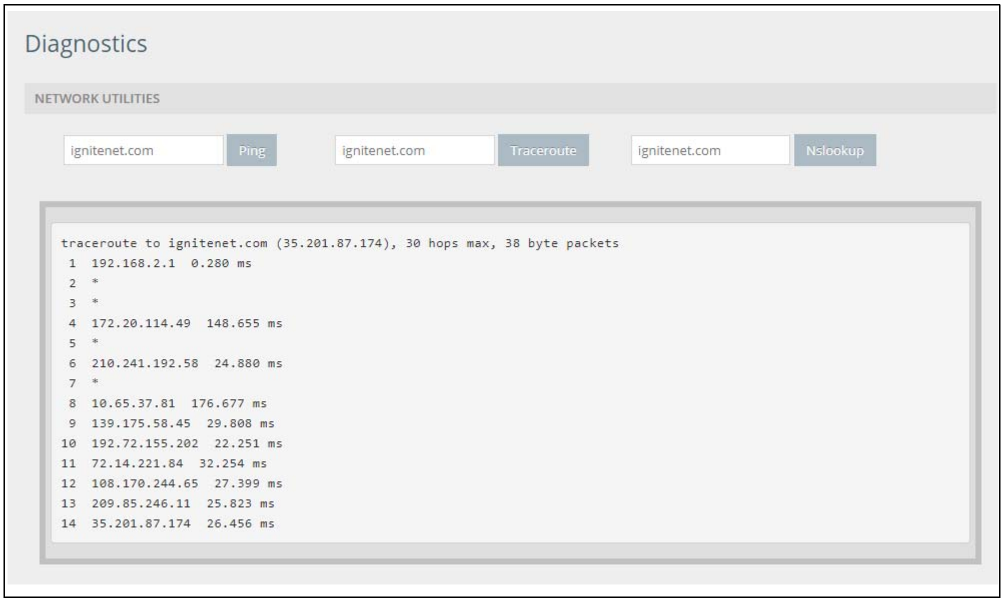
```
PING ignitenet.com (35.201.87.174): 56 data bytes
64 bytes from 35.201.87.174: seq=0 ttl=50 time=405.803 ms
64 bytes from 35.201.87.174: seq=1 ttl=50 time=45.479 ms
64 bytes from 35.201.87.174: seq=2 ttl=50 time=109.764 ms
64 bytes from 35.201.87.174: seq=3 ttl=50 time=148.704 ms
64 bytes from 35.201.87.174: seq=4 ttl=50 time=141.537 ms

--- ignitenet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 45.479/170.257/405.803 ms
```

Traceroute

Input either an IP address or URL and click the Traceroute button. The traceroute output will be as in Figure 55.

Figure 55: Traceroute - Result

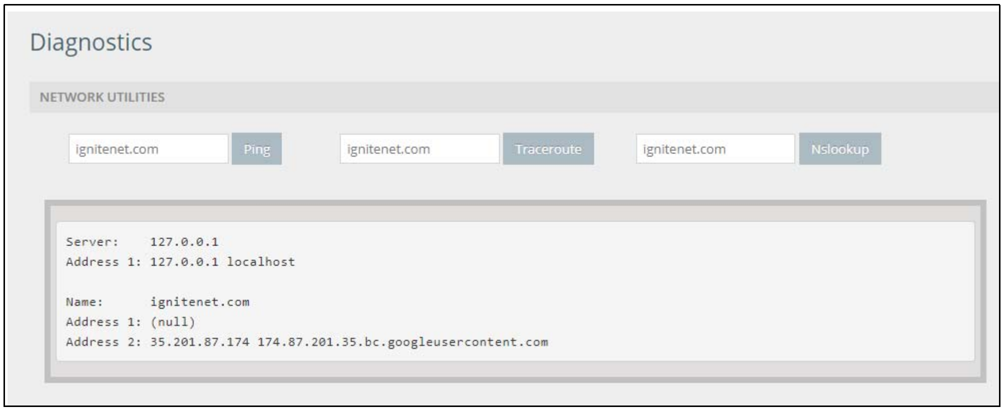


```
traceroute to ignitenet.com (35.201.87.174), 30 hops max, 38 byte packets
 1  192.168.2.1  0.280 ms
 2  *
 3  *
 4  172.20.114.49  148.655 ms
 5  *
 6  210.241.192.58  24.880 ms
 7  *
 8  10.65.37.81  176.677 ms
 9  139.175.58.45  29.808 ms
10  192.72.155.202  22.251 ms
11  72.14.221.84  32.254 ms
12  108.170.244.65  27.399 ms
13  209.85.246.11  25.823 ms
14  35.201.87.174  26.456 ms
```

Nslookup

Input either an IP address or URL and click the Nslookup button. The output of the Nslookup will be as in Figure 56.

Figure 56: Ping - Nslookup Result



```
Server:    127.0.0.1
Address 1: 127.0.0.1 localhost

Name:      ignitenet.com
Address 1: (null)
Address 2: 35.201.87.174 174.87.201.35.bc.googleusercontent.com
```

Speed Test

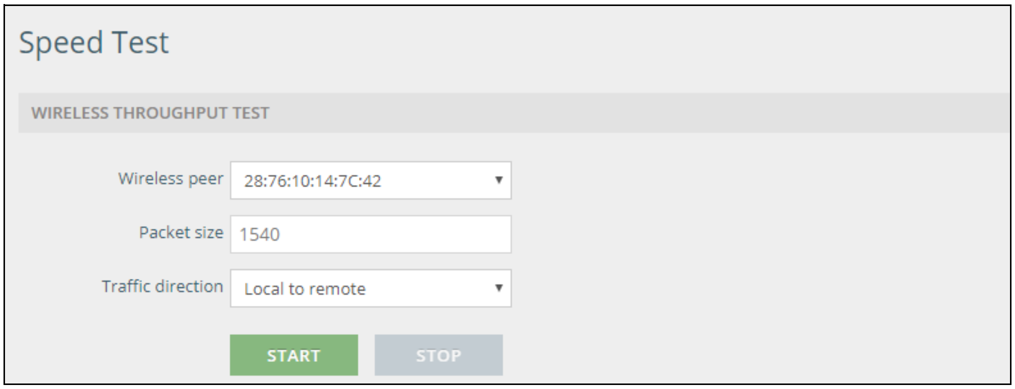
The Speed Test menu provides a radio link speed test tool. Once the tools settings are configured and the test started, the tool will report in graph form the maximum radio link speed between any two connected Metrolinqs.

Wireless Throughput Test

Before starting the radio link speed test, set the following test parameters:

- **Wireless Peer** — Use this drop down menu to select the remote MetroLinq MAC address that corresponds to the radio link to be tested.
- **Packet Size** — Input the IP packet size in bytes which the test will use to measure the radio link speed (Range: 64-1540).
- **Traffic Direction** — Use this drop down menu to select the direction of the speed test transmission. Select either:
  - Local to Remote
  - Remote to Local

Figure 57: Speed Test Settings



Speed Test

WIRELESS THROUGHPUT TEST

Wireless peer: 28:76:10:14:7C:42

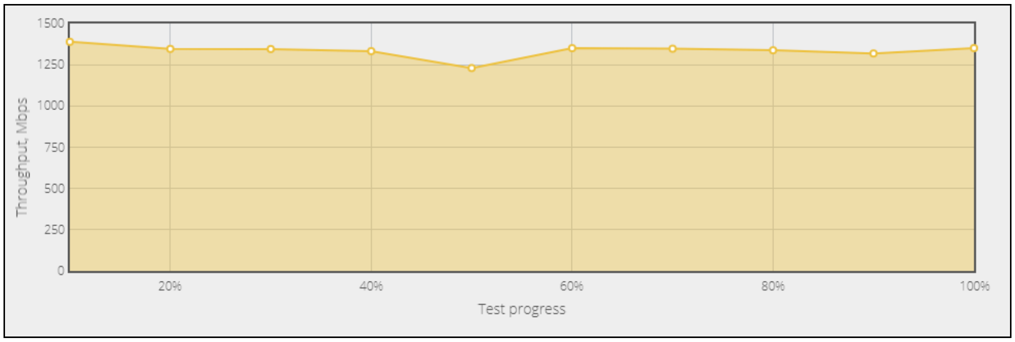
Packet size: 1540

Traffic direction: Local to remote

Speed Test Output

After clicking the Speed Test start button a graph of the radio link data throughput speed will be displayed as shown in Figure 58.

Figure 58: Speed Test Output



Section III

Appendices

This section provides additional information and includes these items:

A Troubleshooting

Operational and Performance Issues

Table 4: Operational and Performance Troubleshooting Chart

Symptom	Action
Low or Unexpected RSSI	◆ Verify the radio link LOS and F1 are clear of obstructions. If there is significant blockage, relocate the MetroLinq mounting position to reduce the blockage. ◆ Verify the parameters 'Tx power' and 'ACK timeout' are configured correctly. If the link is longer than 50 meters, it is recommended to set them to the maximum values. ◆ Verify the channel configuration is suitable for the location or try using a different channel. Atmospheric attenuation is different for each channel, so a moderate difference in RSSI should be expected between channels. An extreme difference in RSSI levels between channels may indicate multipath issues. ◆ Verify that the mounting bracket and/or mounting structure is plumb (not crooked). A severely inclined mounting structure can cause polarization mismatch. ◆ Repeat the fine-tuning part of the alignment process. Typically, further alignment is needed, especially for longer PTP links. ◆ To reduce multipath, relocate the MetroLinq device approximately one meter in any direction and repeat the alignment process. ◆ If no signal is obtained using 'Aiming Mode' or LinqAssist, verify that both units are powered on and the link alignment tools are operated as instructed.
No Wireless Connection	If the RSSI levels are sufficient for the link, but there is no wireless connection in the dashboard: ◆ Verify that the 60 GHz radio is enabled. ◆ Verify that the SSID and encryption are correctly configured. ◆ Verify that the 'ACK timeout' is correctly configured.

Table 4: Operational and Performance Troubleshooting Chart

Symptom	Action
No Network Connection	If there is a wireless connection, but no network connection available through the link: ◆ Verify that the computers or devices used to test the connection are correctly configured. ◆ Verify that the network interfaces are enabled. ◆ Verify that the auto-negotiation settings are correctly set for the L2 network. ◆ Verify that the MTU size is set correctly for the L2 network. ◆ Use diagnostic tools and packet captures between various devices to find where the connection fails.
Low Throughput or Latency	◆ If the MetroLinq model supports it, use the 'Speed Test' utility in the 'System Settings' menu to test the performance across the wireless link. Otherwise, test performance using devices connected directly to the Master and Client MetroLinq's network interfaces. ◆ Check the MCS setting and device dashboard to verify the modulation used on both the Master and Client MetroLinq is correct. ◆ Check the MetroLinq dashboard to verify the wired network interfaces negotiated at the correct rate. If not, check the interface settings are correct on both the MetroLinq and the devices connected to the wired interfaces. ◆ Verify that the MTU size is set correctly.

Problems Accessing the Management Interface

Table 5: Management Interface Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet or web browser	◆ Be sure the wireless bridge is powered up. ◆ Check network cabling between the management station and the wireless bridge. ◆ Check that you have a valid network connection to the wireless bridge and that intermediate switch ports have not been disabled. ◆ Be sure you have configured the wireless bridge with a valid IP address, subnet mask and default gateway. ◆ Be sure the management station has an IP address in the same subnet as the wireless bridge's IP. ◆ If you are trying to connect to the wireless bridge using a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. ◆ If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
Forgot or lost the password	◆ Reset the wireless bridge to factory defaults using its Reset button.

Using System Logs

If a fault does occur, refer to the Quick Start Guide to ensure that the problem you encountered is actually caused by the wireless bridge. If the problem appears to be caused by the wireless bridge, follow these steps:

1. Repeat the sequence of commands or other actions that lead up to the error.

2. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.

3. Record all relevant system settings.

4. Display the log file through the System > Maintenance page, and copy the information from the log file.

5. Download the Troubleshooting Log to a file from the System > Maintenance page.

6. Contact your distributor's service engineer, and send a detailed description of the problem, along with all of the information mentioned in the above steps.

B

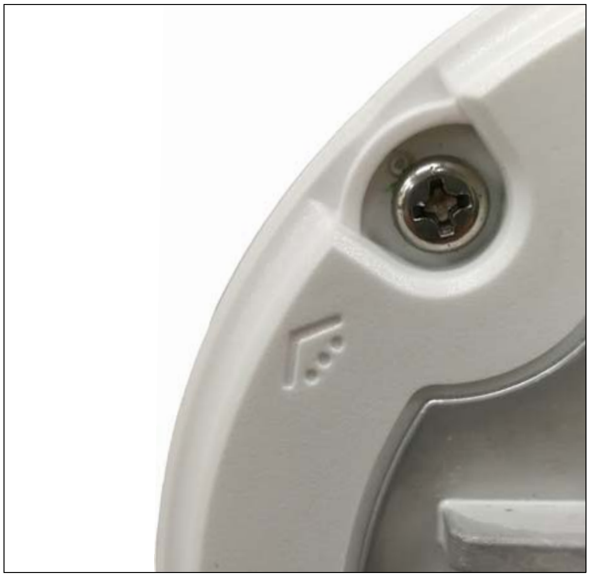
MetroLinq Omni 10G Sectors

Physical Sectors

The MetroLinq Omni includes three 60 GHz sectorized radios. Each sector's antenna provides a 120 horizontal degree beam width and a 32 degree vertical beam width. All three sectors operate in master mode to connect with other MetroLinq models supporting single 60 GHz radios operating in client mode.The sector directions are identified by small arrows on the top panel of the Omni 10G. Next to each arrow are either one, two or three dots with the number of dots corresponding to the Radio# in the Wireless Settings menu.

- Radio#1 — 1 dot
- Radio#2 — 2 dots
- Radio#3 — 3 dots

Figure 59: Sector Direction Indicator



C Device Discovery Tool

Device Discovery Tool

The IgniteNet Discovery tool is a Java .jar file that you can use to locate devices connected to your local network that are up and running.

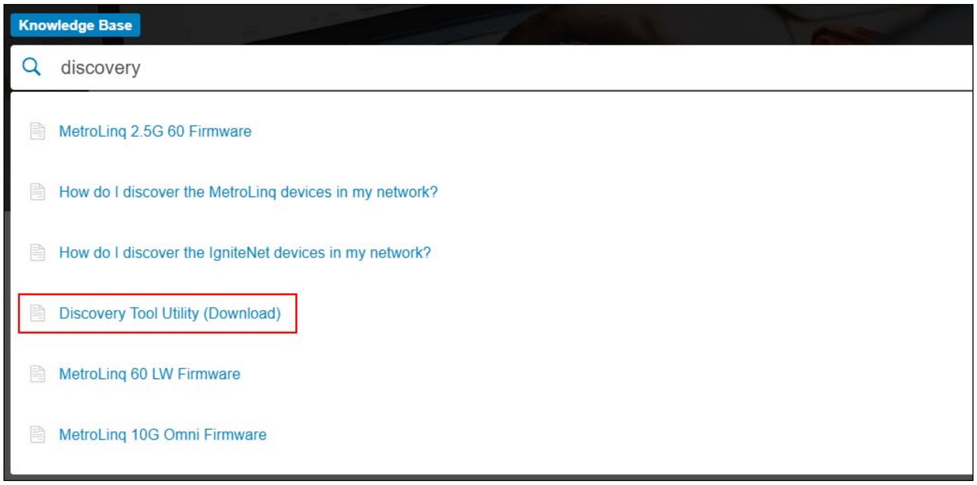
Device Discovery Tool Download

You can download the Device Discovery tool from the IgniteNet Support web site at:

https://support.ignitenet.com

Input the term “discovery” in the *Search help center* text field and click on the Discovery Tool Utility (Download) as shown in Figure 60.

Figure 60: Device Discovery Tool Download



Knowledge Base

discovery

MetroLinq 2.5G 60 Firmware

How do I discover the MetroLinq devices in my network?

How do I discover the IgniteNet devices in my network?

Discovery Tool Utility (Download)

MetroLinq 60 LW Firmware

MetroLinq 10G Omni Firmware

Using the Device Discovery Tool

Prerequisites:

- The computer on which you execute the Device Discovery tool must be connected to the same LAN which your IgniteNet devices are connected to.
- Your computer must have Java installed.

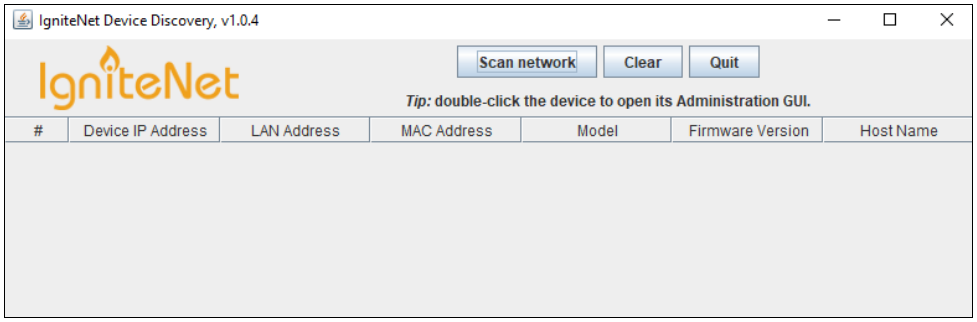
Running the tool

1. To launch the tool, double click the *IgniteNetDiscovery-1.0.4.jar* file downloaded from the support site as described in Device Discovery Tool Download.

Note: If the tool fails to launch, check to make sure Java is installed on your computer and confirm that the file executable.

2. The tool will open as shown in Figure 61 with no devices listed.

Figure 61: Device Discovery Tool Download

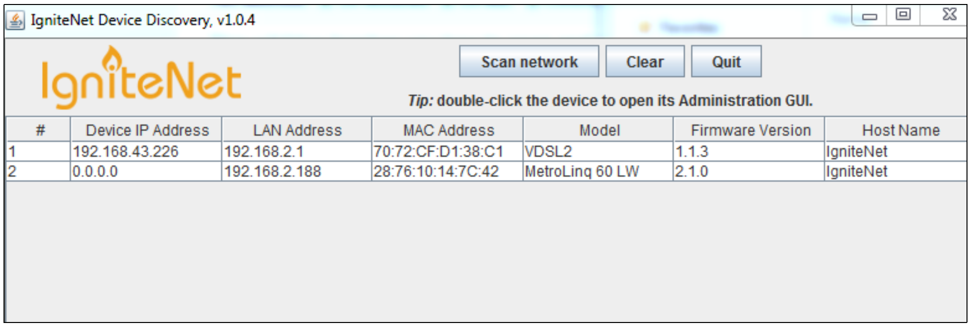


Tip: double-click the device to open its Administration GUI.

#	Device IP Address	LAN Address	MAC Address	Model	Firmware Version	Host Name

3. Click the Scan Network Button to allow the tool to scan your LAN and list any connected IgniteNet devices. The result should be similar to Figure 62.

Figure 62: Device Discovery Tool Download



Tip: double-click the device to open its Administration GUI.

#	Device IP Address	LAN Address	MAC Address	Model	Firmware Version	Host Name
1	192.168.43.226	192.168.2.1	70:72:CF:D1:38:C1	VDSL2	1.1.3	IgniteNet
2	0.0.0.0	192.168.2.188	28:76:10:14:7C:42	MetroLinq 60 LW	2.1.0	IgniteNet

4. Double click a device in the list to open the device's web management page on your default browser.