LUTRON

Application Note #731
Revision B
March 2021

# RadioRA 2 and HomeWorks QS Networking Guide

This document will act as a guide for establishing communication with a RadioRA 2 or HomeWorks QS system and will describe various ways to overcome the network and computer challenges that you may encounter.

## Table of Contents

## 1.0 Glossary and Abbreviations

***HomeWorks Processor*** – This is the basic HomeWorks QS controller and will be the main HomeWorks component connected to any network. Each HomeWorks QS Processor has two RJ45 female connectors, one for the HomeWorks QS LAN/VLAN connection and the other for serviceability.

***Main Repeater*** – This is the basic RadioRA 2 controller and will be the main RadioRA 2 component connected to any network. Each RadioRA 2 Main Repeater has one RJ45 female connector for the RadioRA 2 LAN/VLAN.

***HWQS*** – Abbreviation of HomeWorks QS.

***RA2*** – Abbreviation of RadioRA 2.

***Processor*** – May refer to either/both the HomeWorks QS Processors and RadioRA 2 Main Repeaters.

***Commissioning Machine*** – Refers to the PC or laptop which is running the HomeWorks QS or RadioRA 2 software. The machine must be running a Windows OS.

***Lutron Connect App*** – Phone-based UI to monitor and control HomeWorks and RadioRA 2 systems. Available on HomeWorks and RadioRA 2 software versions 10.X and higher.

***Lutron Designer*** – Client UI for setup and programming of the HomeWorks system. Primary software for all HomeWorks software versions.

***Hop*** – The number of intermediate devices which data packets must pass between source and destination to include layer 3 and layer 2 devices within the network. This includes any device that will delay the data packets from a source processor to a destination processor.

***Hop Limit*** – A hop is one portion of the path that a packet takes from source to destination. Traditionally, the hop limit refers to the time to live (TTL) of that packet before it is discarded. With a Lutron system, the hop limit is not concerned with TTL, rather it is a guideline so that latency of the system commands is kept to a minimum.

***Unicast*** – A communication method over Ethernet TCP or point-to-point communication.

***Master Processor*** – Processor #1 in the system. This processor takes on the role of synchronizing timeclocks in the system, as well as handling communication with the Connect Bridge.

***Multicast*** – A communication method over Ethernet UDP or as one-to-many communication. Lutron systems use multi-source multicast communication so that any device on Ethernet can talk to every other device on the Ethernet at the same time.

***IGMP*** – Lutron processors supports Versions 1, 2, and 3 for multicast communication within a system. Any possible flooding of multicast traffic can be constrained to a set of interested ports by using IGMP snooping.

***PIM*** – If Lutron processors within a system are deployed on different subnets and need routing, PIM is supported in both sparse and dense modes. PIM is typically not required if the connections from the commissioning machine to the processors is configured for Unicast and if all processors are on the same LAN.

***Telnet*** – Telnet is an application layer protocol used to provide a bi-directional text-based communication between client and server devices. Lutron processors will use this protocol over TCP/IP for two main instances:

# 2.0 Network and IT Considerations

## Network Architecture Overview

***What is on the traditional network IP architecture?*** – The HomeWorks Processors/RadioRA 2 Main Repeaters, and client devices (e.g. PC, laptop, tablet, etc.).

***What is NOT on the traditional network IP architecture?*** – The lighting actuators, sensors, and load controllers are not on the network architecture. This includes keypads, wired and wireless temperature sensors, wired and wireless occupancy sensors, thermostats, load controllers, dimmers, switches, lighting panels, fluorescent lamp ballasts, or LED drivers. These devices communicate on a Lutron proprietary wired or wireless communication network.

## Physical Medium

***IEEE 802.3 Ethernet*** – Is the physical medium standard for the network between HomeWorks Processors or RadioRA 2 Main Repeaters. Each HomeWorks Processor and RA2 Main Repeater has female RJ45 connectors for LAN connection.

***CAT5e*** – The minimum network wire specification of the HomeWorks QS and RadioRA 2 LAN/VLAN.

## IP Addressing

***IPv4 –*** The addressing scheme used for the HomeWorks QS and RadioRA 2 systems. The IPv4 address should be static but a DHCP reservation system can also be used. DNS Hostname is not supported. The IPv4 address can be field set to any range, Class A, B, or C. Static will be assumed.

## Class D addressing

***HomeWorks QS/RadioRA 2 System*** – A system is a multicast group of HomeWorks Processors or RA2 Main Repeaters sharing a unique and common class D address that need to share events. Maximum 16 HomeWorks QS Processors on a HomeWorks QS system or two RadioRA 2 Main Repeaters on a RadioRA 2 system. Minimum one HomeWorks QS Processor on a HomeWorks QS system or one RadioRA 2 Main Repeater on a RadioRA 2 system.

***Multicast communications*** – Basic communication to share events between HomeWorks Processors or RadioRA 2 Main Repeaters is based on UDP multicast groups. Below are details on how the Lutron systems deploy this communication scheme.

- All Lutron processors share events and will need a unique and common class D address. The class D multicast address can be field set and specified by the customer.
- Any source multicast is used because any Lutron processor may be enacting the event.
- Multicast communication in Lutron systems is primarily event based (e.g., system trigger or change in state for monitoring). Polling is not a basis of communications in Lutron systems.
- Prior to software version 9.0, the HomeWorks QS commissioning laptop/PC needed to join every multicast group to communicate to the HomeWorks Processors. Commissioning machines hosting software version 9.0 and newer can either communicate to the HomeWorks Processors by joining every multicast group or can be setup as TCP unicast communication. This can be setup during system startup at the customer's discretion. For RadioRA 2, this functionality was introduced in software version 11.0.

**Note:** Multicast communication is still required for communication among the processors in a system.

Setting up the commissioning laptop to talk to a Lutron system using TCP communication only changes processor discovery and transfers to TCP communication.

## 2.0 Network and IT Considerations *(continued)*

### Ports (REQUIRED)

*Processor to Processor within a HomeWorks QS or RadioRA 2 system*
UDP/2056

*Commissioning Machine to Processors* ***UNICAST OPTION***
TCP/51023
- TCP available only for commissioning machine hosting HomeWorks software version 9.0 and newer, or RadioRA 2 software version 11.0 and newer

*Commissioning Machine to Processors* ***MULTICAST OPTION***
UDP/2056

*Upgrading of Processors*
TFTP/69, UDP/777

**Note: Unicast or multicast communication option is configured on site by a Lutron qualified dealer and at the customers determination. System will default to multicast if not specified.**

*Lutron Connect Bridge to Processors*
SFTP/22, TCP/23, UDP/1900, UDP/2647, TCP/4548, UDP/5353, TCP/8081, TCP/8083

*Lutron Connect Bridge to WAN (initiated by the Connect Bridge – NO PORT FORWARDING REQUIRED)*
TCP/80, UDP/123, TCP/443, TCP/7443, TCP/8883

*Lutron Connect Bridge to Third-Party Integrators*
TCP/1900, TCP/4548, TCP/7782, TCP/8081, TCP/8083, TCP/8090

### Ports (OPTIONAL)

*Commissioning Machine to Processors*
TFTP/69, UDP/777
- Only required when upgrading the system

*Processor TELNET*
Source TCP/23
- Only required if the Lutron system is integrating with third-party equipment through Serial/IP
- Prior to version 13.0, default Telnet credentials were available for integrators to use. From 13.0 forward, Telnet credentials need to be set up in the Lutron commissioning software

## 2.0 Network and IT Considerations *(continued)*

### Hop Limit for Unmanaged Networks

The required hop limit of any data packet from a source processor to a destination processor is 6.

**Note:** This rule is only applicable when using an unmanaged network to interconnect the devices of a Lutron system and is required to ensure optimal performance. The hop limit is more of a suggestion than a rule to keep latency down between system processors. The requirement is that all processors must be able to communicate to all other processors with latency under 10 ms.

### Latency Requirements for Managed Networks

Note that for managed networks, the maximum latency between any two Lutron processors should be less than 10 ms. The maximum latency between the Lutron commissioning machine and any processor needs to less than 10 ms.

### Other Protocols Supported

***IGMP*** – Lutron processors supports Versions 1, 2, and 3 for multicast communication within a system. Any possible flooding of multicast traffic can be constrained to a set of interested ports by using IGMP snooping.

***PIM*** – If Lutron processors within a system are deployed on different subnets and need routing, PIM is supported in both sparse and dense modes. PIM is typically not required if the connections from the commissioning machine to the processors is configured for Unicast and if all processors are on the same LAN.

***Telnet*** – Telnet is an application layer protocol used to provide a bi-directional text-based communication between client and server devices. Lutron processors will use this protocol over TCP/IP for two main instances:

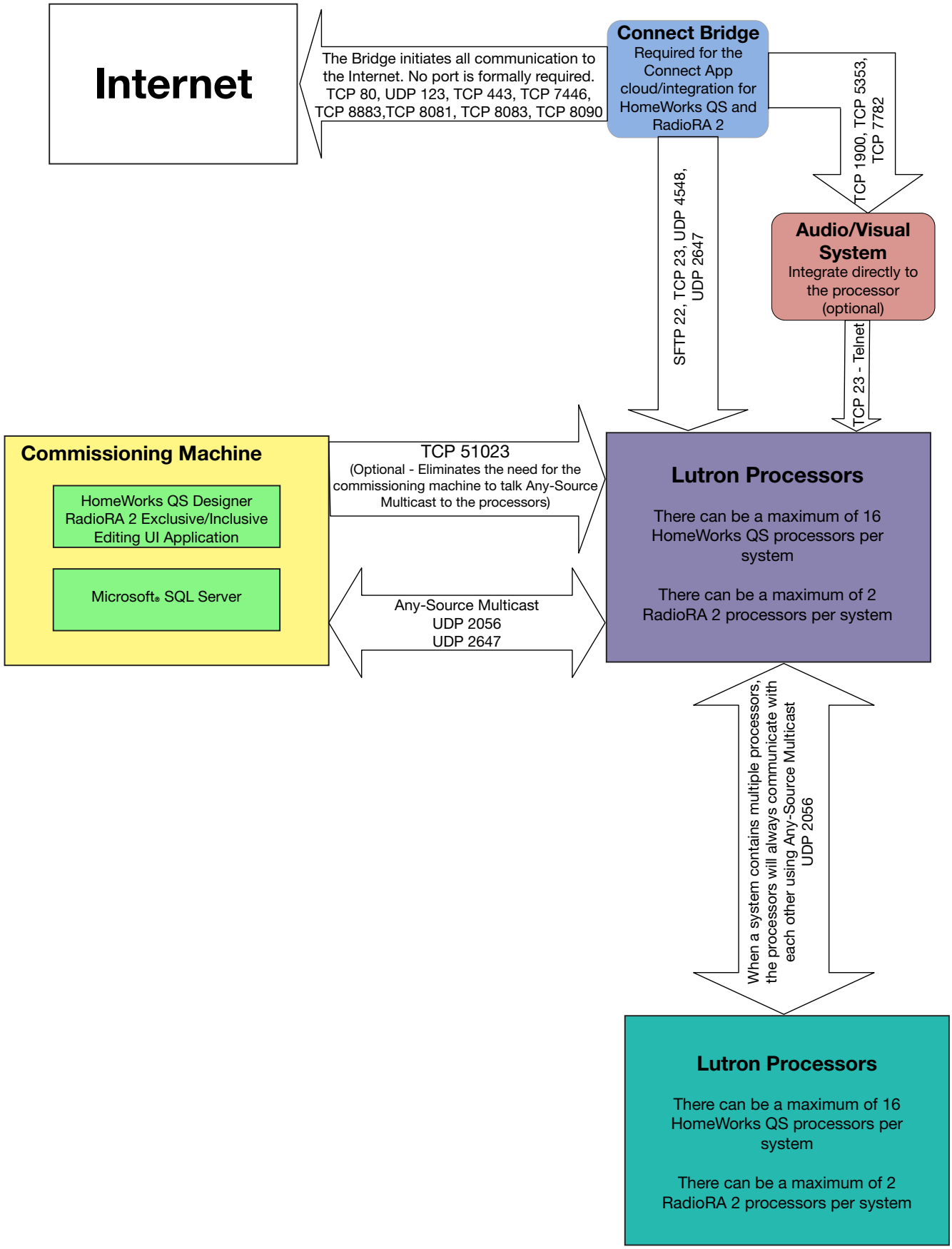
1. Telnet may be used to run diagnostics and during the support file creation process.
2. If there is a third-party system (e.g., a touchscreen) integrating with the Lutron system, it may communicate to a Lutron processor over a Telnet session.

### Communication Speed and Bandwidth

***100 BaseT*** – Is the maximum communications speed required for Lutron processor and commissioning machine communication.

***1.88 Mbps (Megabits per second)*** – Worst case bandwidth in a fully loaded system with 16 processors. Most systems include only 1 to 4 processors.

## 3.0 Communication Port Diagram



## 4.0 Connecting to the RadioRA 2 Main Repeater

**Requirements**

1. Windows® OS running the RadioRA 2 programming software
2. Main Repeater(s)

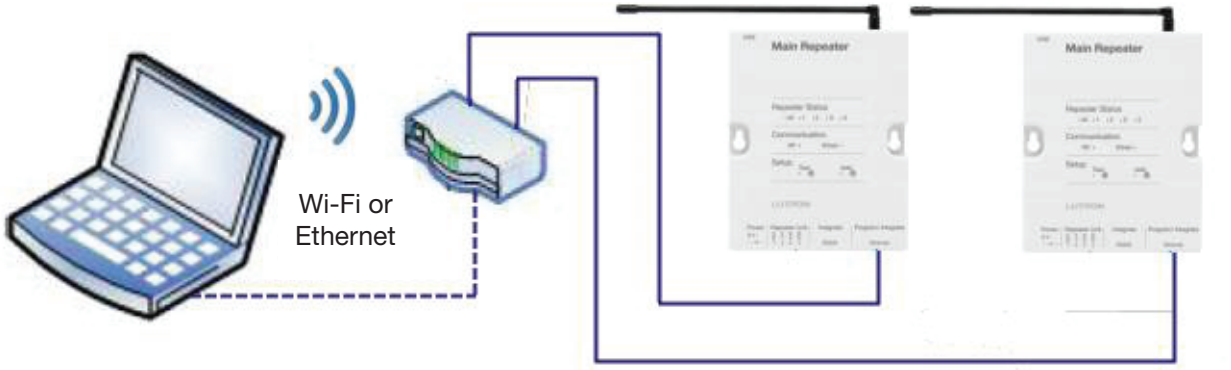
**Recommended**

1. Wired/Wi-Fi Router

During system commissioning, the RadioRA 2 programming software will first make a connection with the Main Repeater(s) through the local area network (LAN). It is recommended to perform commissioning using a connection through a router, either wired or Wi-Fi, but never both wired and Wi-Fi at the same time. Using a router helps to minimize changes to settings on the Windows machine. A wired LAN connection is always recommended for the highest level of reliability. Each Main Repeater includes a variety of communication capabilities including:

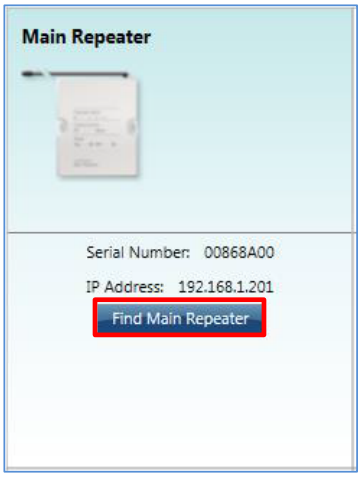
1. ***Clear Connect Wireless***: Used for communication to the up to 99 devices that can be assigned to each Main Repeater (431-437 MHz)
2. ***Wired Repeater Link***: Use a Plenum QS cable to link Repeaters on the same Clear Connect subnet for the purpose of range extension for outbuildings of up to 1000 ft (305 m) between repeaters (guest house, boat house, pool house, etc.)
3. ***RS-232***: Serial communication port used for some third-party integration
4. ***Ethernet***: Used for third-party integration, Connect Bridge access, and database uploads from the RadioRA 2 programming software

**Figure 1: PC to two Main Repeaters: Ethernet or Wi-Fi (Never Ethernet and Wi-Fi at the same time)**



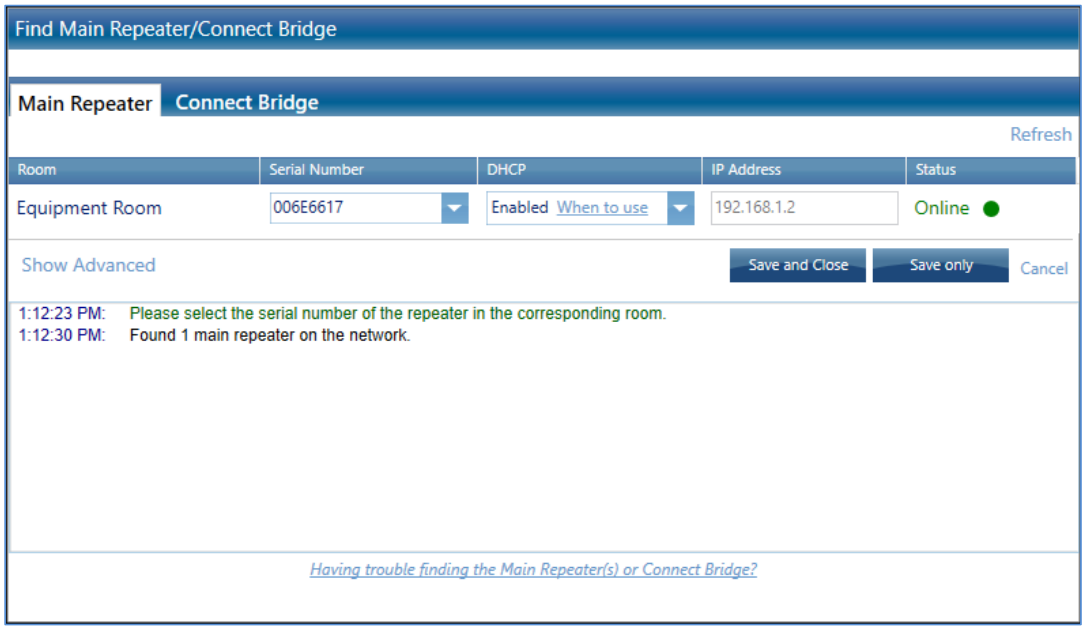

Connect the Windows machine to the same LAN as the Main Repeater(s) and open the RadioRA 2 programming software. Use the Room list on the Design tab, on the left, to select a room which contains a Main Repeater.

Click on the blue **Find Main Repeater** button below the image of the Main Repeater.



## 4.0 Connecting to the RadioRA 2 Main Repeater *(continued)*

The **Find Main Repeater/Connect Bridge** window will open.

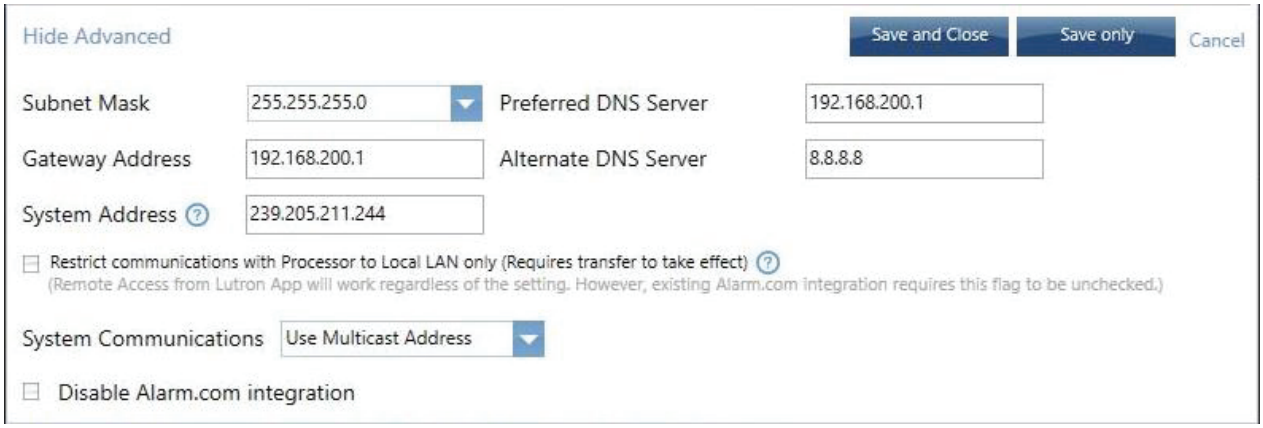



If the programming software was able to locate the Main Repeater(s), it will tell you that it "Found x Main Repeater(s) on the network" where x is typically 1 or 2. The standard fields shown, and their purposes are as follows:

- ***Room***: Name of the room on the area tree where a Main Repeater has been placed
- ***Serial Number***: The unique Lutron serial number for the Main Repeater; found on the product label on the back of each Main Repeater
- ***DHCP***: Options are Enabled or Disabled
  - ***Enabled***: The Main Repeater IP address will be automatically assigned by the DHCP server of the router on the network
    - Used for simple plug and play networks without third-party control systems
    - Set to DHCP Enabled when a DHCP Reserved address is set on the DHCP server of the router for the Main Repeater(s)
  - ***Disabled***: A static IP address will be assigned using the IP address field in the Find Main Repeater window
    - Used when integrating the RadioRA 2 system with third-party control systems
    - Recommended to set the static IP address of each Main Repeater above the DHCP range of the router (common addresses start at 192.168.x.200 and above)
    - On a two Main Repeater system, the two Main Repeaters must have unique addresses
- ***IP Address***: The unique IP address of the Main Repeater on the network; the field will be active for editing when DHCP is set to disabled

## 4.0 Connecting to the RadioRA 2 Main Repeater *(continued)*

In most cases, these setting fields will be the primary ones that will be used to make a connection to the Main Repeater(s). In the case of more advanced network needs, for example a virtual private network (VPN) for remote control/access, the Advanced Settings may need to be configured. They are as follows:




- ***Subnet Mask***: A number screen which the router uses to decide which portions of an address to consider before routing information within the network
  – A common residential LAN subnet mask is 255.255.255.0 which indicates that the first three address octets are the same for all devices on the network and the fourth octet is the field which is used to identify the unique addresses on the network
- ***Gateway Address***: A router address used for the transmission of packets outside of the network. Should be on the same subnet as the devices on the network which will be transmitting the data
- ***Preferred DNS Server***: The preferred or primary domain name system address used for mapping host names to IP address
- ***Alternate DNS Server***: An alternate domain name system address used when the preferred or primary one times out after an unsuccessful connection
- ***System Address***: Multicast Address used for inter-processor communication; this address typically remains unchanged
  – In scenarios where multiple, independent systems are inside the same building, the network can be setup such that each system is on its own smaller LAN or VLAN, incapable of seeing the other systems through the network
  – Each system on the same network must have a unique system address. Changing the last octet to be unique is all that is needed
- ***Restrict Communications with Processor to Local LAN only (Requires transfer to take effect)***: A security feature which disallows all off-network connections to the Main Repeater. This option will not interfere with the Connect mobile app connecting remotely.
- ***Disable Alarm.com Integration:*** Option which disallows communication between the Main Repeater and Alarm.com servers. Keep this option deselected if Alarm.com integration is desired. Select this option if integration with Alarm.com is not a requirement. This option was introduced in RA2 12.2, and HWQS 15.0.

## 4.0 Connecting to the RadioRA 2 Main Repeater *(continued)*

- ***System Communications***: Changes how the software on the commissioning machine communicates with the Main Repeaters in the system
  - ***Use Multicast Address***: The software will communicate to the Main Repeaters in the system using multicast
    - Compatible with most unmanaged networks
  - ***Use Repeater's Address***: The software will communicate to the Main Repeaters in the system using TCP
    - Most often used with managed networks which do not support multicast traffic
    - This setting only changes software-to-processor communication to TCP. Inter-processor communication will remain multicast
    - This option is only available when DHCP is disabled
  - ***Use Remote Programming***: The software will direct communication to the IP address specified in the "Remote Programming Address" box which appears. This IP address should be the router's external WAN IP address. Port forwarding of the port number which appears in the "Port" box will need to be set up on the router to forward the traffic to the Main Repeater IP address. **There is inherent risk exposing a Main Repeater to the WAN using port forwarding. If new unexplained control issues arise, disable port forwarding and use a different communication method.**

After completing configuration of all necessary settings on the Find Main Repeater window, click **Save and Close**. For more information on setting up a virtual private network and/or domain name service for remote access or programming of the Lutron system, please see Application Note #231 (P/N 048231) at www.lutron.com.

For more information on setting up multiple independent systems in the same building, please see Application Note #688 (P/N 048688) at www.lutron.com.

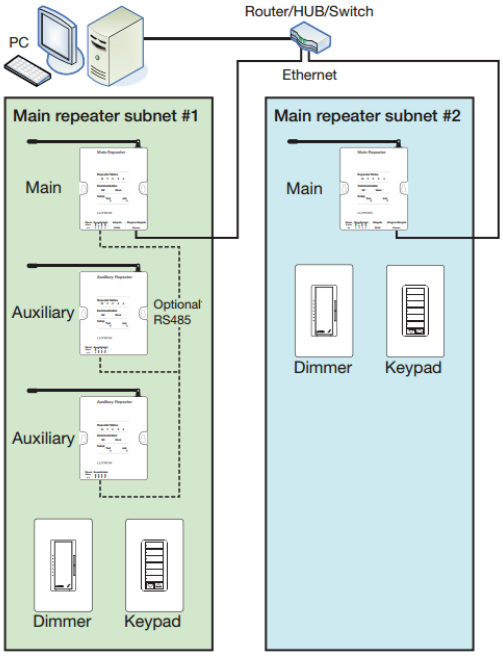
## 4.0 Connecting to the RadioRA 2 Main Repeater *(continued)*

### 4.1 Important Notes when Connecting to a Two Main Repeater System

Using two Main Repeaters in RadioRA 2 allows for systems that can scale as large as 200 devices. The inclusive software is required for commissioning a two Main Repeater system.

RadioRA 2 uses an architecture that essentially has what is defined as two device links, each owned by a Main Repeater. Each link allows for up to 100 total devices where the Main Repeater takes one address and four addresses are reserved for Auxiliary Repeaters. The RF links, while they use the same protocol, utilize two different wireless channels or frequencies and thus the two Main Repeaters do not communicate to each other using Clear Connect Wireless.

All communication between Main Repeaters must be done through the local area network with each Main Repeater being tied to its own port on a switch or router. The subnet referred to in the below image refers to the RF subnet of each repeater, not to the networking subnet of the Main Repeaters.

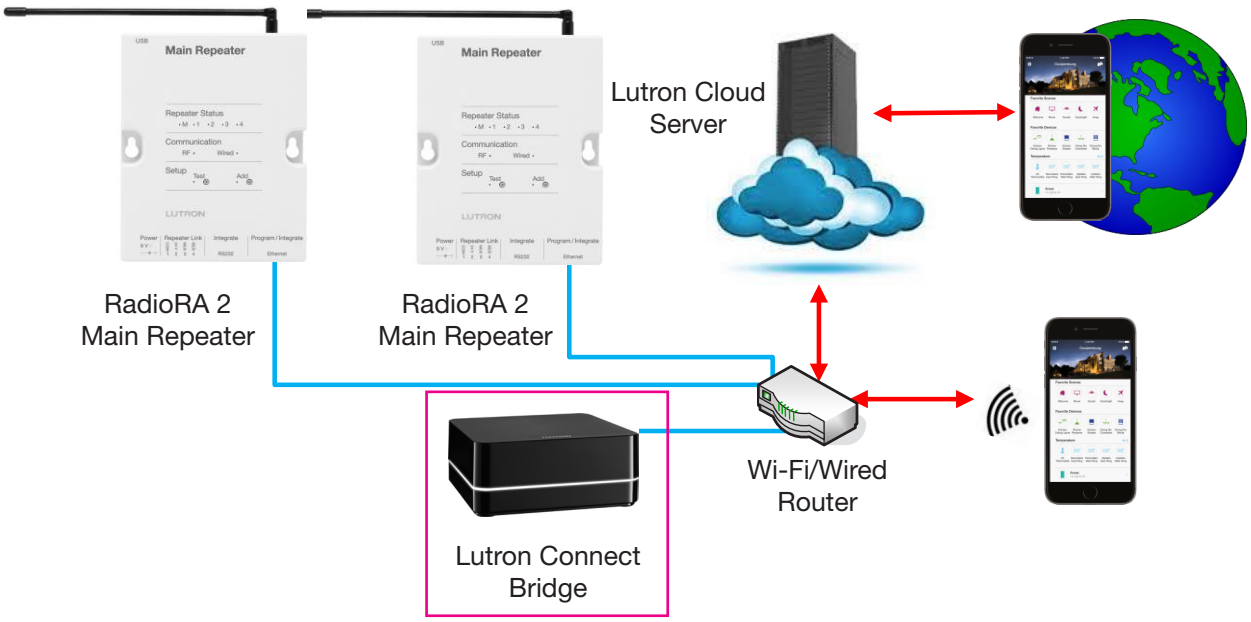


## 5.0 Connecting to the Lutron Connect Bridge (RadioRA 2)

**Requirements**

1. Windows machine running the RadioRA 2 programming software
2. Main Repeater(s)
3. Lutron Connect Bridge (max of 1 per system)
4. Wired/Wi-Fi Router or Network switch to place the Connect Bridge onto the same network as the Main Repeater(s)
5. Internet access (for initial setup of Lutron Connect and for remote access to the system)

**Figure 2: RadioRA 2 with Connect Bridge One-Line**

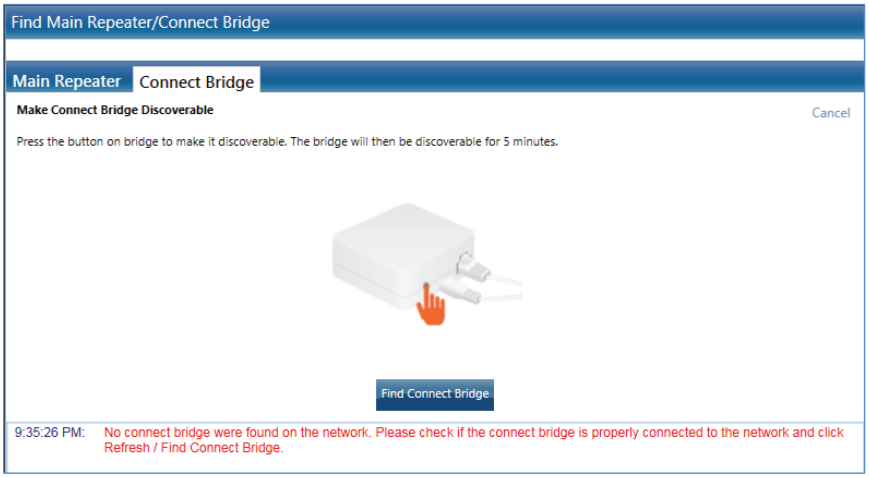



Connect the Windows machine to the same LAN as the Main Repeater(s) and Connect Bridge. Open the RadioRA 2 programming software. Use the Room list on the Design tab, on the left, to select a room which contains the Connect Bridge.

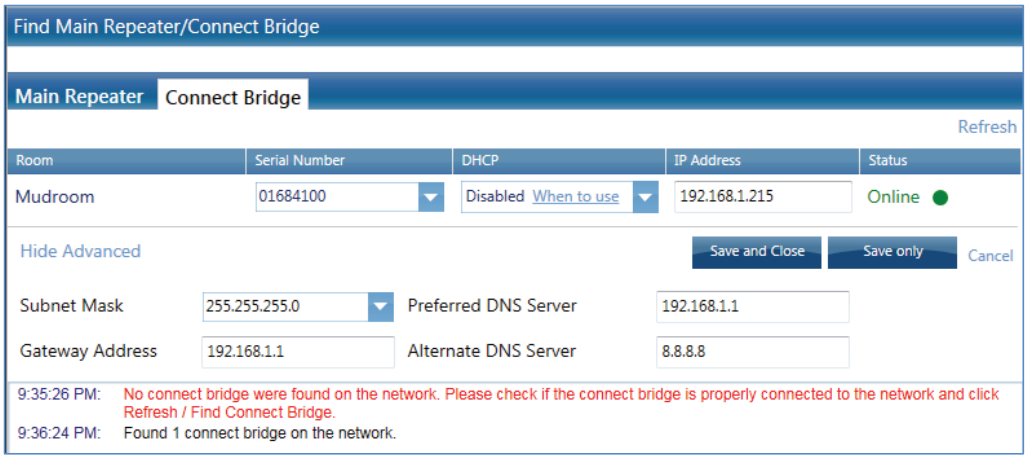
Click on the blue **Find Connect Bridge** button below the image of the Connect Bridge.

## 5.0 Connecting to the Lutron Connect Bridge (RadioRA 2) *(continued)*

The **Find Main Repeater/Connect Bridge** window will open.




Initially, no Connect Bridge will be found. The Bridge must be placed into discovery mode by pressing the button on the Bridge (as described in the illustration within the software). Discovery mode will last for five minutes. After pressing the button on the Bridge, click on **Find Connect Bridge** to try to discover the Bridge.




If the programming software was able to locate the Connect Bridge, it will tell you that it “Found 1 Connect Bridge on the network.” The standard fields and their purposes are as follows:

- ***Room***: Name of the room on the area tree where the Connect Bridge has been placed
- ***Serial Number***: The unique Lutron serial number for the Connect Bridge; found on the product label on the bottom of each Connect Bridge
- ***DHCP***: Options are Enabled or Disabled
  - ***Enabled***: The Connect Bridge IP address will be automatically assigned by the DHCP server of the router on the network
    - ***Option 1***: Used for simple plug and play networks without third-party control systems
    - ***Option 2***: Set to DHCP Enabled when a DHCP Reserved address is set on the DHCP server of the router for the Main Repeater(s)
  - ***Disabled***: A static IP address will be assigned using the IP address field in the Find Main Repeater/Connect Bridge window
    - Recommended to set the static IP address of the Connect Bridge above the DHCP range of the router (common addresses start at 192.168.x.200 and above)
    - The Connect Bridge must have a unique IP address
- ***IP Address***: The unique IP address of the Connect Bridge on the network; the field will be active for editing on when DHCP is set to disabled

## 5.0 Connecting to the Lutron Connect Bridge (RadioRA 2) *(continued)*

In most cases, these setting fields will be the primary ones that will be used to make a connection to the Connect Bridge. In the case of more advanced network needs, the Advanced Settings may need to be configured. They are as follows:

- ***Subnet Mask***: A number screen which the router uses to decide which portions of an address to consider before routing information within the network
  - A common residential LAN subnet mask is 255.255.255.0 which indicates that the first three address octets are the same for all devices on the network and the fourth octet is the field which is used to identify the unique addresses on the network
- ***Gateway Address***: A router address used for the transmission of packets outside of the network. Should be on the same subnet as the devices on the network which will be transmitting the data
- ***Preferred DNS Server***: The preferred or primary domain name system address used for mapping host names to IP address
- ***Alternate DNS Server***: An alternate domain name system address used when the preferred or primary one times out after an unsuccessful connection

For more information on setting up the Connect Bridge and Lutron Connect Mobile Application, refer to the Lutron Connect Setup Guide App Note #649 (P/N 048649) at www.lutron.com

After completing configuration of all necessary settings on the Find Main Repeater/Connect Bridge window, click on **Save and Close**.

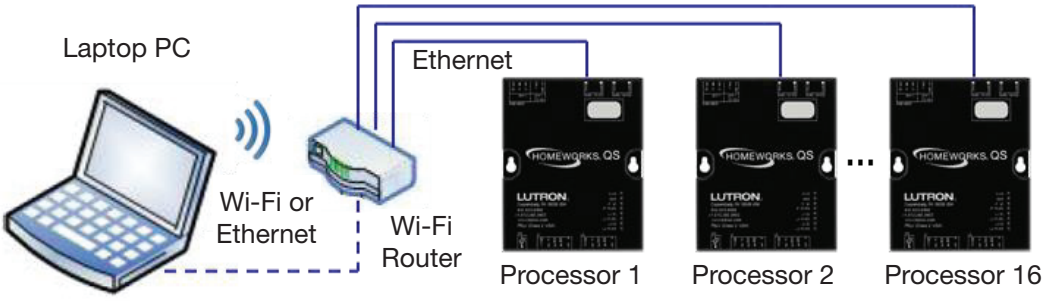
## 6.0 Connecting to HomeWorks QS Processors

**Requirements**

1. Windows machine running the HomeWorks QS programming software
2. HomeWorks QS Processor(s)
3. Wired/Wi-Fi Router or network switch to place the processors and PC onto the same network

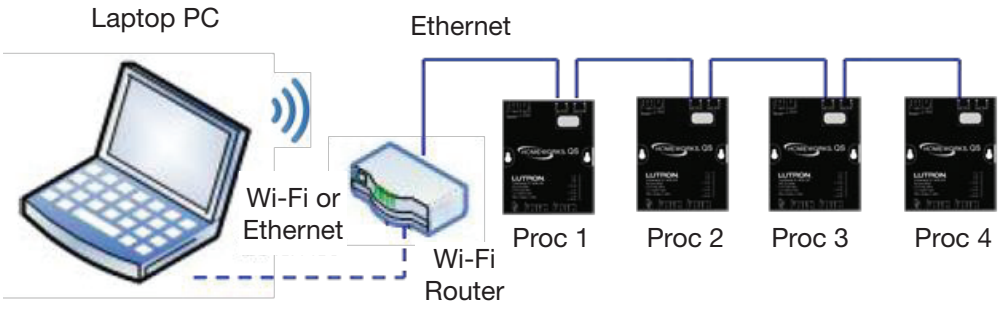
During system commissioning, the HomeWorks QS programming software will first try to make a connection with the processor(s) through the local area network (LAN). It is typically necessary to perform commissioning using a connection through a router, either wired or Wi-Fi, due to the number of processors that can be on a single system (up to 16 total). Using a router helps to minimize changes to settings on the commissioning machine. A wired LAN connection is always recommended for the highest level of reliability.

**Figure 3: PC to Processor(s): Wired or Wi-Fi Connection (Never Ethernet and Wi-Fi at the Same Time)**



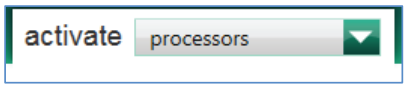

In systems with many processors, switch/router ports can be conserved by daisy-chaining processors off one port. Up to 4 processors can be wired in this manner. Refer to section 3.1 for more information on Ethernet hopping of multiple processors from a single switch/router port.

**Figure 4: PC to Processor(s): Wired or Wi-Fi Connection w/ Daisy-Chaining (Never Ethernet and Wi-Fi at the Same Time)**

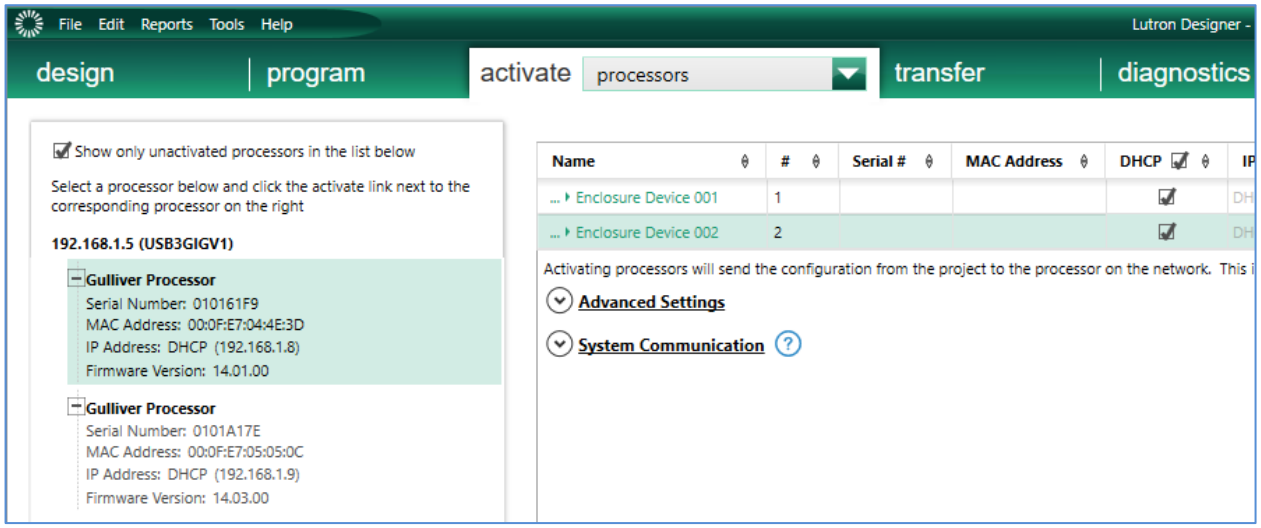


## 6.0 Connecting to HomeWorks QS Processors *(continued)*

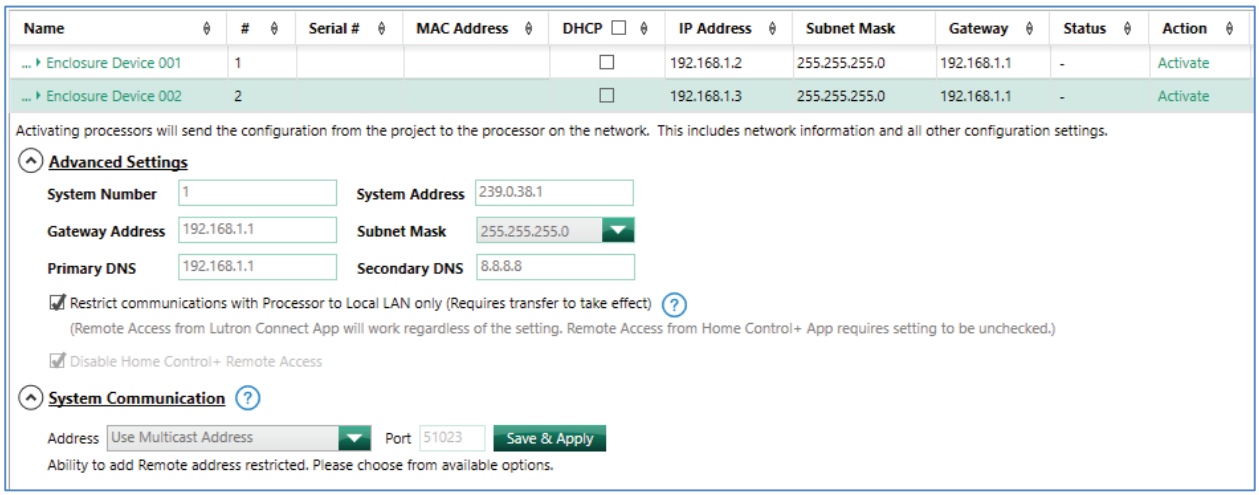
Connect the commissioning machine to the same LAN as the processor(s) and open the HomeWorks QS programming software. Go to the Activate tab and choose the option **activate > processors**.




Un-activated processors discovered on the network will display on the left side of the Activation screen. Each processor will display its Lutron device serial number, MAC address, current IP address, and current firmware version. The serial number and MAC address of each processor can be found on the unit label on the front of the processor. The current IP address for a processor discovered for the first time is one that likely originated from the DHCP server of the local router. DHCP is the default mode of each processor.




On the right side of the activation screen, a row for each processor in your database design will appear with a link to activate the processor on the far right. Prior to activation, it is necessary to properly configure all network settings.



## 6.0 Connecting to HomeWorks QS Processors *(continued)*

- ***Name:*** Displays the area tree breakdown of each processor
- ***#:*** A number which identifies each processor in the database. Processor #1 takes on the role of the "master processor." See 1.0 Glossary and Abbreviations section for more information.
- ***Serial Number:*** The unique Lutron serial number for the processor; found on the product label on the front of each processor
- ***MAC Address:*** The unique MAC address for the processor; found on the product label on the front of each processor
- ***DHCP***: Options are Enabled (checked) or Disabled (unchecked)
  - ***Enabled:*** The processor IP address will be automatically assigned by the DHCP server of the router on the network
    - ***Option 1***: Used for simple plug and play networks without third-party control systems
    - ***Option 2***: Set to DHCP Enabled when a DHCP Reserved address is set on the DHCP server of the router for the HomeWorks QS Processor(s)
  - ***Disabled:*** A static IP address will be assigned using the IP address field in the activate processors screen
    - Used when integrating the HomeWorks QS system with a third-party control system
    - Recommended to set the static IP address of each processor above the DHCP range of the router (common addresses start at 192.168.x.200 and above)
    - Each processor must have a unique IP address
- ***IP Adress***: The unique IP address of the processor on the network; the field will be active for editing on when DHCP is set to disabled (unchecked)
- ***Subnet Mask***: A number screen which the router uses to decide which portions of an address to consider before routing information within the network
  - A common residential LAN subnet mask is 255.255.255.0 which indicates that the first three address octets are the same for all devices on the network and the fourth octet is the field which is used to identify the unique addresses on the network
- ***Gateway***: A router address used for the transmission of packets outside of the network. Should be on the same subnet as the devices on the network which will be transmitting the data
- ***Preferred DNS Server***: The preferred or primary domain name system address used for mapping host names to IP address
- ***Secondary DNS Server***: An alternate domain name system address used when the preferred or primary one times out after an unsuccessful connection
- ***System Number***: A unique identifier for a system to differentiate systems on the same network. Every system on the same network must have a unique system number
- ***System Address***: Multicast address used for inter-processor communication; this address typically remains unchanged
  - In scenarios where multiple, independent systems are inside the same building, the network can be setup such that each system is on its own smaller LAN, incapable of seeing the other systems through the network
  - Every system on the same network must have a unique system address
- ***Restrict Communications with Processor to Local LAN Only (Requires Transfer to Take Effect)***: A security feature which disallows all off-network connections system
- ***System Address***: A security feature which disallows Telnet connections to be made with the system. This option is automatically set when the restrict communications option is enabled (checked)
- ***System Communications***: Changes how the software on the commissioning machine communicates with the Main Repeaters in the system
  - ***Use Multicast Address***: The software will communicate to the Main Repeaters in the system using multicast traffic
    - Compatible with most unmanaged networks
  - ***<IP Address>***: The software will communicate to the processor IP address specified in the system using TCP traffic
    - Most often used with managed networks which do not support multicast traffic
    - This setting changes software-to-processor communication to TCP. Inter-processor communication will remain multicast
    - This option is only available when DHCP is disabled

## 6.0 Connecting to HomeWorks QS Processors *(continued)*

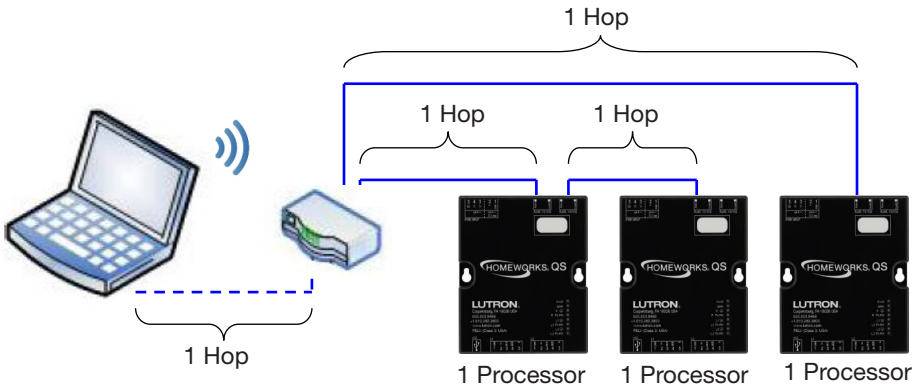
For more information on setting up a virtual private network and/or domain name service for remote access or programming of the Lutron system, refer to Application Note #231 (P/N 048231) at www.lutron.com

For more information on setting up multiple independent systems in the same building, refer to Application Note #688 (P/N 048688) at www.lutron.com

After completing configuration of all of the necessary settings for each processor, activate each processor by clicking on them one by one using the list of un-activated processors on the left side of the screen and then click on the word Activate on the far right of the screen for each individual processor. The status field should say "Good ✓." Be sure to activate the correct processor to the placeholder in the software. Incorrect processor activation will lead to the inability to activate devices to the system.

### 6.1 Network Hops with HomeWorks QS Processors

For optimal system performance, no more than 5 Ethernet hops should exist between any two processors or any processor and the PC in the HomeWorks QS system. An Ethernet hop is best described as a connection between two devices (router, switch, processor, or PC). In the following example, there is only 1 Ethernet hop between processor 1 and processor 2, but there are 3 Ethernet hops between processor 2 and processor 3.

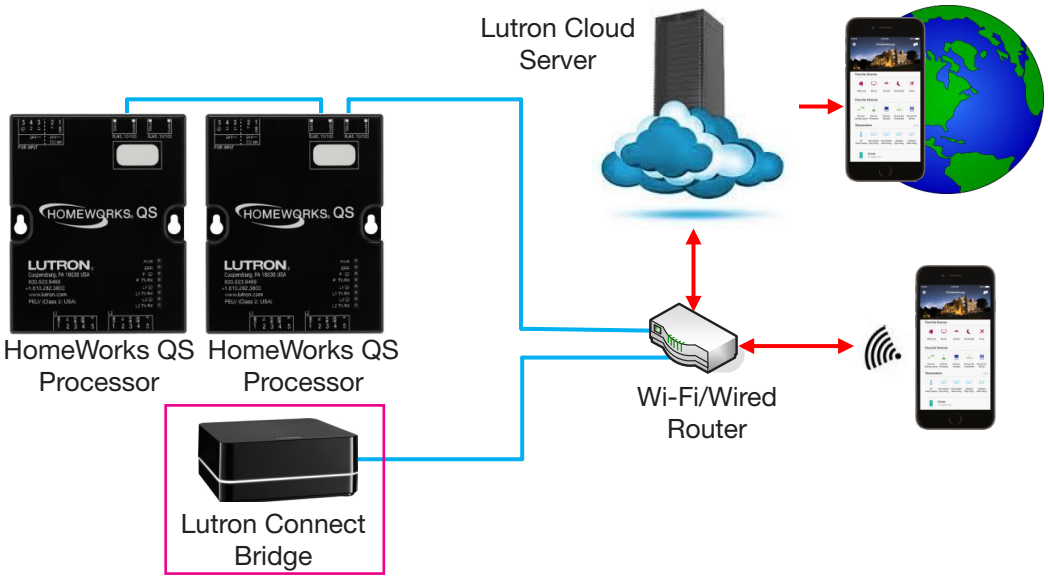


## 7.0 Connecting to the Lutron Connect Bridge (HomeWorks QS)

**Requirements**

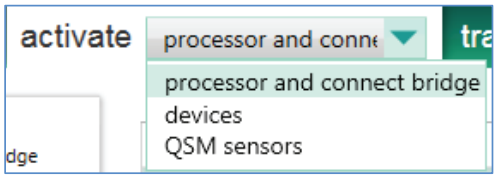
1. Windows machine running the HomeWorks QS programming software
2. HomeWorks QS Processor(s)
3. Lutron Connect Bridge (max of 1 per system)
4. Wired/Wi-Fi Router or network switch to place the Connect Bridge onto the same network as the processor(s)
5. Internet access (for the initial setup of Lutron Connect)

**Figure 5: HomeWorks QS with Connect Bridge One-Line**

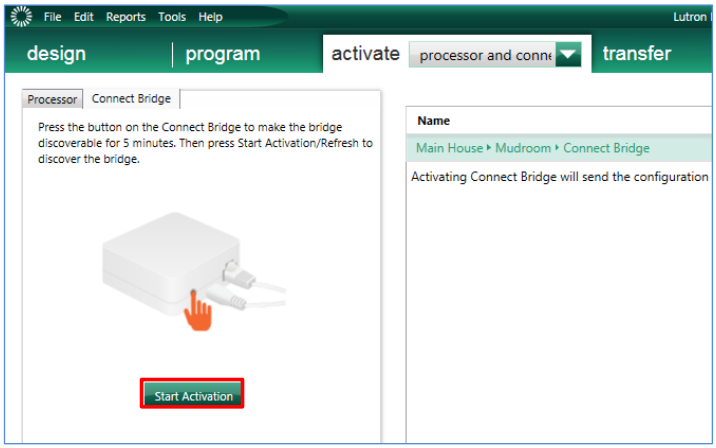



**Note:** The HWQS processor does not support forwarding mDNS discovery packets, so the Connect Bridge should not be plugged directly into the spare Ethernet port on any HWQS processor.

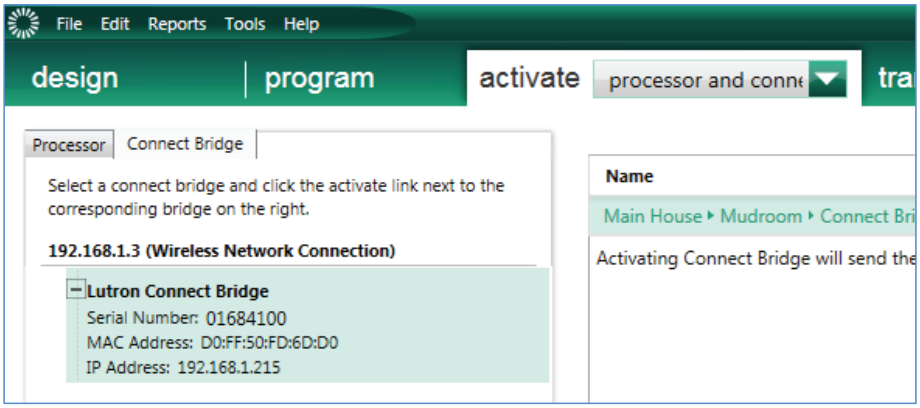
Connect the commissioning machine to the same LAN as the processor(s) and Connect Bridge and open the HomeWorks QS programming software. Go to the activate tab and choose the option **activate > processor and Connect Bridge**.




Initially, no Connect Bridge will be found. The Bridge must be placed into discovery mode by pressing the button on the Bridge (as described in the illustration within the software). Discovery mode will last for five minutes. After pressing the button on the Bridge, click on **Start Activation**.

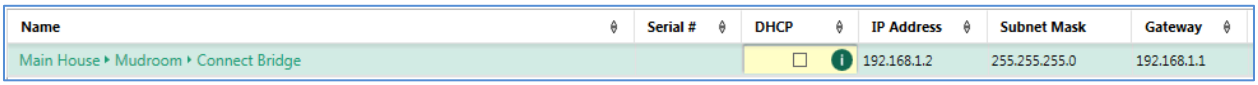


## 7.0 Connecting to the Lutron Connect Bridge (HomeWorks QS) *(continued)*




An un-activated bridge discovered on the network will display on the left side of the activation screen. The bridge will display its Lutron device serial number, MAC address, and current IP address. The serial number and MAC address of each bridge can be found on the unit label on the bottom of the Bridge. The current IP address for a bridge discovered for the first time is one that likely originated from the DHCP server of the local router. DHCP is the default mode of each bridge.

On the right side of the activation screen, a row for each processor in your database design will appear with a link to activate the processor on the far right. Prior to activation, it is necessary to properly configure all network settings.




- ***Name:*** Displays the area tree breakdown of the bridge
- ***Serial Number:*** The unique Lutron serial number for the Connect Bridge; found on the product label on the bottom of each Connect Bridge
- ***DHCP***: Options are Enabled (checked) or Disabled (unchecked)
  - ***Enabled:*** The processor IP address will be automatically assigned by the DHCP server of the router on the network
    - ***Option 1***: Used for simple plug and play networks without third-party control systems
    - ***Option 2***: Set to DHCP Enabled when a DHCP Reserved address is set on the DHCP server of the router for the HomeWorks QS Processor(s)
  - ***Disabled:*** A static IP address will be assigned using the IP address field in the activate processors screen
    - Recommended to set the static IP address of each processor above the DHCP range of the router (common addresses start at 192.168.x.200 and above)
    - The Connect Bridge must have a unique IP address
- ***IP Adress***: The unique IP address of the Connect Bridge on the network; the field will be active for editing on when DHCP is set to disabled
- ***Subnet Mask***: A number screen which the router uses to decide which portions of an address to consider before routing information within the network
  - o A common residential LAN subnet mask is 255.255.255.0 which indicates that the first three address octets are the same for all devices on the network and the fourth octet is the field which is used to identify the unique addresses on the network
- ***Gateway Address***: A router address used for the transmission of packets outside of the network. Should be on the same subnet as the devices on the network which will be transmitting the data

For more information on setting up the Connect Bridge and Lutron Connect Mobile Application, refer to the Lutron Connect Setup Guide App Notw (P/N 048649) at www.lutron.com

After completing configuration of all necessary settings for the bridge, activate the bridge by clicking on the word Activate on the far right of the screen. The status field should say “Good ✓”.

# 8.0 Best Practices

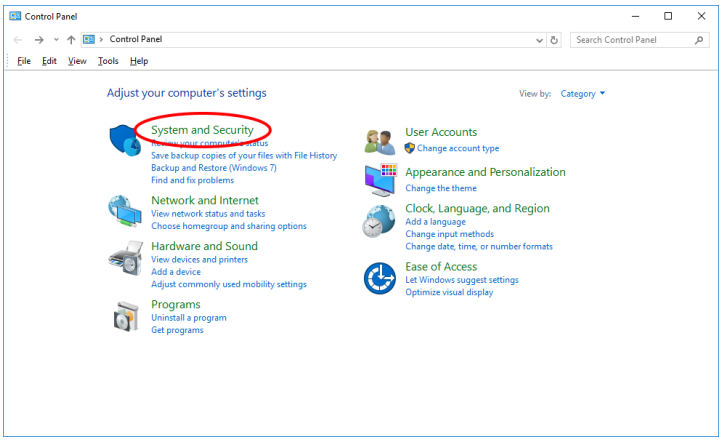
## 8.1 Firewalls and Security Programs

Often times the difficulty of establishing communication between the PC and the processor(s) has to do with a program or programs that are restricting the Lutron Programming Software from sending the necessary communications to the processor. The PC is using these software features to protect itself and the user from security issues such as viruses. There are two things that you can do to mitigate connection issues when confronted by these PC features.

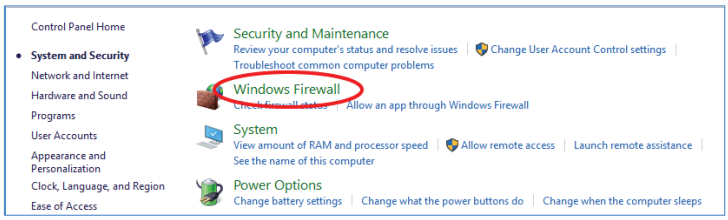
### 8.1.1 Check Inbound Firewall Rules

Depending on the operating system, the process to see the current firewall status and allow programs through the firewall may be different. The below screenshots were captured using Windows 10. From the Start menu, search for and open Control Panel. Click on **System and Security**.

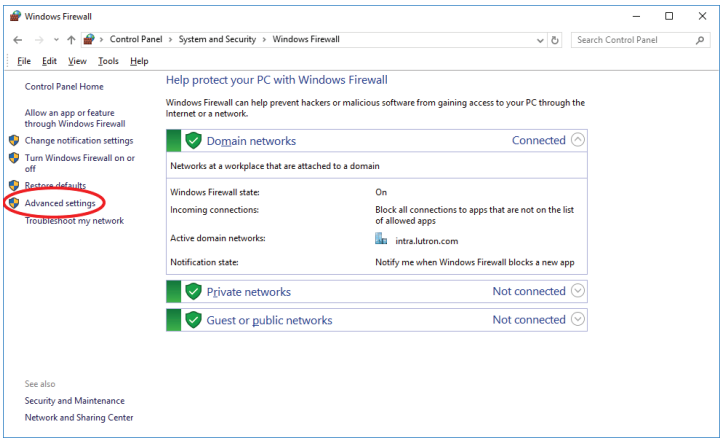
**Note:** Even with all firewalls disabled, it has been seen on multiple machines that firewall rules to block Lutron software can still operate.




Here you can check on the Windows Firewall status or allow programs through the Windows Firewall. Click **Windows Firewall**.




This screen will show the status of each of the Windows firewalls on the machine. In the left pane, click **Advanced settings**.

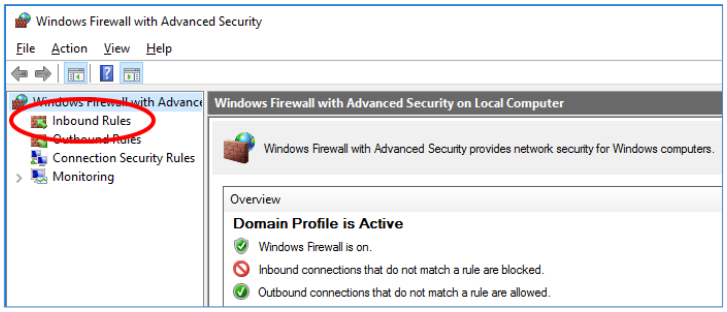


# 8.0 Best Practices *(continued)*

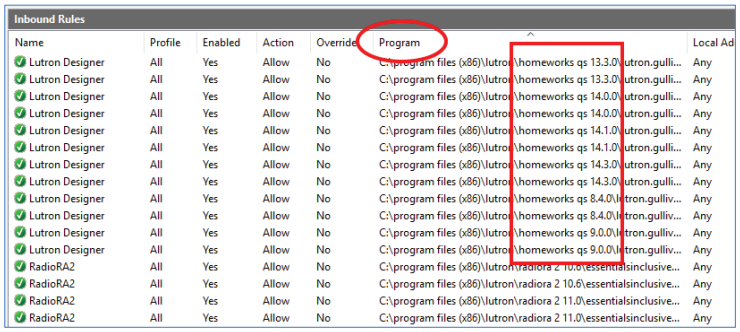
## 8.1 Firewalls and Security Programs *(continued)*

### 8.1.1 Check Inbound Firewall Rules *(continued)*

From here more details are given as to the status of each firewall as well as options to manage the firewalls. In the left pane, click **Inbound Rules**.



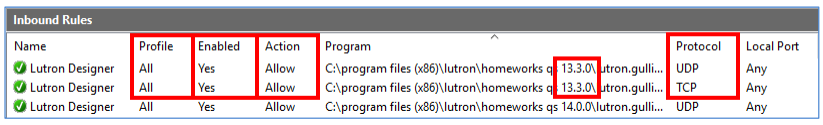

All the inbound firewall rules are listed here. RadioRA 2 software rules are listed with the name “RadioRA2”, and all HomeWorks QS software rules are listed with the name “Lutron Designer”. For the version of software that is having trouble communicating, go to the RadioRA2/Lutron Designer rows and find and expand the column named Program to reveal the version number of software to which the rules correspond.




Check the following for the rules with the troublesome version of software:

- There should be two rules per version of software (they may not be listed next to each other)
- One rule should have the protocol set as UDP
- The other rule should have the protocol set as TCP
- The rules are enabled
- The actions are set to Allow
- The profile is set to All

If the rules are completely missing, proceed to Section 5.1.2. If changes to the rules are needed, close the Lutron software and refer to the steps below.

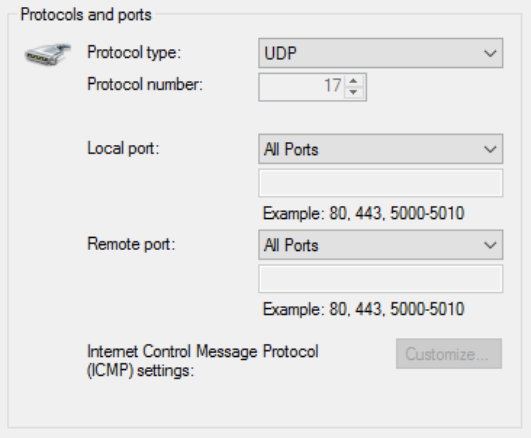



If the rule is not enabled, right-click the rule and click **Enable Rule**. If any of the other items differ, then right-click the problem rule and select Properties. The option to change a rule to TCP vs UDP is in the Protocols and Ports tab.

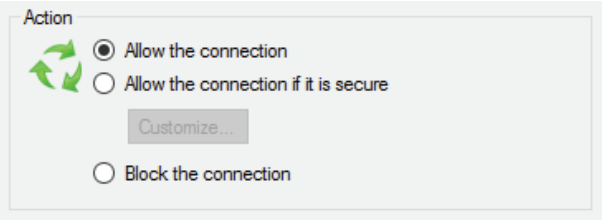
# 8.0 Best Practices *(continued)*

## 8.1 Firewalls and Security Programs *(continued)*

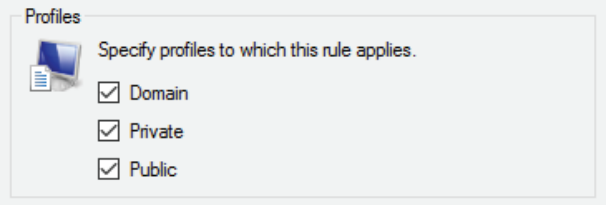
### 8.1.1 Check Inbound Firewall Rules *(continued)*




The option to Allow the rule is in the **General** tab.




The option to set the profile is under the **Advanced** tab. To get "All" the profiles (Domain, Private, and Public) must be selected (checked).




After saving the changes to the firewall, restart the Lutron software.

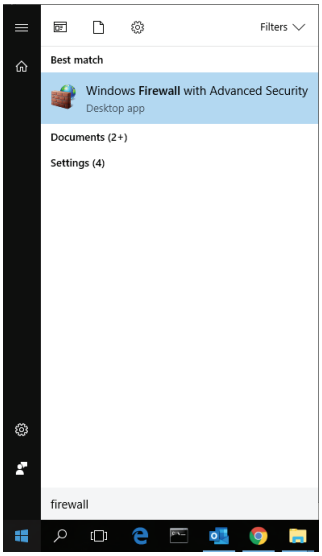
# 8.0 Best Practices *(continued)*

## 8.1 Firewalls and Security Programs *(continued)*

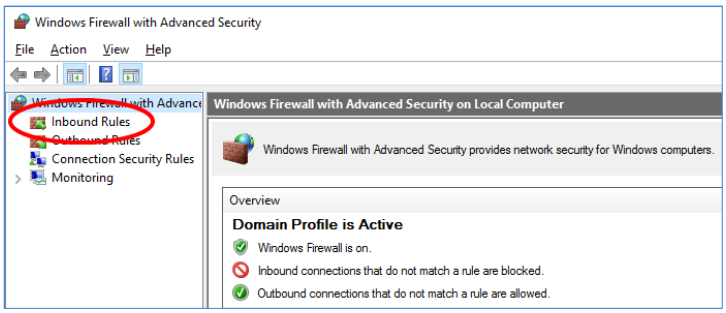
### 8.1.2 Allow Lutron Programs through the Firewall

Firewall rules for Lutron software are created during the installation process of the software. In cases where the firewall dialog is closed, the rule may be missing from the Windows Firewall inbound rules list. This section covers checking the firewall to make sure the rules are present, and if they are missing, how to add rules to the firewall.

From the Start menu, search for firewall and click **Windows Firewall with Advanced Security**.




In the pane on the left, click **Inbound Rules.**



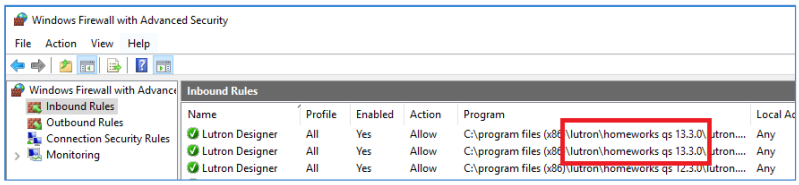

All the inbound firewall rules are listed here. RadioRA 2 software rules are listed with the name “RadioRA2”, and all HomeWorks QS software rules are listed with the name “Lutron Designer”. For the version of software that is having trouble communicating, go to the RadioRA2/Lutron Designer rows and find and expand the column named Program to reveal the version number of software to which the rules correspond.

# 8.0 Best Practices *(continued)*

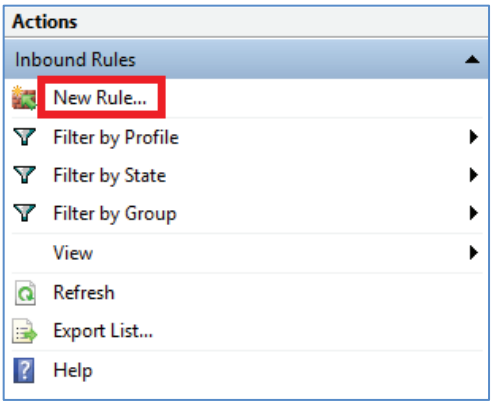
## 8.1 Firewalls and Security Programs *(continued)*

### 8.1.2 Allow Lutron Programs through the Firewall *(continued)*

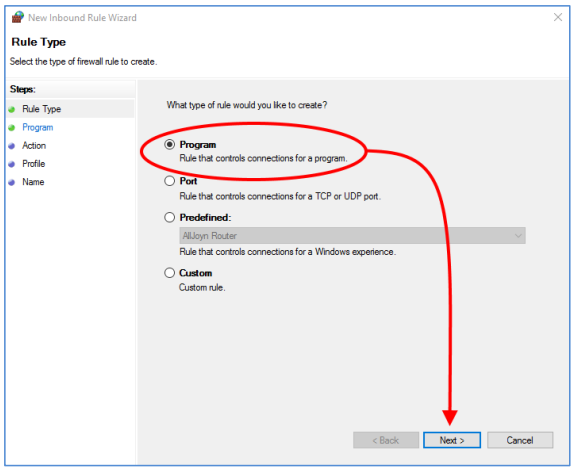
In the **Program** column, check to make sure the version of software you are having issue with appears in the list two times. The two firewall rules may not be in order.




In the event that the firewall rules are missing, click **New Rule…** in the Actions pane on the right side of the window.




Ensure Program is selected and click **Next >**.



# 8.0 Best Practices *(continued)*

## 8.1 Firewalls and Security Programs *(continued)*

### 8.1.2 Allow Lutron Programs through the Firewall *(continued)*

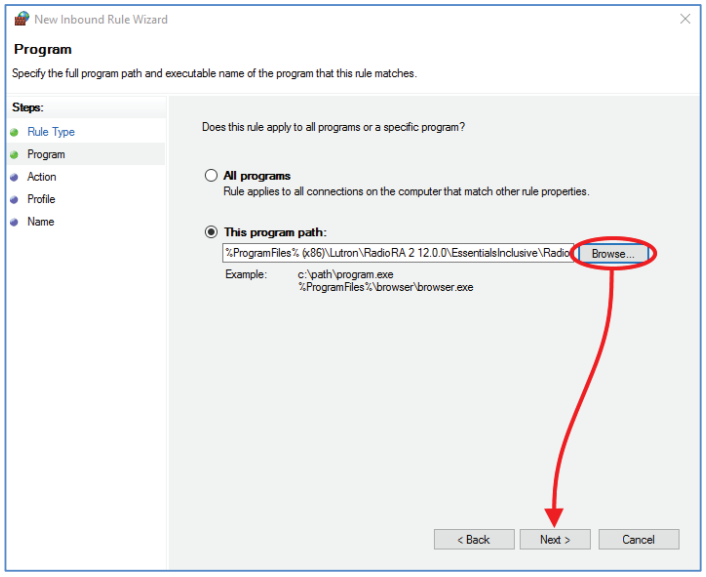
Click **Browse…** and navigate to "C:\Program Files (x86)\Lutron" and select the software you want to create a rule for, and then click **Next >**.

For HomeWorks QS:

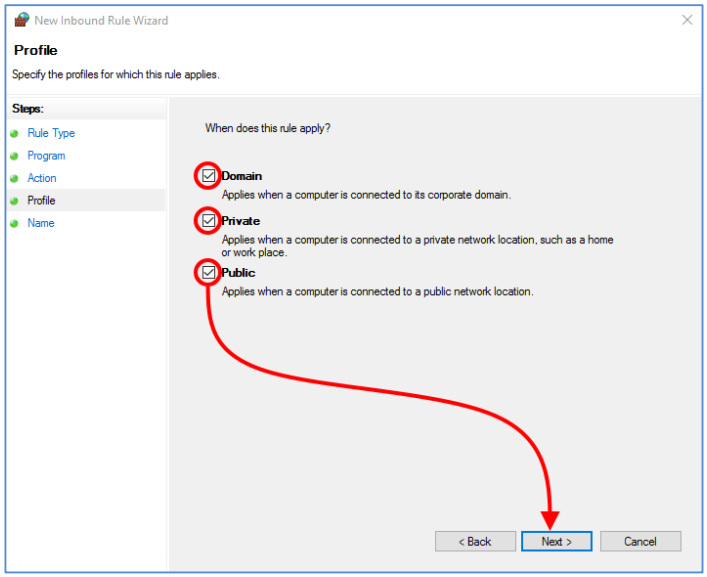
"C:\Program Files (x86)\Lutron\HomeWorks QS <version number>\Lutron.Gulliver.QuantumResi.exe"

For RadioRA 2:

"C:\Program Files (x86)\Lutron\RadioRA 2 <version number>\EssentialsInclusive\RadioRA2.exe"




Ensure Allow the connection is selected, and click **Next >**. Ensure Domain, Private, and Public are all selected. Click **Next >**.




For ease of finding this rule in the future, enter a name for the rule which matches the naming convention we use for other HomeWorks QS and RadioRA 2 rules. Then click **Finish**.

- "Lutron Designer" when naming a HomeWorks QS rule
- "RadioRA2" when naming a RadioRA 2 rule

# 8.0 Best Practices *(continued)*

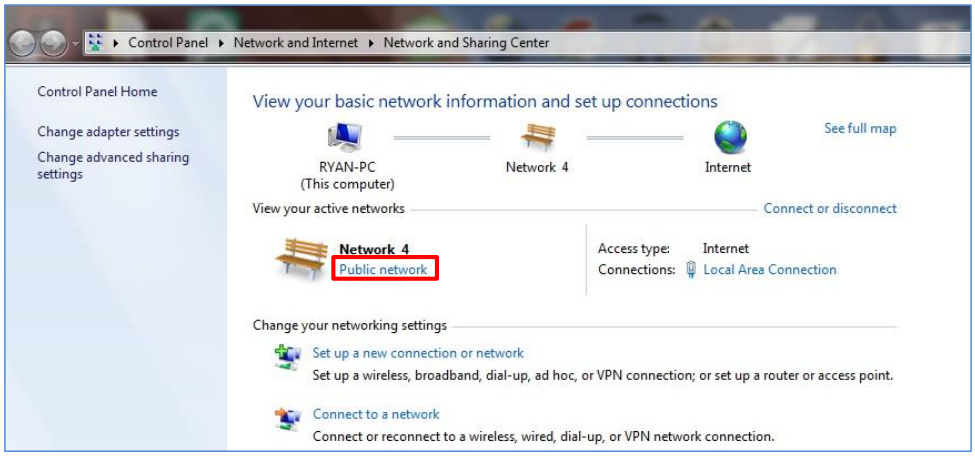
## 8.1 Firewalls and Security Programs *(continued)*

### 8.1.3 Using a Work or Home Network Connection to the System

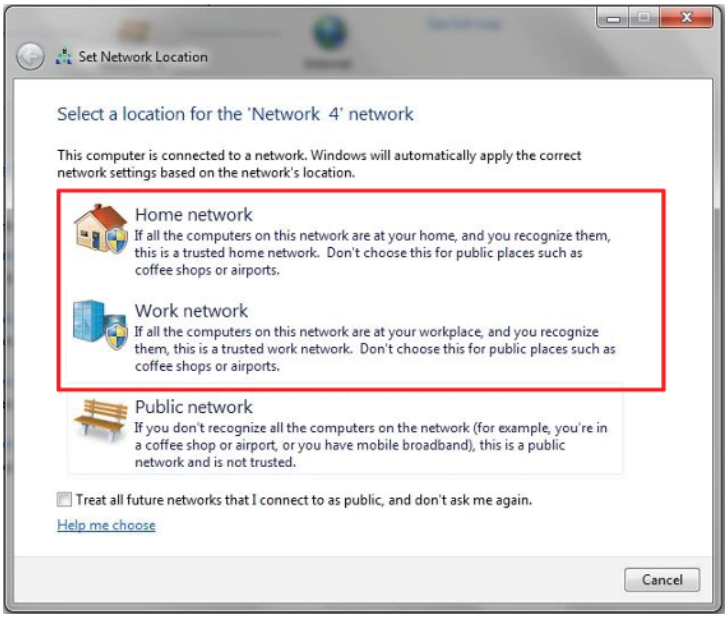
One potential source of firewall issues may result from the default configuration of the type of network that the Windows machine is connected to. Windows machines can be inadvertently set to identify every network as Public, by default. Public networks will typically have the greatest threat for issues such as viruses and demand the greatest level of security protection. As a result, the firewall will be in a state where it is most active and may cause interruptions when connecting to Lutron processors, typically during the first connection to the processors.

The network type can be changed to Work or Home to avoid issues. This can be done by first going to the Network and Sharing Center in the Control Panel.

Underneath the network name, click on the link that says **Public network**.




In the network type window that opens, select either Work or Home for the network type.

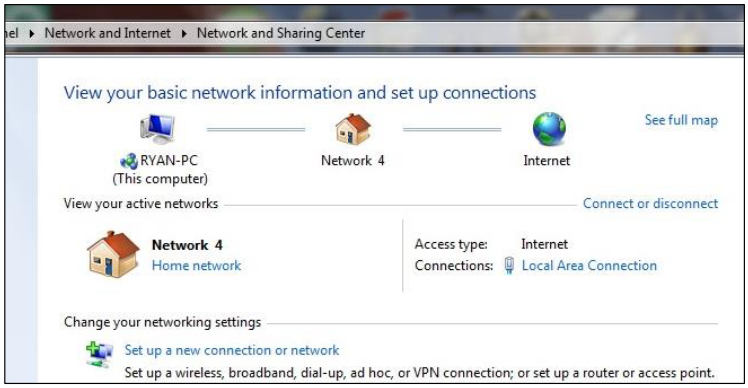


# 8.0 Best Practices *(continued)*

## 8.1 Firewalls and Security Programs *(continued)*

### 8.1.3 Using a Work or Home Network Connection to the System *(continued)*

Verify that the type of network has changed and proceed with attempting to connect to the Lutron system again. Changing to Home or Work will enable more through the firewall as the network will be more trusted than Public.



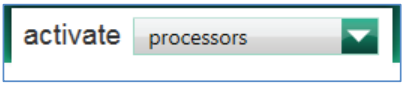

Note that some PCs may not allow changing this setting if managed by a corporate domain. Contact your corporate IT administrator for assistance.

### 8.1.4 Force TCP Software-to-Processor Communication

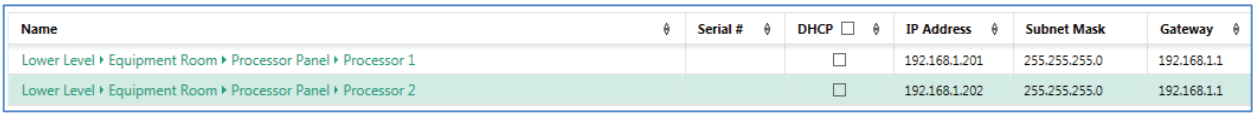
Firewalls can sometimes block the broadcast and multicast communication between the programming software and the processor(s). The HomeWorks QS and RadioRA 2 programming software allows the programmer to force the software to utilize TCP communication instead of multicast which can also help get around firewall blockage. Note that there may be issues switching over to the TCP communication mode if the processors have not already been activated via multicast. Please also note that this will only change the communication method for software-to-processor communication. Communication between processors will remain multicast.

#### 8.1.4.1 Changing to TCP Communication in HomeWorks QS

In order to force the HomeWorks QS software to use TCP communication, first go to the activate tab and select the option for **processors**.

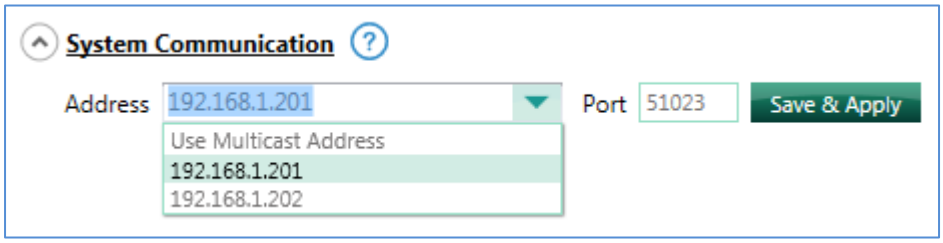



Proceed to activate the processors to the database. Be sure to uncheck the option for DHCP and set static IP addresses.



| Name | Serial # | DHCP ☐ | IP Address | Subnet Mask | Gateway |
|---|---|---|---|---|---|
| Lower Level ▸ Equipment Room ▸ Processor Panel ▸ Processor 1 | | ☐ | 192.168.1.201 | 255.255.255.0 | 192.168.1.1 |
| Lower Level ▸ Equipment Room ▸ Processor Panel ▸ Processor 2 | | ☐ | 192.168.1.202 | 255.255.255.0 | 192.168.1.1 |

Below the table listing the system processors and network setting information are three drop down menus. Expand the one titled System Communication. Using the drop down menu change the selection from Use Multicast Address to one of the static IP addresses of one of the processors in the system. Click on **Save & Apply.**



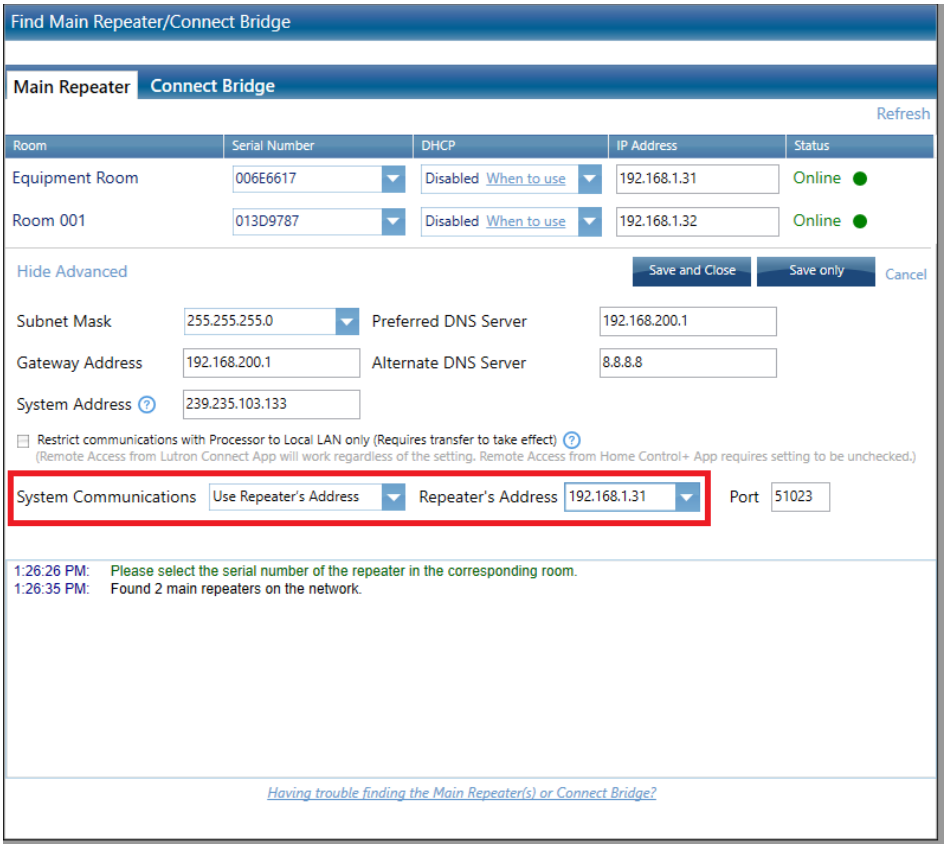
# 8.0 Best Practices *(continued)*

## 8.1 Firewalls and Security Programs *(continued)*

### 8.1.4 Force TCP Software-to-Processor Communication *(continued)*

#### 8.1.4.2 Changing to TCP Communication in RadioRA 2

In order to force the RA2 software to use TCP communication, first locate a Main Repeater in the room tree and press the Find Main Repeater button. Proceed to activate the Main Repeaters in the database. Be sure to disable the option for DHCP and set static IP addresses. Below the table listing the system Main Repeaters, expand the Show Advanced option. Next to System Communications, use the drop down menu and select Use Repeater's Address. This will set Main Repeater #1 to be the Main Repeater with which the software will communicate via TCP.



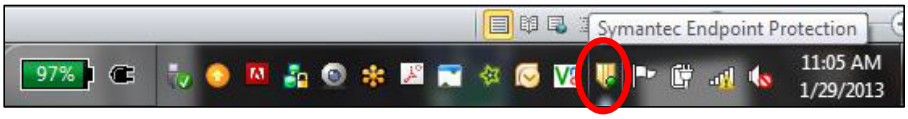
# 8.0 Best Practices *(continued)*

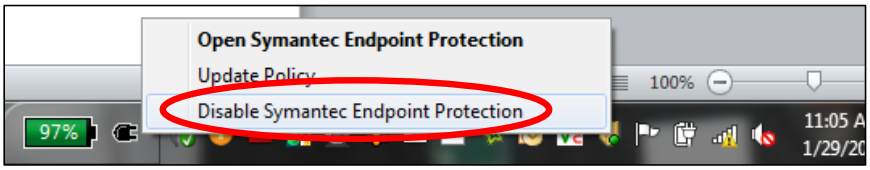
## 8.1 Firewalls and Security Programs *(continued)*

### 8.1.5 Disable Firewall Temporarily

If there is a special security program or firewall running on the PC, it may be necessary to disable those features while programming the Lutron system. Firewalls and security programs protect your PC from threats such as viruses. When a Lutron system tries to find the processor for the first time on a job, it utilizes a UDP (User Datagram Protocol) Broadcast to find all processors on the network. Since broadcast commands are not directed at specific devices (all devices on the network hear the command) security programs can often block this to prevent security breaches if unintended devices answer back, potentially gaining access to your PC through the host software program.

The below images reflect the disabling of one such security program from the system tray. This security program is called Symantec and by right clicking on the shield, a disable option appears.




In this case, the security program manages the Windows Firewall so disabling the security program subsequently disables the Windows Firewall. If there is no separate security program, or if the security program is not directly linked to the PC firewall, it may be necessary to disable the firewall or, at the very least, allow the Lutron programming software through the firewall.

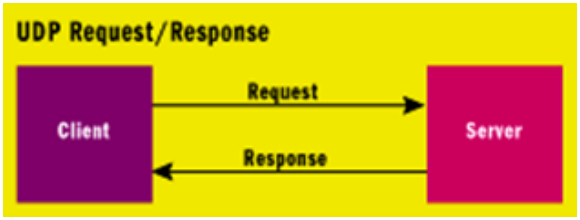
After the work to the Lutron system has been completed, re-enable your firewall and security programs to ensure that your PC is protected. Disabling the firewall and security programs should only be used as a quick and temporary solution. Long term, it would be wise to allow the Lutron software programs through the firewall so that you can be adequately protected from threats while maintaining the ability to establish communication with the system processors.

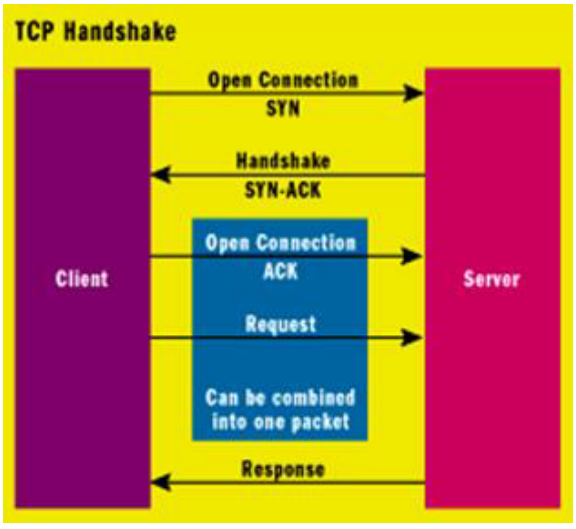
# 8.0 Best Practices *(continued)*

## 8.2 Using Wi-Fi with Lutron Programming Software

Utilization of Wi-Fi during certain processes of the Lutron system commissioning process allows for the convenience of not having to physically wire into the network while on the job site. While using Wi-Fi is convenient, it can also be problematic for a number of reasons such as inconsistent connectivity and also another layer of security built into the router which may not allow some packets of information to go from your laptop, through the network and to the processor.

Both the HomeWorks QS and RadioRA 2 programming software use User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) for communication over Ethernet to the HWQS Processor or RA2 Main Repeater. TCP is a reliable means of communication between network devices involving a number of handshake steps between the client and server. UDP is a method of communication that is targeting efficiency but thus has less handshaking to verify the successful receipt of data packets. The handshaking differences between UDP and TCP are shown below.




The HWQS Processor or RA2 Main Repeater firmware update process uses UDP Multicast to send the required information to all of the processors on the system simultaneously to reduce the time required to update the firmware. If the Wi-Fi connection is unstable it is possible for the communication to drop packets and, as a result of UDP not handshaking as often, these dropped packets may go unnoticed and lead to improper system performance.

# 8.0 Best Practices *(continued)*

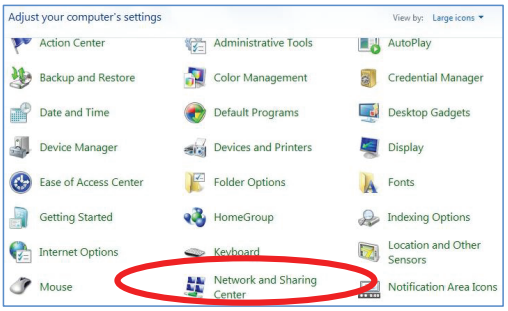
## 8.3 Running Windows OS on Mac

Lutron programming software is designed to run on Windows operating systems. In order to run the programming software on Mac hardware, Windows must be utilized either as a virtual machine (ex. Parallels or Fusion) or by booting the Mac up using only the Windows software (Bootcamp). Bootcamp setup is the same as setting up a Windows machine to connect to a Lutron processor. As a result of increased complexity, the following focuses on using virtual machine connections.

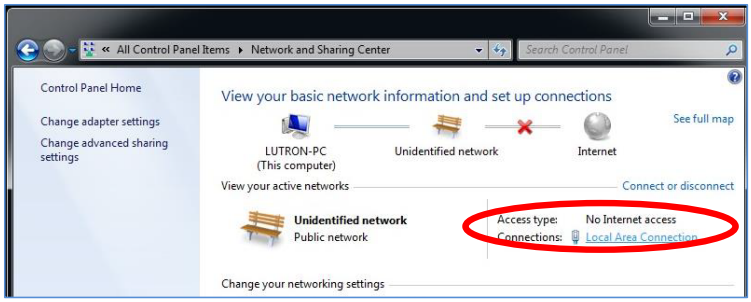
### 8.3.1 Parallels and VMware Fusion

Parallels and VMware Fusion software allow for simultaneous or parallel operation of two operating systems: Windows and Mac OS. From a networking standpoint, the two operating systems each appear as a device on the network when using a bridged connection. On one side you have the actual Mac hardware running the Mac OS. On the other, you have a virtual machine emulating the Windows OS. As a result of this setup, initial connection to the Lutron processor(s) requires a few settings to be implemented to ensure a successful connection. The example below is using a wired connection into the LAN.

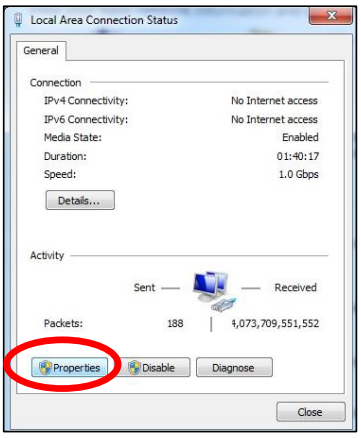
Proper setup can be accomplished in three simple steps. First, go to the Windows OS desktop and set a static IP address. To do this, first go to the Control Panel. Click on Network and Sharing Center. If you do not see this option, change the View By option to Large or Small Icons.




In the Network and Sharing Center window, click on **Local Area Connection** (or sometimes called Ethernet).




On the Local Area Connection Status window, select the option for **Properties**.

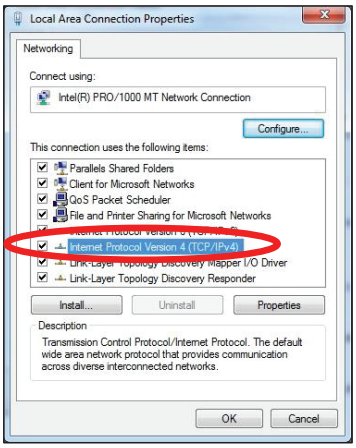


# 8.0 Best Practices *(continued)*

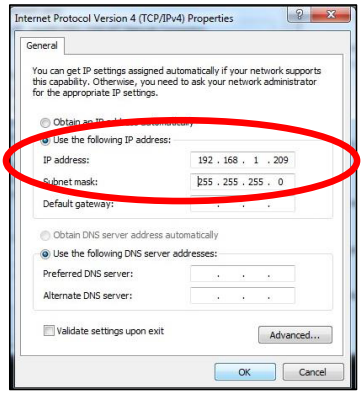
## 8.3 Running Windows OS on Mac *(continued)*

### 8.3.1 Parallels and VMware Fusion *(continued)*

Next, select **Internet Protocol Version 4** and click on **Properties**.




Set up the IP address and subnet mask as a static IP address. Make sure that this address is outside of the DHCP range of the DHCP server on the LAN router and does not conflict with any other address on the LAN.




Next, go to the Mac OS side and set a static IP address using the Settings menu. This IP address must be different than the address being used by the Windows OS. This is because there are two machines running on the network (despite the fact that it is the same Mac hardware). First, go to **System Preferences**.

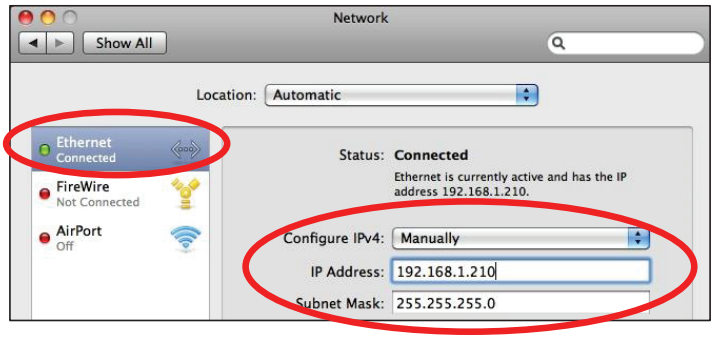

Select **Network** from the System Preferences window.

# 8.0 Best Practices *(continued)*

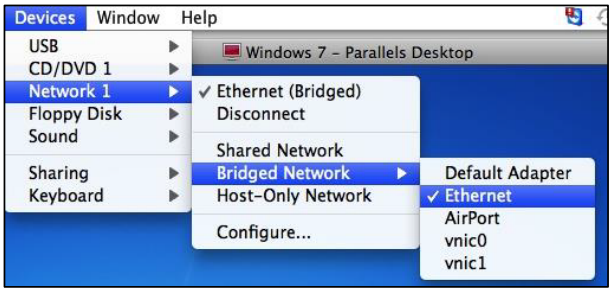
## 8.3 Running Windows OS on Mac *(continued)*

### 8.3.1 Parallels and VMware Fusion *(continued)*

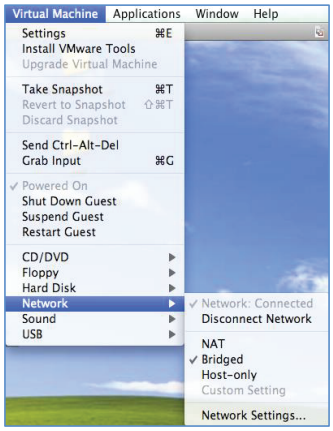
In the Network settings window, set the IP address for the Mac LAN adapter to a different address than all other network devices, including the Windows virtual machine, and click on **Apply** to save the settings.




The last step is the set the network type to Bridged. To do this in Parallels, go to the Windows Desktop view and go to the **Devices** menu in the upper left (you may need to bring your mouse pointer to the upper left corner for the menu bar to appear). In the **Devices** menu, select the **Network** sub menu, and then select **Bridged Network**. Select **Ethernet** as the bridged network option.




To do this in VMware Fusion, go to the Windows Desktop view and go to the Virtual Machine menu in the upper left (you may need to bring your mouse pointer to the upper left corner for the menu bar to appear). In the **Virtual Machine** menu, select the **Network** sub menu, and then select **Bridged**.

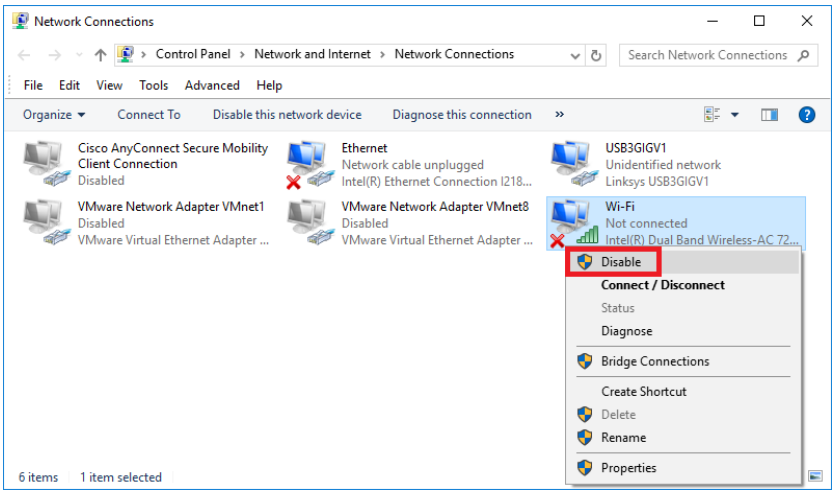



**Note:** If you are not using a wired Ethernet connection, your bridged network selection may not be called Ethernet. Examples would be a USB to Ethernet converter or using Wi-Fi (AirPort).

# 8.0 Best Practices *(continued)*

## 8.4 Multiple Network Adapters

It is recommended that you use a wired LAN connection. When using a wired LAN connection from your PC to the network and/or processor(s) it is good practice to disable the Wi-Fi Network Adapter on the PC. Having the wireless adapter enabled while using the local wired connection will often cause issues when trying to connect to the Lutron system. Completely disabling the adapter removes all possibilities for accidental wireless network connections.

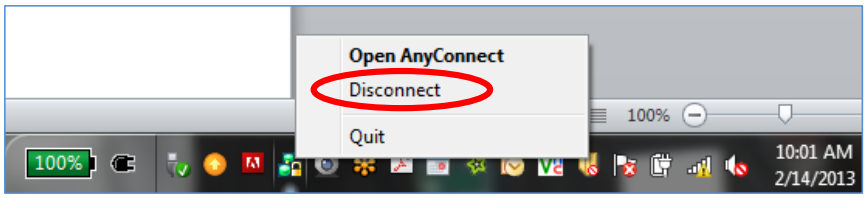



Once you have completed working with the Lutron system, and wish to restore Wi-Fi capabilities, remember to enable the Wi-Fi Network Adapter.

# 8.0 Best Practices *(continued)*

## 8.5 VPN Connections

An open VPN connection, used for the purposes of receiving emails, for example, may limit communications between the PC programming tool and the Lutron processor when connecting to the Lutron system over a local network. When trying to communicate with the Lutron system, it will be prudent to disconnect from this VPN connection. The image, below, shows the Disconnect option for the Cisco AnyConnect VPN connection.




Obviously, if you are using a VPN connection to connect to a client's house using the wide area network (WAN) to access the house for programming purposes, this would not apply. Disconnecting from the VPN only applies when you are using a local network connection to the Lutron system.

Note that not all VPNs support transmitting multicast data through them which is used extensively in Lutron software. Check with the VPN vendor to find out whether their VPN supports transmitting multicast traffic across their connection. As a general rule, everything in the software uses multicast communication when interacting with systems. Examples of multicast usage includes, but is not limited to processor discovery, processor upgrades, device activation, system transfer, system diagnostics mode, setting shade limits, and the Terminal window. The System Address is the multicast address used for most multicast communication to the system, besides processor discovery which is hard-coded to 224.0.37.42.

If your VPN does not support multicast traffic, then there are a couple possible options for remote software access to the system which includes:

- Force the communication method to TCP.
  - Refer to section 5.1.4 in this guide for changing to TCP communication for steps on how to set this up.
  - Enables you to discover processors and transfer to the system remotely
- VPN into a PC that is on the Lutron system's network and use the Lutron software from that PC.
  - This will bypass any multicast blockage caused by the VPN.

For more information on setting up a VPN to remotely access Lutron systems, refer to Application Note #231 (P/N 048231) at www.lutron.com

# 8.0 Best Practices *(continued)*

## 8.6 Internet Group Management Protocol (IGMP)

Internet Group Management Protocol (IGMP) is an IP networking protocol used to establish multicast groups. There are three versions of IGMP: v1, v2, and v3. The HomeWorks QS Processor and RadioRA 2 Main Repeater support all three versions.

In a network, multicast communication is used to allow a small group of clients to communicate with each other. With multicast communication, a single message can be sent out to all members of a group at once, as opposed to unicast communication which would require the message to be sent once for each member. For example, an online movie-on-demand service would use unicast communication. It sends the movie out to each viewer individually (each viewer requests the movie at different times). An online video conference can use multicast communication. A single presenter sends out one video to all the viewers at once (with all viewers watching at the same time).

An example of multicast in a Lutron system is an operating system (OS) firmware update for a new revision of the system programming software. Regardless of the number of RA2 Main Repeaters or HWQS Processors, the firmware update is performed to all processors simultaneously using multicast. This allows for a more efficient firmware upgrade when compared to legacy systems.

### 8.6.1 How do switches route multicast traffic?

While IGMP is used to define network groups, the network switches often have no knowledge of the location of group members. If the switches do not know what physical ports group members are on, then there is only one way to guarantee that all group members get the message: broadcast the message to all physical ports. This method works because clients in the group will hear the message and clients not in the group will process it and then drop it.

The issue with converting multicast traffic to broadcast traffic is the huge overhead on every device which has to process and drop messages they were never supposed to receive. This will cause unnecessary network traffic and, if there are other issues in the network, this broadcasted multicast traffic will compound those issues. Depending on the nature of other network issue, broadcasting multicast traffic may cause an intermittent loop where traffic is repeated unnecessarily. IGMP Snooping allows network switches to handle multicast network traffic correctly.

### 8.6.2 What is IGMP Snooping?

IGMP Snooping is a setting on many managed and “smart” network switches. It is used to discover which physical ports group members reside on. Once the network switch knows the location of group members, it will only route multicast traffic to those locations. Devices that are not in the group will never see any of the group messages, significantly decreasing network traffic. This is a great method to limit total traffic seen by clients without having to set up VLANs. The appendices, in sections 7.0 and 8.0, portray Lutron processors on networks with Snooping disabled and enabled.

### 8.6.3 IGMP Snooping and Lutron Residential Systems

The HomeWorks QS and RadioRA 2 systems relies heavily on multicast traffic to cut back on total network traffic and provide timely system response. This is most effective when network switches can properly direct multicast traffic and not broadcast it. If, for instance, a two processor HomeWorks QS system is connected to a switch with IGMP Snooping enabled, no multicast traffic generated by the HomeWorks QS Processors will ever enter the rest of the network. By the same token the HomeWorks QS system will not receive multicast traffic from other devices on the network (multi room audio systems, video conferencing software, etc.).

Regardless of where multicast traffic comes it should not be treated the same as broadcast traffic if at all possible. Treating multicast traffic properly limits exposure to network issues (including but not limited to network loops).

Limiting these network issues is done by enabling IGMP Snooping on the network switch. Having IGMP Snooping enabled will ensure that the network operates efficiently and that all devices on the network can handle the traffic directed at them.

IGMP Snooping may require an IGMP Querier to be on the network. An IGMP Querier helps keep multicast membership reports up-to-date and helps prevent the membership reports from becoming stale. If multicast traffic seems to work for a short time, then fail, it might be because there is no IGMP Querier on the network.

What is required depends on the networking equipment being used on site and what settings they have available on them. As a last resort, if there are issues getting multicast to properly route on the network, disabling IGMP Snooping on all switches/routers will cause the network equipment to treat the multicast traffic as broadcast traffic if you need to get the system working.

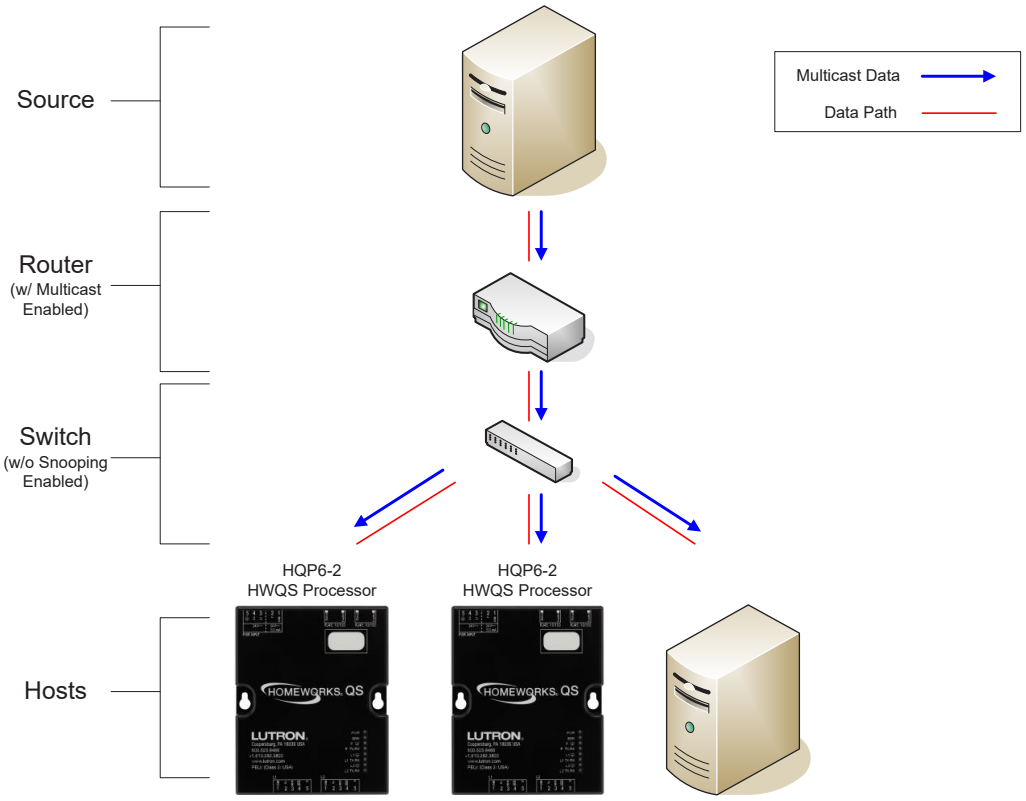
# 8.0 Best Practices *(continued)*

## 8.6 Internet Group Management Protocol (IGMP) *(continued)*

### 8.6.4 Connect Bridge and Lutron Residential Systems

The Lutron Connect Bridge creates a link between a RadioRA 2 or HomeWorks QS system and the Lutron cloud, enabling local and remote access to your system via the Lutron Connect mobile app. Making a local connection to the Bridge involves using mDNS to discover the Bridge on the local network. If the Bridge is not discovered, then the phone will reach out to Lutron servers which maintains communication with the Connect Bridge (provided an Internet connection is preset at the Bridge). The Bridge starts the initial communication to Lutron servers, the servers will never initiate first contact to the Bridge. In addition to using mDNS, the Connect Bridge utilizes other multicast traffic to keep track of the Lutron processors on the network. For control of the Lutron system, the Connect Bridge establishes a Telnet connection to the master processor in the system.

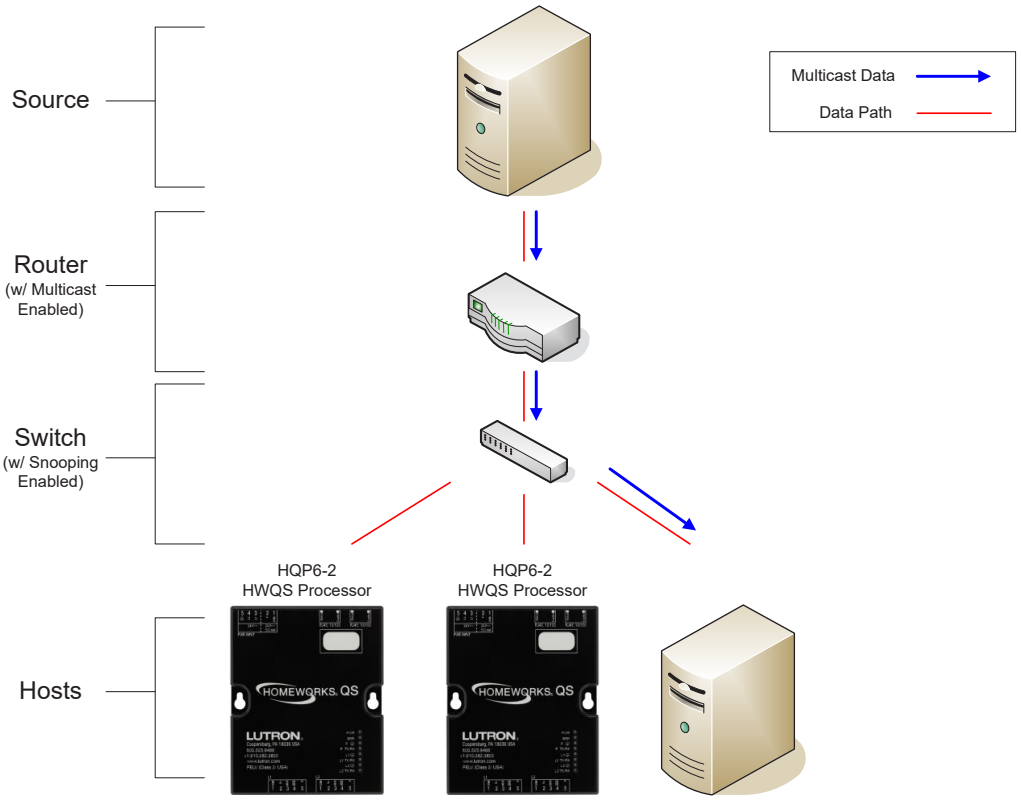
### 8.6.5 Appendix – HWQS System on Network with Snooping Disabled



# 8.0 Best Practices *(continued)*

## 8.6 Internet Group Management Protocol (IGMP) *(continued)*

### 8.6.6 Appendix – HWQS System on Network with Snooping Enabled



# 8.0 Best Practices *(continued)*

## 8.7 Setting Static IP Addresses

### 8.7.1 General Static IP Best Practices

Setting static IP addresses on Lutron processors is typically preferred. Configuring a static IP address is ideal for integration with third-party systems that communicate with Lutron systems over IP. The idea is very similar to that of the Postal Service delivering a letter to a specific house in a suburban town. In that town it is a guarantee that each house has a unique address. It is also a guarantee that the addresses on the homes within that neighborhood are fixed or static, making it easy for the Postal service worker to deliver the message. If the address of the home randomly changed after an electrical brown out, the Postal Service would be confused and would likely deliver the message to the incorrect house. The latter scenario is similar to network devices configured as DHCP, where the network device requests and address from the DHCP server of the router and is automatically assigned an address which can alter over time.

Setting up static IP addresses is simple to do but there are best practices to follow anytime that this occurs.

1. All addresses must be unique so be sure to map out all addresses on the network and ensure that there is no overlap
2. Set the static addresses outside of the DHCP range of the router on the local area network
   a. Removes the potential for overlap as devices like mobile phones or tablets come and go from the network
   b. Connect to the router and log onto the router (default username and password are usually simple and something like admin/admin or admin/password; typically a label is on the router indicating what the default log in is)

### 8.7.2 DHCP Reservation vs. Setting Static IP in the Programming Software

There are two different ways to set a static IP address on a Main Repeater or HomeWorks QS Processor: DHCP reservation or using the Lutron programming software.

A DHCP reservation is a way of using the router to automatically assign the same IP address to a network device, every time the device requests an address from the DHCP server. This type of address is configured in the router, using the DHCP reservation table.

There are pros and cons to doing each. The below table illustrates this.

| | Pros | Cons |
|---|---|---|
| **Programming Software** | – Easy to do, using the same screen used to discover and activate the Lutron processor | – Cannot easily change the address without having the programming software or sending a command via telnet |
| **DHCP Reservation** | – Easy for network management since Lutron processors will be handled the same way as all other network devices | – Router could get replaced with little warning and all addressing lost<br>– Requires additional coordination with the party responsible for the networking equipment on the site |

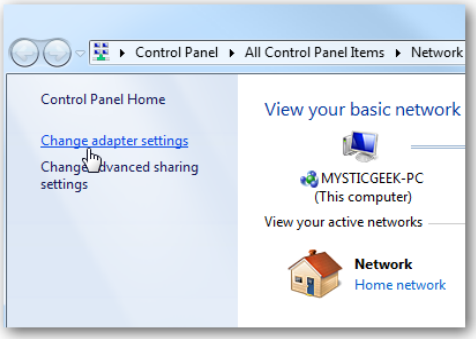
# 8.0 Best Practices *(continued)*

## 8.7 Setting Static IP Addresses *(continued)*

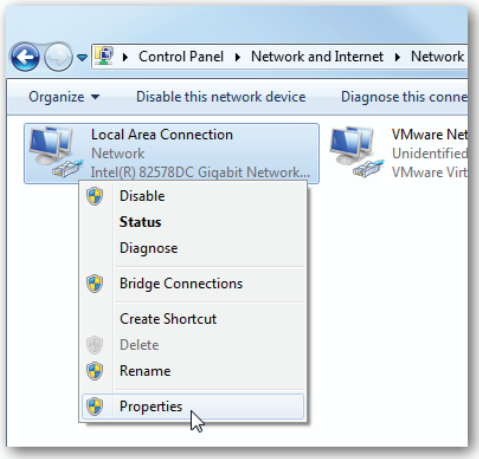
### 8.7.3 Setting a Static IP Address in Windows

Setting a static IP address on Windows is done using the Network and Sharing Center which is a subset of the Control Panel. While the process to get to the Network and Sharing Center varies slightly between Windows 7, 8, and 10 the program itself looks similar. It is recommended to use the search function in Windows to find the Network and Sharing Center.

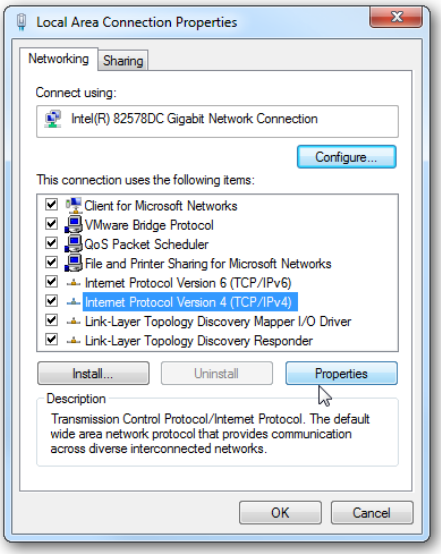
From the Network and Sharing Center, click on **Change adapter settings**.




Right-click on the network adapter being used (Wi-Fi or Local Area Connection) and select **Properties**.




Highlight Internet Protocol Version 4 (TCP/IPv4) then click the **Properties** button.

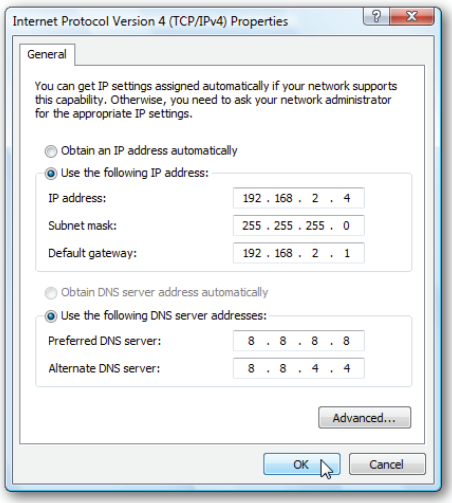


# 8.0 Best Practices *(continued)*

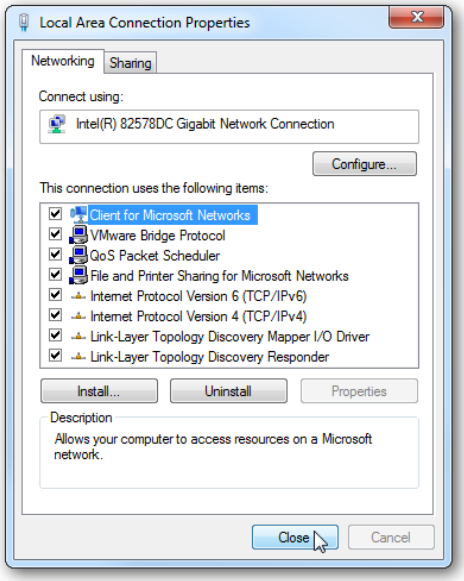
## 8.7 Setting Static IP Addresses *(continued)*

### 8.7.3 Setting a Static IP Address in Windows *(continued)*

Now change the IP, Subnet Mask and Default Gateway addresses by selecting the option to Use the following IP address. Click **OK** to finish.




**Close** out of the Network Connection Properties screen before the changes go into effect.



# 9.0 Troubleshooting

## 9.1 RadioRA 2 Find Main Repeater/Connect Bridge Error Codes

The below table displays all possible error codes that can be encountered when attempting to Find Main Repeaters and the Connect Bridge on a network along with potential remedies/solutions.

| Error Message | Potential Remedy |
|---|---|
| No Main Repeaters were found on the network. Please check if the Main Repeater is properly connected to the network and click Refresh. | 1. Check that the Repeater(s) are powered and connected to the router.<br>2. Allow exception for the software through the firewall or turn off firewall. See Section 5.1.2/5.1.5.<br>3. Turn off any active VPN connections. See Section 5.5.<br>4. If using a wired LAN connection, disconnect from any Wi-Fi networks. Vice versa for when using Wi-Fi. See Section 5.4.<br>5. For Macs running Parallels or VM, ensure that you are using a Bridged network connection. See Section 5.3.1. |
| Only one Main Repeater was found on the network. Please check to ensure that both Main Repeaters are properly connected to the network and then click "Refresh." | 1. Check that the Repeater(s) are powered and connected to the router.<br>2. Allow exception for the software through the firewall or turn off firewall. See Section 5.1.2/5.1.5.<br>3. Power cycle the Main Repeater that is not being found.<br>4. Try to direct connect to the Main Repeater which is not being found.<br>5. If you have a different router, try to discover both Main Repeaters using the different router. |
| No Connect Bridge was found on the network. Please check if the Connect Bridge is properly connected to the network and click Refresh. | 1. Check that the Connect Bridge is powered and connected to the same local area network as the Main Repeater(s).<br>2. Ensure that the button was pressed on the Connect Bridge in order to enable Discovery Mode.<br>3. Power cycle the Connect Bridge and try the activation process again.<br>4. Factory default the Connect Bridge and try again. |
| No Connect Bridge was found on the network. Please check if the Connect Bridge is properly connected to the network. | 1. Check that the Connect Bridge is powered and connected to the same local area network as the Main Repeater(s).<br>2. Ensure that the button was pressed on the Connect Bridge in order to enable Discovery Mode.<br>3. Power cycle the Connect Bridge and try the activation process again.<br>4. Factory default the Connect Bridge and try again. |
| Safe Mode Detected. | Follow on-screen steps for resolution. |
| The Main Repeater was found on multiple PC network connections (wired or Wi-Fi). Please disconnect the extra connections and refresh to try again. | The PC has multiple network connections to the same LAN.<br>1. Disable all but one and then re-start software. See Section 5.4.<br>2. Best practice - use a wired connection, when possible. |
| PC and Main Repeater cannot communicate using the IP address: xxx.xxx.xxx.xxx. Please pick an IP address in the range between: 'yyy.yyy.yyy.yyy to zzz.zzz.zzz.zzz'. | Main Repeater and PC have IP addresses on different subnets.<br>1. Ensure that both devices are on the same subnet by changing the IP addresses to the correct scheme. |
| Communication to the repeater has failed. Please check if all devices are connected and click Refresh. | 1. Check that the Repeater(s) are powered and connected to the router<br>2. Allow exception for the software through the firewall or turn off firewall. See Section 5.1.2/5.1.5.<br>3. Turn off any active VPN connections. See Section 5.5.<br>4. If using a wired LAN connection, disconnect from any Wi-Fi networks. Vice versa for when using Wi-Fi. See Section 5.4.<br>5. For Macs running Parallels or VM, ensure that you are using a Bridged network connection. See Section 5.3.1. |

## 9.0 Troubleshooting *(continued)*

### 9.1 RadioRA 2 Find Main Repeater/Connect Bridge Error Codes *(continued)*

| Error Message | Potential Remedy |
|---|---|
| Activation Request Timed out for Connect Bridge. | 1. Check that the Connect Bridge is powered and connected to the same local area network as the Main Repeater(s).<br>2. Ensure that the button was pressed on the Connect Bridge in order to enable Discovery Mode.<br>3. Power cycle the Connect Bridge and try the activation process again.<br>4. Factory default the Connect Bridge and try again. |
| An error has occurred. Please try again. | 1. Re-start the RadioRA 2 programming software.<br>2. Check that the Repeater(s) are powered and connected to the router; power cycle Main Repeater.<br>3. Allow exception for the software through the firewall or turn off firewall. See Section 5.1.2/5.1.5.<br>4. If using a wired LAN connection, disconnect from any Wi-Fi networks. Vice versa for when using Wi-Fi. See Section 5.4. |
| Communication to the repeater with serial number yyyyyyyy failed. Please check if the Main Repeater is properly connected to the network and click "Refresh." | All devices on a LAN must have a unique IP address.<br>1. Ensure that each Main Repeater's IP address is unique from all other network devices.<br>2. Set the IP addresses outside of the DHCP range of the router. |
| The same serial number is selected for multiple repeaters. Please select a unique serial number for each repeater. | Two Main Repeater system where, in the Find Main Repeater window, a serial number that is already in use is being assigned to the second Main Repeater.<br>1. Choose the second, correct, serial number for the Main Repeater. |
| Cannot assign the same IP address to multiple Main Repeaters. Please make sure each Main Repeater has a unique IP address and try again. | All devices on a LAN must have a unique IP address.<br>1. Ensure that each Main Repeater's IP address is unique from all other network devices.<br>2. Set the IP addresses outside of the DHCP range of the router. |
| Cannot use IP address xxx.xxx.xxx.xxx for the repeater with serial number yyyyyyyy. The IP address is already being used by another device on the network. Please select another IP address for this repeater. | All devices on a LAN must have a unique IP address.<br>1. Ensure that each Main Repeater's IP address is unique from all other network devices.<br>2. Set the IP addresses outside of the DHCP range of the router. |
| Communication to the Connect Bridge with serial number yyyyyyyy failed. Please check if the Connect Bridge is properly connected to the network and click "Refresh." | 1. Check that the Connect Bridge is powered and connected to the same local area network as the Main Repeater(s).<br>2. Ensure that the button was pressed on the Connect Bridge in order to enable Discovery Mode.<br>3. Power cycle the Connect Bridge and try the activation process again.<br>4. Factory default the Connect Bridge and try again. |
| Communication to the bridge has failed. Please check if all devices are connected and click Refresh. | 1. Check that the Connect Bridge is powered and connected to the same local area network as the Main Repeater(s).<br>2. Ensure that the button was pressed on the Connect Bridge in order to enable Discovery Mode.<br>3. Power cycle the Connect Bridge and try the activation process again.<br>4. Factory default the Connect Bridge and try again. |

## 9.0 Troubleshooting *(continued)*

### 9.1 RadioRA 2 Find Main Repeater/Connect Bridge Error Codes *(continued)*

| Error Message | Potential Remedy |
|---|---|
| Cannot use IP address xxx.xxx.xxx.xxx for the Connect Bridge with serial number yyyyyyyy. The IP address is already being used by another device on the network. Please select another IP address for this Connect Bridge. | All devices on a LAN must have a unique IP address.<br>1. Ensure that each Main Repeater's IP address is unique from all other network devices.<br>2. Set the IP addresses outside of the DHCP range of the router. |
| The Main Repeater did not get an IP address from a DHCP server on the network. Please connect a router (or other DHCP server) to the network or set 'DHCP' to 'Disabled'. | 1. Connect the Main Repeater(s) to a router to allow for an address to be assigned from the DHCP server.<br>2. Set the Main Repeater to DHCP Disabled and provide a static IP address. |
| Communication to the Main Repeater failed. Please review network settings and check if all devices are connected correctly. | 1. Check that the Repeater(s) are powered and connected to the router.<br>2. Allow exception for the software through the firewall or turn off firewall. See Section 5.1.2/5.1.5.<br>3. Turn off any active VPN connections. See Section 5.5.<br>4. If using a wired LAN connection, disconnect from any Wi-Fi networks. Vice versa for when using Wi-Fi. See Section 5.4.<br>5. For Macs running Parallels or VM, ensure that you are using a Bridged network connection. See Section 5.3.1. |
| The connection to the repeater was changed after opening RadioRA 2. Please restart RadioRA 2, and try again. | Network adapter change after opening the programming software.<br>1. Restart the RadioRA 2 programming software. |
| IP multicast failed for repeater with serial number xxx.xxx.xxx.xxx. Please check the network connections to this repeater and firewall settings and try again. | 1. Allow exception for the software through the firewall or turn off firewall. See Section 5.1.2/5.1.5.<br>2. Best practice - restart the RadioRA 2 software after making changes. |
| Main Repeaters are on different network. All the Main Repeaters should be on the same network. | Multiple Main Repeaters on a system but the current IP addresses of each are on different subnets.<br>1. Make sure that the two Main Repeaters are connected to the same local area network.<br>2. Ensure that the IP addresses of each Main Repeater follow the numbering of the local area network. |
| Could not establish connection to processor with IP Address: xxx.xxx.xxx.xxx. | 1. Check that the Repeater(s) are powered and connected to the router.<br>2. Allow exception for the software through the firewall or turn off firewall. See Section 5.1.2/5.1.5.<br>3. Turn off any active VPN connections. See Section 5.5.<br>4. If using a wired LAN connection, disconnect from any Wi-Fi networks. Vice versa for when using Wi-Fi. See Section 5.4.<br>5. For Macs running Parallels or VM, ensure that you are using a Bridged network connection. See Section 5.3.1. |

# 9.0 Troubleshooting *(continued)*

## 9.2 HomeWorks QS Activate Processors/Connect Bridge Error Codes

The below table displays all possible error codes that can be encountered when attempting to activate processors and the Connect Bridge on a network along with potential remedies/solutions.

| Error Message | Remedy |
|---|---|
| The current subsystem does not contain any activated processors to allow for a transfer. | 1. Verify that processors have been added to the database in Design > equipment.<br>2. Verify that the processors are activated using activate > processors and Connect Bridge. |
| Communication to one or more processors failed. | 1. Check that the Processor(s) are powered and connected to the network.<br>2. Allow exception for the software through the firewall or turn off firewall. See Section 5.1.2/5.1.5.<br>3. Turn off any active VPN connections. See Section 5.5.<br>4. If using a wired LAN connection, disconnect from any Wi-Fi networks. Vice versa for when using Wi-Fi. See Section 5.4.<br>5. For Macs running Parallels or VM, ensure that you are using a Bridged network connection. See Section 5.3.1.<br>6. Re-try activate > processors. |
| Processor upgrade cannot be continued, because no processor is available. | 1. Check that the processor(s) are powered and connected to the network.<br>2. Allow exception for the software through the firewall or turn off firewall. See Section 5.1.2/5.1.5.<br>3. Turn off any active VPN connections. See Section 5.5.<br>4. If using a wired LAN connection, disconnect from any Wi-Fi networks. Vice versa for when using Wi-Fi. See Section 5.4.<br>5. For Macs running Parallels or VM, ensure that you are using a Bridged network connection. See Section 5.3.1.<br>6. Re-try activate > processors. |
| Communications to one or more processors failed.<br>Would you like to continue the OS upgrade?<br>This may cause the system to behave in an unexpected manner. | 1. Check that the processor(s) are powered and connected to the network.<br>2. Allow exception for the software through the firewall or turn off firewall. See Section 5.1.2/5.1.5.<br>3. Turn off any active VPN connections. See Section 5.5.<br>4. If using a wired LAN connection, disconnect from any Wi-Fi networks. Vice versa for when using Wi-Fi. See Section 5.4.<br>5. For Macs running Parallels or VM, ensure that you are using a Bridged network connection. See Section 5.3.1.<br>6. Re-try activate > processors. |
| Transfer cannot complete because there are no components to transfer. | Nothing is activated to the system; activate devices. |
| Unable to find processor. Note that the communication mechanism is set to a specific processor's IP address in the "System Communication" section of Processor Activation.<br>If the processor at that address has had its network configuration changed, or the processor was replaced, please revert to multicast to discover the processors. Also disable any firewalls and router filtering of multicast messages during this process. | 1. Check that the processor(s) are powered and connected to the network.<br>2. Allow exception for the software through the firewall or turn off firewall. See Section 5.1.2/5.1.5.<br>3. Turn off any active VPN connections. See Section 5.5.<br>4. If using a wired LAN connection, disconnect from any Wi-Fi networks. Vice versa for when using Wi-Fi. See Section 5.4.<br>5. For Macs running Parallels or VM, ensure that you are using a Bridged network connection. See Section 5.3.1.<br>6. Re-try activate > processors. |

## 9.0 Troubleshooting *(continued)*

### 9.2 HomeWorks QS Activate Processors/Connect Bridge Error Codes *(continued)*

| Error Message | Remedy |
|---|---|
| Status while activating a processor or Bridge shows “Subnet Conflict.” | Some other device on the network is using the same IP address; change the processor/Bridge IP address or the address of the other conflicting device and re-try activation. |
| Status while activating a processor shows “Not Responding.” | 1. Check that the processor(s) are powered and connected to the network.<br>2. Allow exception for the software through the firewall or turn off firewall. See Section 5.1.2/5.1.5.<br>3. Turn off any active VPN connections. See Section 5.5.<br>4. If using a wired LAN connection, disconnect from any Wi-Fi networks. Vice versa for when using Wi-Fi. See Section 5.4.<br>5. For Macs running Parallels or VM, ensure that you are using a Bridged network connection. See Section 5.3.1.<br>6. Re-try activate > processors. |

# 9.0 Troubleshooting *(continued)*

## 9.3 Using a Direct Connection to a Lutron Processor

During the troubleshooting process, it may become important to attempt a direct connection from the Windows computer to the Lutron processor. This can be useful as the removal of all potential network issues causing components between the Windows computer and Lutron processor. This helps to narrow down the troubleshooting and get closer to a root cause by minimizing the scope of the network.

In a direct connection, the only components now on the LAN are the Lutron processor and Windows computer.

**Figure 6: PC to RadioRA 2 Main Repeater: Direct Connection**

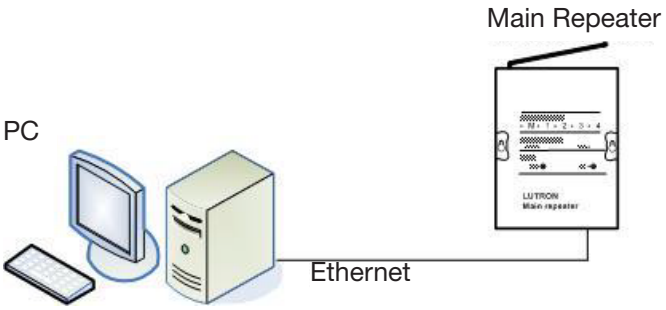



**Figure 7: PC to HomeWorks QS Processor: Direct Connection**

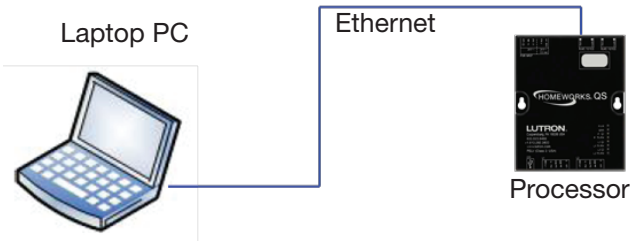
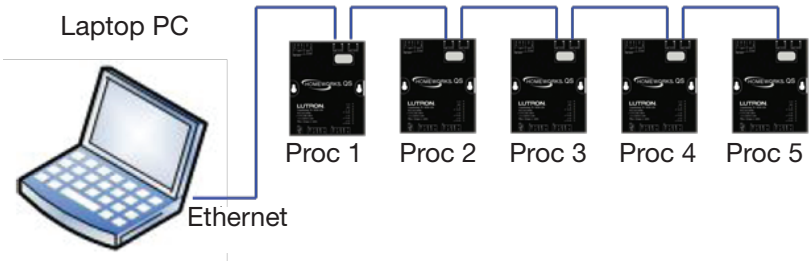



**Figure 8: PC to Multiple HomeWorks QS Processors: Direct Connection**



# 9.0 Troubleshooting *(continued)*

## 9.3 Using a Direct Connection to a Lutron Processor

### 9.3.1 Direct Connection using Static IP Address

Start by configuring a static IP address on Windows by using the Network and Sharing Center. Refer to Section 5.7.3 for directions on how to set a static IP in Windows.

If a Mac is being used with VM Ware or Parallels software, refer to Section 5.3.1 for information on how to configure both the Windows and Mac OS for static IP addresses.

Once the computer running the RadioRA 2 or HomeWorks QS programming software is setup with a static IP address, open the programming software and open the database for the residence.

If the system is a RadioRA 2 system, proceed to Section 2.0 to configure a static IP address on the Main Repeater and to then attempt to find the Main Repeater on the network.

If the system is a HomeWorks QS system, proceed to Section 4.0 to configure a static IP address on the HomeWorks QS Processor and to then attempt to discover the processor on the network.

### 9.3.2 Direct Connection using Link Local Addressing

A link local address is an address that the computer and Lutron processor will negotiate after a couple of minutes of a direct connection once both devices have determined that there is no DHCP server on the network to assign each device an address. This is an alternative approach to using a static IP and is beneficial for those who may have trouble configuring their Windows machine with a static IP address.

Connect the Lutron processor to the Windows machine in one of the methods shown in Section 6.3. Wait approximately 2 minutes for the two devices to negotiate the link local addresses upon discovering that there was no DHCP server on the network.

Proceed to open the RadioRA 2 or HomeWorks QS programming software and attempt to locate the processors using Find Main Repeater (RA2) or activate > processors (HWQS).

## 10.0 Frequently Asked Questions

***What is a network?***
A network is a set of devices that are connected together to exchange digital information or commands. Devices can include desktop computers, laptops, Wi-Fi routers, or Lutron processors. A local area network, or LAN, is a network of devices that are connected together by physical wires or over Wi-Fi and are in close physical proximity to each other.

***What is an IP address?***
An IP address, or Internet Protocol address, is a unique way to identify a device on your network. An IP address is analogous to a house number. On any given street, all the house numbers are unique just as on any given network all the IP addresses are unique.

An IP address consists of 4 "octets" of numbers ranging from 0 to 255.

Example:
IP address: 192.168.1.100

***How does a device on my network get an IP address?***
Devices can get an IP address in multiple ways:

1. The device can have a static IP address assigned to it. The static IP address can be manually changed using configuration software for that device. See "What is a static IP address?"
2. A network device can hand out IP addresses when the network is powered up. See "What is DHCP?"
3. A device can choose its own IP address if set to DHCP and no network device is handing out IP addresses. See "What is Link Local?"

***What is DHCP?***
DHCP, or Dynamic Host Configuration Protocol, defines a series of events which would allow devices to systematically allocate IP addresses. In networks where DHCP is used, one device, called the DHCP host, is responsible for handing out IP addresses to all the other devices. The IP addresses are temporary and are re-allocated any time the host or devices are powered up.

The DHCP host hands out IP addresses from a range that was set up during the host's configuration. Devices that would like to receive IP addresses from the DHCP host are set up to obtain IP addresses automatically using DHCP. The DHCP host is usually your home router.

Example:
DHCP IP address range: 192.168.1.100 to 192.168.1.149

***What is a static IP address?***
A static IP address is an IP address that doesn't change. A static IP address is manually configured before the network is used. Static IP configuration requires careful planning so that all devices have unique IP addresses.

***What is Link Local?***
If a device is configured to use DHCP but no DHCP server exists on the network, the device may choose to implement the Link Local protocol. This protocol allows the device to assume an IP address and verifies that no other device is using that IP address. This process may take up to two minutes. Link Local IP addresses all begin with 169.254.x.x.

Example:
Link Local IP address: 169.254.1.123

## 10.0 Frequently Asked Questions *(continued)*

***Can I mix a DHCP network with a static IP addresses?***
Yes, however careful planning must be given to the static IP addresses. The static IP addresses cannot be the same as the DHCP host's IP address and must fall outside of the range of the IP addresses the DHCP host hands out.

Example:
– Router (DHCP host) IP address: 192.168.1.1
– Router DHCP range: 192.168.1.100 to 192.168.1.150
– HomeWorks QS Processor static IP address: 192.168.1.2
– Wi-Fi laptop using DHCP: given out from router. Changes each time laptop is connected to network

***What is a subnet mask?***
A subnet mask is used to tell what messages are for this network and which are for another network. A subnet mask consists of 4 "octets" of numbers ranging from 0 to 255. The subnet masks should match on all devices that are part of the same network.

Example:
Subnet mask: 255.255.255.0

The 255 in the first three octets forces the listening device to listen to any messages where the first three octets of the incoming IP address match. If the receiving device's IP address is 192.168.1.100 and the incoming message is from IP address 192.168.1.2, then the device should listen.

***What is a straight through or patch Ethernet cable?***
A straight through or patch Ethernet cable (often referred to as simply an Ethernet cable) is a cable consisting of 4 pairs of twisted wire with an RJ-45 connector on each end. The wires connect straight through from one connector to the other (i.e. pin 1 connects to pin 1, pin 2 connects to pin 2, etc). This is the most common type of network cable and is used when connecting a device to a network through a router or switch.

***What is a crossover Ethernet cable?***
A crossover Ethernet cable is similar to a straight through Ethernet cable, with the exception that the pairs of wire are reversed from one connector to the other. This allows the transmit pairs on one connector to connect to the receive pairs on the other connector. This cable is often used when connecting two devices directly without a router in between, however it is not necessary in HomeWorks QS or RadioRA 2.

***What is a Wide Area Network?***
A wide area network is collection of networks that are not physically connected together. Accessing your home network remotely from an office or other place away from your home is a WAN. The Internet is the most commonly known Wide Area Network.

***How does your home network connect to the Internet?***

Your home network is connected to the Internet via a gateway device. Cable modems and DSL modems are examples of gateway devices. Sometimes gateway devices are also routers.

***What is a gateway IP address?***

A gateway is a device that connects your network to the Internet such as a cable modem or DSL router. The gateway address only needs to be setup when you want to remotely access a device on your network from another device on the Internet. If your network is not connected to the Internet, then the gateway address is not used. If your device does not need to be accessed from the Internet, then the gateway address is also not used. The gateway address on a device should be set to the address of the gateway device. In most cases this is your network router.

Example:
– Router IP address: 192.168.1.1
– Gateway address of devices attached to router: 192.168.1.1

## 10.0 Frequently Asked Questions *(continued)*

***What is a VLAN?***
A virtual local area network (VLAN) is a segmented local area network created through the utilization of managed switches. VLANs are implemented on networks that have a lot of devices tied to it (200+) or a lot of broadcast traffic. The switches help to only pass the commands that the devices housed on the VLAN wish to listen to and not allow them to be bombarded with extraneous network traffic.

***What is the difference between a LAN and a VLAN?***
Normally, in a local area network, the routers create the broadcast domain. In VLANs, the managed switches can create the broadcast domains and, because switches can talk between themselves, ports on different switches can share the same VLAN.

***Why would I use a VLAN over simply sub-netting the network?***
While each VLAN will have its own unique subnet, VLANs are different from sub-netting in that devices in a VLAN do not have to be connected to the same physical router or switch. For example, Switch A can have a port which is tied to VLAN 5 and so could a second switch, Switch B. Switch A and B are two different physical pieces of equipment but devices on the ports share the same VLAN and thus can talk to each other.

***Can I use a Layer 2 switch for VLAN functionality?***
Yes, Layer 2 switches can be used but they would then require a router to pass commands across VLANs. Layer 3 switches are switches that maintain normal switch functionality with the addition of routing capabilities. They can be used in place of a Layer 2 switch and router.

***What needs to be implemented within the VLAN switch settings for HomeWorks QS to work?***
As Lutron systems, such as HomeWorks QS, rely upon multicast communication for various system operations, it is imperative that multicast be allowed to travel through the VLAN and across VLANs. Settings that should be enabled within the switches for each VLAN are:

1. Routing Information Protocol (RIP) or Open Shortest Path First (OSPF)
2. Protocol Independent Multicast (PIM) – PIM is a group of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN. It uses more traditional routing protocols to send information such as RIP or OSPF.
   a. Dense Mode (DM) or Sparse Mode (SM)
      i. Dense Mode – builds shortest path trees by flooding the network with multicast and then prunes branches where no receivers are present, not as scalable
      ii. Sparse Mode – uses a shared tree or rendezvous point (RP) to then send unicast data out to devices, very scalable

Enabling these settings differs based on the switch hardware being employed for the VLAN implementation. VLANs should be designed and setup by a qualified networking professional with a solid understanding of VLAN implementation. If you are not qualified or unfamiliar with VLAN implementation, we recommend outsourcing the network design and implementation to an IT professional in your area.

***What is the best way to go about troubleshooting issues that arise during implementation of the VLAN setup?***
If you are experiencing issues with network connectivity between processors on a VLAN network, we recommend isolating the processors from the network, via direct connections, to help determine if the issue is caused by the network or the processors. If an issue with the network is determined, please contact an IT professional in your local area, for further assistance.

## Lutron Contact Numbers

**WORLD HEADQUARTERS**
**USA**
**Lutron Electronics Co., Inc.**
**7200 Suter Road**
**Coopersburg, PA 18036-1299**
TEL: +1.610.282.3800
FAX: +1.610.282.1243

support@lutron.com

www.lutron.com/support

**North & South America**
**Customer Assistance**
**USA, Canada, Caribbean:**
1.844.LUTRON1 (1.844.588.7661)
**Mexico:**
+1.888.235.2910
**Central/South America:**
+1.610.282.6701

**UK AND EUROPE:**
**Lutron EA Limited**
**125 Finsbury Pavement**
**4th floor, London EC2A 1NQ**
**United Kingdom**
TEL: +44.(0)20.7702.0657
FAX: +44.(0)20.7480.6899
FREEPHONE (UK): 0800.282.107
Technical Support: +44.(0)20.7680.4481

lutronlondon@lutron.com

**ASIA:**
**Lutron GL Ltd.**
**390 Havelock Road**
**#07-04 King's Centre**
**Singapore 169662**
TEL: +65.6220.4666
FAX: +65.6220.4333
Technical Support: 800.120.4491

lutronsea@lutron.com

**Asia Technical Hotlines**
Northern China: 10.800.712.1536
Southern China: 10.800.120.1536
Hong Kong: 800.901.849
Indonesia: 001.803.011.3994
Japan: +81.3.5575.8411
Macau: 0800.401
Taiwan: 00.801.137.737
Thailand: 001.800.120.665853
Other Countries: +65.6220.4666